© 2019 SPLUNK INC.

Splunk Security Essentials 3.0: Driving the Content that Drives You



SEC2013

Wednesday, October 23, 2019 | 03:30 PM - 05:30 PM

.conf19

splunk>





David Veuve

Principal Security Strategist | Splunk

Johan Bjerke

Principal Sales Engineer | Splunk

© 2019 SPLUNK INC.

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

© 2019 SPLUNK INC.

Agenda

1. What is Splunk Security Essentials (SSE)
2. Introduction to BOTS
3. Finding Content
4. Being Prescriptive
5. Learning Splunk for Security
6. Improving your Production Deployment
7. Measuring Success

© 2019 SPLUNK INC.

What is SSE?

Section subtitle goes here



.conf19

splunk>

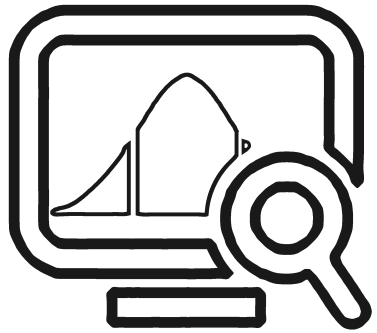
© 2019 SPLUNK INC.

Splunk Security Essentials is the free Splunk app that makes security easier.

© 2019 SPLUNK INC.

Widely Deployed Today

Proven and Stable



50k

Over 50,000 downloads

6k

Over 6,000 reporting installs

30

30 releases

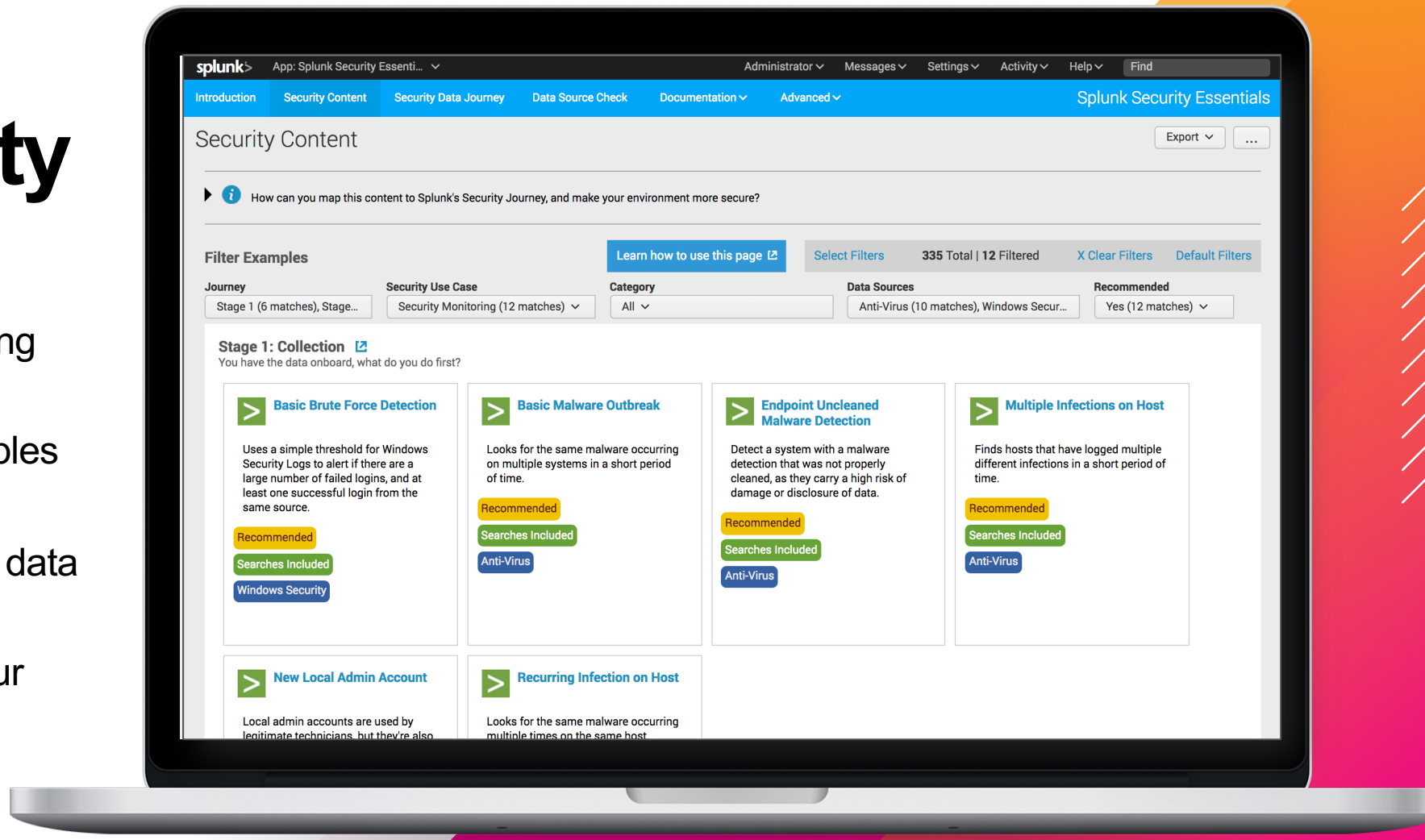
2.8

Essentials has been around for nearly three years

Splunk Security Essentials

Learn to improve your security using Splunk's analytics-driven security:

- Common use cases and examples to get started
- Data onboarding guides for top data sources
- Understand how to improve your security
- Scales from small to massive companies
- Save searches, send results to ES/UBA



© 2019 SPLUNK INC.

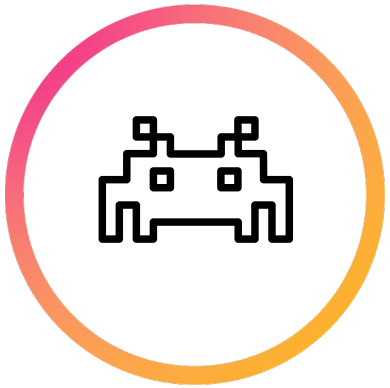
splunk> turn data into doing

© 2019 SPLUNK INC.

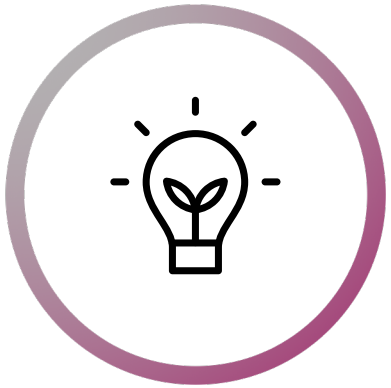
Four Pillars

Four ways in which SSE has delivered value to users

Finding Content



Learning Splunk Security



Improve Production



Measure Your Success



© 2019 SPLUNK INC.

Security Journey

DESCRIPTION

Find anomalous behavior and unknown threats by applying machine learning, data science and advanced statistics to analyze the users, endpoint devices, and applications in your environment.

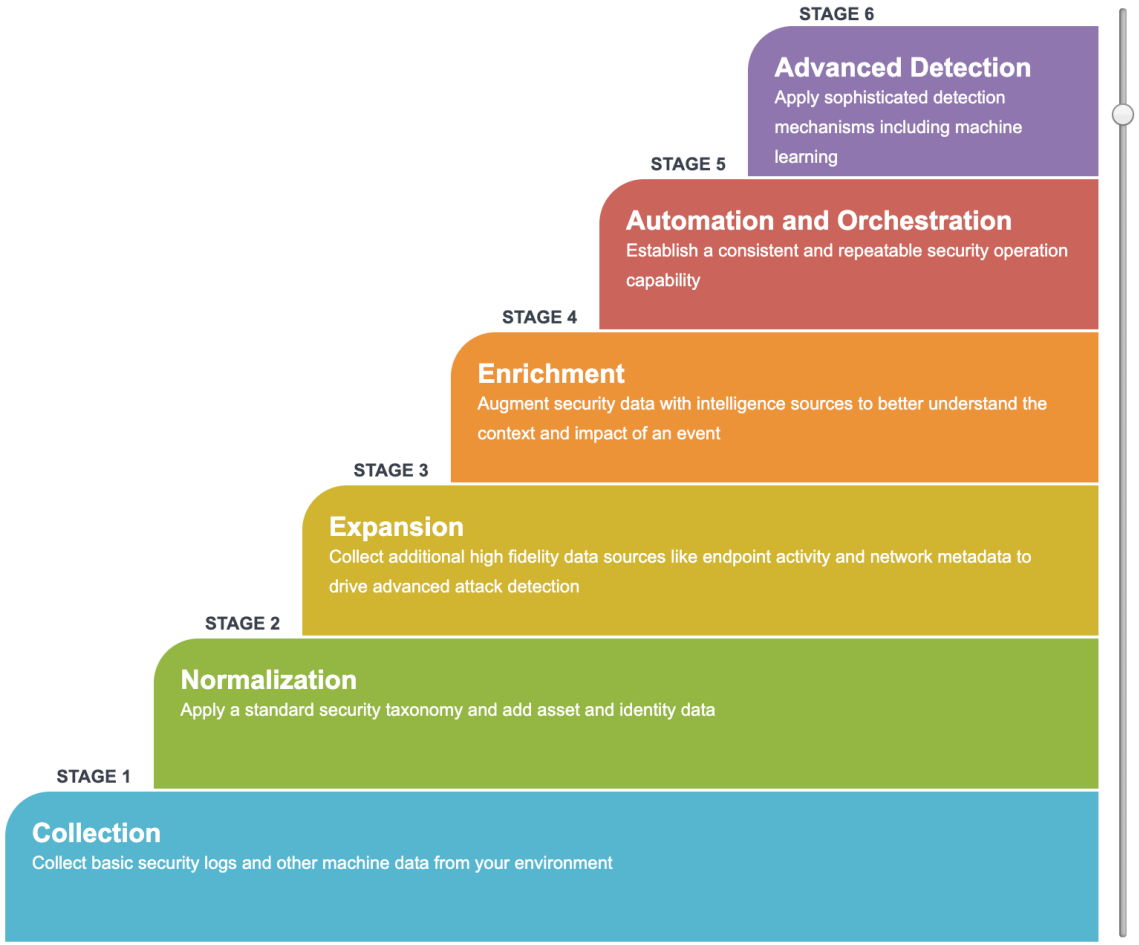
MILESTONES

At this stage, you have given yourself a fighting chance to detect adversaries and insiders even when they leave only subtle traces of their activity.

- You are employing the most advanced techniques available to identify unknown threats.
- You are employing new detection mechanisms as they become available, leveraging your team's expertise and leveraging outside research organizations.

CHALLENGES

- At this stage, you will be challenged to constantly improve your security organization.
- To gain new capabilities, your team will likely be required to perform new research.
- Although you are at the top of your game, there are no guarantees and the most advanced adversaries may still successfully attack your organization.



SELECTED STAGE 6

SECURITY USE CASE APPLICABILITY

- Security Monitoring
- Compliance
- Incident Investigation & Forensics
- Incident Response
- SOC Automation
- Advanced Threat Detection
- Insider Threat

DATA SOURCES

This stage focuses more on what you do with the data you have vs. onboarding new sources.

© 2019 SPLUNK INC.

MITRE | ATT&CK™

splunk> turn data into doing

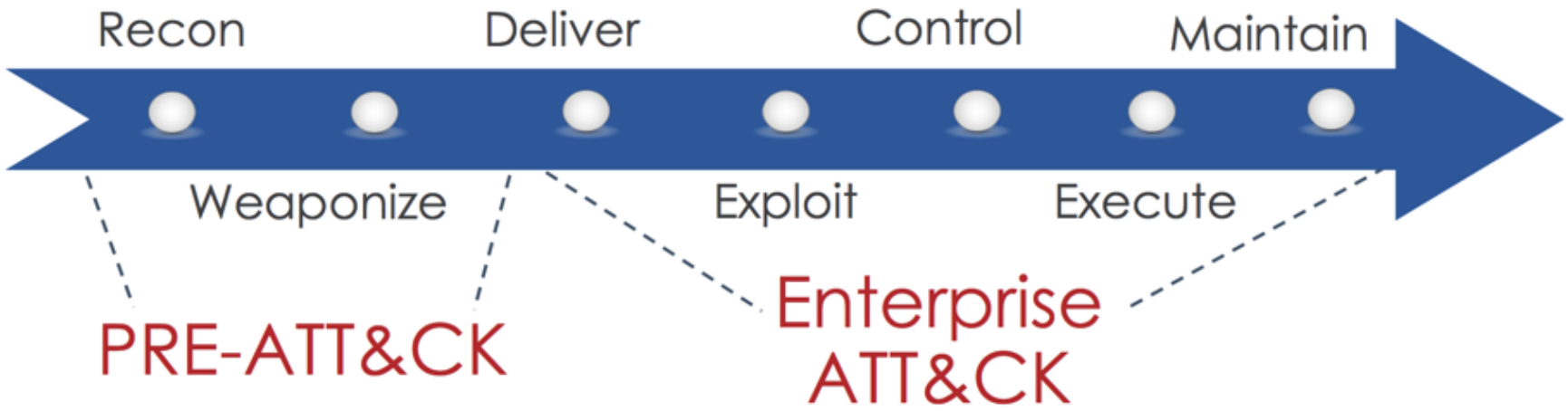
© 2019 SPLUNK INC.

Introduction to MITRE ATT&CK™

A knowledge base of adversary behavior

- Based on real-world observations
- Free, open, globally accessible, and community-driven
- A common language

Mobile ATT&CK



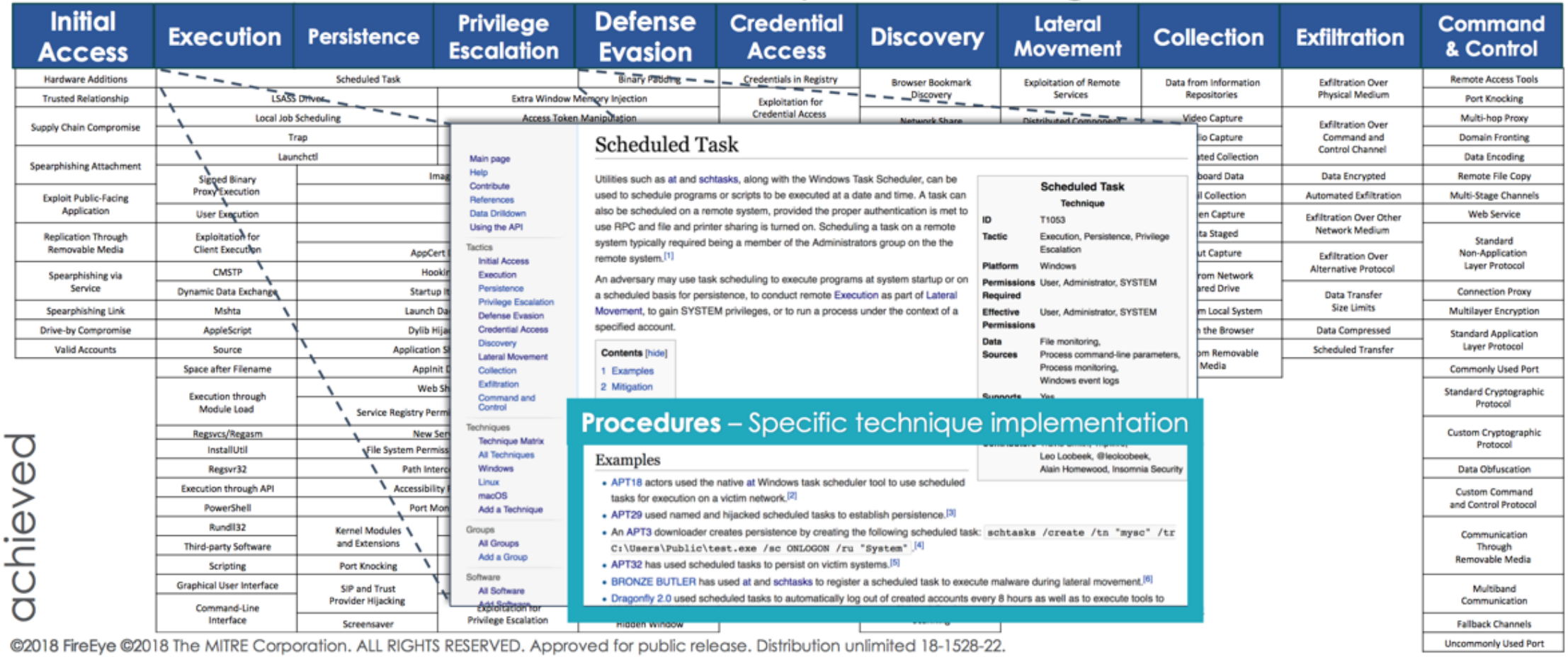
https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

© 2019 SPLUNK INC.

Breaking Down Enterprise ATT&CK

Tactics: the adversary's technical goals

Techniques: how the goals are achieved



©2018 FireEye ©2018 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 18-1528-22.

https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2018/presentations/cds18-technical-s05-att&cking-fin7.pdf

© 2019 SPLUNK INC.

TECHNIQUES
All
Initial Access +
Execution +
Persistence +
Privilege Escalation -
Access Token Manipulation
Accessibility Features
AppCert DLLs
AppInit DLLs
Application

Scheduled Task

Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system. [1]

An adversary may use task scheduling to execute programs at system startup or on a scheduled basis for persistence, to conduct remote Execution as part of Lateral Movement, to gain SYSTEM privileges, or to run a process under the context of a specified account.

ID: T1053

Tactic: Execution, Persistence, Privilege Escalation

Platform: Windows

Permissions Required: Administrator, SYSTEM, User

Effective Permissions: SYSTEM, Administrator, User

Data Sources: File monitoring, Process monitoring, Process command-line parameters, Windows event logs

Supports Remote: Yes

© 2019 SPLUNK INC.

References

1. Microsoft. (2005, January 21). Task Scheduler and security. Retrieved June 8, 2016.
2. Carvey, H.. (2014, September 2). Where you AT?: Indicators of lateral movement using at.exe on Windows 7 systems. Retrieved January 25, 2016.
3. Dunwoody, M. and Carr, N.. (2016, September 27). No Easy Breach DerbyCon 2016. Retrieved October 4, 2016.
4. Moran, N., et al. (2014, November 21). Operation Double Tap. Retrieved January 14, 2016.
5. Carr, N.. (2017, May 14). Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations. Retrieved June 18, 2017.
6. Dahan, A. (2017, May 24). OPERATION COBALT KITTY: A LARGE-SCALE APT IN ASIA CARRIED OUT BY THE OCEANLOTUS GROUP. Retrieved November 5, 2018.
7. Dahan, A. (2017). Operation Cobalt Kitty. Retrieved December 27, 2018.
8. Dumont, R. (2019, March 20). Fake or Fake: Keeping up with OceanLotus decoys. Retrieved April 1, 2019.
9. Security Response attack Investigation Team. (2019, March 27). Elfin: Relentless Espionage Group Targets Multiple
41. Chiu, A. (2016, June 27). New Ransomware Variant "Nyetya" Compromises Systems Worldwide. Retrieved March 26, 2019.
42. Lee, B., Falcone, R. (2018, February 23). OopsIE! OilRig Uses ThreeDollars to Deliver New Trojan. Retrieved July 16, 2018.
43. Lee, B., Falcone, R. (2018, July 25). OilRig Targets Technology Service Provider and Government Agency with QUADAGENT. Retrieved August 9, 2018.
44. Falcone, R., et al. (2018, September 04). OilRig Targets a Middle Eastern Government and Adds Evasion Techniques to OopsIE. Retrieved September 24, 2018.
45. Lunghi, D., et al. (2017, December). Untangling the Patchwork Cyberespionage Group. Retrieved July 10, 2018.
46. PowerShellMafia. (2012, May 26). PowerSploit - A PowerShell Post-Exploitation Framework. Retrieved February 6, 2018.
47. PowerSploit. (n.d.). PowerSploit. Retrieved February 6, 2018.
48. ClearSky Cyber Security. (2018, November). MuddyWater Operations in Lebanon and Oman: Using an Israeli compromised domain for a two-stage campaign. Retrieved November 29, 2018.
49. Sardiwal, M, et al. (2017, December 7). New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group,

© 2019 SPLUNK INC.

Mapping to ATT&CK: the Manual, Human Way

All of the backdoors identified - excluding RoyalDNS - required APT15 to create batch scripts in order to install its persistence mechanism. This was achieved through the use of a simple Windows run key.

Analysis of the commands executed by APT15 reaffirmed the group's preference to 'live off the land'. They utilised Windows commands reconnaissance activities such as tasklist.exe, ping.exe, netstat.exe, n systeminfo.exe, ipconfig.exe and bcp.exe

APT15 was also observed using Mimikatz to dump credentials and generate Kerberos golden tickets. This allowed the group to persist in th ent of

up also used keyloggers and their own .NET tool to enumerate folders and dump data from Microsoft Exchange mailboxes.

Scripting (T1064)

Registry Run Keys / Startup Folder (T1060)

Command-Line Interface (T1059)

Discovery - T1057, T1018, T1049, T1082, T1016

Cred Dumping (T1003)

Input Capture (T1056)

Pass the Ticket (T1097)

Email Collection (T1114)

© 2019 SPLUNK INC.

MITRE ATT&CK

Key Concepts

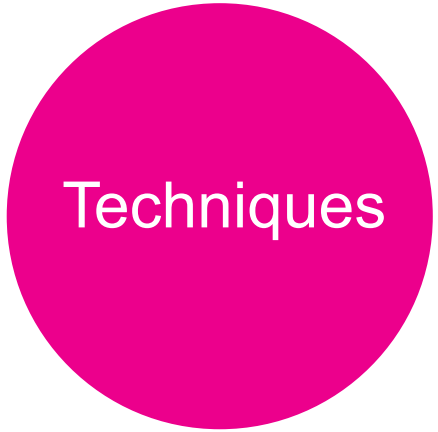


Initial Access

Discovery

Exfiltration

…



Scheduled Task

Credential Dumping

Pass the Ticket

…



APT10

OilRig

Violent Memmes

…

© 2019 SPLUNK INC.

History of Security Essentials



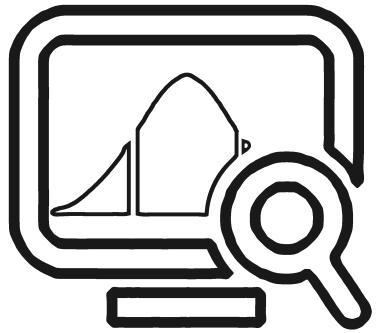
.conf19

splunk>

© 2019 SPLUNK INC.

Widely Deployed Today

Proven and Stable



50k

Over 50,000 downloads

6k

Over 6,000 reporting installs

30

30 releases

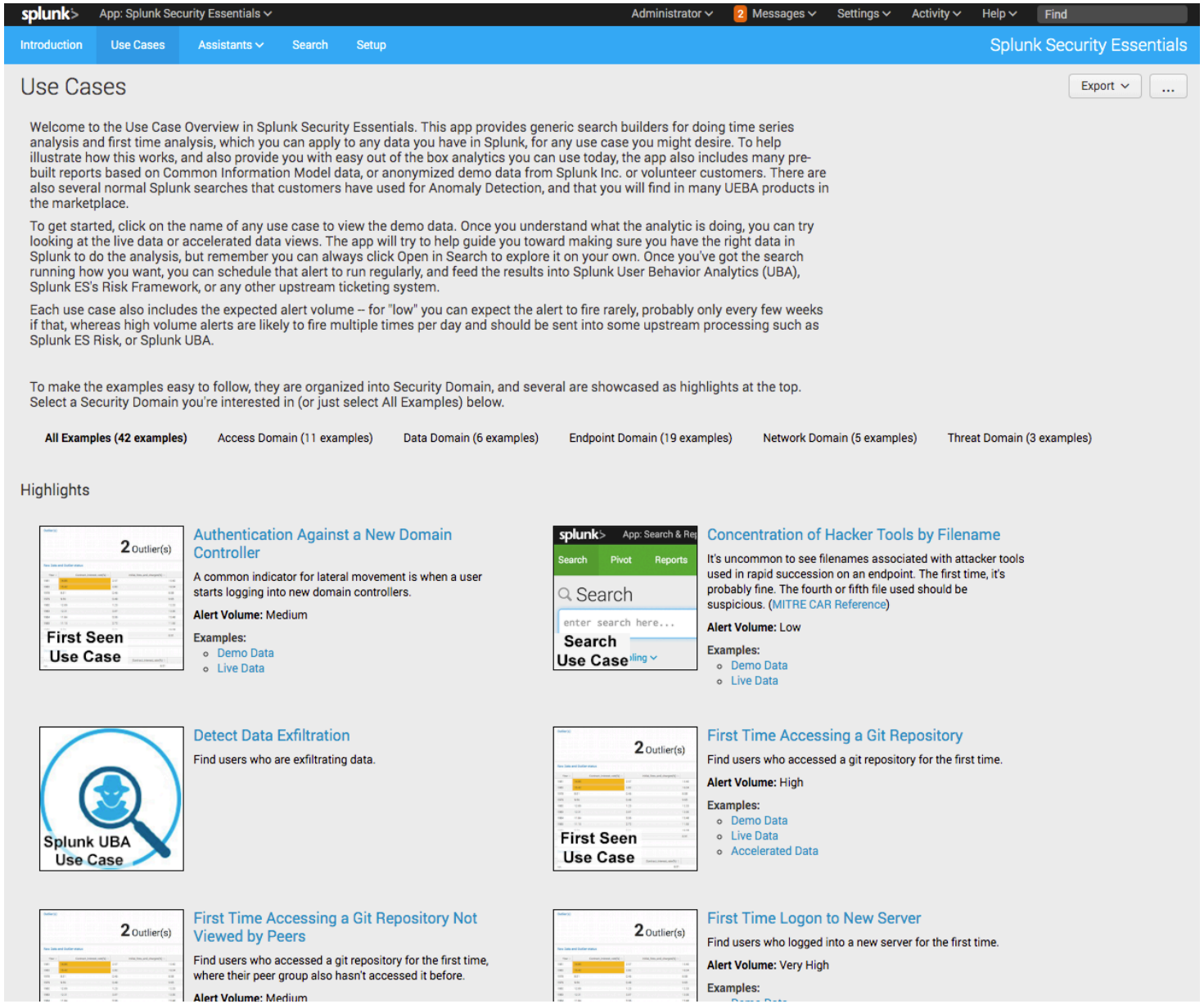
2.8

Essentials has been around for nearly three years

© 2019 SPLUNK INC.

SSE 1.0

Jan 07, 2017

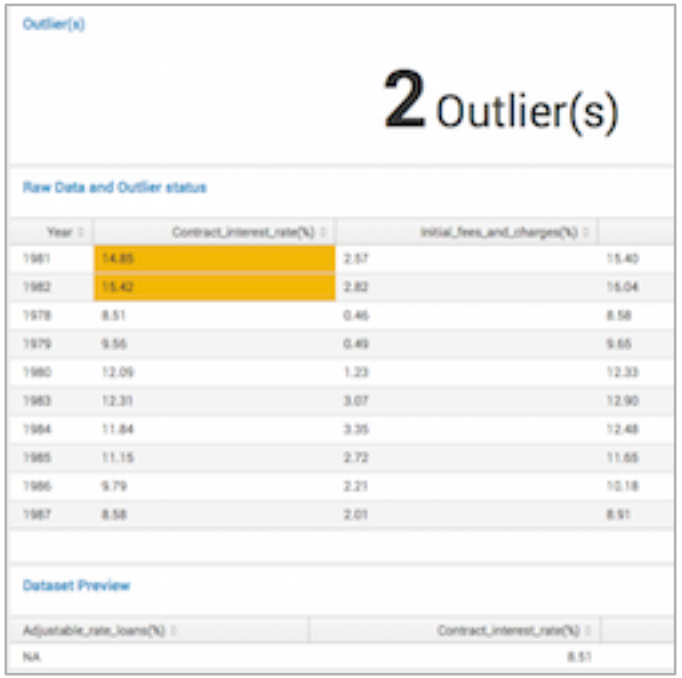


splunk> .conf19

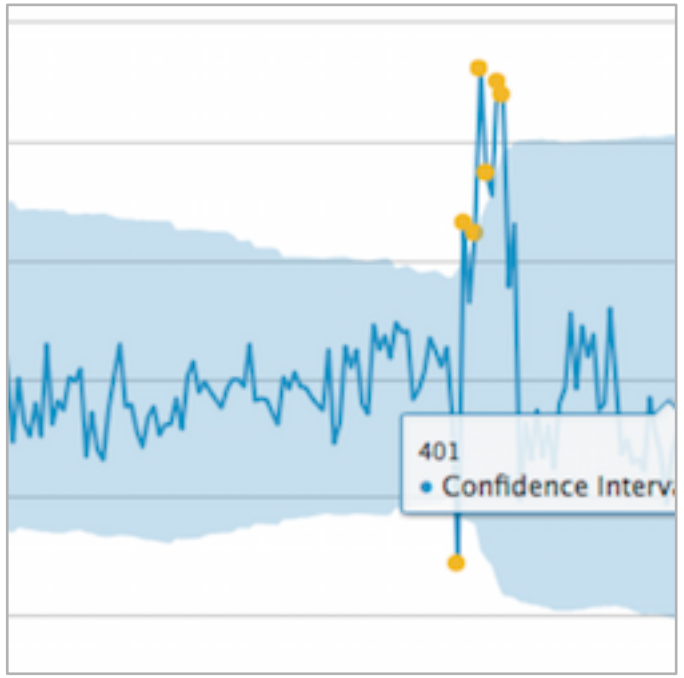
© 2019 SPLUNK INC.

Splunk Security Essentials

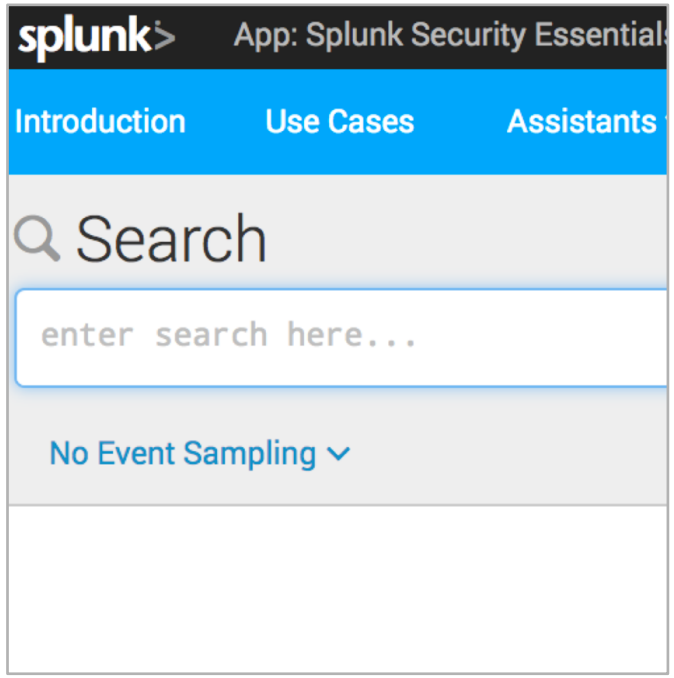
Types of Use Cases



First Time Seen
powered by stats



Time Series Analysis with
Standard Deviation

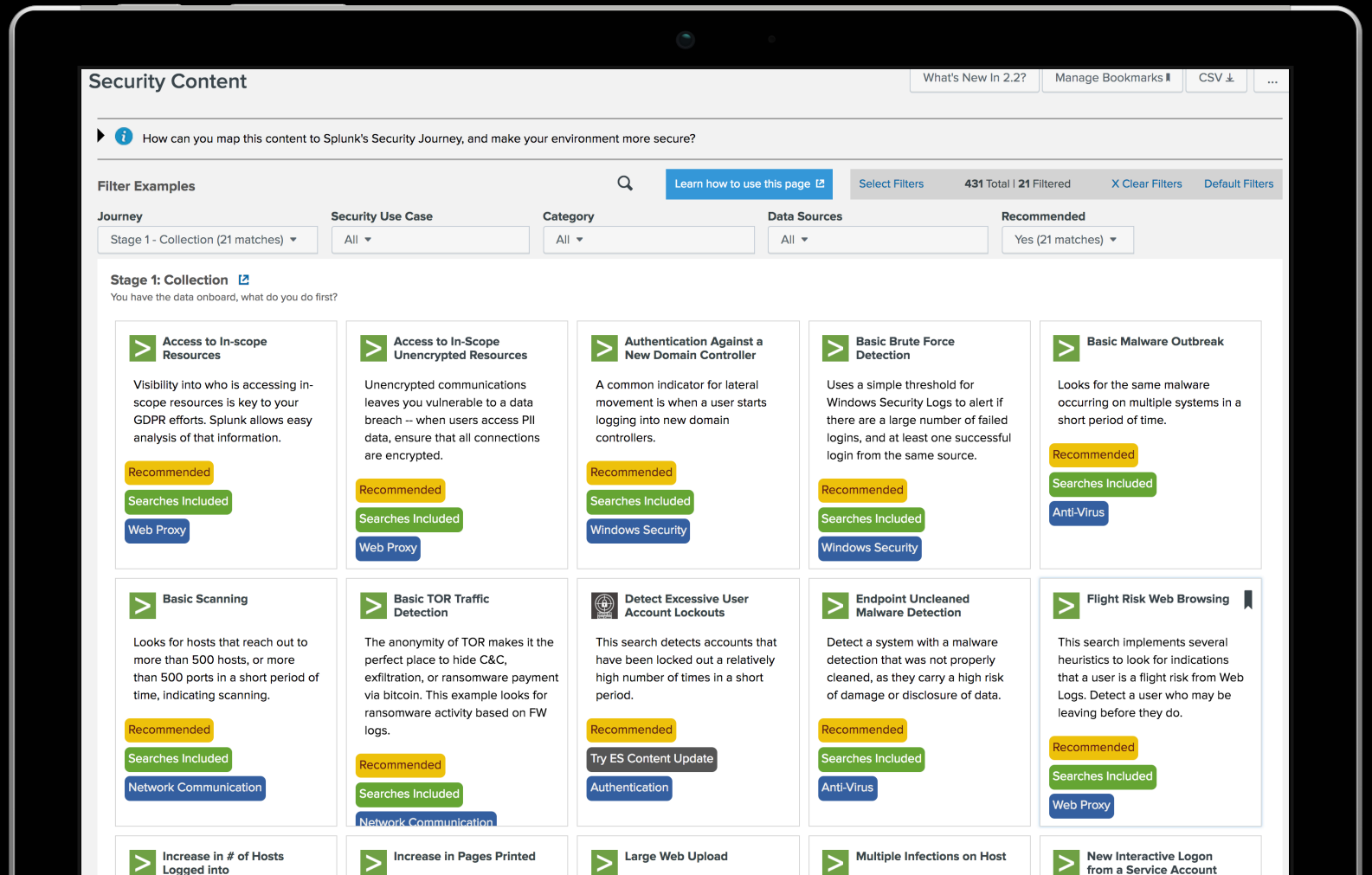


General Security Analytics
Searches

© 2019 SPLUNK INC.

SSE 2.0

Feb 22, 2018



125 Examples, with 180+ Searches

Each includes:

- Description
- Relevance
- How to Implement
- How to Respond
- Known False Positives
- Line-by-Line SPL Documentation
- And More!

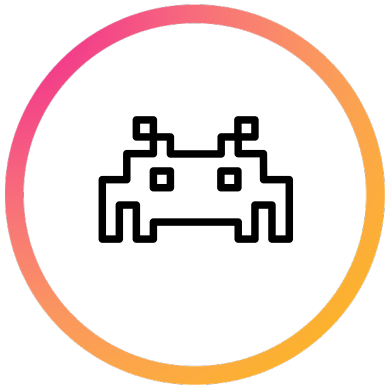
splunk> .conf19

© 2019 SPLUNK INC.

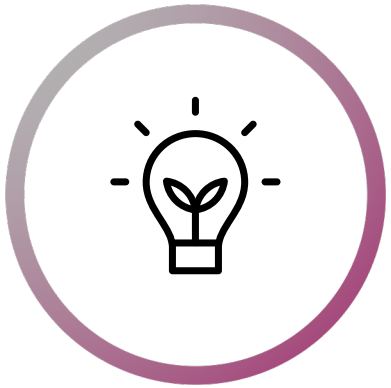
SSE 3.0

Oct 11, 2019

Finding Content



Learning Splunk Security



Improve Production

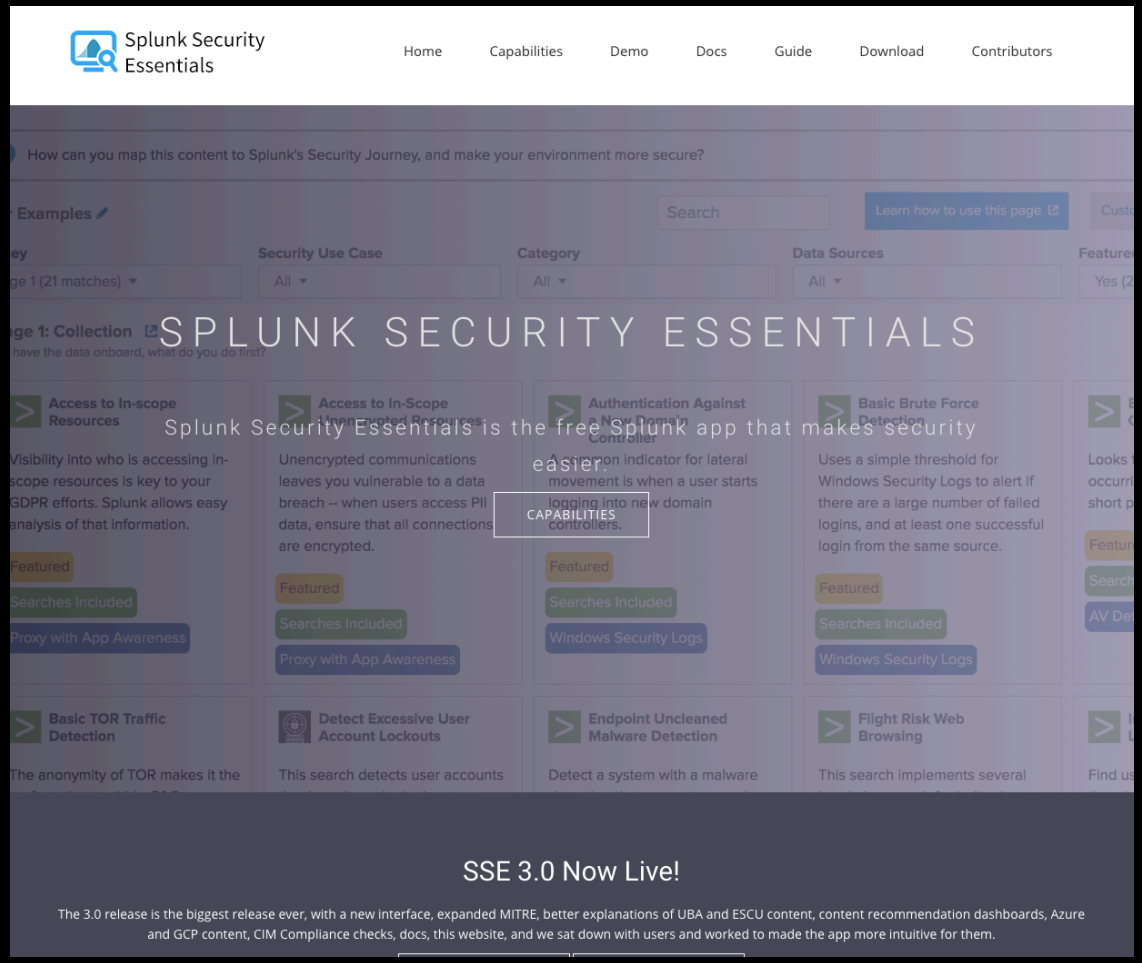


Measure Your Success

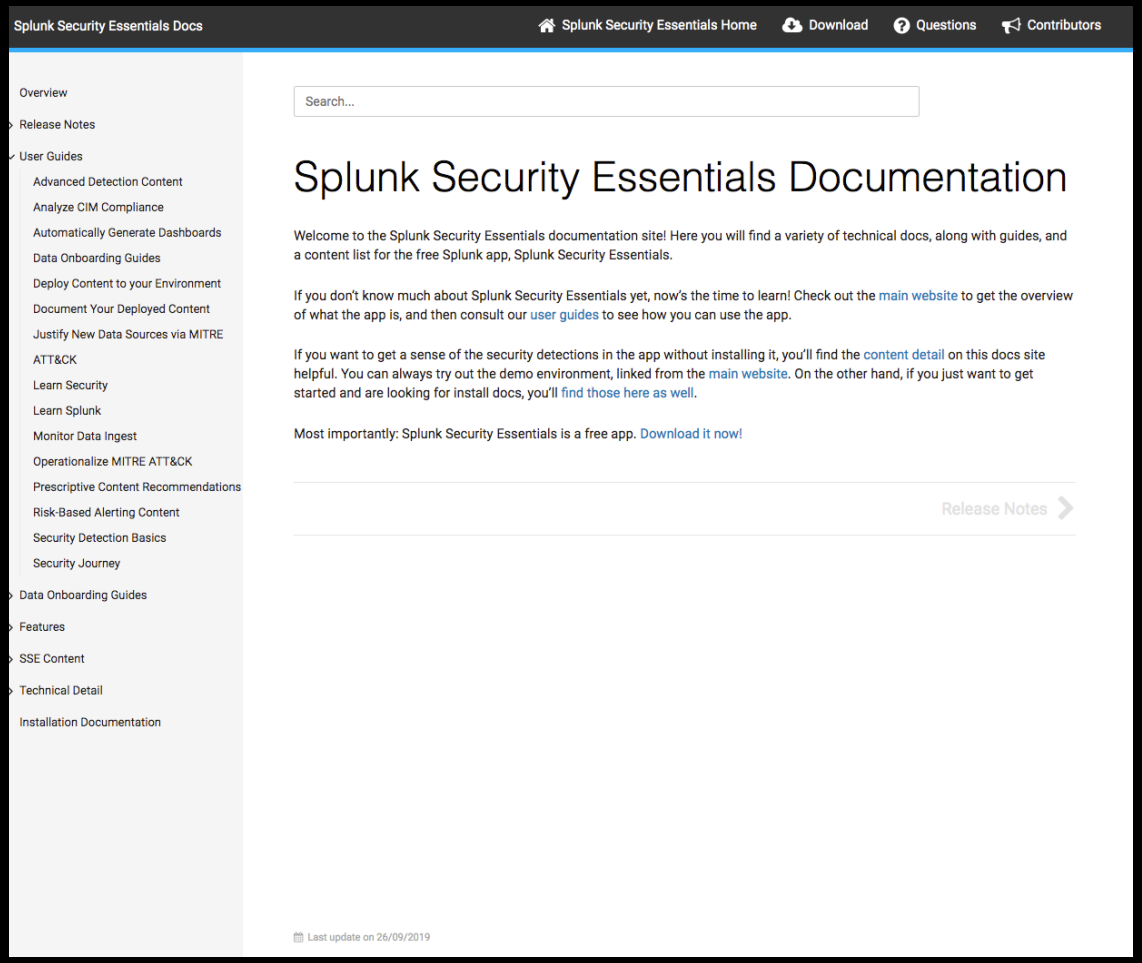


© 2019 SPLUNK INC.

And a Website! And a Docs Site!



https://www.splunksecurityessentials.com



https://docs.splunksecurityessentials.com

splunk> .conf19

© 2019 SPLUNK INC.

SSE is a Huge Team Effort

+ Brian Cusick

+ Josef Kuepker


David Veuve


Johan Bjerke


Cody Harris


James Brodsky


Ryan Kovar


Dave Herrald


John Stoner


Lily Lee


Filip Wijnholds


Michel Oosterhof



Derek King


Jon Nussbaum



Ryan Lait


Richard Hensen


Simon O'Brien


Tom Smit


Steve Brant


Tim Frazier


Ian Richardson


Ian Forrest


Han Leivens


Nick Roy


Tony Cihak


Jeswanth Manikonda

© 2019 SPLUNK INC.

Hands On!



.conf19

splunk>

© 2019 SPLUNK INC.

Log On!

Alert a room monitor if you run into issues!



© 2019 SPLUNK INC.

BOTS 4 – Violent Memmes



.conf19

splunk>

What is BOTS?

Training

Competition



Realistic

FUN!


Premium
FROTHLY
Quality


FROTHY
Premium
Quality

© 2019 SPLUNK INC.



1 SOCIO-POLITICAL AXIS

- Seeking to obtain high end Western Beers for production in their breweries

ADVERSARY

- Nation-state sponsored adversary
- Uses German naming conventions



CAPABILITIES

- PowerShell
- Spearphishing
- Domain Fronting
- Ticket Passing

INFRASTRUCTURE

- German Based DigitalOcean servers
- Enom Registered DNS

2 TECHNICAL AXIS

- Metasploit
- Credential Dumping (Mimikatz)
- User svc_print for Account Persistence
- Remote Desktop Protocol
- Schtasks.exe for beacon and persistence
- PSExec for lateral movment
- Yandex browser

VICTIMS

Western innovative Brewers and Home Brewing companies

VIOLENT MEMES

THREATCONNECT

Thanks ThreatConnect!



© 2019 SPLUNK INC.

Finding Content



.conf19

splunk>

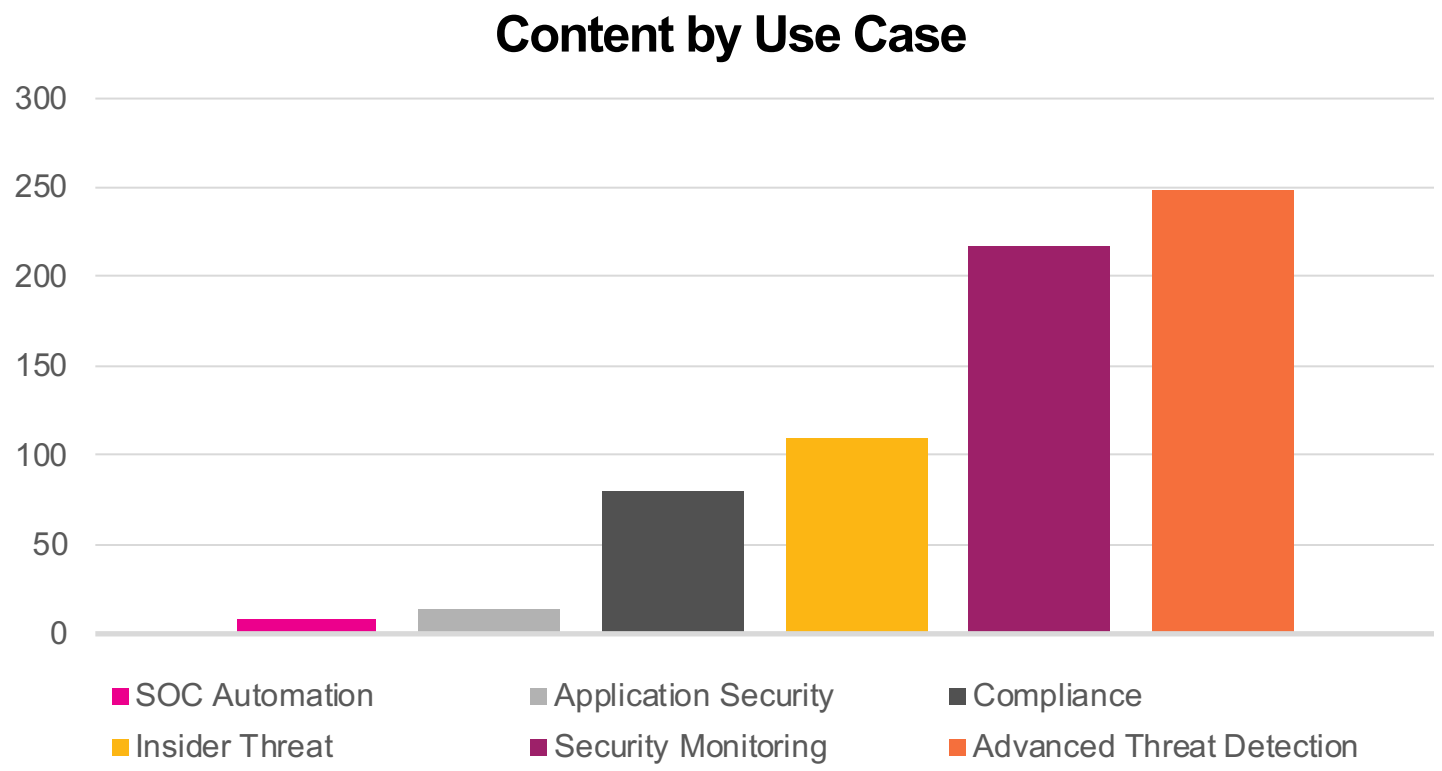
© 2019 SPLUNK INC.

120+ Native Detections

Directly Usable Content

Each detection includes:

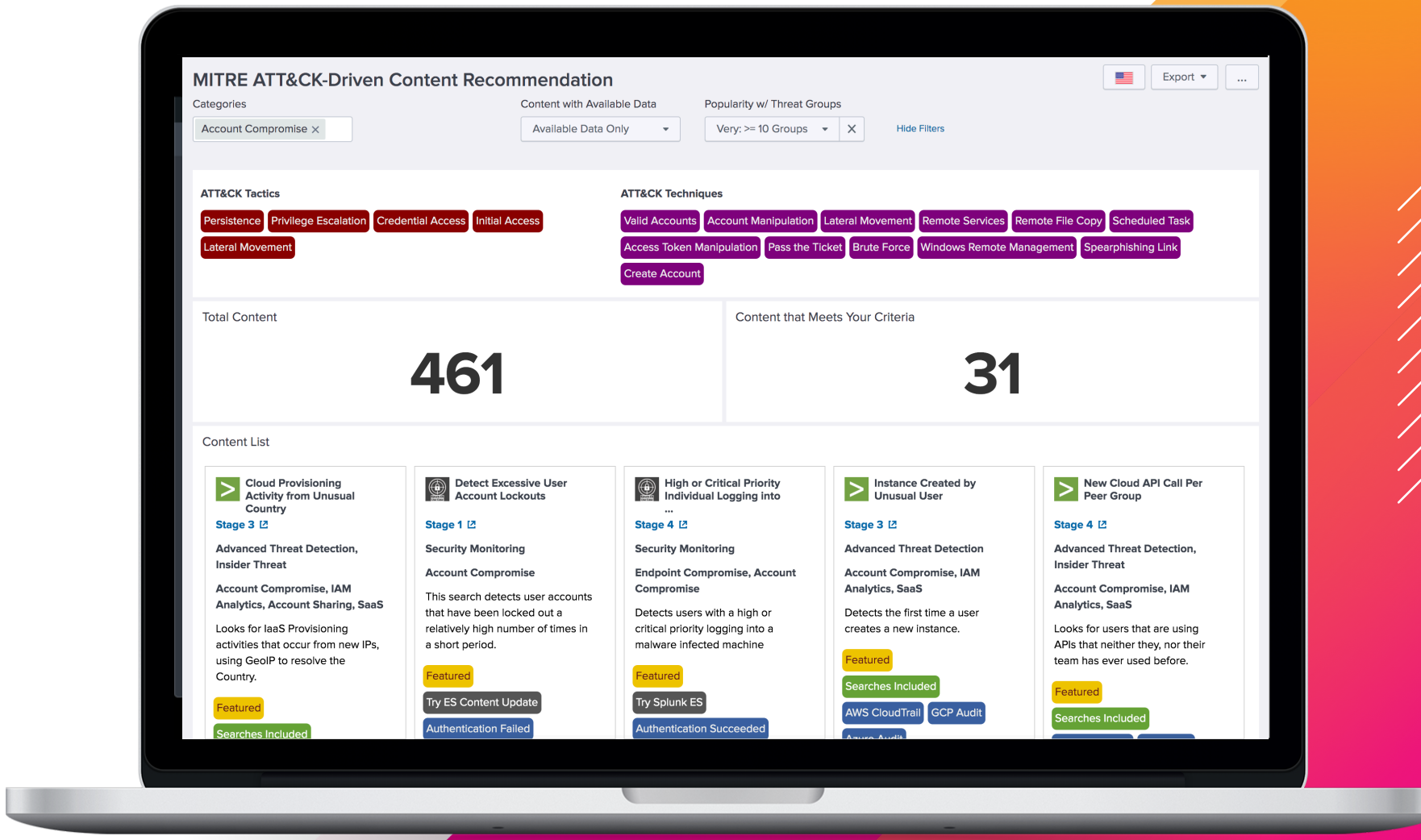
- Production searches including line-by-line docs
- Documented known false positives, response recommendations, implementation guidance
- Demo data and sample screenshots
- MITRE ATT&CK Tactics and Techniques, Kill Chain Phases
- Many contain related dashboard panels



Prescriptive Content

What To Do Next?

SSE understands what data you have, and what content you already use. It uses that to recommend what to do next.



splunk> turn data into doing

© 2019 SPLUNK INC.

© 2019 SPLUNK INC.



Splunk User Behavior Analytics™



Splunk Enterprise Security™



Splunk ES Content Update™



Also includes and maps content from Splunk Premium Solutions

© 2019 SPLUNK INC.

Hands-On

David



.conf19

splunk>

© 2019 SPLUNK INC.

QUICK! We need some advanced detections!

splunk>enterprise App: Splunk Security Essentials ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Home | Security Content ▾ | Analytics Advisor ▾ | Security Operations ▾ | Data ▾ | Advanced ▾ | Documentation ▾

Home

Welcome to Splunk Security Essentials! Below you will find the primary areas where Splunk users get value from this app. Within each, you
go, and what (if anything) you need to configure. The goal of this free app is to help you be more successful more quickly with Splunk for S
out the docs site or ask for help on Splunk Answers. Happy Splunking!

We need some advanced detections!

Find Content

- Security Detection Basics
- Advanced Detection Content
- Prescriptive Content Recommendations
- Risk-Based Alerting Content

Learn

- Learn Splunk
- Learn Security
- Security Journey
- Data Onboarding Guides

Help Deploy

- Operationalize MITRE ATT&CK
- Monitor Data Ingest
- Automatically Generate Dashboards
- Deploy Content to your Environment
- Analyze CIM Compliance

- Justify New Data Sources via MITRE ATT&CK
- Document Your Deployed Content

splunk>enterprise App: Splunk Security Essentials ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Home | Security Content ▾ | Analytics Advisor ▾ | Security Operations ▾ | Data ▾ | Advanced ▾ | Documentation ▾

Home

Welcome to Splunk Security Essentials! Below you will find the primary areas where Splunk users get value from this app. Within each, you
go, and what (if anything) you need to configure. The goal of this free app is to help you be more successful more quickly with Splunk for
out the docs site or ask for help on Splunk Answers. Happy Splunking!

We need some advanced detections!

Find Content	Learn	Help Deploy	Measure
Security Detection Basics	Advanced Detection Content	Prescriptive Content Recommendations	Risk-Based Alerting Content



Find Content | Learn | Help

Security Detection Basics | Advanced Detection Content | Prescriptive Conte

We need some advanced detections!

Advanced Detection Content

For those who have their SIEM basics under control, this guide shows you far more security content, and also recommends additional capabilities such as leveraging MITRE ATT&CK to help you view the right information.

Launch Content Clicking a use case below will bring you to the Security Content page.

Security Monitoring



Security (continuous) monitoring enables you to analyze a continuous stream of near real-time snapshots of the state of risk to your security data, the network, endpoints, as well as cloud devices, systems and applications.

Advanced Threat Detection



An advanced threat (APT) is a set of stea[illegible]y and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity. APTs usually targets either private organizations, states or both for business or political motives.

Insider Threat



Insider threats come from current or former employees, contractors, or partners who have access to the corporate network and intentionally or accidentally exfiltrate, misuse or destroy sensitive data. They often have legitimate access to access and download sensitive material, easily evading traditional security products. Nothing to fear, Splunk

Compliance



In nearly all environments, there are regulatory requirements of one form or another - when dealing with the likes of GDPR, HIPAA, PCI, SOC, and even the 20 Critical Security Controls, Splunk enables customers to create correlation rules and reports to identify threats to sensitive data or key employees and to automatically demonstrate compliance.

Advanced Filters By Default

splunk>enterprise App: Splunk Security Essentials ▾ Administrator ▾ 16 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Home | Security Content ▾ | Analytics Advisor ▾ | Security Operations ▾ | Data ▾ | Advanced ▾ | Documentation ▾

Security Content

How can you map this content to Splunk's Security Journey, and make your environment more secure?

Filter | Search | Learn how to use this page | Customize Filters | 458 Total | 61 Filtered | Clear | Default | Share

Journey	Security Use Case	Category	Data Sources	Featured
All selected (6)	Advanced Threat Detection (6...	All	All	All

ATT&CK Tactic	ATT&CK Technique	MITRE Threat Groups	Search Included
All	All	All	Yes (61 matches)

Stage 1: Collection

You have the data onboard, what do you do first?

Authentication Against a New Domain Controller

A common indicator for lateral movement is when a user starts logging into new domain controllers.

Featured | Searches Included | Lateral Movement | Remote Services

Basic TOR Traffic Detection

The anonymity of TOR makes it the perfect place to hide C&C, exfiltration, or ransomware paymen via bitcoin. This example looks for ransomware activity based on FW logs.

Featured | Searches Included | Exfiltration

Increase in # of Hosts Logged into

Find users who log into more hosts than they typically do.

Featured | Searches Included | Lateral Movement | Remote Services

New Interactive Logon from a Service Account

In most environments, service accounts should not log on interactively. This search finds new user/host combinations for accounts starting with "svc_."

Featured | Searches Included | Privilege Escalation | Persistence

New Local Admin Account

Local admin accounts are used by legitimate technicians, but they're also used by attackers. This search looks for newly created accounts that are elevated to local admins.

Featured | Searches Included | Defense Evasion | Persistence

Windows Event Log Clearing Events

Basic Dynamic DNS Detection

First Time Logon to New Server

Hosts Sending To More Destinations Than

Hosts Where Security Sources Go Quiet

Advanced Filters By Default

splunk>enterprise App: Splunk Security Essentials ▾ Administrator ▾ 16 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Home | Security Content ▾ | Analytics Advisor ▾ | Security Operations ▾ | Data ▾ | Advanced ▾ | Documentation ▾

Security Content

How can you map this content to Splunk's Security Journey, and make your environment more secure?

Filter | Search | Learn how to use this page | Customize Filters | 458 Total | 61 Filtered | Clear | Default | Share

Journey: All selected (6) ▾
Security Use Case: Advanced Threat Detection (6... ▾
Category: All ▾
Data Sources: All ▾
Featured: All ▾

ATT&CK Tactic: All ▾
ATT&CK Technique: All ▾
MITRE Threat Groups: All ▾
Search Included: Yes (61 matches) ▾

Stage 1: Collection

You have the data onboard, what do you do first?

Authentication Against a New Domain Controller

Basic TOR Traffic Detection

Increase in # of Hosts Logged into

New Interactive Logon from a Service Account

In most environments, service accounts should not log on interactively. This search finds new user/host combinations for accounts starting with "svc_."

Featured | Searches Included | Privilege Escalation | Persistence

New Local Admin Account

Local admin accounts are used by legitimate technicians, but they're also used by attackers. This search looks for newly created accounts that are elevated to local admins.

Featured | Searches Included | Defense Evasion | Persistence

Windows Event Log Clearing Events

Basic Dynamic DNS Detection

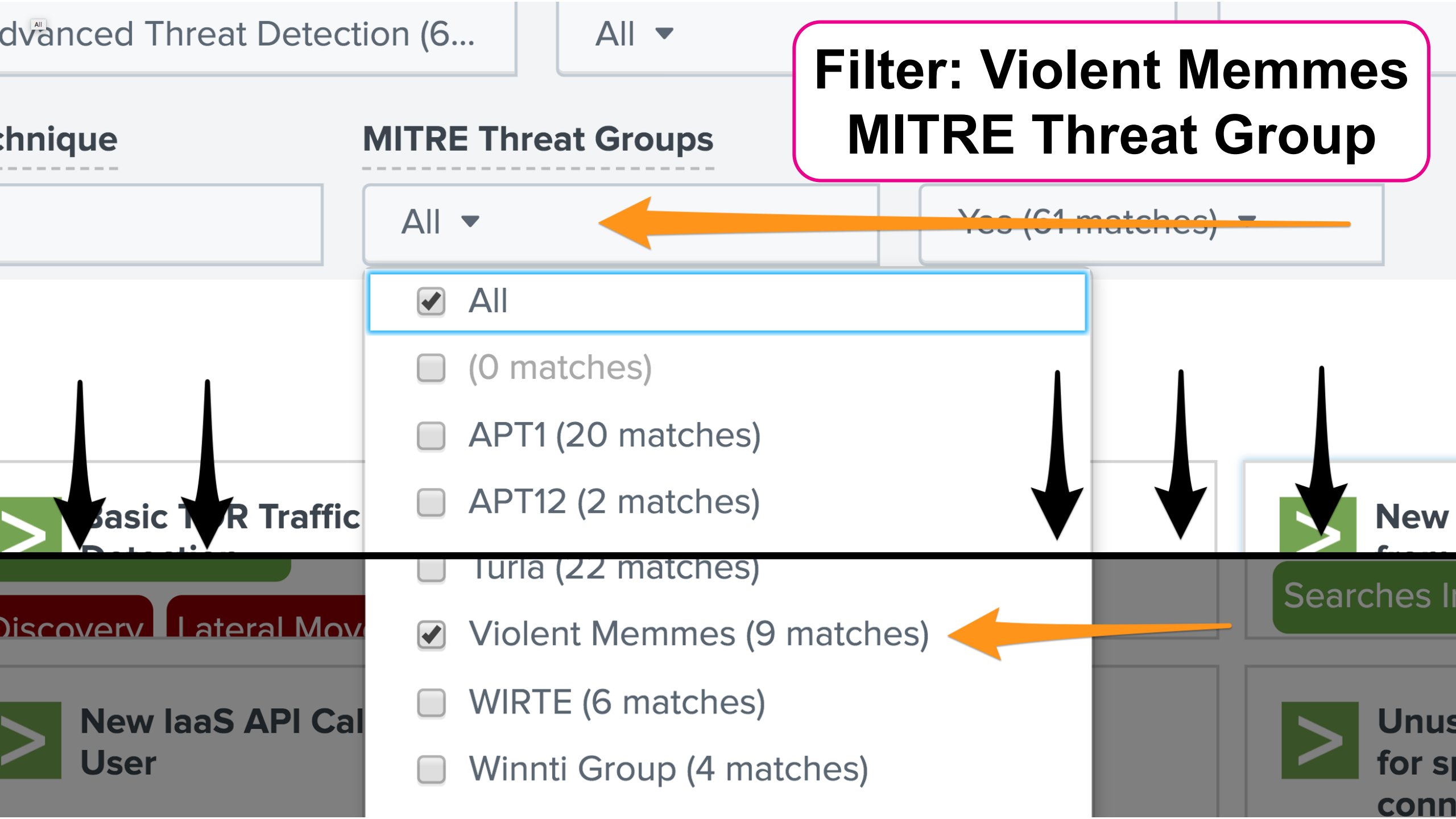
First Time Logon to New Server

Hosts Sending To More Destinations Than

Hosts Where Security Sources Go Quiet

Key Filters:

- MITRE ATT&CK Tactic
- MITRE ATT&CK Technique
- MITRE Threat Groups


dvanced Threat Detection (6...
All
Filter: Violent Memmes
MITRE Threat Group
chnique
MITRE Threat Groups
All
All
(0 matches)
APT1 (20 matches)
APT12 (2 matches)
Turla (22 matches)
Violent Memmes (9 matches)
WIRTE (6 matches)
Winnti Group (4 matches)
Searches I
New IaaS API Cal
User

Stage 1: Collection

You have the data onboard, what do you do first?



New Local Admin Account

Local admin accounts are used by legitimate technicians, but they're also used by attackers. This search looks for newly created accounts that are elevated to local admins.

Featured

Searches Included

Defense Evasion

Persistence

First Time Logon to New Server

Find users who logged into a new server for the first time.

Searches Included

Lateral Movement

Remote Services

Remote Desktop Protocol

Short Lived Adr Accounts

A technique used by a create an account, tak actions, and then dele away. This search will accounts on the local

Searches Included

Defense Evasion

Per

Create Account

New Local Admin Account

Security Content / New Local Admin Account

Assistant: Simple Search

Learn how to use this page

View Demo Data Live Data

Description

Local admin accounts are used by legitimate technicians, but they're also used by attackers. This search looks for newly created accounts that are elevated to local admins.

Use Case

Advanced Threat Detection, Security Monitoring, Compliance

Category

Endpoint Compromise

Security Impact

New local admin accounts are often a source of concern. Most organizations will deploy a small number of local admin accounts, used for particular applications or for access in the case of an issue contacting their network domain controller. On the other hand, malware, malicious intruders, and even insiders love to create local admin accounts because it allows them to maintain access through password changes, account deactivations, or in the case of malicious insiders, leaving the company. Whenever a local admin account is created on a host, particularly a privileged host, it is important to make sure that it is valid.

Alert Volume

Medium (?)

SPL Difficulty

Medium

Bookmark Status

Not Bookmarked

Data Availability

Good

Journey

Stage 1

MITRE ATT&CK Tactics (Click for Detail)

Defense Evasion, Persistence

MITRE ATT&CK Techniques (Click for Detail)

Valid Accounts, Create Account

MITRE Threat Groups (Click for Detail)

APT18, APT28, APT3, APT32, APT33, APT39, Carbanak, Dragonfly 2.0, FIN10, FIN4, FIN5, FIN6, FIN8, Leafminer, Leviathan, Night Dragon, OilRig, PittyTiger, Soft Cell, Stolen Pencil, Suckfly, TEMP.Veles, Threat Group-1314, Threat Group-3390, Violent Memmes, menuPass

Kill Chain Phases

Command and Control

mall number of
ontacting their
ers love to create
s, account
dmin account is

MITRE ATT&CK Tactics (Click for Detail)

Defense Evasion | Persistence

MITRE ATT&CK Techniques (Click for Detail)

Valid Accounts | Create Account

MITRE Threat Groups (Click for Detail)

APT18 | APT28 | APT3 | APT32 | APT33 | APT39 | Carbanak | Dragonfly 2.0 | FIN10 | FIN4 | FIN5 | FIN6 | FIN8 | Leafminer | Leviathan | Night Dragon | OilRig | PittyTiger | Soft Cell | Stolen Pencil | Suckfly | TEMP.Veles | Threat Group-1314 | Threat Group-3390 | Violent Memmes | nenuPass

Kill Chain Phases

Command and Control

Data Sources

Windows Security

Export ...

Assistant: Simp

Description

Local admin a
elevated to lo

Live Data

Use Case

Advanced T

Category

Endpoint Co

Security In

New local a
local admin
network dor
local admin
deactivation
created on a

Alert Volu

Medium (?)

SPL Difficu

Medium

Threat Group: Violent Memmes

Description

Violent Memmes (also known as APT404 / SUSTAINABLE PARADOX / CUBIC ZIRCONIA / SNARKY BEAR) is a hacker group identified by the FRPCENK threat intelligence company as a most likely Russian advanced actor. The group has been known to have advanced capabilities in exploiting windows machines along with knowledge of industrial control system processes.
Very little is known about the group other than a recent spat of activity in 2019 detected by the threat intelligence group FRPCENK. The group's name "VIOLENT MEMMES" was coined after analysts at FRPCENK consistently saw references to the Violent Femmes in the group's malware and C2 communications. Combined with their use of stego in internet memes and the occasional utilization of Violent Femmes band members (victor.delorenzo[@]gmail[.]com) in spear phishing campaigns, FRPCENK analyst Rtan Krowbar reported that "When you add it up, the name was obvious."
The VIOLENT MEMMES reportedly uses spearphishing and off-the-shelf hacking tools like Metasploit and PowerShell exploits to gain footholds on victim infrastructure. The group also uses social engineering and bribery to gain access to onsite locations. Finally, they have more than a passing knowledge of industrial control systems (ICS). Although the group appears to be primarily interested in stealing intellectual property if given the opportunity they will cause intentional physical damage to breweries. (Citation: FRPCENK)

Links

Splunk

Techni

One technique used by Violent Memmes For New Local Admin Account

> **T1136: Create Account**

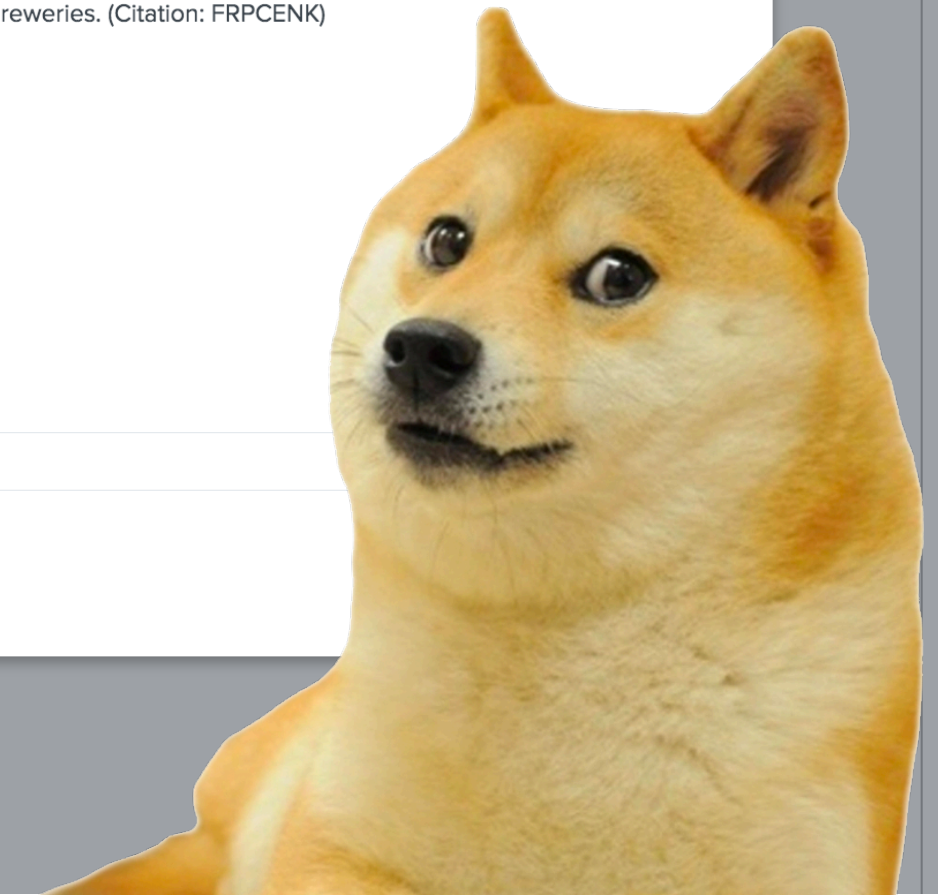
MITRE ATT&CK Summary: Violent Memmes used Create Account when attacking other organizations. (Citation: FRPCENK)

Source Name	Description
FRPCENK Research Organization	Operation Violent Memmes: NOT Good Feelings

What Team!

FRPCENK?

Such Intel!

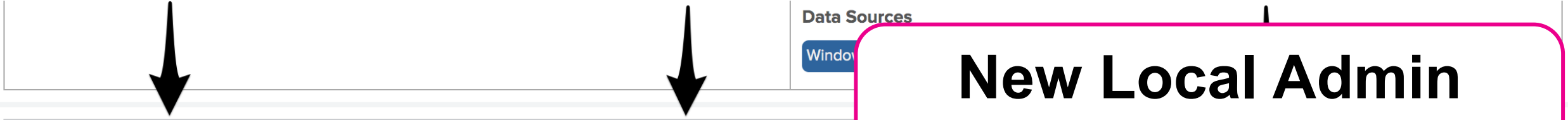


Kill Chain Phases

Command and Control

Data Sources

Windows Security



New Local Admin Account

> Related Splunk Capabilities

> How to Implement

> Known False Positives

> How To Respond

> SPL Mode

> Help

DEMO DATA You're looking at the *Demo* search right now. Did you know that we have 2 searches for this example? **Scroll Up** to the top to see the other searches.

Outlier(s)

1

Outlier(s)

Raw Event(s)

158

Raw Event(s)

Outliers Only

Account_Name	EventCode	Group_Name	Message
-	4720	Administrators	A member was added to a security-enabled local group. Subject: Security ID: S-1-5-21-2206723804-4039538768-2100233310-1109 Account Name: dveuve
dveuve	4732		A member was added to a security-enabled local group. Subject: Security ID: S-1-5-21-530973380-1803174443-1567984831-1004 Account Name: msmith_
msmith			A user account was created. Subject: Security ID: S-1-5-21-2206723804-4039538768-2100233310-1109 Account Name: dveuve Account Domain: CORP Logo
msmith_admin			A user account was created. Subject: Security ID: S-1-5-21-530973380-1803174443-1567984831-1004 Account Name: msmith_admin Account Domain: IP-(

Data Sources

Windo

New Local Admin Account

- Related Splunk Capabilities
- How to Implement
- Known False Positives
- How To Respond
- SPL Mode
- Help

DEMO DATA You're looking at the *Demo* search right now. Did you know that we have 2 searches for this example? **Scroll Up** to the top to see the other searches.

Outlier(s)

1

Outlier(s)

Raw Event(s)

158

Raw Event(s)

Outliers Only

Account_Name	EventCode	Group_Name	Message
-	4720	Administrators	A member was added to a security-enabled local group. Subject: Security ID: S-1-5-21-2206723804-4039538768-2100233310-1109 Account Name: dveuve
dveuve	4732		A member was added to a security-enabled local group. Subject: Security ID: S-1-5-21-530973380-1803174443-1567984831-1004 Account Name: msmith_
msmith			A user account was created. Subject: Security ID: S-1-5-21-2206723804-4039538768-2100233310-1109 Account Name: dveuve Account Domain: CORP Logo
msmith_admin			A user account was created. Subject: Security ID: S-1-5-21-530973380-1803174443-1567984831-1004 Account Name: msmith_admin Account Domain: IP-(

Home

Administrator ▾ 16 Messages ▾ Settings ▾

mentation ▾ Configuration

New Local Admin Account

Export ▾ ...

Learn how to use this page

View Demo Data | Live Data

created accounts that are

mark Status

ookmarked

Data Sources

Windows Security

Data Check	Status	Open in Search	Resolution (if needed)
Must have Windows Security Logs	✓	Open in Search	Begin ingesting Windows Security Logs
Must have Local Account Management Logs (Event ID 4720)	✓	Open in Search	Turn on Account Management Audit Logs in your Local Windows Security Policy (docs)
Must have Local Group Management Logs (Event ID 4732)	✓	Open in Search	Turn on Group Management Audit Logs in your Local Windows Security Policy (docs)

Schedule in ES

Enter a search

```
index=* source="*WinEventLog:Security" EventCode=4720 OR (EventCode=4732 Administrators)
| transaction Security_ID maxspan=180m connected=false
| search EventCode=4720 (EventCode=4732 Administrators)
 | table _time EventCode Account_Name Target_Account_Name Message
```

All time

✓ 1 event (10/15/16 12:00:00.000 PM to 10/17/19 2:54:35.000 AM)

Smart Mode

Detect New Values | Line-by-Line SPL Documentation

- Related Splunk Capabilities
- How to Implement
- Known False Positives
- How To Respond
- SPL Mode
- Help

If you do not see the SPL above

Outlier(s)

Raw Event(s)



al Wind Policy (docs)

Wi docs)

Schedule in ES

NOT YET!

All time

© 2019 SPLUNK INC.

Minor 3.0 Content Improvements

- Added GCP and Azure searches AWS detections
- The SPL is easier to find
- Search engine on Security Content page is improved
- Many small UI improvements

© 2019 SPLUNK INC.

Okay, We Found Some Content…

© 2019 SPLUNK INC.

Okay, we found some content…

But can we be more methodical?

© 2019 SPLUNK INC.

Being Prescriptive



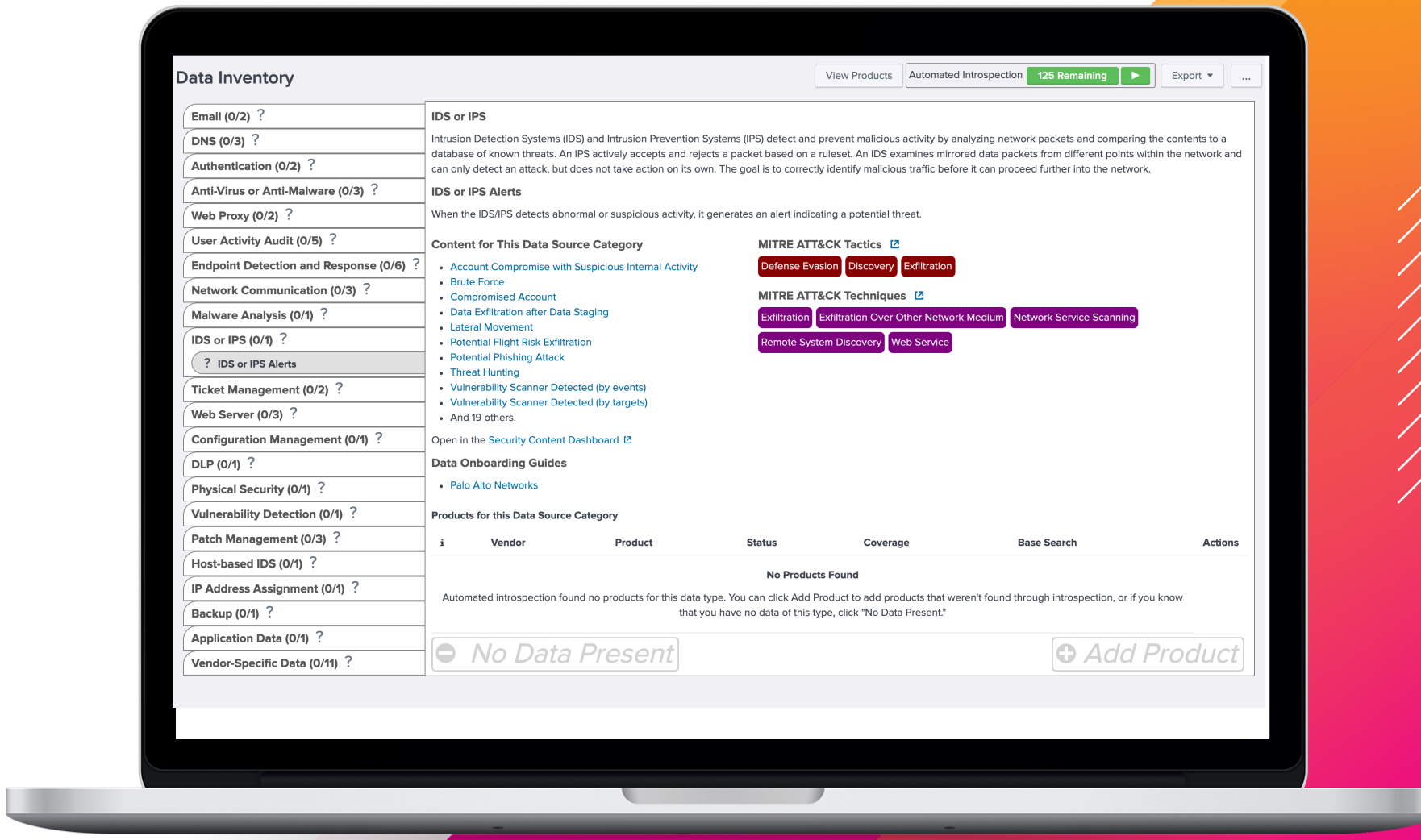
.conf19

splunk>

Configure SSE

The manual way

To take advantage of the full power of SSE you need to go through the configuration steps.



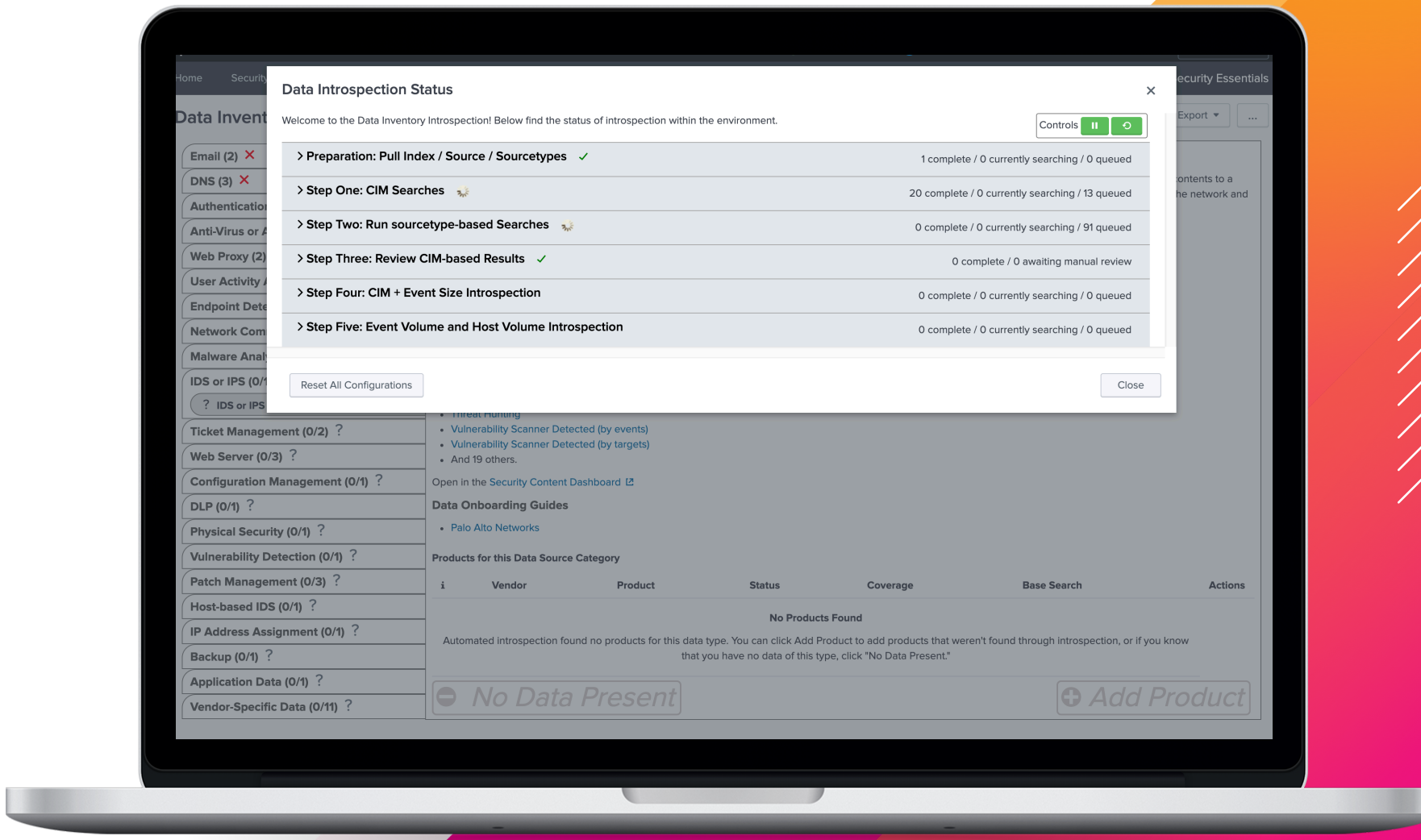
splunk> turn data into doing

© 2019 SPLUNK INC.

Configure SSE

The automatic way

SSE comes with an option to run an automated data introspection job.



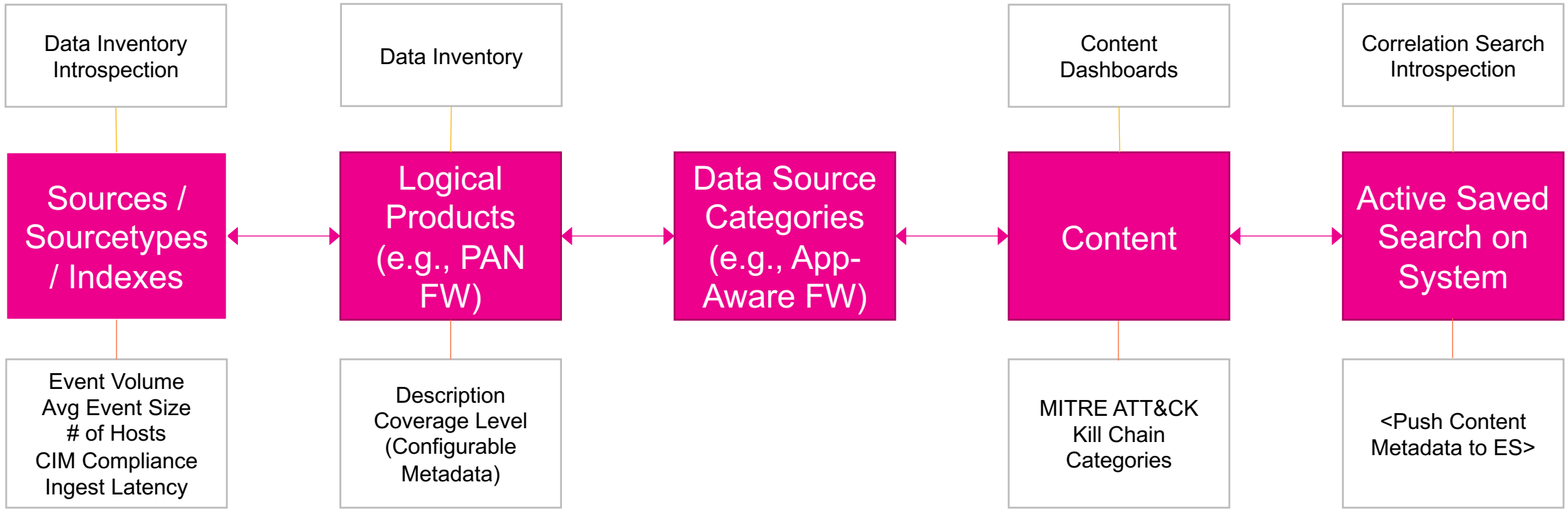
splunk> turn data into doing

© 2019 SPLUNK INC.

© 2019 SPLUNK INC.

Connecting Products to Data to Content

How does it work?



© 2019 SPLUNK INC.

Hands-On



.conf19

splunk>

Data Inventory

- Data Inventory
- Data Availability
- Data Source Check
- Security Data Journey
- Data Source Onboarding Guides

View Products | Automated Introspection Completed | Export | ...

- Email (2) ✓
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Ticket Management (2) ✓
- Web Server (2/3)
- Configuration Management (1) ✓
- DLP (1) ✗
- Physical Security (0/1) ?
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

Data Inve

The goal o ave, and fee
prescriptiv urity operatio

On this page, we will walk you through a variety of data types used by the
take 20-30 minutes, and you can always come back to answer questions
this automation through the Automated Introspection menu at the top of

Ready to get started?

Data Source Introspection

Data Inventory

View Products | Automated Introspection Completed | Export | ...

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (2) ✓
- Anti-Virus or Anti-Malware (3) ✓
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Ticket Management (2) ✓
- Web Server (2/3)
- Configuration Manag
- DLP (1) ✗
- Physical Sec
- Vulnera
- Pat

Email

Email is a significant component of day-to-day business (and personal) activity and can be accessible not only on corporate desktop computers but also mobile devices, including personal devices, which introduces new vulnerabilities and has become a critical part of enterprise cybersecurity efforts. Email messages and activity logs across these endpoints can provide critical insight ity that might warrant more in-depth investigation. For example, attackers may be sending emails with malicious code attached in ious code is hosted, targeting recipients, in order to obtain intellectual property or personally identifiable info ernal threats leveraging email may include transmitting data to external email accounts.

TMI!!!

he Simple Mail Transfer Protocol (SMTP). Relevant data sources include all the devices or ogs or protocol-specific wire data sources like Splunk Stream, Bro/Zeek, or a network

- E
- Emails from ains
- Emails with Lo ains
- Monitor Email P rand Abuse
- Phishing Investigation and Response
- ishing Attempt
- Attack
- Reset Emails
- ed
- tent Dashboard
- des

ATT&CK Tactics

Command and Control | Defense Evasion | Execution | Initial Access

MITRE ATT&CK Techniques

Custom Command and Control Protocol | Exploitation for Client Execution | Spearphishing Attachment | Spearphishing Link | Standard Application Layer Protocol

Kill Chain Phases

Delivery

urce Category

oduct	Status	Coverage	Base Search	Actions
ffice 365	Complete		index="main" sourcetype="ms:o365:reporting:messagetrace"	Update / Delete ×



Data Inventory

View Products | Automated Introspection Completed | Export | ...

Data Source

Data Source Category

Linked Content

Data Source Introspection

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (2) ✓
- Anti-Virus or Anti-Malware (3) ✓
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Ticket Management (2) ✓
- Web Server (2/3)
- Configuration Management (1) ✓
- DLP (1) ✗
- Physical Security (0/1) ?
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

Email

(and personal) activity and can be accessible not c
and has become a critical part of enterprise cybers
that might warrant more in-depth investigation. For
attached in a file or embedding a link to a website where the malicious code is hosted, targeting recipients
information/personal data, as well as command and control. In addition, internal threats leveraging email m

Incoming Messages

Inbound messages are messages that th e Simple Mail Transfer P
users generating email protocol traffic on the network captured from message trace logs or protocol-specific wire data sources like Splunk Stream, Bro/Zeek, or a network analysis solution like ExtraHop.

Content for This Data Source Category

- Email Attachments With Lots Of Spaces
- Emails from Outside the Organization with Company Domains
- Emails with Lookalike Domains
- Monitor Email For Brand Abuse
- Phishing Investigation and Response
- Possible Phishing Attempt
- Potential Phishing Attack
- Spike in Password Reset Emails
- Suspicious Behavior
- Threat Activity Detected
- And 2 others.

Open in the Security Content Dashboard

MITRE ATT&CK Tactics

Command and Control | Defense Evasion | Execution | Initial Access

MITRE ATT&CK Techniques

Custom Command and Control Protocol | Exploitation for Client Execution | Spearphishing Attachment | Spearphishing Link | Standard Application Layer Protocol

Kill Chain Phases

Delivery

Data Onboarding Guides

- Office 365

Product

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
>	Microsoft	Office 365	Complete		index="main" sourcetype="ms:o365:reporting:messagetrace"	Update / Delete ×

Add Product

Data Inventory

View Products | Automated Introspection Completed | Export | ...

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (2) ✓
- Anti-Virus or Anti-Malware (3) ✓
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Ticket Management (2) ✓
- Web Server (2/3)
- Configuration Management (1) ✓
- DLP (1) ✗
- Physical Security (0/1) ?
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗

Email

Email is a significant component of day-to-day business (and personal) activity and can be accessible no
personal devices, which introduces new vulnerabilities and has become a critical part of enterprise cybe
can provide critical insights into communication activity that might warrant more in-depth investigation. F
attached in a file or embedding a link to a website where the malicious code is hosted, targeting recipie
information/personal data, as well as command and control. In addition, internal threats leveraging emai

Data Source Introspection

Incoming Messages

Inbound messages are messages that the mail servers receive into the network via the Simple Mail Transfer Protocol (SMTP). Relevant data sources include all the devices or users generating email protocol traffic on the network captured from message trace logs or protocol-specific wire data sources like Splunk Stream, Bro/Zeek, or a network analysis solution like ExtraHop.

Content for This Data Source Category

- Email Attachments With Lots Of Spaces
- Emails from Outside the Organization with Company Domains
- Emails with Lookalike Domains
- Monitor Email For Brand Abuse
- Phishing Investigation and Response
- Possible Phishing Attempt
- Potential Phishing Attack
- Spike in Password Reset Emails
- Suspicious Behavior
- Threat Activity Detected
- And 2 others.

Open in the Security Content Dashboard

MITRE ATT&CK Tactics

Command and Control | Defense Evasion | Execution | Initial Access

MITRE ATT&CK Techniques

Custom Command and Control Protocol | Exploitation for Client Execution | Spearphishing Attachment | Spearphishing Link | Standard Application Layer Protocol

Kill Chain Phases

Delivery

Data Onboarding Guides

- Office 365

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
>	Microsoft	Office 365	Complete		index="main" sourcetype="ms:o365:reporting:messagetrace"	Update / Delete ×

© 2019 SPLUNK INC.

Data Inventory Introspection

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
☑	Microsoft	Office 365	Complete	✎	index="main" source	Update ✎ Delete ✕

Description

Automation: Added completely by automation for DSC DS001MAIL-ET03Send. Search that generated it: index= tag=email earliest=0 | head 300000| stats count by index sourcetype*

# of Hosts	Average Event Size	Typical Events Per Day	CIM Coverage	TERM Search
1.5 hosts	510.55 bytes	104 events	0% (?)	index="main" sourcetype="ms:o365:reporting:messagetrace"

⊕ Add Product

Event Volume
Avg Event Size
# of Hosts
CIM Compliance

Data Inventory

View Products | Automated Introspection Completed | Export | ...

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Ticket Management (2) ✓
- Web Server (2/3)
- Configuration Management (1) ✓
- DLP (1) ✗
- Physical Security (0/1) ?
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

Email

Email is a significant component of day-to-day business (and personal) activity and can be accessible not only on corporate desktop computers but also mobile devices, including personal devices, which introduces new vulnerabilities and has become a critical part of enterprise cybersecurity efforts. Email messages and activity logs across these endpoints can provide critical insights into communication activity that might warrant more in-depth investigation. For example, attackers may be sending emails with malicious code attached in a file or embedding a link to a website where the malicious code is hosted, targeting recipients, in order to obtain intellectual property or personally identifiable information/personal data, as well as command and control. In addition, internal threats leveraging email may include transmitting data to external email accounts.

Incoming Messages

Inbound messages are messages that the mail servers receive into the network via the Simple Mail Transfer Protocol (SMTP). Relevant data sources include all the devices or users generating email protocol traffic on the network captured from message trace logs or protocol-specific wire data sources like Splunk Stream, Bro/Zeek, or a network analysis solution like ExtraHop.

Content for This Data Source Category

- Email Attachments With Lots Of Spaces
- Emails from Outside the Organization with Company Domains
- Emails with Lookalike Domains
- Monitor Email For Brand Abuse
- Phishing Investigation and Response
- Possible Phishing Attempt
- Potential Phishing Attack
- Spike in Password Reset Emails
- Suspicious Behavior
- Threat Activity Detected
- And 2 others.

Open in the Security Content Dashboard

MITRE ATT&CK Tactics

Command and Control | Defense Evasion | Execution | Initial Access

MITRE ATT&CK Techniques

Custom Command and Control Protocol | Exploitation for Client Execution | Spearphishing Attachment | Spearphishing Link | Standard Application Layer Protocol

Kill Chain Phases

Delivery

Data Onboarding Guides

- Office 365

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
›	Microsoft	Office 365	Complete		index="main" sourcetype="ms:o365:reporting:messagetrace"	Update / Delete ×

Add Product

Products in environment

Data Inventory

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Ticket Management (2) ✓
- Web Server (2/3)
- Configuration Management (1) ✓
- DLP (1) ✗
- Physical Security (0/1) ?
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

Choose Existing Product

Add New Product

Assign Existing Product

Vendor Name	Product Name	Data Source Categories Already Mapped To
AWS	CloudTrail	AWS Cloudtrail
AWS	CloudWatch	Host Performance
AWS	Config	General Config Management Logs
AWS	VPC Flow Logs	Basic Traffic Logs
Azure	Active Directory	Successful Authentication Failed Authentication
Microsoft	Office 365	Outgoing Messages Incoming Messages
Microsoft	Sysmon	Object Change
Microsoft	Update Log	System eligible for patch Patch Applied Patch Failed
Microsoft	Windows Application Log	Application Logs
Microsoft	Windows Domain Controller	Domain Controller's Windows Security Logs
Microsoft	Windows Host and Server	Object Change on Removable Storage Windows Security Logs
Microsoft	Windows Powershell	Microsoft Powershell Logs

Cancel

g data to external email accounts.

evant data sources include all the devices or
ke Splunk Stream, Bro/Zeek, or a network

nitial Access

r Client Execution | Spearphishing Attachment

Actions

Update | Delete ×

Add Product

Data Inventory

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Ticket Management (2) ✓
- Web Server (2/3)
- Configuration Management (1) ✓
- DLP (1) ✗
- Physical Security (0/1) ?
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

View Products | Automated Introspection Completed | Export

Choose Existing Product

Add New Product

Add new product manually

Assign Existing Product

Vendor Name	Product Name	Data Source Categories Already Mapped To
AWS	CloudTrail	AWS Cloudtrail
AWS	CloudWatch	Host Performance
AWS	Config	General Config Management Logs
AWS	VPC Flow Logs	Basic Traffic Logs
Azure	Active Directory	Successful Authentication Failed Authentication
Microsoft	Office 365	Outgoing Messages Incoming Messages
Microsoft	Sysmon	Object Change
Microsoft	Update Log	System eligible for patch Patch Applied Patch Failed
Microsoft	Windows Application Log	Application Logs
Microsoft	Windows Domain Controller	Domain Controller's Windows Security Logs
Microsoft	Windows Host and Server	Object Change on Removable Storage Windows Security Logs
Microsoft	Windows Powershell	Microsoft Powershell Logs

Cancel

ellectual property or personally identifiable
g data to external email accounts.

evant data sources include all the devices or
ke Splunk Stream, Bro/Zeek, or a network

nitial Access

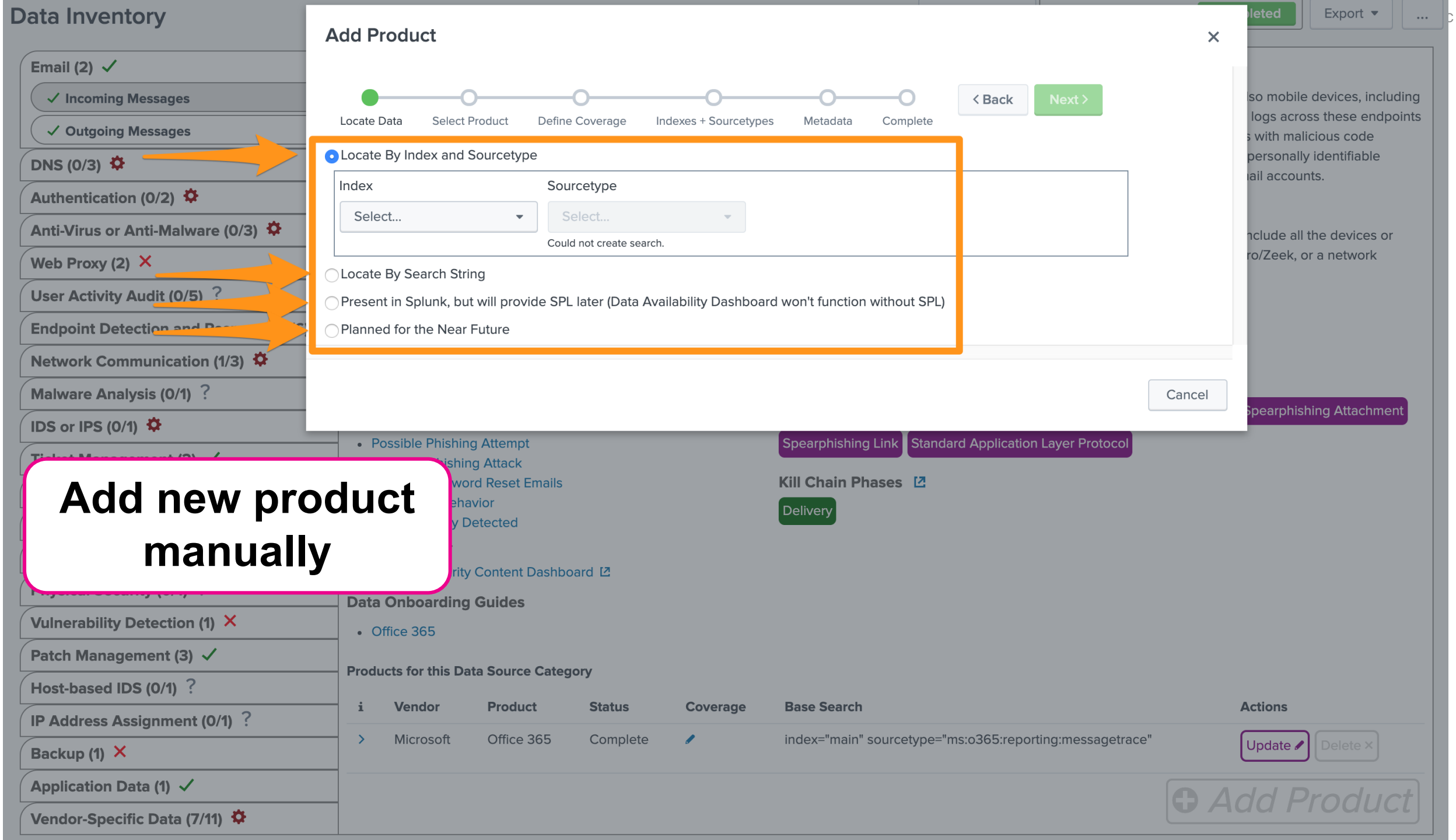
r Client Execution | Spearphishing Attachment

Actions

ace"

Update | Delete ×

Add Product


Data Inventory
Email (2)
Incoming Messages
Outgoing Messages
DNS (0/3)
Authentication (0/2)
Anti-Virus or Anti-Malware (0/3)
Web Proxy (2)
User Activity Audit (0/5)
Endpoint Detection and
Network Communication (1/3)
Malware Analysis (0/1)
IDS or IPS (0/1)
Vulnerability Detection (1)
Patch Management (3)
Host-based IDS (0/1)
IP Address Assignment (0/1)
Backup (1)
Application Data (1)
Vendor-Specific Data (7/11)
Add Product
Locate Data
Select Product
Define Coverage
Indexes + Sourcetypes
Metadata
Complete
Back
Next
Locate By Index and Sourcetype
Index
Sourcetype
Select...
Select...
Could not create search.
Locate By Search String
Present in Splunk, but will provide SPL later (Data Availability Dashboard won't function without SPL)
Planned for the Near Future
Cancel
Add new product manually
Possible Phishing Attempt
Spearphishing Link
Standard Application Layer Protocol
Kill Chain Phases
Delivery
Spearphishing Attachment
Data Onboarding Guides
Office 365
Products for this Data Source Category
Vendor
Product
Status
Coverage
Base Search
Actions
Microsoft
Office 365
Complete
index="main" sourcetype="ms:o365:reporting:messagetrace"
Update
Delete

Data Inventory

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

Add Product

Locate Data — Select Product — Define Coverage — Indexes + Sourcetypes — Metadata — Complete

< Back | Next >

- ○ Locate By Index and Sourcetype
- ◉ Locate By Search String
- ○ Present in Splunk, but will provide SPL later (Data Availability Dashboard won't function without SPL)
- ○ Planned for the Near Future

Cancel

Add new product manually

- Possible Phishing Attempt
- …hishing Attack
- …sword Reset Emails
- …ehavior
- …ty Detected

…urity Content Dashboard

Data Onboarding Guides

- Office 365

Spearphishing Link | Standard Application Layer Protocol

Kill Chain Phases

Delivery

…so mobile devices, including … logs across these endpoints …s with malicious code …personally identifiable …ail accounts.

…nclude all the devices or …ro/Zeek, or a network

Spearphishing Attachment

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
>	Microsoft	Office 365	Complete		index="main" sourcetype="ms:o365:reporting:messagetrace"	Update / Delete ×

Add Product

Data Inventory

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

Add Product

Locate Data — Select Product — Define Coverage — Indexes + Sourcetypes — Metadata — Complete

< Back | Next >

- ○ Locate By Index and Sourcetype
- ○ Locate By Search String
- ◉ Present in Splunk, but will provide SPL later (Data Availability Dashboard won't function without SPL)
- ○ Planned for the Near Future

Cancel

Add new product manually

- Email Attachments With Lots Of Spaces
- Emails from Outside the Organization with Company Domains
- Emails with Lookalike Domains
- Monitor Email For Brand Abuse
- Phishing Investigation and Response
- Possible Phishing Attempt
- ishing Attack
- sword Reset Emails
- ehavior
- ty Detected
- urity Content Dashboard

Data Onboarding Guides

- Office 365

Command and Control | Defense Evasion | Execution | Initial Access

MITRE ATT&CK Techniques

Custom Command and Control Protocol | Exploitation for Client Execution | Spearphishing Attachment | Spearphishing Link | Standard Application Layer Protocol

Kill Chain Phases

Delivery

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
>	Microsoft	Office 365	Complete		index="main" sourcetype="ms:o365:reporting:messagetrace"	Update / Delete ×

⊕ Add Product

Data Inventory

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

Add Product

Locate Data — Select Product — Define Coverage — Indexes + Sourcetypes — Metadata — Complete

< Back | Next >

- ○ Locate By Index and Sourcetype
- ○ Locate By Search String
- ○ Present in Splunk, but will provide SPL later (Data Availability Dashboard won't function without SPL)
- ◉ Planned for the Near Future

Cancel

Add new product manually

- Email Attachments With Lots Of Spaces
- Emails from Outside the Organization with Company Domains
- Emails with Lookalike Domains
- Monitor Email For Brand Abuse
- Phishing Investigation and Response
- Possible Phishing Attempt
- …hishing Attack
- …sword Reset Emails
- …ehavior
- …ty Detected
- …urity Content Dashboard

Command and Control | Defense Evasion | Execution | Initial Access

MITRE ATT&CK Techniques

Custom Command and Control Protocol | Exploitation for Client Execution | Spearphishing Attachment | Spearphishing Link | Standard Application Layer Protocol

Kill Chain Phases

Delivery

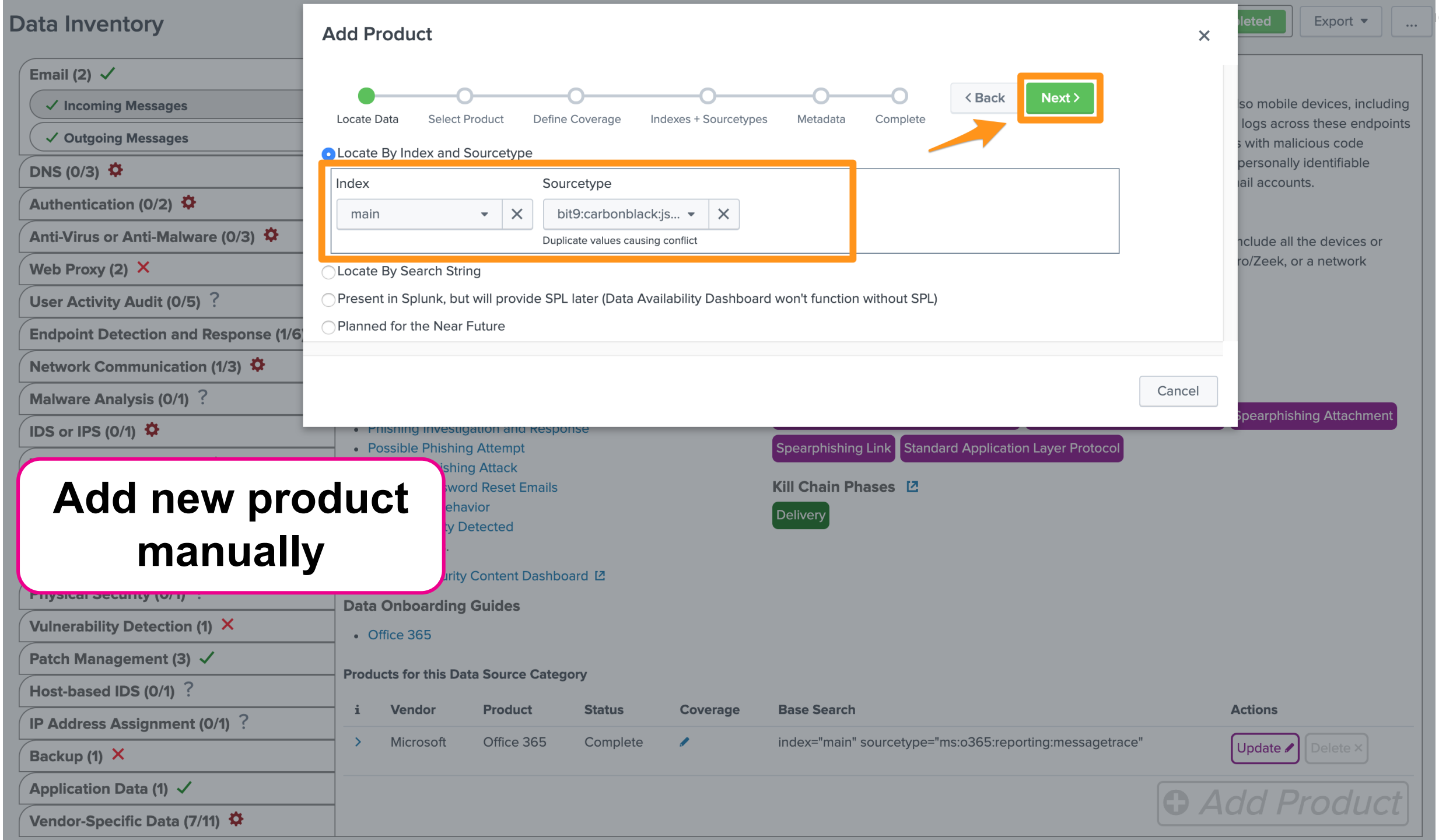
Data Onboarding Guides

- Office 365

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
>	Microsoft	Office 365	Complete	✎	index="main" sourcetype="ms:o365:reporting:messagetrace"	Update ✎ Delete ✕

⊕ Add Product


Data Inventory
Email (2)
Incoming Messages
Outgoing Messages
DNS (0/3)
Authentication (0/2)
Anti-Virus or Anti-Malware (0/3)
Web Proxy (2)
User Activity Audit (0/5)
Endpoint Detection and Response (1/6)
Network Communication (1/3)
Malware Analysis (0/1)
IDS or IPS (0/1)
Vulnerability Detection (1)
Patch Management (3)
Host-based IDS (0/1)
IP Address Assignment (0/1)
Backup (1)
Application Data (1)
Vendor-Specific Data (7/11)
Add Product
Locate Data
Select Product
Define Coverage
Indexes + Sourcetypes
Metadata
Complete
Back
Next
Locate By Index and Sourcetype
Index
main
Sourcetype
bit9:carbonblack:js...
Duplicate values causing conflict
Locate By Search String
Present in Splunk, but will provide SPL later (Data Availability Dashboard won't function without SPL)
Planned for the Near Future
Cancel
Add new product manually
Export
Spearphishing Attachment
Spearphishing Link
Standard Application Layer Protocol
Kill Chain Phases
Delivery
Data Onboarding Guides
Office 365
Products for this Data Source Category
Vendor
Product
Status
Coverage
Base Search
Actions
Microsoft
Office 365
Complete
index="main" sourcetype="ms:o365:reporting:messagetrace"
Update
Delete

Data Inventory

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

Add Product

Locate Data — Select Product — Define Coverage — Indexes + Sourcetypes — Metadata — Complete

< Back | Next >

- ○ Select from Pre-Configured Products
- ◉ Manually Specify
  - Vendor: Carbon Black
  - Product: Carbon Black CB Response
- ○ Do Not Specify Now

Cancel

Add new product manually

- Emails from Outside the Organization with Company Domains
- Emails with Lookalike Domains
- Monitor Email For Brand Abuse
- Phishing Investigation and Response
- Possible Phishing Attempt
- …hishing Attack
- …sword Reset Emails
- …Behavior
- …ity Detected
- …s.

…urity Content Dashboard

Data Onboarding Guides

- Office 365

MITRE ATT&CK Techniques

Custom Command and Control Protocol | Exploitation for Client Execution | Spearphishing Attachment | Spearphishing Link | Standard Application Layer Protocol

Kill Chain Phases

Delivery

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
>	Microsoft	Office 365	Complete		index="main" sourcetype="ms:o365:reporting:messagetrace"	Update / Delete ×

Add Product

…so mobile devices, including
…logs across these endpoints
…s with malicious code
…personally identifiable
…ail accounts.

…nclude all the devices or
…ro/Zeek, or a network

Data Inventory

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Physical Security (0/1) ?
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

Add Product

Locate Data — Select Product — Define Coverage — Indexes + Sourcetypes — Metadata — Complete

< Back | Next >

For most data sources, there can be gray areas for looking at what your coverage levels really are. For example, you might have Next-Gen Firewalls but only in your main offices, or you might have process launch logs but only from servers. This option allows you to specify your realistic level of coverage for this product.

0% How Is Your Coverage? 100%

100 % Complete

Reset

Cancel

How much of the data is in Splunk?

Add new product manually

Kill Chain Phases

Delivery

Data Onboarding Guides

- Office 365

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
>	Microsoft	Office 365	Complete		index="main" sourcetype="ms:o365:reporting:messagetrace"	Update / Delete ×

Add Product

Data Inventory

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

Add new product manually

Add Product

Locate Data → Select Product → Define Coverage → Indexes + Sourcetypes → Metadata → Complete

< Back | Next >

Status:

Validation success, received:

```
(index=main sourcetype=bit9:carbonblack:json)
```

Edit

Cancel

- Emails from Outside the Organization with Company Domains
- Emails with Lookalike Domains
- Monitor Email For Brand Abuse
- Phishing Investigation and Response
- Possible Phishing Attempt
- ishing Attack
- sword Reset Emails
- ehavior
- ty Detected

urity Content Dashboard

Data Onboarding Guides

- Office 365

MITRE ATT&CK Techniques

Custom Command and Control Protocol | Exploitation for Client Execution | Spearphishing Attachment | Spearphishing Link | Standard Application Layer Protocol

Kill Chain Phases

Delivery

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
>	Microsoft	Office 365	Complete		index="main" sourcetype="ms:o365:reporting:messagetrace"	Update / Delete ×

Add Product

Export

...

so mobile devices, including logs across these endpoints with malicious code personally identifiable ail accounts.

nclude all the devices or ro/Zeek, or a network

Data Inventory

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

Add new product manually

Add Product

Locate Data → Select Product → Define Coverage → Indexes + Sourcetypes → Metadata → Complete

< Back | Next >

Description

Added manually by Johan

Optional Description for Product

Cancel

- Email Attachments With Lots Of Spaces
- Emails from Outside the Organization with Company Domains
- Emails with Lookalike Domains
- Monitor Email For Brand Abuse
- Phishing Investigation and Response
- Possible Phishing Attempt
- ishing Attack
- sword Reset Emails
- Behavior
- ity Detected
- s.

urity Content Dashboard

Command and Control | Defense Evasion | Execution | Initial Access

MITRE ATT&CK Techniques

Custom Command and Control Protocol | Exploitation for Client Execution | Spearphishing Attachment | Spearphishing Link | Standard Application Layer Protocol

Kill Chain Phases

Delivery

Data Onboarding Guides

- Office 365

Products for this Data Source Category

Vendor	Product	Status	Coverage	Base Search	Actions
Microsoft	Office 365	Complete		index="main" sourcetype="ms:o365:reporting:messagetrace"	Update / Delete ×

Add Product

Data Inventory

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Ticket Management (2) ✓
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗
- Application Data (1) ✓
- Vendor-Specific Data (7/11)

Add new product manually

Add Product

Locate Data → Select Product → Define Coverage → Indexes + Sourcetypes → Metadata → Complete

< Back | Finish >

Complete!

Cancel | Complete

Export

...so mobile devices, including ...logs across these endpoints ...s with malicious code ...personally identifiable ...ail accounts.

...include all the devices or users generating email protocol traffic on the network captured from message trace logs or protocol-specific wire dat... ...es like Splunk Stream, Bro/Zeek, or a network analysis solution like ExtraHop.

Content for This Data Source Category

- Email Attachments With Lots Of Spaces
- Emails from Outside the Organization with Company Domains
- Emails with Lookalike Domains
- Monitor Email For Brand Abuse
- Phishing Investigation and Response
- Possible Phishing Attempt
- Potential Phishing Attack
- ...ssword Reset Emails
- ...Behavior
- ...vity Detected
- ...rs.

...curity Content Dashboard

MITRE ATT&CK Tactics

Command and Control | Defense Evasion | Execution | Initial Access

MITRE ATT&CK Techniques

Custom Command and Control Protocol | Exploitation for Client Execution | Spearphishing Attachment | Spearphishing Link | Standard Application Layer Protocol

Kill Chain Phases

Delivery

...arding Guides

- Office 365

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
>	Microsoft	Office 365	Complete		index="main" sourcetype="ms:o365:reporting:messagetrace"	Update / Delete ×
>	Carbon Black	Carbon Black CB Response	Analyzing CIM and Event Size	100%	index="main" sourcetype="bit9:carbonblack:json"	Update

© 2019 SPLUNK INC.

There must be a quicker way?

Automated Introspection

Data I

View Products | Automated Introspection Completed | Export | ...

- Email
- DNS (
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
  - Object Change
  - Process Launch
  - Process Launch with CLI
  - Process Launch with Executable Hash
  - ✓ Object Change on Removable Storage
  - Listening Port(s)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Ticket Management (2) ✓
- Web Server (2/3)
- Configuration Management (1) ✓
- DLP (1) ✗
- Physical Security (0/1) ?
- Vulnerability Detection (1) ✗

and Response

l Response (EDR) solutions monitor endpoints (servers, laptops, desktops, and mobile devices) for suspicious tivity like malware and other cyber threats
k than a simple signature or pattern and evade traditional anti-virus/anti-malware. Endpoints provide critical forensic data including process actions, file access information, network events, and endpoint configuration changes. The EDR can filter, enrich and monitor the data for signs of malicious behavior.

Object Change

An object, such as a file, directory, registry key, or other artifact was created, modified, accessed or deleted.

Content for This Data Source Category

- Abnormally High Number of Endpoint Changes By User
- Batch File Write to System32
- Common Ransomware Extensions
- Common Ransomware Notes
- Detect Path Interception By Creation Of program.exe
- Disabling Remote User Account Control
- Email files written outside of the Outlook directory
- Investigate GDPR Breaches Using ES
- Registry Keys Used For Persistence
- Threat Activity Detected
- And 17 others.

Open in the Security Content Dashboard

Data Onboarding Guides

- Windows Security Logs
- Windows Process Launch Logs
- Microsoft Sysmon

MITRE ATT&CK Tactics

Collection | Command and Control | Defense Evasion | Execution | Exfiltration | Impact | Initial Access | Lateral Movement | Persistence | Privilege Escalation

MITRE ATT&CK Techniques

Accessibility Features | AppInit DLLs | Application Shimming | Authentication Package | Change Default File Association | Command and Control | Custom Command and Control Protocol | Data Encrypted for Impact | Data Staged | Disabling Security Tools | Email Collection | Execution | File Permissions Modification | Modify Existing Service | Modify Registry | New Service | Port Monitors | Registry Run Keys / Startup Folder | Scripting | Spearphishing Attachment | Standard Application Layer Protocol

Kill Chain Phases

Actions on Objectives | Command and Control | Delivery | Installation

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
>	Microsoft	Sysmon	Complete		index="main" sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"	Update / Delete ×

Five introspection steps

Home | Security Content | Analytics Advisor | Security Operations | Data | Advanced | Documentation | Configuration | Splunk Security Essentials

Export ...

of introspection within the environment.

Controls

> Preparation: Pull Index / Source / Sourcetypes	0 complete / 0 currently searching / 1 queued
> Step One: CIM Searches ✓	33 complete / 0 currently searching / 0 queued
> Step Two: Run sourcetype-based Searches ✓	91 complete / 0 currently searching / 0 queued
> Step Three: Review CIM-based Results ?	0 complete / 13 awaiting manual review
> Step Four: CIM + Event Size Introspection ✓	25 complete / 0 currently searching / 0 queued
> Step Five: Event Volume and Host Volume Introspection ✓	25 complete / 0 currently searching / 0 queued

Reset All Configurations

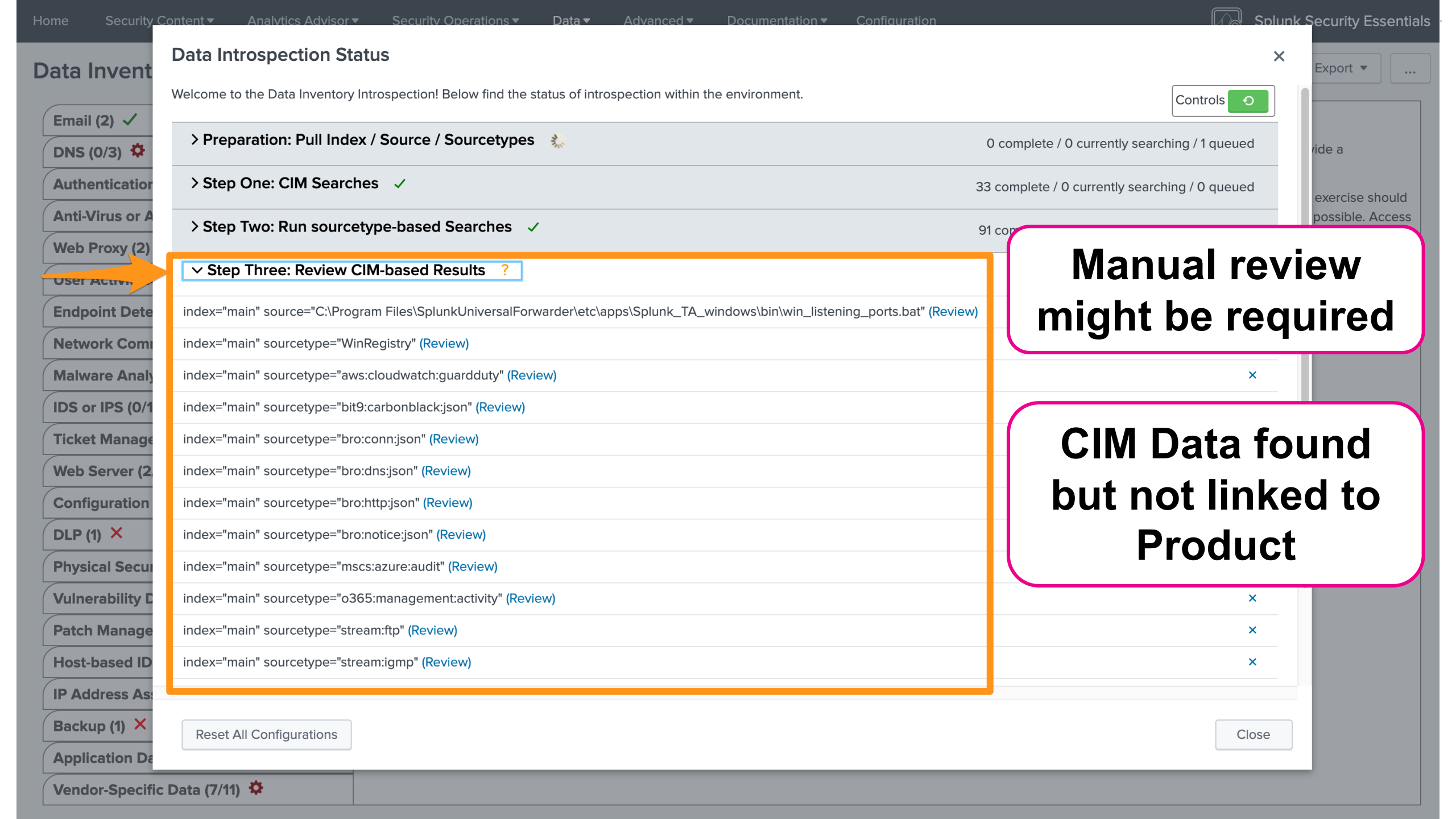
Close

Email (2) ✓
DNS (0/3)
Authentication
Anti-Virus or A
Web Proxy (2)
User Activity A
Endpoint Dete
Network Comm
Malware Analy
IDS or IPS (0/1
Ticket Manage
Web Server (2/3)
Configuration Management (1) ✓
DLP (1) ✗
Physical Security (0/1) ?
Vulnerability Detection (1) ✗
Patch Management (3) ✓
Host-based IDS (0/1) ?
IP Address Assignment (0/1) ?
Backup (1) ✗
Application Data (1) ✓
Vendor-Specific Data (7/11)

ide a

exercise should
possible. Access

Automated Introspection


Home
Security Content
Analytics Advisor
Security Operations
Data
Advanced
Documentation
Configuration
Splunk Security Essentials
Data Invent
Export
Email (2)
DNS (0/3)
Authentication
Anti-Virus or A
Web Proxy (2)
Endpoint Dete
Network Com
Malware Analy
IDS or IPS (0/1
Ticket Manage
Web Server (2
Configuration
DLP (1)
Physical Secu
Vulnerability D
Patch Manage
Host-based ID
IP Address As
Backup (1)
Application Da
Vendor-Specific Data (7/11)
Data Introspection Status
Welcome to the Data Inventory Introspection! Below find the status of introspection within the environment.
Controls
Preparation: Pull Index / Source / Sourcetypes
0 complete / 0 currently searching / 1 queued
Step One: CIM Searches
33 complete / 0 currently searching / 0 queued
Step Two: Run sourcetype-based Searches
Step Three: Review CIM-based Results
index="main" source="C:\Program Files\SplunkUniversalForwarder\etc\apps\Splunk_TA_windows\bin\win_listening_ports.bat" (Review)
index="main" sourcetype="WinRegistry" (Review)
index="main" sourcetype="aws:cloudwatch:guardduty" (Review)
index="main" sourcetype="bit9:carbonblack:json" (Review)
index="main" sourcetype="bro:conn:json" (Review)
index="main" sourcetype="bro:dns:json" (Review)
index="main" sourcetype="bro:http:json" (Review)
index="main" sourcetype="bro:notice:json" (Review)
index="main" sourcetype="mscs:azure:audit" (Review)
index="main" sourcetype="o365:management:activity" (Review)
index="main" sourcetype="stream:ftp" (Review)
index="main" sourcetype="stream:igmp" (Review)
Reset All Configurations
Close
Manual review might be required
CIM Data found but not linked to Product

Data Inventory

View Products | Automated Introspection Completed | Export | ...

- Email (2) ✓
  - ✓ Incoming Messages
  - ✓ Outgoing Messages
- DNS (0/3)
- Authentication (0/2)
- Anti-Virus or Anti-Malware (0/3)
- Web Proxy (2) ✗
- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Ticket Management (2) ✓
- Web Server (2/3)
- Configuration Management (1) ✓
- DLP (1) ✗
- Physical Security (0/1) ?
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?
- Backup (1) ✗

Email

Email is a significant component of day-to-day business (and personal) activity and can be accessible not only on corporate desktop computers but also mobile devices, including personal devices, which introduces new vulnerabilities and has become a critical part of enterprise cybersecurity efforts. Email messages and activity logs across these endpoints can provide critical insights into communication activity that might warrant more in-depth investigation. For example, attackers may be sending emails with malicious code attached in a file or embedding a link to a website where the malicious code is hosted, targeting recipients, in order to obtain intellectual property or personally identifiable information/personal data, as well as command and control. In addition, internal threats leveraging email may include transmitting data to external email accounts.

Incoming Messages

Inbound messages are messages th… sources include all the devices or users generating email protocol traf… Stream, Bro/Zeek, or a network analysis solution like ExtraHop.

Products generating the data

Content for This Data Source C…

- Email Attachments With Lots Of Spaces
- Emails from Outside the Organization with Company Domains
- Emails with Lookalike Domains
- Monitor Email For Brand Abuse
- Phishing Investigation and Response
- Possible Phishing Attempt
- Potential Phishing Attack
- Spike in Password Reset Emails
- Suspicious Behavior
- Threat Activity Detected
- And 2 others.

Open in the Security Content Dashboard

Data Onboarding Guides

- Office 365

Command and Control | Defense Evasion | Execution | Initial Access

MITRE ATT&CK Techniques

Custom Command and Control Protocol | Exploitation for Client Execution | Spearphishing Attachment | Spearphishing Link | Standard Application Layer Protocol

Kill Chain Phases

Delivery

Products for this Data Source Category

i	Vendor	Product	Status	Coverage	Base Search	Actions
⌄	Microsoft	Office 365	Complete	✎	index="main" sourcetype="ms:o365:reporting:messagetrace"	Update ✎ Delete ✕

© 2019 SPLUNK INC.

Products and the Content Mapped to Them

Edit ▾ | More Info ▾ | Add to Dashboard

This expects that you have completed the Data Inventory configuration, and mapped your active content on the Manage Bookmarks page. You will then get a complete view from product to the content that it enables.

✓ 7 results (16/10/2019 09:00:00.000 to 17/10/2019 09:15:06.000)

Job ▾

7 results | 20 per page ▾

Products generating the data

Product	Dataset That Provides Visibility	Data Source Category	Saved Search Name	Description	Total Mapped Content for This Product
AWS CloudTrail	(index="main" sourcetype="aws:cloudtrail")	Vendor-Specific Data > AWS Cloudtrail	ESCU - Detect New Open S3 buckets - Rule	*Automation: Added completely by automation for DSC VendorSpecific-aws-cloudtrail. Search that generated it: | tstats count where earliest=0 latest=now index=* sourcetype=aws*cloudtrail by index sourcetype*	1
Azure Active Directory	(index="main" sourcetype="ms:aad:signin")	Authentication > Failed Authentication Authentication > Successful Authentication	Access - Brute Force Access Behavior Detected - Rule Access - Brute Force Access Behavior Detected - Rule|Identity - Activity from Expired User Identity - Rule		1 2
Microsoft Office 365	(index="main" sourcetype="ms:o365:reporting:messagetrace")	Email > Incoming Messages	ESCU - Monitor Email For Brand Abuse - Rule	*Automation: Added completely by automation for DSC DS001MAIL-ET03Send. Search that generated it: index=* tag=email earliest=0 | head 300000| stats count by index sourcetype*	1
Microsoft Windows Host and Server	(index=main source=WinEventLog:Security) OR (index=main source=XmlWinEventLog:Security) OR (index=main source=wineventlog:security) OR (index=main source=xmlwineventlog:security)	Vendor-Specific Data > Windows Security Logs	ESCU - Detect Mimikatz Via PowerShell And EventCode 4663 - Rule|ESCU - Detect New Local Admin account - Rule	*Automation: Added completely by automation for DSC DS009EndPointIntel-ET05ObjectChangeRemovableStorage. Search that generated it: index=* (source="*winEventLog:Security") 4663 EventCode=4663 removable_storage earliest=0	2

© 2019 SPLUNK INC.

How do we know what detections are currently operational?

Security Content
Overview
Manage Bookmarks
Custom Content
MITRE ATT&CK-Driven Content Recommendation
Risk-based Alerting Content Recommendation

View Products | Automated Introspection Completed | Export | ...

- User Activity Audit (0/5) ?
- Endpoint Detection and Response (1/6)
- Network Communication (1/3)
  - Basic Traffic Logs
  - Application-aware Traffic Logs
  - User-aware Traffic Logs
- Malware Analysis (0/1) ?
- IDS or IPS (0/1)
- Ticket Management (2) ✓
- Web Server (2/3)
- Configuration Management (1) ✓
- DLP (1) ✗
- Physical Security (0/1) ?
- Vulnerability Detection (1) ✗
- Patch Management (3) ✓
- Host-based IDS (0/1) ?
- IP Address Assignment (0/1) ?

Network Communication

Network monitoring is essential for detecting threats originating from both outside and inside the network. Network communication data is a record of communication associated with core networks or data centers, but also distribution networks, WAN connections, and local area networks. Network data can be collected at the network perimeter (e.g., IDS/IPS, firewall logs), via internal networks (e.g., WANs, remote offices), Netflow, packet capture, deep packet inspection, and endpoint forensic data.

Basic Traffic Logs

Network activity data can be recorded by many technologies including host operating systems, firewalls, switches, routers, intrusion detection and prevention systems, and wire data sources. At a minimum, the event record should include the source IP address, source port number, destination IP address, destination port number, and the protocol used.

Content for This Data Source Category

- Account Compromise with Suspicious Internal Activity
- Basic Scanning
- Data Exfiltration after Data Staging
- Download from Internal Server
- IP Investigate and Report
- Investigate GDPR Breaches Using ES
- Lateral Movement
- New Connection to In-Scope Device
- Potential Phishing Attack
- SMB Traffic Spike
- And 52 others.

Open in the Security Content Dashboard

Data Onboarding Guides

- Palo Alto Networks
- Cisco ASA
- AWS VPC Flow

MITRE ATT&CK Tactics

Collection | Command and Control | Credential Access | Discovery | Execution | Exfiltration | Initial Access | Lateral Movement

MITRE ATT&CK Techniques

Commonly Used Port | Custom Command and Control Protocol | Custom Cryptographic Protocol | Data from Information Repositories | Data from Network Shared Drive | Email Collection | Exfiltration Over Alternative Protocol | Exfiltration Over Command and Control Channel | Exfiltration Over Other Network Medium | Exploitation of Remote Services | Hardware Additions | Multi-Stage Channels | Network Service Scanning | Network Share Discovery | Remote Desktop Protocol | Remote File Copy | Remote Services | Remote System Discovery | Service Execution | Standard Application Layer Protocol | Standard Cryptographic Protocol | Standard Non-Application Layer Protocol | Uncommonly Used Port | Valid Accounts | Windows Admin Shares

Kill Chain Phases

Actions on Objectives | Command and Control | Delivery | Reconnaissance

Products for this Data Source Category

Manage Bookmarks

Export | ...

Correlation Search Introspection | Manage List | Add Bookmark

Bookmarked	Waiting on Data	Ready For Deployment	Implementation Issues	Needs Tuning	Fully Implemented	Custom
0	0	0	0	0	13	0

AWS
- Detect New Open S3 buckets

Anti-Virus or Anti-Malware
- Host With A Recurring Malware Infection

Audit Trail
- Detect New Open S3 buckets

Authentication
- Activity from Expired User Identity
- Brute Force Access Behavior Detected

DNS
- Detect hosts connecting to dynamic domain providers

Email
- Monitor Email For Brand Abuse

Endpoint Detection and Response
- Create local admin accounts using net.exe
- Malicious PowerShell Process - Encoded Command
- Prohibited Process Detected
- Suspicious wevtutil Usage

IDS or IPS
- Vulnerability Scanner Detected (by targets)

Windows Security
- Detect Mimikatz Via PowerShell And EventCode 4663
- Detect New Local Admin account

i	Content	Open	Bookmarked	Waiting on Data	Ready for Deployment	Deployment Issues	Needs Tuning	Successfully Implemented	Notes	Remove
>	Activity from Expired User Identity		○	○	○	○	○	●	✎	✕
>	Brute Force Access Behavior Detected		○	○	○	○	○	●	✎	✕
>	Create local admin accounts using net.exe		○	○	○	○	○	●	✎	✕
>	Detect Mimikatz Via PowerShell And EventCode 4663		○	○	○	○	○	●	✎	✕
>	Detect New Local Admin account		○	○	○	○	○	●	✎	✕

Manage Bookmarks

Export | ...

Introspection | Manage List | Add Bookmark

Bookmarked	Waiting on Data	...mented	Custom
0	0	3	0

AWS
- Detect New Open S3 buckets

Anti-Virus or Anti-Malware
- Host With A Recurring Malware Infection

Audit Trail
- Detect New Open S3 buckets

Authentication
- Activity from Expired User Identity
- Brute Force Access Behavior Detected

DNS
- Detect hosts connecting to dynamic domain providers

Email
- Monitor Email For Brand Abuse

Endpoint Detection and Response
- Create local admin accounts using net.exe
- Malicious PowerShell Process - Encoded Command
- Prohibited Process Detected
- Suspicious wevtutil Usage

IDS or IPS
- Vulnerability Scanner Detected (by targets)

Windows Security
- Detect Mimikatz Via PowerShell And EventCode 4663
- Detect New Local Admin account

i	Content	Open	Bookmarked	Waiting on Data	Ready for Deployment	Deployment Issues	Needs Tuning	Successfully Implemented	Notes	Remove
>	Activity from Expired User Identity									
>	Brute Force Access Behavior Detected									
>	Create local admin accounts using net.exe									
>	Detect Mimikatz Via PowerShell And EventCode 4663									
>	Detect New Local Admin account									

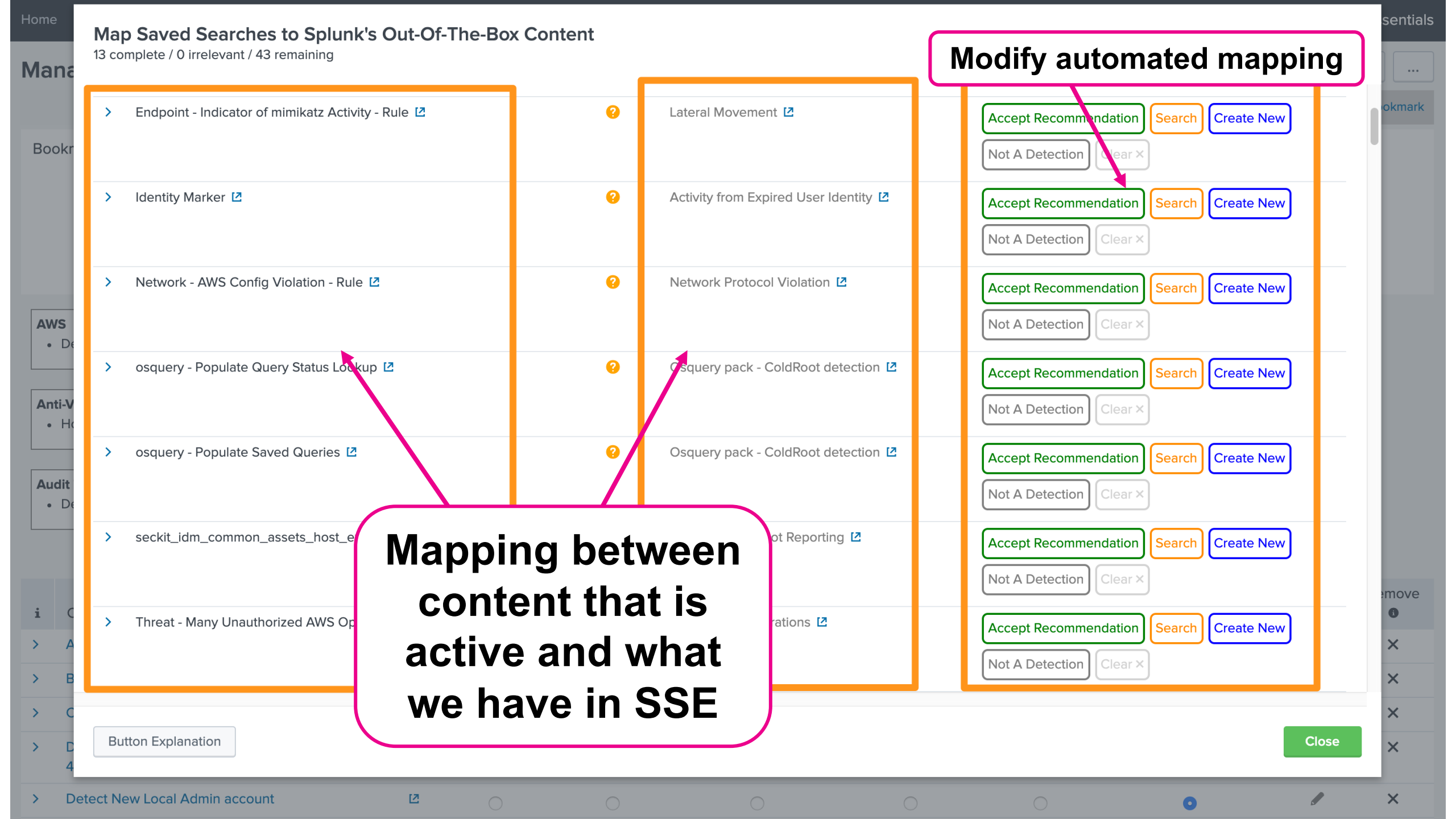
Look for Active Content

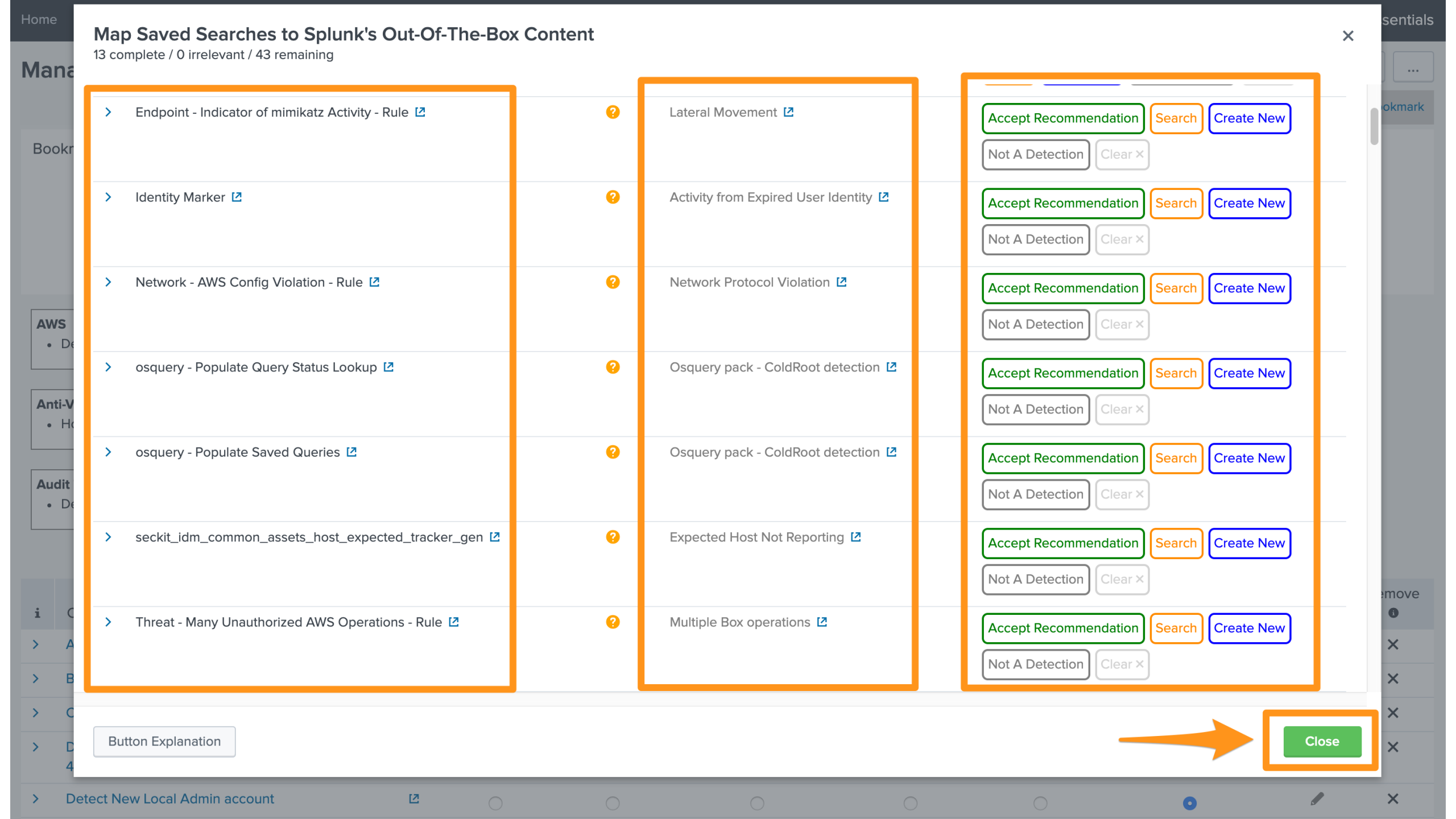
In order to help you prioritize new content via the Analytics Advisor dashboards, it's useful to be able to show your existing levels of coverage and areas of focus. To make this as easy as possible, this app includes a workflow for listing all of your local saved searches and then either mapping them to Splunk's out-of-the-box-content, or creating new content in Splunk Security Essentials that you can tag with all of the metadata you care about.

Finally, remember that you can always come back here and change any of these settings.

Look for Enabled Content

Close


Map Saved Searches to Splunk's Out-Of-The-Box Content
13 complete / 0 irrelevant / 43 remaining
Modify automated mapping
Endpoint - Indicator of mimikatz Activity - Rule
Lateral Movement
Identity Marker
Activity from Expired User Identity
Network - AWS Config Violation - Rule
Network Protocol Violation
osquery - Populate Query Status Lookup
Osquery pack - ColdRoot detection
osquery - Populate Saved Queries
Osquery pack - ColdRoot detection
Threat - Many Unauthorized AWS Op
Accept Recommendation
Search
Create New
Not A Detection
Clear
Mapping between content that is active and what we have in SSE
Button Explanation
Close


Home
sentials
Map Saved Searches to Splunk's Out-Of-The-Box Content
13 complete / 0 irrelevant / 43 remaining
Endpoint - Indicator of mimikatz Activity - Rule
Lateral Movement
Accept Recommendation
Search
Create New
Not A Detection
Clear
Identity Marker
Activity from Expired User Identity
Accept Recommendation
Search
Create New
Not A Detection
Clear
Network - AWS Config Violation - Rule
Network Protocol Violation
Accept Recommendation
Search
Create New
Not A Detection
Clear
osquery - Populate Query Status Lookup
Osquery pack - ColdRoot detection
Accept Recommendation
Search
Create New
Not A Detection
Clear
osquery - Populate Saved Queries
Osquery pack - ColdRoot detection
Accept Recommendation
Search
Create New
Not A Detection
Clear
seckit_idm_common_assets_host_expected_tracker_gen
Expected Host Not Reporting
Accept Recommendation
Search
Create New
Not A Detection
Clear
Threat - Many Unauthorized AWS Operations - Rule
Multiple Box operations
Accept Recommendation
Search
Create New
Not A Detection
Clear
Button Explanation
Close
Detect New Local Admin account

© 2019 SPLUNK INC.

Now when it is setup, let's see what we can do.

Content Overview
MITRE ATT&CK Framework
Cyber Kill Chain

Manage Bo

Export | ...

Correlation Search Introspection | Manage List | Add Bookmark

Bookmarked	Waiting on Data	Ready For Deployment	Implementation Issues	Needs Tuning	Fully Implemented	Custom
0	0	0	0	0	13	0

AWS
- Detect New Open S3 buckets

Anti-Virus or Anti-Malware
- Host With A Recurring Malware Infection

Audit Trail
- Detect New Open S3 buckets

Authentication
- Activity from Expired User Identity
- Brute Force Access Behavior Detected

DNS
- Detect hosts connecting to dynamic domain providers

Email
- Monitor Email For Brand Abuse

Endpoint Detection and Response
- Create local admin accounts using net.exe
- Malicious PowerShell Process - Encoded Command
- Prohibited Process Detected
- Suspicious wevtutil Usage

IDS or IPS
- Vulnerability Scanner Detected (by targets)

Windows Security
- Detect Mimikatz Via PowerShell And EventCode 4663
- Detect New Local Admin account

i	Content	Open	Bookmarked	Waiting on Data	Ready for Deployment	Deployment Issues	Needs Tuning	Successfully Implemented	Notes	Remove
>	Activity from Expired User Identity									
>	Brute Force Access Behavior Detected									
>	Create local admin accounts using net.exe									
>	Detect Mimikatz Via PowerShell And EventCode 4663									
>	Detect New Local Admin account									

Content Overview

Edit | Export | ...

Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.

This dashboard requires that you have gone through the Data Inventory. Click here go to Data Inventory.

Active	Available	Needs data
10	325	123
Content (Active)	Content (Available)	Content (Needs data)

1. Available Content

Click in the graphs below to filter on an area you want to highlight.

Chart View | Radar View | Sankey View | Security Journey View

Split by: App

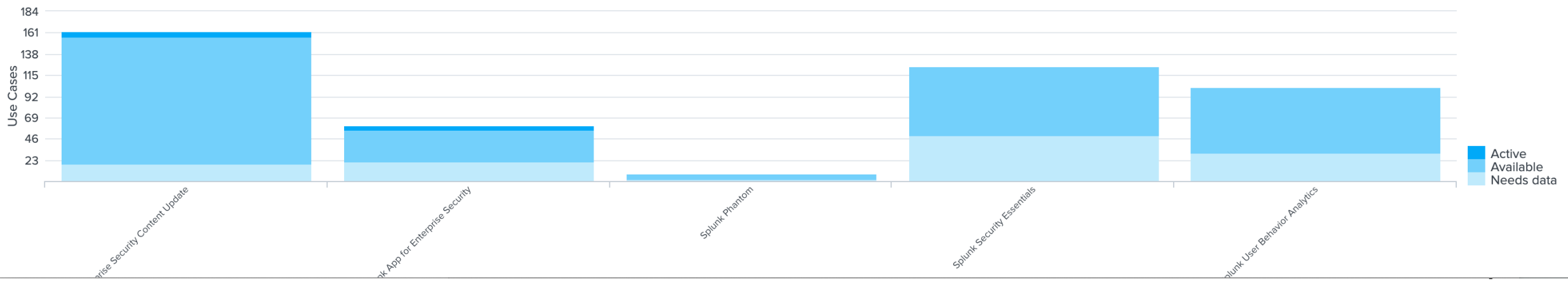
Status: Any

Featured: Yes

Bookmarked: Yes

Highlight Data Source: None

Click to filter



Active content

We have data, but not actived

Edit | Export | ...

Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.

This dashboard requires that you have gone through the Data Inventory. Click here go to Data Inventory.

Active	Available	Needs data
10	325	123
Content (Active)	Content (Available)	Content (Needs data)

Need more data to enable

1. Available Content

Click in the graphs below to filter on an area you want to highlight.

Chart View | Radar View | Sankey View | Security Journey View

Split by: App

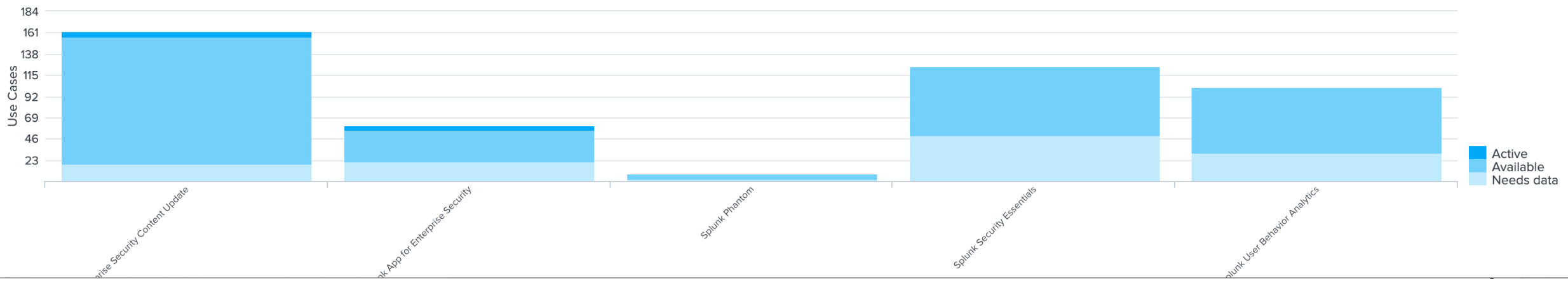
Status: Any

Featured: Yes

Bookmarked: Yes

Highlight Data Source: None

Click to filter



Content Overview

Edit | Export | ...

Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.

This dashboard requires that you have gone through the Data Inventory. Click here go to Data Inventory.

Active	Available	Needs data
10	325	123
Content (Active)	Content (Available)	Content (Needs data)

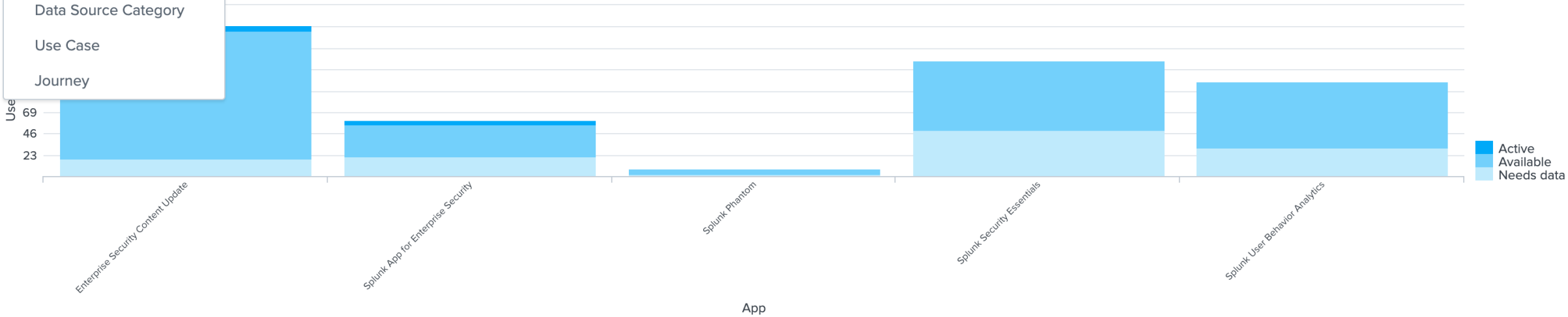
1. Available Content

Click in the graphs below to filter on an area you want to highlight.

Chart View | Radar View | Sankey View | Security Journey View

Split by: App | Status: Any | Featured: Yes | Bookmarked: Yes | Highlight Data Source: None

- App
- Data Source
- Data Source Category
- Use Case
- Journey



Content Overview

Edit | Export | ...

Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.

This dashboard requires that you have gone through the Data Inventory. Click here go to Data Inventory.

Active	Available	Needs data
10	325	123
Content (Active)	Content (Available)	Content (Needs data)

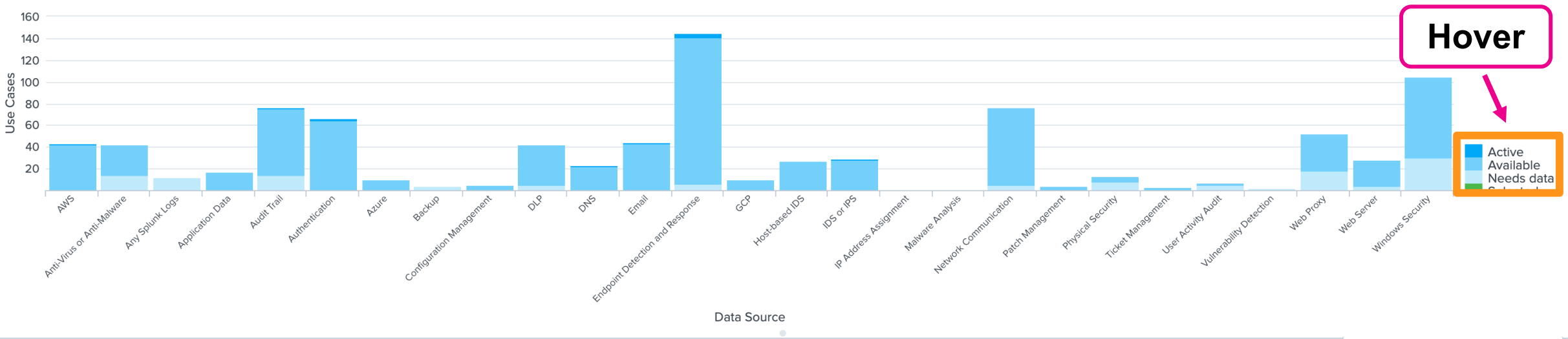
1. Available Content

Click in the graphs below to filter on an area you want to highlight.

Chart View | Radar View | Sankey View | Security Journey View

Split by: Data Source | Status: Any | Featured: Yes | Bookmarked: Yes | Highlight Data Source: None

Click to filter



Content Overview

Edit | Export | ...

Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.

This dashboard requires that you have gone through the Data Inventory. Click here go to Data Inventory.

Active	Available	Needs data
10	325	123
Content (Active)	Content (Available)	Content (Needs data)

1. Available Content

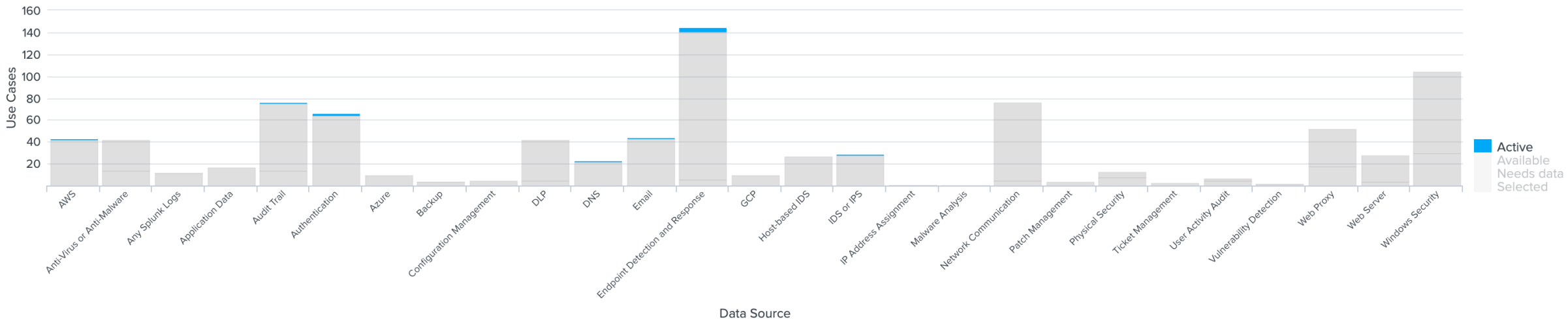
Click in the graphs below to filter on an area you want to highlight.

Data Sources you are getting value from

Chart View | Radar View | Sankey View | Security Journey View

Split by: Data Source | Status: Any | Featured: Yes | Bookmarked: Yes | Highlight Data Source: None

Click to filter



Content Overview

Edit | Export | ...

Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.

This dashboard requires that you have gone through the Data Inventory. Click here go to Data Inventory.

Active	Available	Needs data
10	325	123
Content (Active)	Content (Available)	Content (Needs data)

1. Available Content

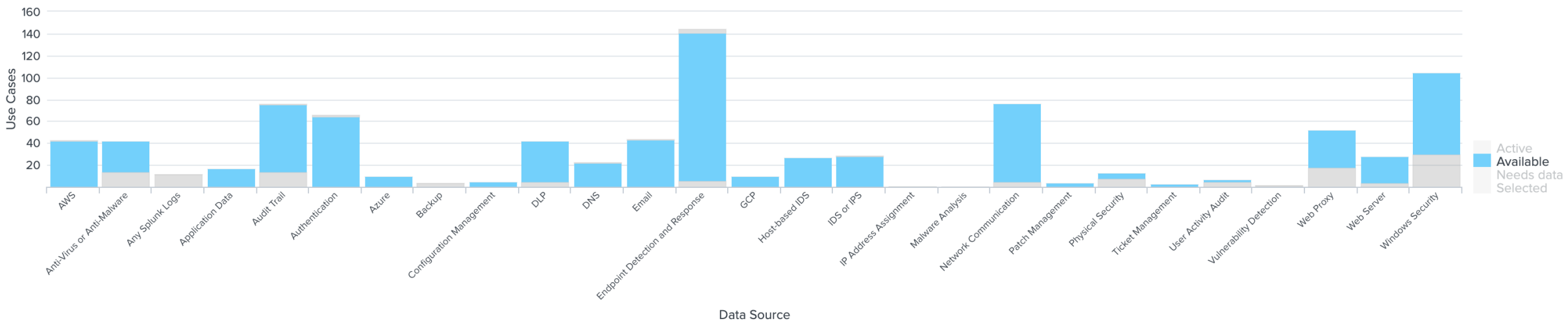
Click in the graphs below to filter on an area you want to highlight.

Data Sources with untapped value

Chart View | Radar View | Sankey View | Security Journey View

Split by: Data Source | Status: Any | Featured: Yes | Bookmarked: Yes | Highlight Data Source: None

Click to filter



Content Overview

Edit | Export | ...

Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.

This dashboard requires that you have gone through the Data Inventory. Click here go to Data Inventory.

Active	Available	Needs data
10	325	123
Content (Active)	Content (Available)	Content (Needs data)

1. Available Content

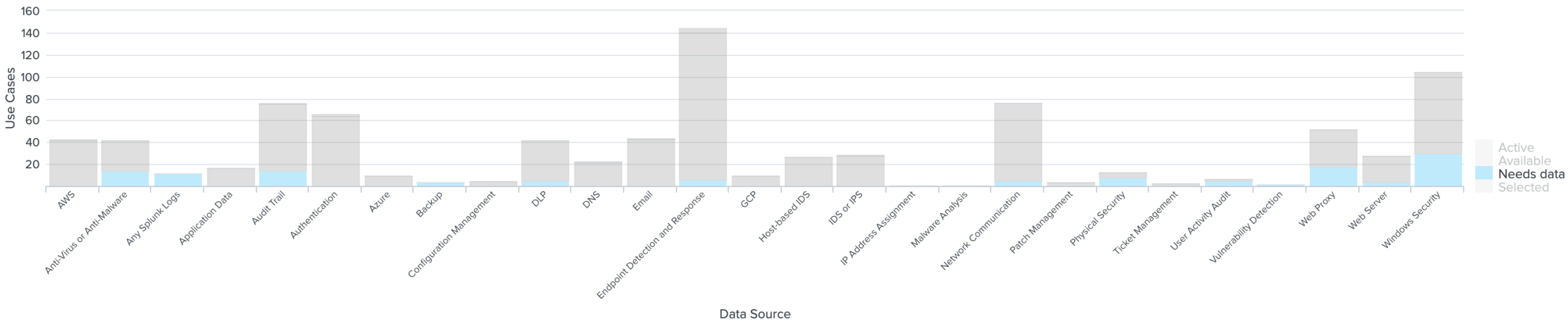
Click in the graphs below to filter on an area you want to highlight.

Data Sources not in Splunk where content exist

Chart View | Radar View | Sankey View | Security Journey View

Split by: Data Source | Status: Any | Featured: Yes | Bookmarked: Yes | Highlight Data Source: None

Click to filter



Content Overview

Edit | Export | ...

Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.

This dashboard requires that you have gone through the Data Inventory. Click here go to Data Inventory.

Active	Available	Needs data
10	325	123
Content (Active)	Content (Available)	Content (Needs data)

1. Available Content

Click in the graphs below to filter on an area you want to highlight.

Chart View | Radar View | Sankey View | Security Journey View

Split by: Data Source | Status: Any | Featured: Yes | Bookmarked: Yes | Highlight Data Source: None

Click to filter



© 2019 SPLUNK INC.

Content selection

Status: Available

Originating app: Any

Use Case: Any

Journey: Any

Data Source: Endpoint Detection...

Data Source Category: Any

Bookmark Status: Any

Featured: Any

Search Filter:

2. Selected Content

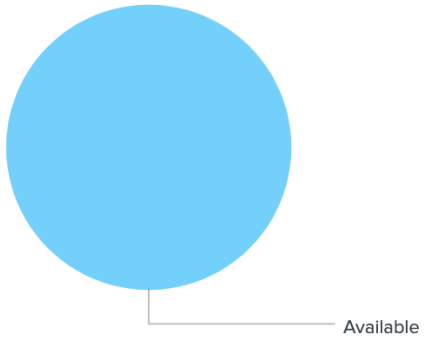
Use the drop downs or tables to further filter your selection.

Selection | Content list | Selection by Data Source | Selection by Data Source Category | Selection by Use Case | Selection by Journey

Total Selected

135

Selection by Status



3. View Content

Click the button below to drill down in to the content.

Drill down to content selection

Content selection

Status: Available | Originating app: Any | Use Case: Any | Journey: Any | Data Source: Endpoint Detection... | Data Source Category: Any

Bookmark Status: Any | Featured: Any | Search Filter:

Content with Status Available

2. Selected Content

Use the drop downs or tables to further filter your selection.

Selection | **Content list** | Selection by Data Source | Selection by Data Source Category | Selection by Use Case | Selection by Journey

	Journey	Status	Title	Data Source	Data Source Category	Use Case	App	Bookmark Status	Featured	Enabled	Data Availability	Data Coverage
1	Stage_1	Available	Remote PowerShell Launches	Endpoint Detection and Response Windows Security	Process Launch Windows Security Logs	Advanced Threat Detection	Splunk Security Essentials	Not Bookmarked	No	No	Good	100 %
2	Stage_1	Available	Disabled Update Service	Endpoint Detection and Response	Process Launch	Security Monitoring	Splunk Security Essentials	Not Bookmarked	No	No	Good	100 %
3	Stage_2	Available	Spike in File Writes	Endpoint Detection and Response	Object Change	Security Monitoring Advanced Threat Detection	Enterprise Security Content Update	Not Bookmarked	No	No	Good	100 %
4	Stage_2	Available	Investigate GDPR Breaches Using ES	Authentication Web Proxy Endpoint Detection and Response Application Data Anti-Virus or Anti-Malware Network Communication	Malware Detected Malware Definition Updates Application Logs Successful Authentication Failed	Compliance	Splunk App for Enterprise Security	Not Bookmarked	Yes	No	Good	100 %

© 2019 SPLUNK INC.

Content selection

Status: Available | Originating app: Any | Use Case: Any | Journey: Any | Data Source: Endpoint Detection... | Data Source Category: Any

Bookmark Status: Any | Featured: Any | Search Filter:

Content with Status Available split by Data Source

2. Selected Content

Use the drop downs or tables to further filter your selection.

Selection | Content list | **Selection by Data Source** | Selection by Data Source Category | Selection by Use Case | Selection by Journey

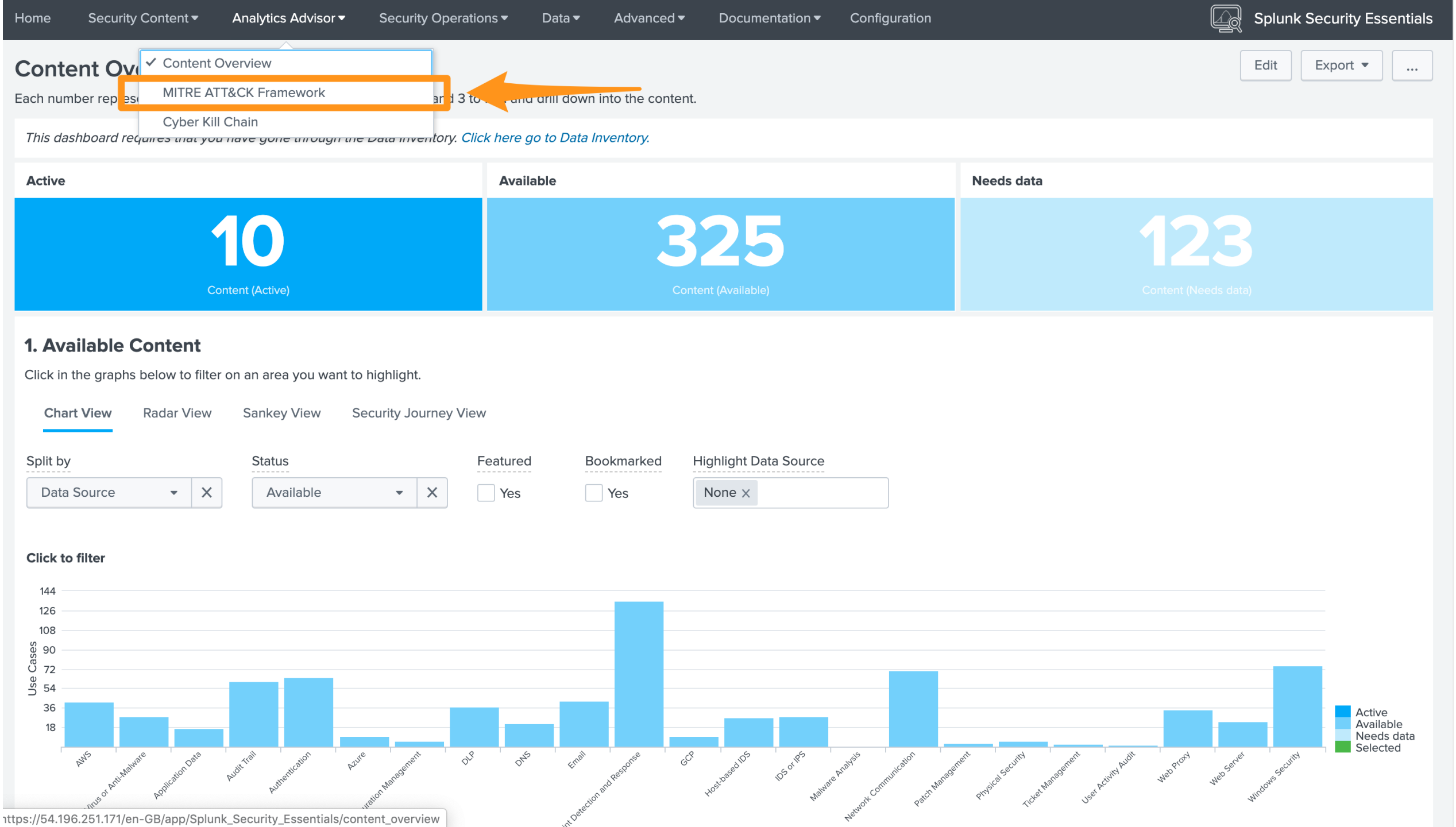
Click to filter

	Data Source	Total	Active	Available	Needs data	Selected
1	Endpoint Detection and Response	135	0	135	0	0
2	Windows Security	42	0	42	0	0
3	Network Communication	28	0	28	0	0
4	Web Proxy	28	0	28	0	0
5	DLP	26	0	26	0	0
6	Email	26	0	26	0	0
7	Authentication	21	0	21	0	0
8	Anti-Virus or Anti-Malware	18	0	18	0	0
9	Host-based IDS	17	0	17	0	0
10	IDS or IPS	17	0	17	0	0

« Prev 1 2 Next »

© 2019 SPLUNK INC.

What about MITRE ATT&CK?


Home
Security Content
Analytics Advisor
Security Operations
Data
Advanced
Documentation
Configuration
Splunk Security Essentials
Content Overview
MITRE ATT&CK Framework
Cyber Kill Chain
Edit
Export
...
Content Ov
Each number rep
and 3 to
and drill down into the content.
This dashboard requires that you have gone through the Data Inventory. Click here go to Data Inventory.
Active
10
Content (Active)
Available
325
Content (Available)
Needs data
123
Content (Needs data)
1. Available Content
Click in the graphs below to filter on an area you want to highlight.
Chart View
Radar View
Sankey View
Security Journey View
Split by
Data Source
Status
Available
Featured
Yes
Bookmarked
Yes
Highlight Data Source
None
Click to filter
Use Cases
144
126
108
90
72
54
36
18
AWS
Application Data
Audit Trail
Authentication
Azure
DLP
DNS
Email
GCP
Host-based IDS
IDS or IPS
Malware Analysis
Network Communication
Patch Management
Physical Security
Ticket Management
User Activity Audit
Web Proxy
Web Server
Windows Security
Active
Available
Needs data
Selected
https://54.196.251.171/en-GB/app/Splunk_Security_Essentials/content_overview

MITRE ATT&CK Framework

Edit | Export | ...

Each number represents a piece of content. Follow the headlines 1, 2 and 3 to find and drill down into the content.

For more details check the MITRE ATT&CK Navigator.

Active	Available	Needs data
9	251	95
Content (Active)	Content (Available)	Content (Needs data)

1. Available Content

Click in the graphs below to filter on an area you want to highlight.

MITRE ATT&CK Matrix | Chart View | Radar View | Sankey View | Security Journey View

Color by: Total

MITRE ATT&CK Threat Group: None

Highlight Data Source: None ×

Show Only Available Content: ☐ Yes

Show Only Popular Techniques: ☐ Yes

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation	Firmware Corruption
Spearphishing via	Execution through	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop	Data from Removable	Exfiltration Over Physical	Domain Fronting	Inhibit System

Scroll down

Color by

Total

- Total
- Active
- Available
- Needs data

MITRE ATT&CK Threat Group

None

Highlight Data Source

None ×

Show Only Available Content

Yes

Show Only Popular Techniques

Yes

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port	Data Destruction
Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media	Data Encrypted for Impact
Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy	Defacement
AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol	Disk Content Wipe
AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol	Disk Structure Wipe
Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding	Endpoint Denial of Service
Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation	Firmware Corruption
BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting	Inhibit System Recovery
Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Domain Generation Algorithms	Network Denial of Service
Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture		Fallback Channels	Resource Hijacking
Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels	Runtime Data Manipulation
Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture		Multi-hop Proxy	Service Stop
Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture		Multiband Communication	Stored Data Manipulation
Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content			Multilayer Encryption	Transmitted Data Manipulation
DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software			Port Knocking	
Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares			Remote Access Tools	
External Remote Services	Plist Modification	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management			Remote File Copy	
File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery				Standard Application Layer Protocol	
Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery				Standard Cryptographic Protocol	
Hooking	SID-History Injection	Extra Window Memory Injection		System Service Discovery				Standard Non-Application Layer Protocol	
Hypervisor	Scheduled Task	File Deletion		System Time Discovery				Uncommonly Used Port	
Image File Execution Options Injection	Service Registry Permissions Weakness	File Permissions Modification		Virtualization/Sandbox Evasion				Web Service	
Kernel Modules and Extensions	Setuid and Setgid	File System Logical Offsets							
LC_LOAD_DYLIB Addition	Startup Items	Gatekeeper Bypass							
Launch Agent	Sudo	Hidden Files and Directories							
Launch Daemon	Sudo Caching	Hooking							
Launchctl	Valid Accounts	Image File Execution Options Injection							
LC_LOAD_DYLIB Addition	Web Shell	Indicator Blocking							
Local Job Scheduling		Indicator Removal from Tools							
Login Item		Indicator Removal on Host							
Logon Scripts		Indirect Command Execution							
Modify Existing Service		Install Root Certificate							
Netsh Helper DLL		InstallUtil							
New Service		Launchctl							
Office Application Startup		LC_LOAD_DYLIB Addition							
Path Interception		Masquerading							
Plist Modification		Modify Existing Service							
Port Knocking		Network Share Connection Removal							
Port Monitors		NTFS File Attributes							
Redundant Access		Obfuscated Files or Information							
Registry Run Keys / Startup Folder		Parent PID Spoofing							
Rundll32		Path Interception							
Scheduled Task		Plist Modification							
Screensaver		Port Knocking							
Security Support Provider		Port Monitors							
Service Registry Permissions Weakness		Process Doppelgänging							
Setuid and Setgid		Process Hollowing							
Shortcut Modification		Process Injection							
SIP and Trust Provider Hijacking		Redundant Access							
Startup Items		Regsvcs/Regasm							
System Firmware		Regsvr32							
Systemd Service		Rootkit							
Time Providers		Rundll32							
Valid Accounts		Scripting							
Web Shell		Signed Binary Proxy Execution							
Windows Management Instrumentation Event Subscription		Signed Script Proxy Execution							
Winlogon Helper DLL		SIP and Trust Provider Hijacking							
		Software Packing							
		Space after Filename							
		Template Injection							
		Timestomp							
		Trusted Developer Utilities							
		Valid Accounts							
		Web Service							
		XSL Script Processing							

Color by: Active

MITRE ATT&CK Threat Group: None

Highlight Data Source: None

Show Only Available Content: Yes

Show Only Popular Techniques: Yes

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Domain Generation Algorithms	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture		Fallback Channels	Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels	Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture		Multi-hop Proxy	Service Stop
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture		Multiband Communication	Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content			Multilayer Encryption	Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software			Port Knocking	
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares			Remote Access Tools	
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management			Remote File Copy	
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery					
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery					
	Scheduled Task	Hooking	SID-History Injection	Extra Window Memory Injection		System Service Discovery					
	Scripting	Hypervisor	Scheduled Task	File Deletion		System Time Discovery					
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Permissions Modification		Virtualization/Sandbox Evasion				Web Service	
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	File System Logical Offsets							
	Signed Script Proxy	LC_LOAD_DYLIB Addition	Startup Items	Gatekeeper Bypass							

Not so good coverage with active detections

Color by: Available

MITRE ATT&CK Threat Group: None

Highlight Data Source: None

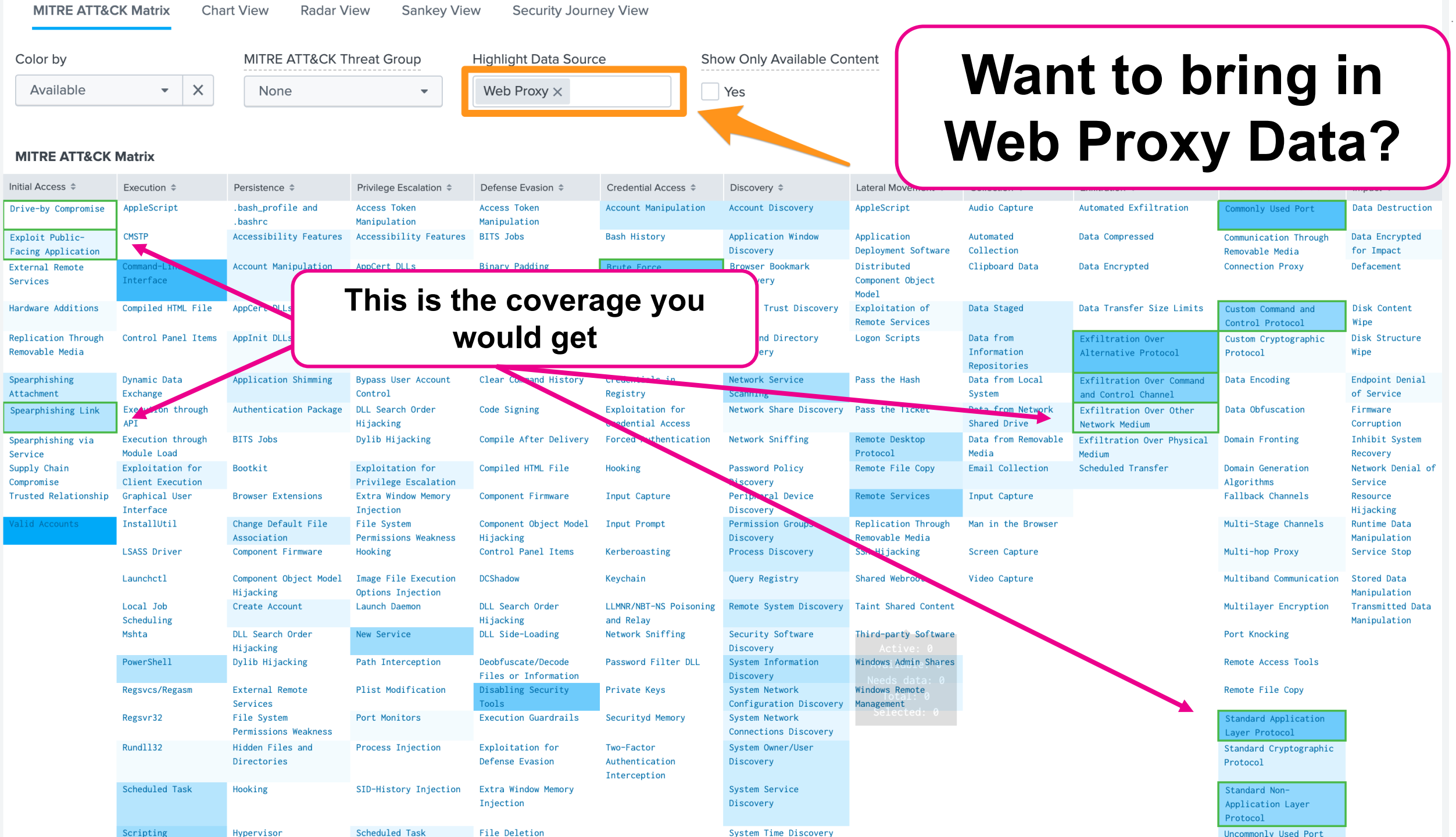
Show Only Available Content: Yes

Show Only Popular Techniques: Yes

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Domain Generation Algorithms	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture		Fallback Channels	Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels	Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture		Multi-hop Proxy	Service Stop
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture		Multiband Communication	Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content			Multilayer Encryption	Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software			Port Knocking	
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares			Remote Access Tools	
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management			Remote File Copy	
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery					
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery					
	Scheduled Task	Hooking	SID-History Injection	Extra Window Memory Injection		System Service Discovery					
	Scripting	Hypervisor	Scheduled Task	File Deletion		System Time Discovery					
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Permissions Modification		Virtualization/Sandbox Evasion					
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	File System Logical Offsets							
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Gatekeeper Bypass							

Potentially good coverage against multiple MITRE Tactics


MITRE ATT&CK Matrix
Chart View
Radar View
Sankey View
Security Journey View
Color by
Available
MITRE ATT&CK Threat Group
None
Highlight Data Source
Web Proxy
Show Only Available Content
Yes
Want to bring in Web Proxy Data?
This is the coverage you would get
MITRE ATT&CK Matrix
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts
AppleScript
CMSTP
Command-Line Interface
Compiled HTML File
Control Panel Items
Dynamic Data Exchange
Execution through API
Execution through Module Load
Exploitation for Client Execution
Graphical User Interface
InstallUtil
LSASS Driver
Launchctl
Local Job Scheduling
Mshta
PowerShell
Regsvcs/Regasm
Regsvr32
Rundll32
Scheduled Task
Scripting
.bash_profile and .bashrc
Accessibility Features
Account Manipulation
AppCert DLLs
AppInit DLLs
Application Shimming
Authentication Package
BITS Jobs
Bootkit
Browser Extensions
Change Default File Association
Component Firmware
Component Object Model Hijacking
Create Account
DLL Search Order Hijacking
Dylib Hijacking
External Remote Services
File System Permissions Weakness
Hidden Files and Directories
Hooking
Hypervisor
Access Token Manipulation
Accessibility Features
Binary Padding
Bypass User Account Control
DLL Search Order Hijacking
Dylib Hijacking
Exploitation for Privilege Escalation
Extra Window Memory Injection
File System Permissions Weakness
Hooking
Image File Execution Options Injection
Launch Daemon
New Service
Path Interception
Plist Modification
Port Monitors
Process Injection
SID-History Injection
Scheduled Task
Access Token Manipulation
BITS Jobs
Binary Padding
Clear Command History
Code Signing
Compile After Delivery
Compiled HTML File
Component Firmware
Component Object Model Hijacking
Control Panel Items
DCShadow
DLL Search Order Hijacking
DLL Side-Loading
Deobfuscate/Decode Files or Information
Disabling Security Tools
Execution Guardrails
Exploitation for Defense Evasion
Extra Window Memory Injection
File Deletion
Account Manipulation
Bash History
Brute Force
Credentials in Registry
Exploitation for Credential Access
Forced Authentication
Hooking
Input Capture
Input Prompt
Kerberoasting
Keychain
LLMNR/NBT-NS Poisoning and Relay
Network Sniffing
Password Filter DLL
Private Keys
Securityd Memory
Two-Factor Authentication Interception
Account Discovery
Application Window Discovery
Browser Bookmark Discovery
Domain Trust Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
AppleScript
Application Deployment Software
Distributed Component Object Model
Exploitation of Remote Services
Logon Scripts
Pass the Hash
Pass the Ticket
Remote Desktop Protocol
Remote File Copy
Remote Services
Replication Through Removable Media
Shared Webroot
Taint Shared Content
Third-party Software
Windows Admin Shares
Windows Remote Management
Audio Capture
Automated Collection
Clipboard Data
Data Staged
Data from Information Repositories
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Email Collection
Input Capture
Man in the Browser
Screen Capture
Video Capture
Automated Exfiltration
Data Compressed
Data Encrypted
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Command and Control Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Scheduled Transfer
Commonly Used Port
Communication Through Removable Media
Connection Proxy
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Data Obfuscation
Domain Fronting
Domain Generation Algorithms
Fallback Channels
Multi-Stage Channels
Multi-hop Proxy
Multiband Communication
Multilayer Encryption
Port Knocking
Remote Access Tools
Remote File Copy
Standard Application Layer Protocol
Standard Cryptographic Protocol
Standard Non-Application Layer Protocol
Uncommonly Used Port
Data Destruction
Data Encrypted for Impact
Defacement
Disk Content Wipe
Disk Structure Wipe
Endpoint Denial of Service
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Resource Hijacking
Runtime Data Manipulation
Service Stop
Stored Data Manipulation
Transmitted Data Manipulation
Active: 0
Needs data: 0
Total: 0
Selected: 0

© 2019 SPLUNK INC.



Color by

Available

MITRE ATT&CK Threat Group

None

viol

Violent Memmes

Highlight Data Source

None ×

Show Only Available Content

Yes

Show Only Popular Techniques

Yes

MITRE ATT&CK Matrix

Initial Access	Execution	Pe	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Domain Generation Algorithms	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture		Fallback Channels	Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels	Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture		Multi-hop Proxy	Service Stop
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture		Multiband Communication	Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content			Multilayer Encryption	Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software			Port Knocking	
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares			Remote Access Tools	
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management			Remote File Copy	
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery				Standard Application Layer Protocol	
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery				Standard Cryptographic Protocol	
	Scheduled Task	Hooking	SID-History Injection	Extra Window Memory Injection		System Service Discovery				Standard Non-Application Layer Protocol	
	Scripting	Hypervisor	Scheduled Task	File Deletion		System Time Discovery				Uncommonly Used Port	
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Permissions Modification		Virtualization/Sandbox Evasion				Web Service	
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	File System Logical Offsets							
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Gatekeeper Bypass							

Color by: Available

MITRE ATT&CK Threat Group: Violent Memmes

Highlight Data Source: None

Show Only Available Content: Yes

Show Only Popular Techniques: Yes

MITRE ATT&CK Matrix

Techniques known to be used by Violent Memmes

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation					Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs					Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs				Discovery	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Domain Generation Algorithms	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture		Fallback Channels	Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels	Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture		Multi-hop Proxy	Service Stop
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture		Multiband Communication	Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content			Multilayer Encryption	Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software			Port Knocking	
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares			Remote Access Tools	
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management			Remote File Copy	
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery				Standard Application Layer Protocol	
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery				Standard Cryptographic Protocol	
	Scheduled Task	Hooking	SID-History Injection	Extra Window Memory Injection		System Service Discovery				Standard Non-Application Layer Protocol	
	Scripting	Hypervisor	Scheduled Task	File Deletion		System Time Discovery				Uncommonly Used Port	
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Permissions Modification		Virtualization/Sandbox Evasion				Web Service	
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	File System Logical Offsets							
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Gatekeeper Bypass							

Color by: Available

MITRE ATT&CK Threat Group: Violent Memmes

Highlight Data Source: None

Show Only Available Content: Yes

Show Only Popular Techniques: Yes

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Domain Generation Algorithms	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture		Fallback Channels	Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels	Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture		Multi-hop Proxy	Service Stop
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	Shared Webroot	Video Capture		Multiband Communication	Stored Data Manipulation
	Local Job Scheduling	Create Account	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content			Multilayer Encryption	Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	DLL Side-Loading	Network Sniffing	Security Software Discovery	Third-party Software			Port Knocking	
	PowerShell	Dylib Hijacking	Path Interception	Deobfuscate/Decode Files or Information	Password Filter DLL	System Information Discovery	Windows Admin Shares			Remote Access Tools	
	Regsvcs/Regasm	External Remote Services	Plist Modification	Disabling Security Tools	Private Keys	System Network Configuration Discovery	Windows Remote Management			Remote File Copy	
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Disc				Standard Application Layer Protocol	
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery				Standard Cryptographic Protocol	
	Scheduled Task	Hooking	SID-History Injection	Extra Window Memory Injection		System Service Discovery				Standard Non-Application Layer Protocol	
	Scripting	Hypervisor	Scheduled Task	File Deletion		System Time Discovery				Uncommonly Used Port	
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	File Permissions Modification		Virtualization/Sandbox Evasion				Web Service	
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	File System Logical Offsets							
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Gatekeeper Bypass							

Active: 0
Available: 6
Needs data: 6
Total: 12
Selected: 0
Threat Groups:
Violent Memmes

Scroll Down

© 2019 SPLUNK INC

Content selection

Status: Any

Originating app: Any

MITRE ATT&CK Tactic: Initial Access

MITRE ATT&CK Technique: Spearphishing Link

MITRE ATT&CK Threat Group: Violent Memmes

Data Source: Any

Data Source Category: Any

Bookmark Status: Any

Featured: Any

Search Filter:

2. Selected Content

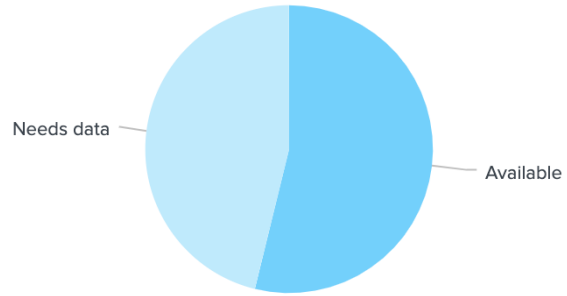
Use the drop downs or tables to further filter your selection.

Selection | Content list | Selection by Data Source | Selection by Data Source Category | Selection by MITRE ATT&CK Tactic | Selection by MITRE ATT&CK Technique | Selection by MITRE Threat Group

Total Selected

12

Selection by Status



3. View Content

Click the button below to drill down in to the content.

Drill down to content selection

Security Content

What's New In 3.0? | Manage Bookmarks | Export | ...

INC.

How can you map this content to Splunk's Security Journey, and make your environment more secure?

Filter

Search

Learn how to use this page

Customize Filters | **458** Total | **12** Filtered | Clear | Default | Share

Journey	Security Use Case	Category	Data Sources	Featured	ATT&CK Technique
All selected (6)	All	All	All	All	Spearphishing Link (12 ma...

ATT&CK Tactic	MITRE Threat Groups	Originating App	Data Source Category	Content Enabled	Data Availability
Initial Access (12 matches) ...	Violent Memmes (12 matc...	All	All	All	All

Stage 1: Collection

You have the data onboard, what do you do first?

Basic Malware Outbreak

Looks for the same malware occurring on multiple systems in a short period of time.

Featured
Searches Included
Initial Access | Execution
Privilege Escalation

Endpoint Uncleaned Malware Detection

Detect a system with a malware detection that was not properly cleaned, as they carry a high risk of damage or disclosure of data.

Featured
Searches Included
Execution | Initial Access
User Execution

Multiple Infections on Host

Finds hosts that have logged multiple different infections in a short period of time.

Featured
Searches Included
Initial Access | Execution
Drive-by Compromise

Recurring Infection on Host

Looks for the same malware occurring multiple times on the same host.

Featured
Searches Included
Initial Access | Execution
Drive-by Compromise

Content list pre-filtered to your selection

Scroll Down

Stage 2: Normalization

You've applied Common Information Model, opening you to detections shared from others, and premium apps.

Host With Multiple Infections

Alerts when a host with multiple infections is discovered.

INC.

Emails with Lookalike Domains

Emailing from a domain name that is similar to your own is a common phishing technique, such as splunk.com receiving an email from spiunk.com. This search will detect those similar domains.

Featured

Searches Included

Initial Access

High Or Critical Priority Host With Malware Detected

Alerts when an infection is noted on a host with high or critical priority.

Featured

Initial Access | Execution

Drive-by Compromise

Spearphishing Attachment

Host Sending Excessive Email

Alerts when an host not designated as an e-mail server sends excessive e-mail to one or more target hosts.

Initial Access

Spearphishing Attachment

Spearphishing Link

Possible Phishing Attempt

Triggered by external email monitoring tools when a specific user or group is a possible target of a spear phishing campaign.

Initial Access

Spearphishing Attachment

Spearphishing Link

Stage 5: Automation and Orchestration

You are monitoring your SOC with Splunk.

Stage 6: Advanced Detection

You have the highest level of detection!

Suspicious Domain Name

Triggered when a user visits a suspicious domain name that appears to be algorithmically generated.

Adversary OPSEC | Initial Access

Command and Control

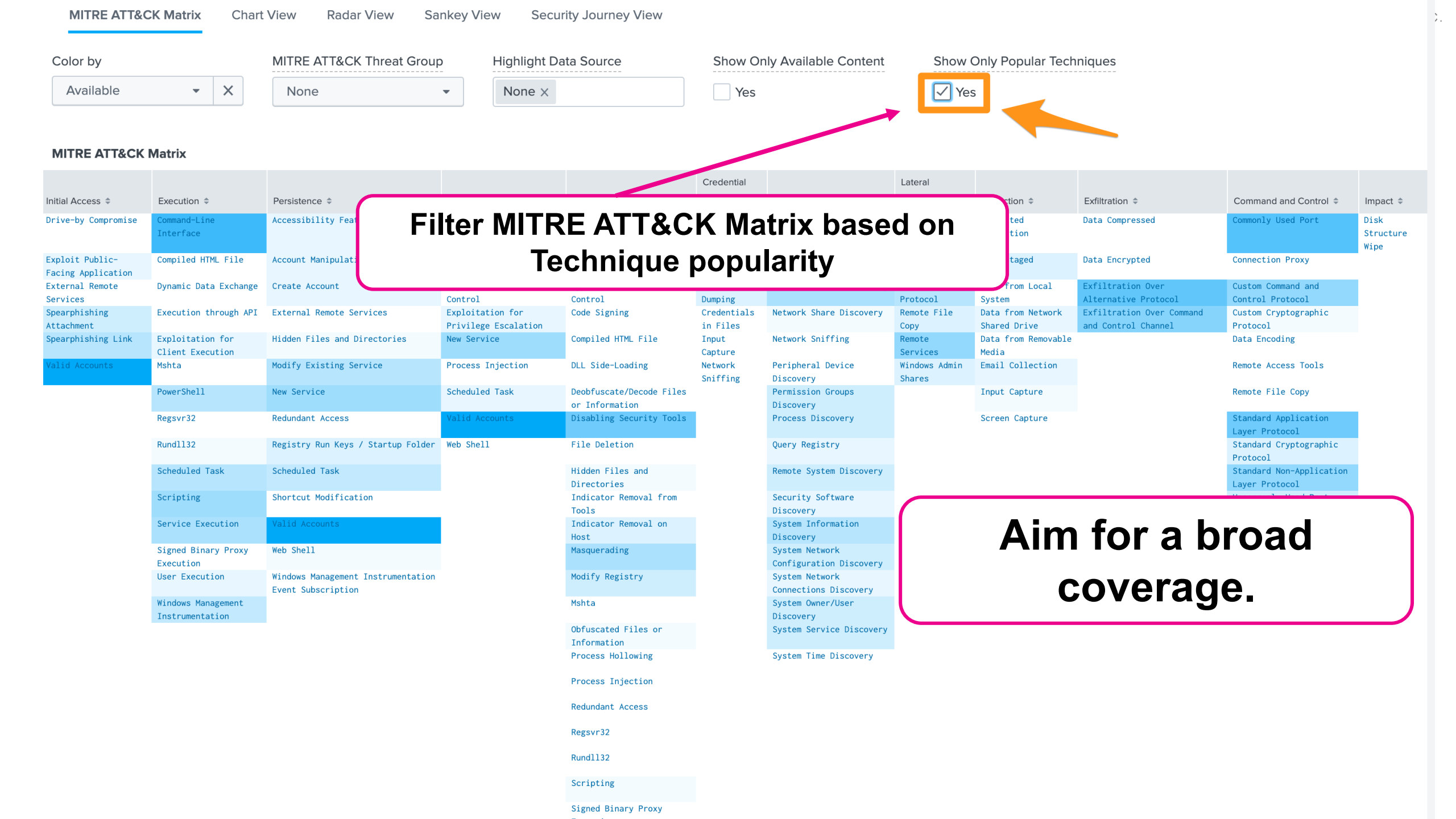
Domain Generation Algorithms (DGA)

Bookmark selection for tracking

Bookmark All | Remove All Bookmarks

Don’t get Tunnel Vision




MITRE ATT&CK Matrix
Chart View
Radar View
Sankey View
Security Journey View
Color by
Available
MITRE ATT&CK Threat Group
None
Highlight Data Source
None
Show Only Available Content
Yes
Show Only Popular Techniques
Yes
MITRE ATT&CK Matrix
Filter MITRE ATT&CK Matrix based on Technique popularity
Aim for a broad coverage.

© 2019 SPLUNK INC.

Learn Splunk for Security



.conf19

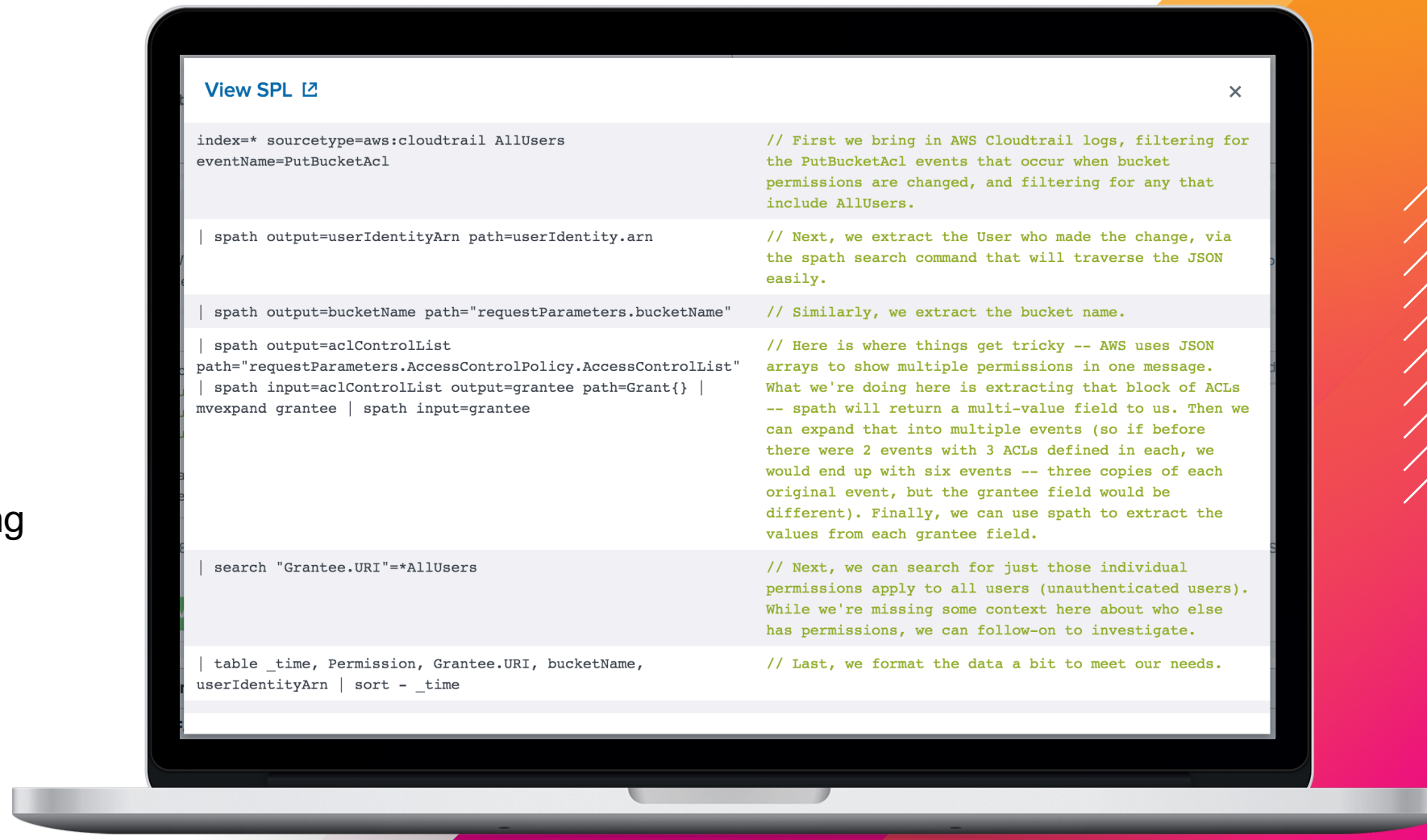
splunk>

Extensive Docs

Focused To Your Needs

SSE contains Data Onboarding docs, SPL docs, Security Context, and App docs

Wherever you are in your journey, SSE will help



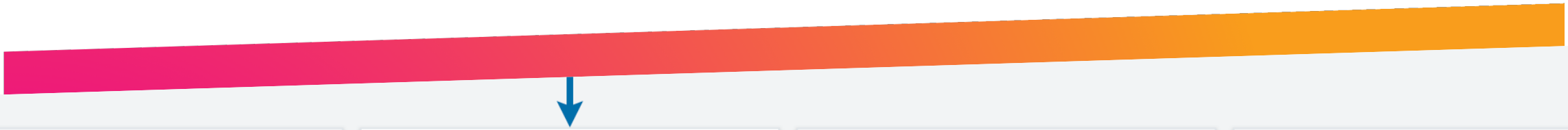
splunk> turn data into doing

© 2019 SPLUNK INC.

© 2019 SPLUNK INC.

Content Guides to Useful Docs

Whether you're new to Splunk or new to security, be guided to the right content



Learn Splunk | **Learn Security** | Security Journey | Data Onboarding Guides

Learn Security

If you're new to security itself, it can be difficult to even understand the content recommendations made. This guide points you to content that has the best written explanations and documentation, targeted specifically at folks just getting started.

Launch Feature

	Launch: Security Contents Page	Launch w/ tour	The Security Contents Page is the main landing page for Splunk Security Essentials, providing a complete list of content and the ability to drill-down into any individual item. It's the kicking off point for

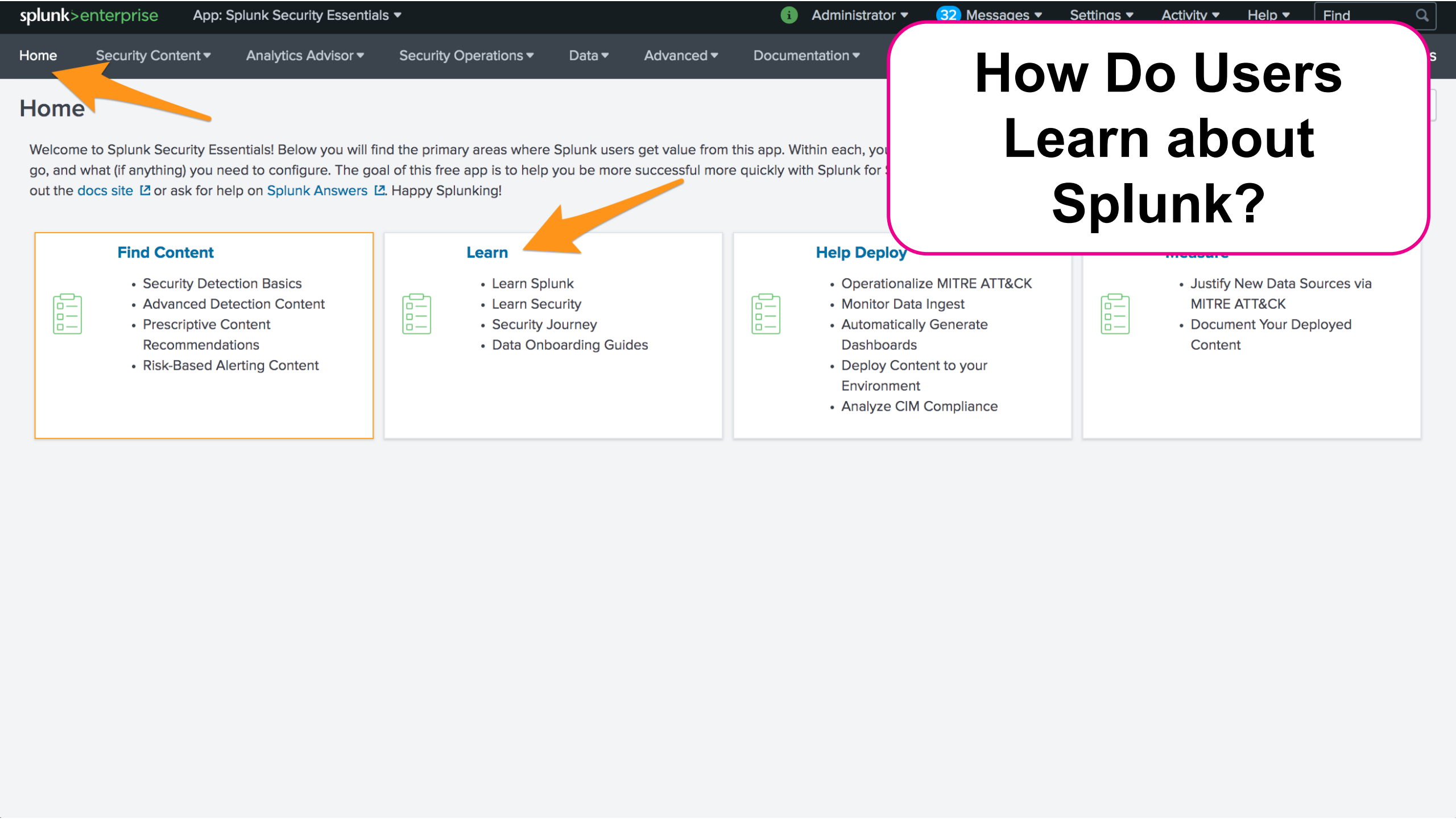
© 2019 SPLUNK INC.

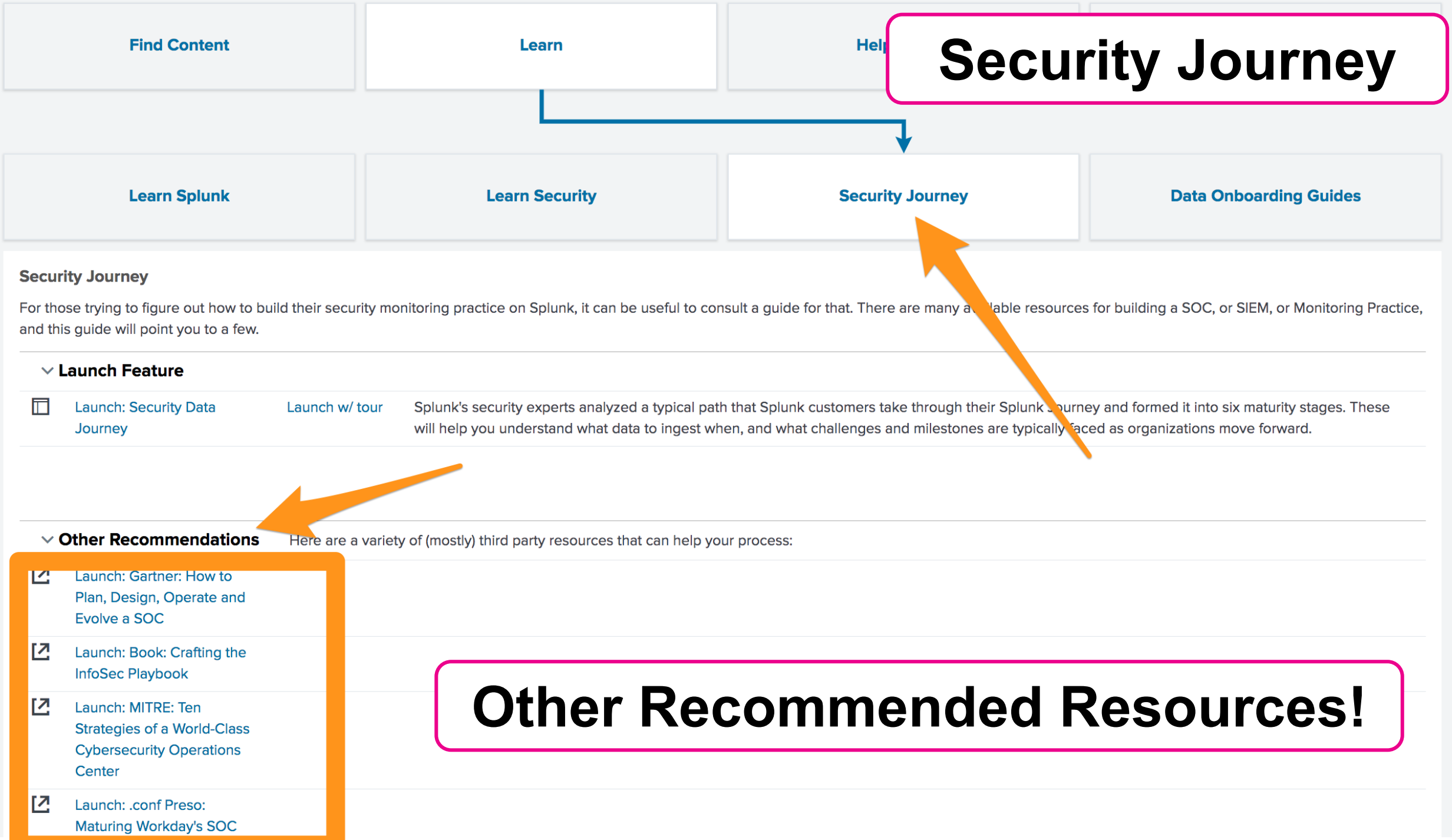
Hands-On



.conf19

splunk>


splunk>enterprise
App: Splunk Security Essentials
Administrator
32 Messages
Settings
Activity
Help
Find
Home
Security Content
Analytics Advisor
Security Operations
Data
Advanced
Documentation
How Do Users Learn about Splunk?
Home
Welcome to Splunk Security Essentials! Below you will find the primary areas where Splunk users get value from this app. Within each, you
go, and what (if anything) you need to configure. The goal of this free app is to help you be more successful more quickly with Splunk for
out the docs site or ask for help on Splunk Answers. Happy Splunking!
Find Content
Security Detection Basics
Advanced Detection Content
Prescriptive Content Recommendations
Risk-Based Alerting Content
Learn
Learn Splunk
Learn Security
Security Journey
Data Onboarding Guides
Help Deploy
Operationalize MITRE ATT&CK
Monitor Data Ingest
Automatically Generate Dashboards
Deploy Content to your Environment
Analyze CIM Compliance
Justify New Data Sources via MITRE ATT&CK
Document Your Deployed Content


Find Content
Learn
Help
Security Journey
Learn Splunk
Learn Security
Security Journey
Data Onboarding Guides
Security Journey
For those trying to figure out how to build their security monitoring practice on Splunk, it can be useful to consult a guide for that. There are many available resources for building a SOC, or SIEM, or Monitoring Practice, and this guide will point you to a few.
Launch Feature
Launch: Security Data Journey
Launch w/ tour
Splunk's security experts analyzed a typical path that Splunk customers take through their Splunk journey and formed it into six maturity stages. These will help you understand what data to ingest when, and what challenges and milestones are typically faced as organizations move forward.
Other Recommendations
Here are a variety of (mostly) third party resources that can help your process:
Launch: Gartner: How to Plan, Design, Operate and Evolve a SOC
Launch: Book: Crafting the InfoSec Playbook
Launch: MITRE: Ten Strategies of a World-Class Cybersecurity Operations Center
Launch: .conf Preso: Maturing Workday's SOC
Other Recommended Resources!

© 2019 SPLUNK INC.

Security Journey

DESCRIPTION

Find anomalous behavior and unknown threats by applying machine learning, data science and advanced statistics to analyze the users, endpoint devices, and applications in your environment.

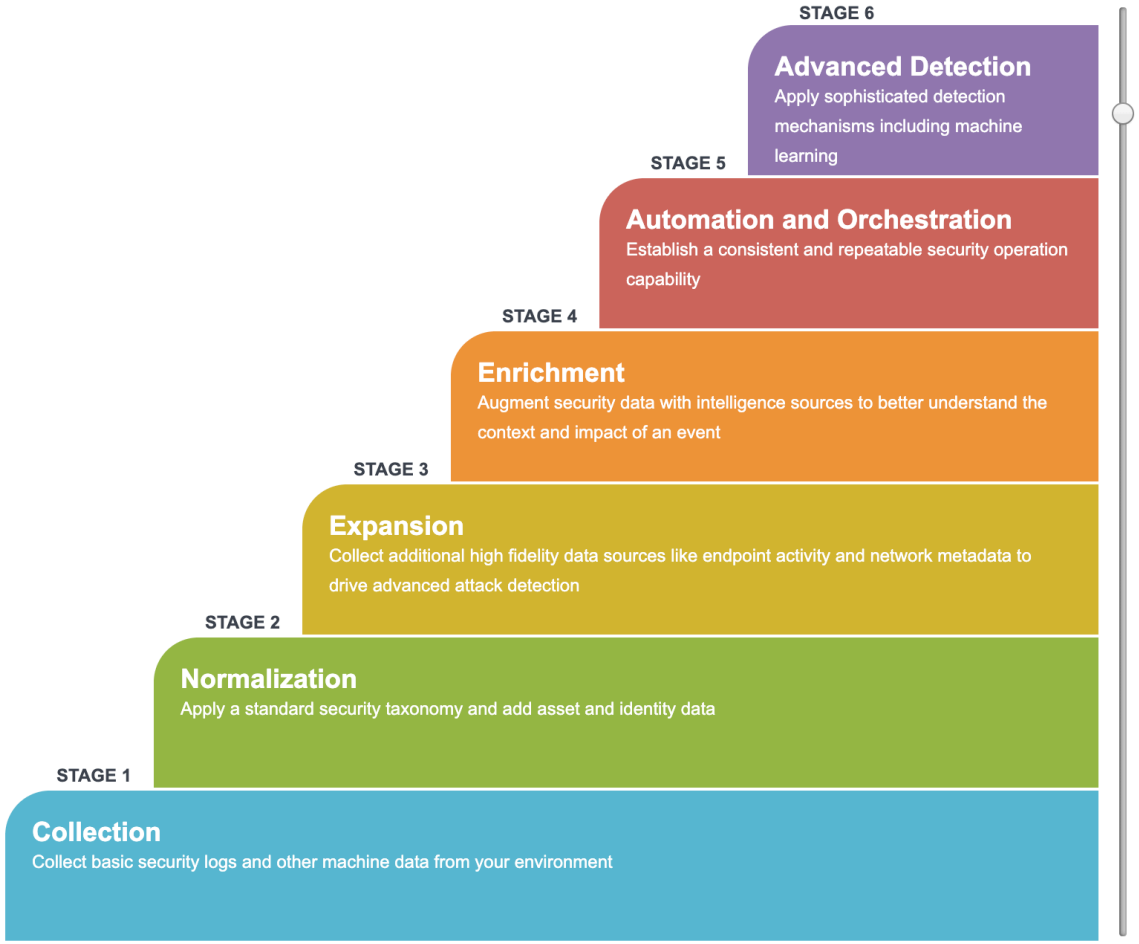
MILESTONES

At this stage, you have given yourself a fighting chance to detect adversaries and insiders even when they leave only subtle traces of their activity.

- You are employing the most advanced techniques available to identify unknown threats.
- You are employing new detection mechanisms as they become available, leveraging your team's expertise and leveraging outside research organizations.

CHALLENGES

- At this stage, you will be challenged to constantly improve your security organization.
- To gain new capabilities, your team will likely be required to perform new research.
- Although you are at the top of your game, there are no guarantees and the most advanced adversaries may still successfully attack your organization.



SELECTED STAGE 6

SECURITY USE CASE APPLICABILITY

- Security Monitoring
- Compliance
- Incident Investigation & Forensics
- Incident Response
- SOC Automation
- Advanced Threat Detection
- Insider Threat

DATA SOURCES

This stage focuses more on what you do with the data you have vs. onboarding new sources.

splunk> .conf19

Welcome to Splunk Security Essentials! Below you will find the primary areas where Splunk users get value from this app. Within each, you
go, and what (if anything) you need to configure. The goal of this free app is to help you be more successful more quickly with Splunk for
out the docs site or ask for help on Splunk Answers. Happy Splunking!

Data Onboarding Guides

Find Content | Learn | Help

Learn Splunk | Learn Security | Security Journey | Data Onboarding Guides

Data Onboarding Guides

Getting data in can be tricky, and there are lots of ways to do it. This app contains documentation created in late 2017 for several of the products most popular with Splunk users that show not just how to ingest the data, but how to configure the products to generate the right kind of data.

Launch Feature

Launch: Data Source Onboarding Guides	Launch w/ tour	Nine data source onboarding guides that are simple enough to use, but also blessed by Splunk's professional services. These will tell you not only how to ingest data into Splunk, but also how to configure the systems in order to send the right data in the first place!

Welcome to Splunk Security Essentials! Below you will find the primary areas where Splunk users get value from this app. Within each, you will see a guide showing you where to go, and what (if anything) you need to configure. The goal of this free app is to help you be more successful more quickly with Splunk for Security. If you run into any issues, check out the docs site or ask for help on Splunk Answers. Happy Splunking!

Demo Mode

Find Content | **Learn** | **Help Deploy** | **Measure**

Learn Splunk | **Learn Security** | **Security Journey** | **Data Onboarding Guides**

Data Onboarding Guides

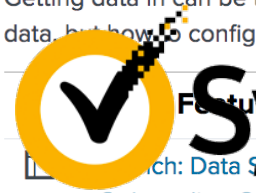
Getting data in can be tricky, and there are lots of ways to do it. This app contains documentation created in late 2017 for several of the products most popular[illegible]n Splunk users that show not just t[illegible] data, but how to configure the products to generate the right kind of data.

Feature

[illegible]ch: Data Source Onboarding Guides

Launch w/ tour

Nine data source onboarding guides that are simple enough to use, but also blessed by Splunk's professional ser[illegible] you not only how to ingest data into Splunk, but also how to configure the systems in order to send the right data in the first place!








Learn Security

Home

Welcome to Splunk Security Essentials! Below you will find the primary areas where Splunk users get value from this app. Within each, you will see a guide showing you where to go, and what (if anything) you need to configure. The goal of this free app is to help you be more successful more quickly with Splunk for Security. If you run into any issues, check out the docs site or ask for help on Splunk Answers. Happy Splunking!

Demo Mode

Find Content | **Learn** | **Help Deploy** | **Measure**

Learn Splunk | **Learn Security** | **Security Journey** | **Data Onboarding Guides**

Learn Security

If you're new to security itself, it can be difficult to even understand the content recommendations m[illegible]e. This guide points you to content that has the best written explanations and documentation, targeted specifically at folks just getting started.

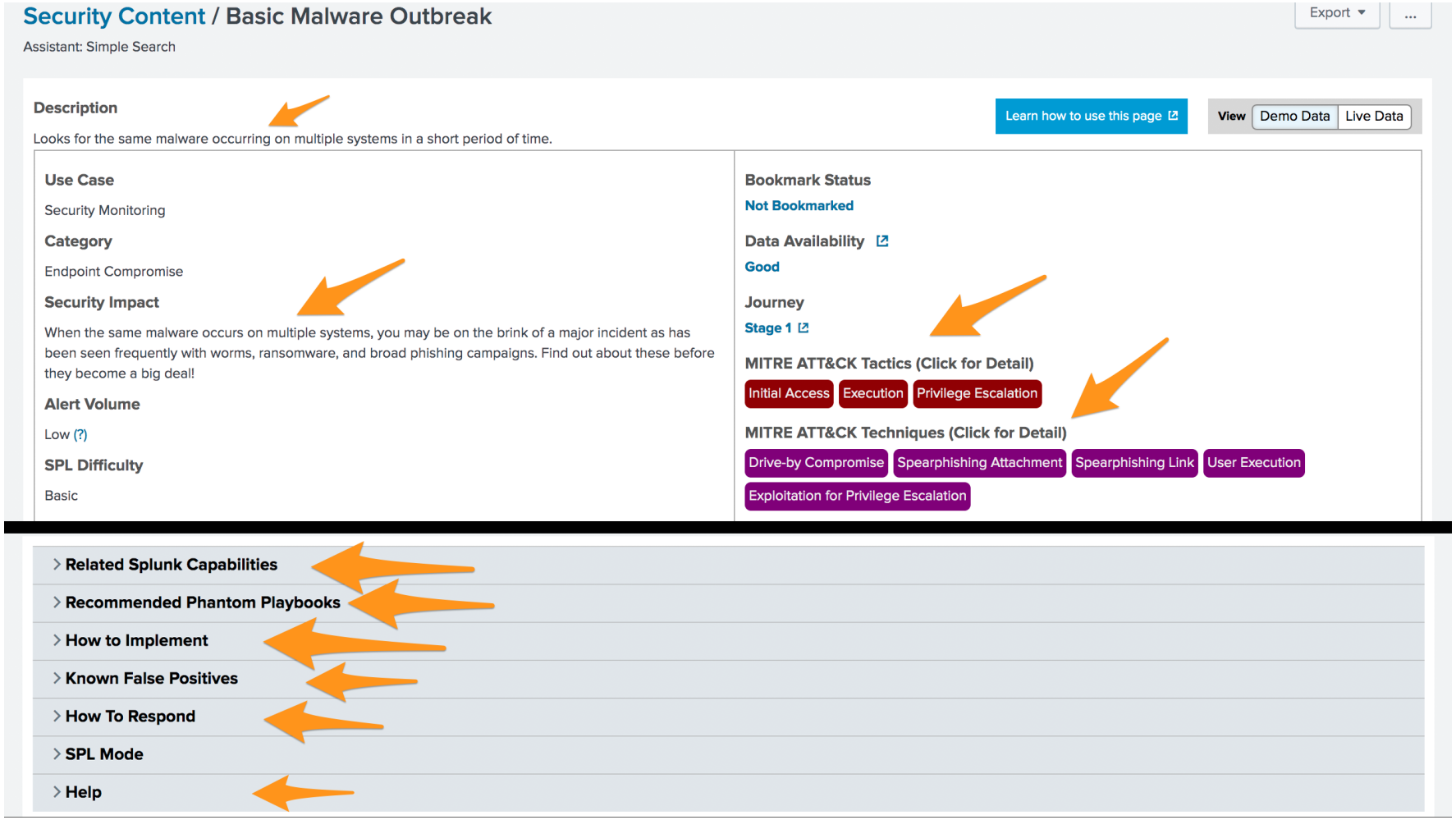
Launch Feature

Launch: Security Contents Page	Launch w/ tour	The Security Contents Page is the main landing page for Splunk Security Essentials, providing a complete list of content and the ability to drill-down into any individual item. It's the kicking off point for viewing all content in the app, and has a wealth of filters to help you hone in on exactly what you want.

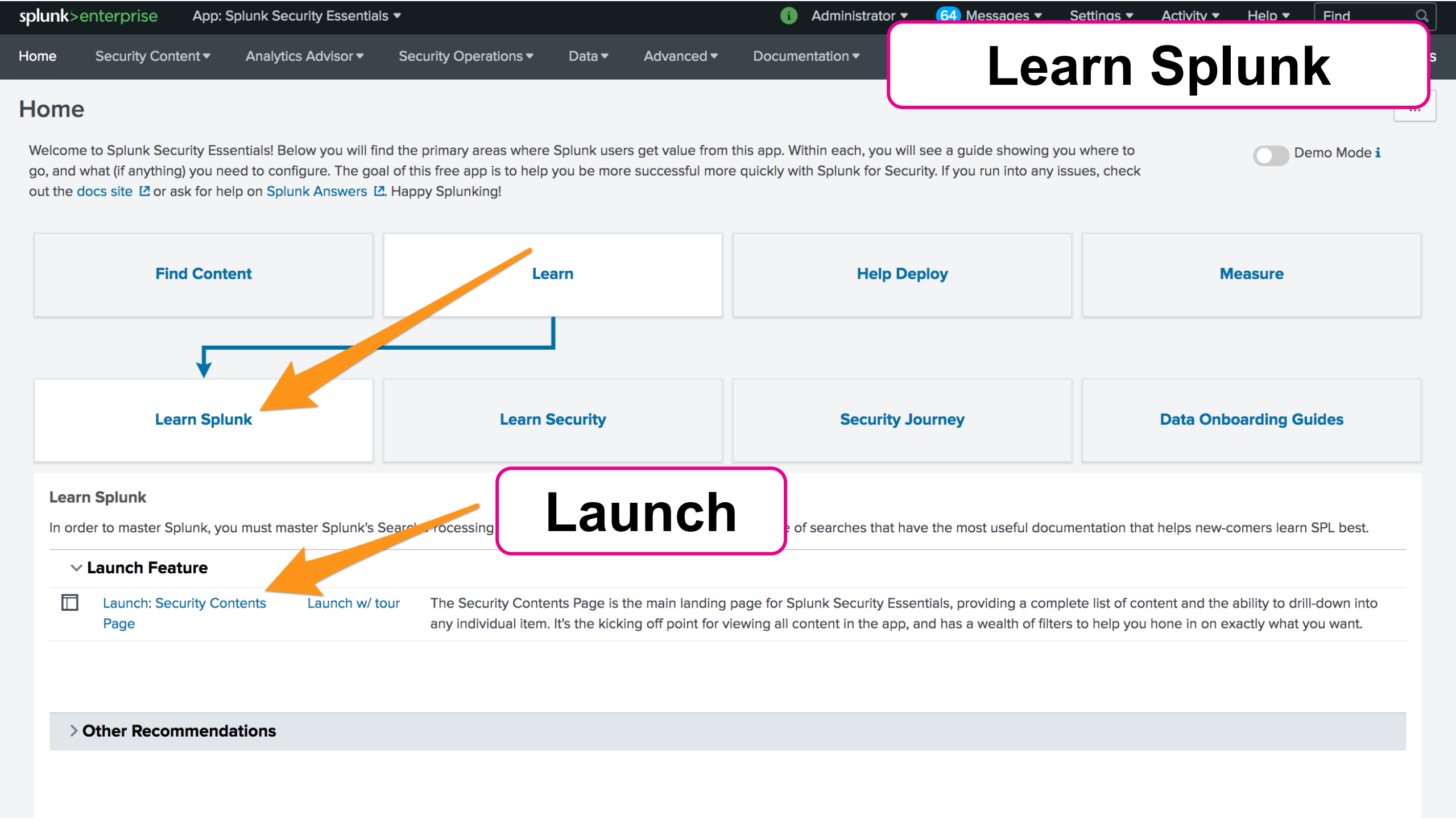
Other Recommendations

© 2019 SPLUNK INC.

Security Concepts Applied Through Detections



splunk> .conf19


splunk>enterprise
App: Splunk Security Essentials
Administrator
64 Messages
Settings
Activity
Help
Find
Home
Security Content
Analytics Advisor
Security Operations
Data
Advanced
Documentation
Learn Splunk
Home
Welcome to Splunk Security Essentials! Below you will find the primary areas where Splunk users get value from this app. Within each, you will see a guide showing you where to go, and what (if anything) you need to configure. The goal of this free app is to help you be more successful more quickly with Splunk for Security. If you run into any issues, check out the docs site or ask for help on Splunk Answers. Happy Splunking!
Demo Mode
Find Content
Learn
Help Deploy
Measure
Learn Splunk
Learn Security
Security Journey
Data Onboarding Guides
Launch
Learn Splunk
In order to master Splunk, you must master Splunk's Search Processing
of searches that have the most useful documentation that helps new-comers learn SPL best.
Launch Feature
Launch: Security Contents Page
Launch w/ tour
The Security Contents Page is the main landing page for Splunk Security Essentials, providing a complete list of content and the ability to drill-down into any individual item. It's the kicking off point for viewing all content in the app, and has a wealth of filters to help you hone in on exactly what you want.
Other Recommendations

splunk>enterprise App: Splunk Security Essentials ▾ Administrator ▾ 80 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Home | Security Content ▾ | Analytics Advisor ▾ | Security Operations ▾ | Data ▾ | Advanced ▾ | Documentation ▾

Learn Splunk

Security Content

How can you map this content to Splunk's Security Journey, and make your environment more secure?

Filter | Search | Learn how to use this page | Customize Filters | 458 Total | 10 Filtered | Clear | Default | Share

Journey: All sel

Data Sources: All

Featured: All

Advance: None

Detections with good SPL docs

Stage 1: Collection

You have the data onboard, what do you do first?

Hosts Where Security Sources Go Quiet

A frequent concern of SOCs is that their data feeds will disappear. This search will look on a host-by-host basis for when your security sources stop reporting home.

Searches Included

Sources Sending Many DNS Requests

A common method for Data Exfiltration is to send out many DNS or Ping requests, embedding data into the payload. This is often not logged.

Searches Included

Scroll Down



Emails with Lookalike Domains

Emailing from a domain name that is similar to your own is a common phishing technique, such as splunk.com receiving an email from spiunk.com. This search will detect those similar domains.

Featured

Searches Included

Pull I... User...

To focus detection or response on privileged users, you must first build a list of accounts that have elevated rights or access to privileged information.

Featured

Searches Included

U... C... D...

Find use... analyze... across ... analyzin... compan...

Feature...

Searche...

Emails with Lookalike Domains

Emails with Lookalike Domains

Security Content / Emails with Lookalike Domains

Assistant: Simple Search

Description

Emailing from a domain name that is similar to your own is a common phishing technique, such as splunk.com receiving an email from spiunk.com. This search will detect those similar domains.

Learn how to use this page

View: Demo Data | Live Data | Accelerated Data

Use Case

Advanced Threat Detection

Category

Endpoint Compromise, SaaS

Alert Volume

Very Low (?)

SPL Difficulty

Advanced

Scroll Down



Bookmark Status

Not Bookmarked

Data Availability

Good

Journey

Stage 4

MITRE ATT&CK Tactics (Click for Detail)

Initial Access

MITRE ATT&CK Techniques (Click for Detail)

Spearphishing Link

MITRE Threat Groups (Click for Detail)

APT28 APT29 APT32 APT33 APT39 Cobalt Group Dragonfly 2.0 Elderwood FIN4 FIN8 Leviathan Magic Hound Night Dragon OilRig Patchwork Stolen Pencil TA505 Turla Violent Memmes

Kill Chain Phases

Delivery

Data Check	Status	Open in Search	Resolution (if needed)
Must have Demo Lookup	✓	Open in Search	Verify that lookups installed with Splunk Security Essentials is present
Must have URL Toolbox Installed (provides Levenshtein lookalike detection and domain parsing)	✓	Open in Search	The URL Toolbox app, writte… t also Levenshtein similarity checking (e.g., t… ownload here.

Schedule in ES

Enter a search

```
| `Load_Sample_Log_Data("Email Logs")`
| stats count by Sender
| rex field=Sender "\@(?<domain_detected>.*)"
| stats sum(count) as count by domain_detected
| eval domain_detected=mvfilter(domain_detected!="mycompany.com" AND domain_detected!="company.com" AND d…tected!="mycompan…estheenvironment.com")
| eval list="mozilla" | `ut_parse_extended(domain_detected, list)`
| foreach ut_subdomain_level* [eval orig_domain=domain_detected, domain_detected=mvappend(domain_detected, '<<FIELD>>' . "."
| fields orig_domain domain_detected ut_domain count
| eval word1=mvappend(domain_detected, ut_domain), word2 = mvappend("mycompany.com", "comp…panylove
| lookup ut_levenshtein_lookup word1 word2 | eval ut_levenshtein= min(ut_levenshtein)
| where ut_levenshtein < 3
| fields - domain_detected ut_domain | rename orig_domain as top_level_domain_in_incoming_e…any_domains_used count as
    num_occurrences ut_levenshtein as Levenshtein_Similarity_Score
```

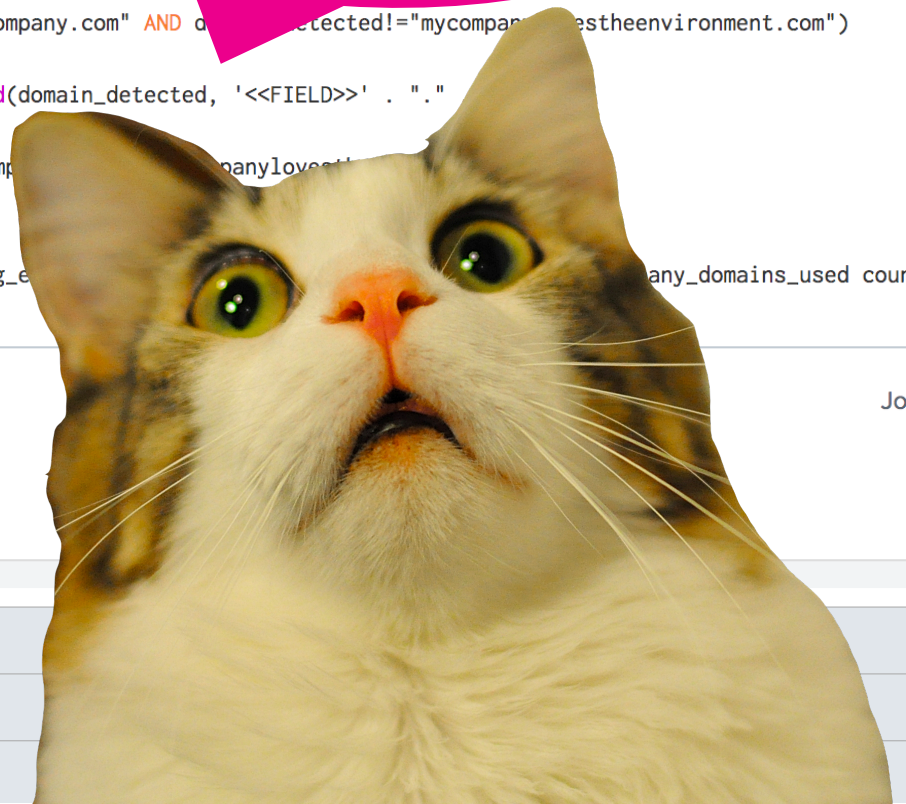
All time

✓ 3 results (1/1/70 12:00:00.000 AM to 10/17/19 3:36:51.000 AM)

Job ▾ ⏸ ■ Smart Mode ▾

Detect New Values | Line-by-Line SPL Documentation

THAT'S A LOT OF SPL!



> **Recommended Phantom Playbooks**

> **How to Implement**

> **Known False Positives**

Data Check	Status	Open in Search	Resolution (if needed)
Must have Demo Lookup	✓	Open in Search	Verify that lookups installed with Splunk Security Essentia
Must have URL Toolbox Installed (provides Levenshtein lookalike detection and domain parsing)	✓	Open in Search	The URL Toolbox app, written by Cedric Le Roux, not only p similarity checking (e.g., typo detection) and Shannon entropy detection (random characters). Download here.

Line-by-Line SPL Documentation

Enter a search

```
| `Load_Sample_Log_Data("Email Logs")`
| stats count by Sender
| rex field=Sender "\@(?<domain_detected>.*)"
| stats sum(count) as count by domain_detected
| eval domain_detected=mvfilter(domain_detected!="mycompany.com" AND domain_detected!="company.com" AND domain_detected!="mycompanylovestheenvironment.com")
| eval list="mozilla" | `ut_parse_extended(domain_detected, list)`
| foreach ut_subdomain_level* [eval orig_domain=domain_detected, domain_detected=mvappend(domain_detected, '<<FIELD>>' . "." . ut_tld)]
| fields orig_domain domain_detected ut_domain count
| eval word1=mvappend(domain_detected, ut_domain), word2 = mvappend("mycompany.com", "company.com", "mycompanylovestheenvironment.com")
| lookup ut_levenshtein_lookup word1 word2 | eval ut_levenshtein= min(ut_levenshtein)
| where ut_levenshtein < 3
| fields - domain_detected ut_domain | rename orig_domain as top_level_domain_in_incoming_email word1 as domain_names_analyzed word2 as company_domains_used count as
    num_occurrences ut_levenshtein as Levenshtein_Similarity_Score
```

All time

✓ 3 results (1/1/70 12:00:00.000 AM to 10/17/19 3:36:51.000 AM)

Job | Smart Mode

Detect New Values | Line-by-Line SPL Documentation



> **Recommended Phantom Playbooks**

> **How to Implement**

> **Known False Positives**

Line-by-Line SPL Documentation

View SPL

`| `Load_Sample_Log_Data("Email Logs")``	`// First we start source address (t`
`| stats count by Sender`	`// This is an inte per source address, so we don't end up running over the same email many times`
`| rex field=Sender "\@(?<domain_detected>.*)"`	`// Next we are going to extract the domain -- probably this should actually occur before the last stats, but the performance is similar and this way it matches the accelerated search where this step is required.`
`| stats sum(count) as count by domain_detected`	`// Now we aggregate per actual domain we will analyze, for performance reasons`
`| eval domain_detected=mvfilter(domain_detected!="mycompany.com" AND domain_detected!="company.com" AND domain_detected!="mycompanylovestheenvironment.com")`	`// Let's filter out any domains that our organization owns and expects to receive email from. You can have several domains here (I recommend no more than 10-20 -- eventually urltoolbox will get tired and stop doing adding Levenshtein fields, so you can look for null ut_levenshtein later if you are pushing this boundary).`
`| eval list="mozilla" | `ut_parse_extended(domain_detected, list)``	`// Now we use the free URL Toolbox app to parse out subdomains from the top level domains. We want to analyze each one, so that an attacker can't send mycompany.yourithelpdesk.com and get through, or mail.mycampany.com.`
`| foreach ut_subdomain_level* [eval orig_domain=domain_detected, domain_detected=mvappend(domain_detected, '<<FIELD>>' . "." . ut_tld)]`	`// The field we are going to pass to the Levenshtein algorithm is domain_detected, so let's add each subdomain to the multi-value field domain_detected.`
`| fields orig_domain domain_detected ut_domain_count`	`// This step is not required, but I like to filter down the list`

Data Check | Status | Open in | Resolution (if needed)

Must have Demo

Must have URL T
Levenshtein look
parsing)

Enter a search

```
| `Load_Sample_
| stats count b
| rex field=Ser
| stats sum(cou
| eval domain_d
| eval list="mc
| foreach ut_su
| fields orig_d
| eval word1=mv
| lookup ut_lev
| where ut_leve
| fields - doma
    num_occurre
```

✓ 3 results (1/1/70

Smart Mode

Detect New Val

> Recommer

> How to Implement

> Known False Positives

View SPL

Ahh, now I get it



SPL	Comment
`| `Load_Sample_Lo`	// First we start by pulling our dem source address (this could also work
| stats count	// This is an intensive exercise, so l urce address, so we don't end up
| rex field=Send	// Next we are going to extract the domain should actually occur before the last stats, b is similar and this way it matches the accelerate this step is required.
| stats sum(count) as count by domain_detected	// Now we aggregate per actual domain we will analyze, for performance reasons
| eval domain_detected=mvfilter(domain_detected!="mycompany.com" AND domain_detected!="company.com" AND domain_detected!="mycompanylovestheenvironment.com")	// Let's filter out any domains that our organization owns and expects to receive email from. You can have several domains here (I recommend no more than 10-20 -- eventually urltoolbox will get tired and stop doing adding Levenshtein fields, so you can look for null ut_levenshtein later if you are pushing this boundary).
| eval list="mozilla" | `ut_parse_extended(domain_detected, list)`	// Now we use the free URL Toolbox app to parse out subdomains from the top level domains. We want to analyze each one, so that an attacker can't send mycompany.yourithelpdesk.com and get through, or mail.mycampany.com.
| foreach ut_subdomain_level* [eval orig_domain=domain_detected, domain_detected=mvappend(domain_detected, '<<FIELD>>' . "." . ut_tld)]	// The field we are going to pass to the Levenshtein algorithm is domain_detected, so let's add each subdomain to the multi-value field domain_detected.
| fields orig_domain domain_detected ut_domain_count	// This step is not required, but I like to filter down the list

© 2019 SPLUNK INC.

Improve Production Deployments



.conf19

splunk>

© 2019 SPLUNK INC.

MITRE ATT&CK Throughout App

Utilization Made Easier

Enrich Enterprise Security



ATT&CK Descriptions in Incident Review and risk framework

MITRE Threat Groups



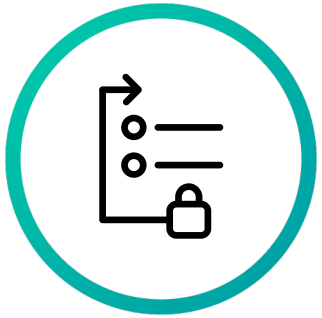
View which detections handle techniques used by which Threat Groups, w/ MITRE's evidence

MITRE-based Content Advice



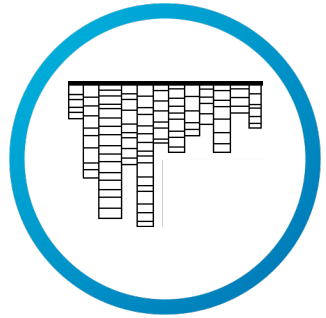
Content Recommendations tied to techniques popular amongst many threat groups

Analyze ES Risk w/ ATT&CK



Drilldown to a customized ATT&CK Matrix, correlate risky events across Tactics, Techniques

View Your ATT&CK Coverage



ATT&CK Matrix highlighting gaps and showing content you can enable for free with existing data

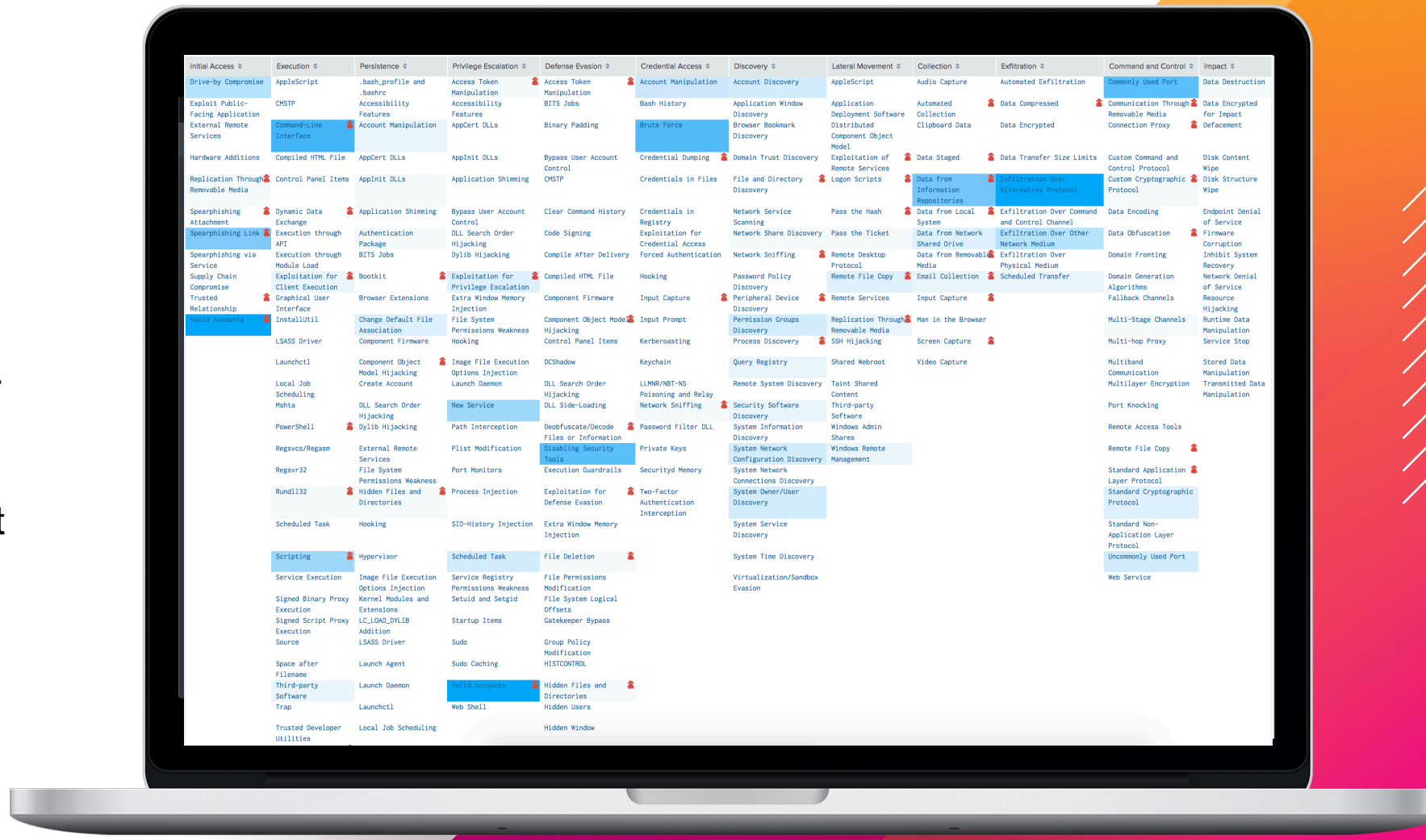
splunk> .conf19

MITRE ATT&CK Matrix

See what techniques you have or don't have coverage for. Drill-down to see those detections.

Annotate with threat groups that target you, or filter for techniques popular with many groups.

Considering a new data source? Highlight the techniques it supports.



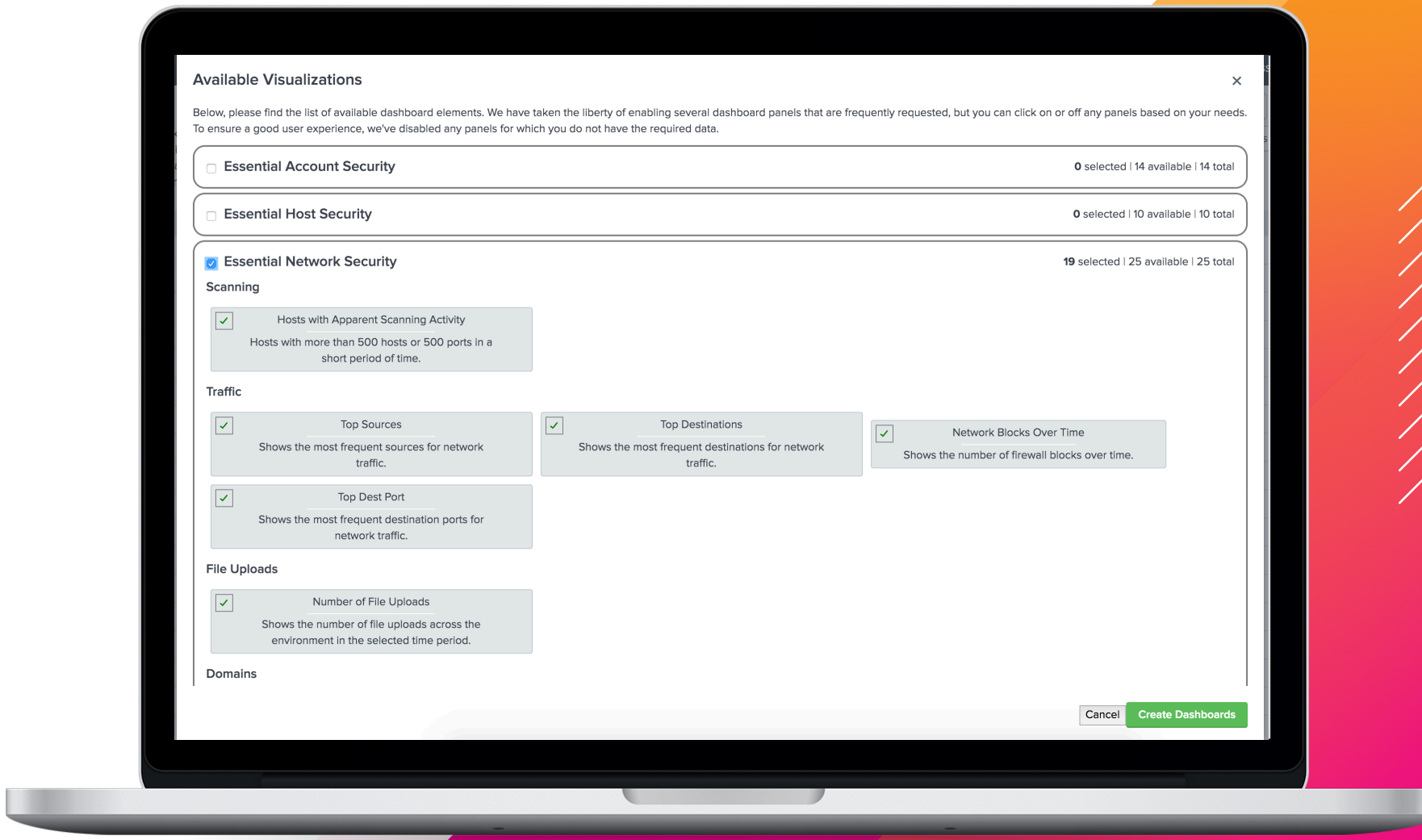
splunk> turn data into doing

© 2019 SPLUNK INC.

Automatic Dashboards

Alternative to Alerts

Driven by what data is in your environment, and follows all of Splunk's dashboard technical best practices



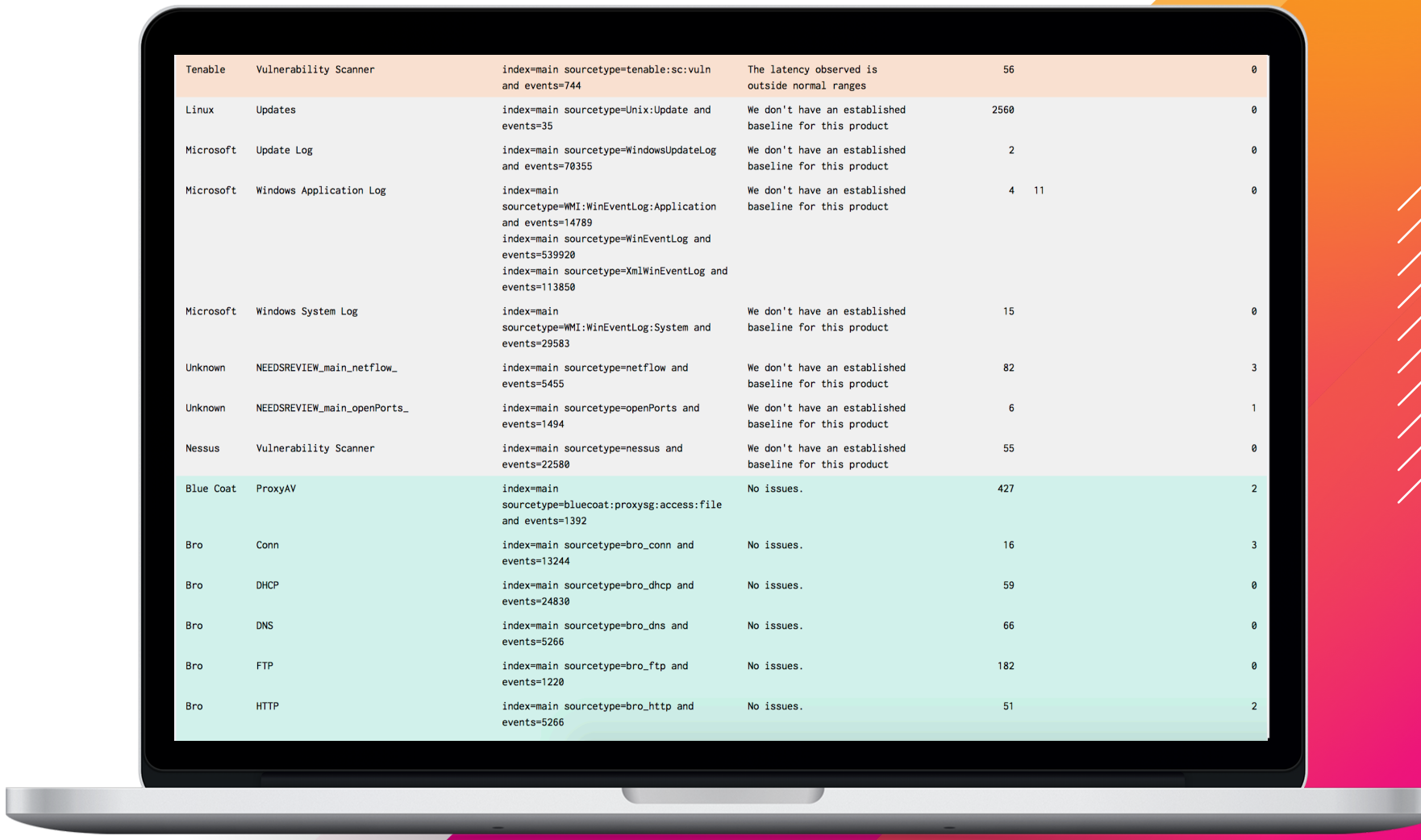
splunk> turn data into doing

© 2019 SPLUNK INC.

Monitor Data Ingest

Understand Lag, and Impacted Detections

Powered by Splunk's Machine Learning Toolkit



Tenable	Vulnerability Scanner	index=main sourcetype=tenable:sc:vuln and events=744	The latency observed is outside normal ranges	56		0
Linux	Updates	index=main sourcetype=Unix:Update and events=35	We don't have an established baseline for this product	2560		0
Microsoft	Update Log	index=main sourcetype=WindowsUpdateLog and events=70355	We don't have an established baseline for this product	2		0
Microsoft	Windows Application Log	index=main sourcetype=WMI:WinEventLog:Application and events=14789 index=main sourcetype=WinEventLog and events=539920 index=main sourcetype=XmlWinEventLog and events=113850	We don't have an established baseline for this product	4	11	0
Microsoft	Windows System Log	index=main sourcetype=WMI:WinEventLog:System and events=29583	We don't have an established baseline for this product	15		0
Unknown	NEEDSREVIEW_main_netflow_	index=main sourcetype=netflow and events=5455	We don't have an established baseline for this product	82		3
Unknown	NEEDSREVIEW_main_openPorts_	index=main sourcetype=openPorts and events=1494	We don't have an established baseline for this product	6		1
Nessus	Vulnerability Scanner	index=main sourcetype=nessus and events=22580	We don't have an established baseline for this product	55		0
Blue Coat	ProxyAV	index=main sourcetype=bluecoat:proxysg:access:file and events=1392	No issues.	427		2
Bro	Conn	index=main sourcetype=bro_conn and events=13244	No issues.	16		3
Bro	DHCP	index=main sourcetype=bro_dhcp and events=24830	No issues.	59		0
Bro	DNS	index=main sourcetype=bro_dns and events=5266	No issues.	66		0
Bro	FTP	index=main sourcetype=bro_ftp and events=1220	No issues.	182		0
Bro	HTTP	index=main sourcetype=bro_http and events=5266	No issues.	51		2

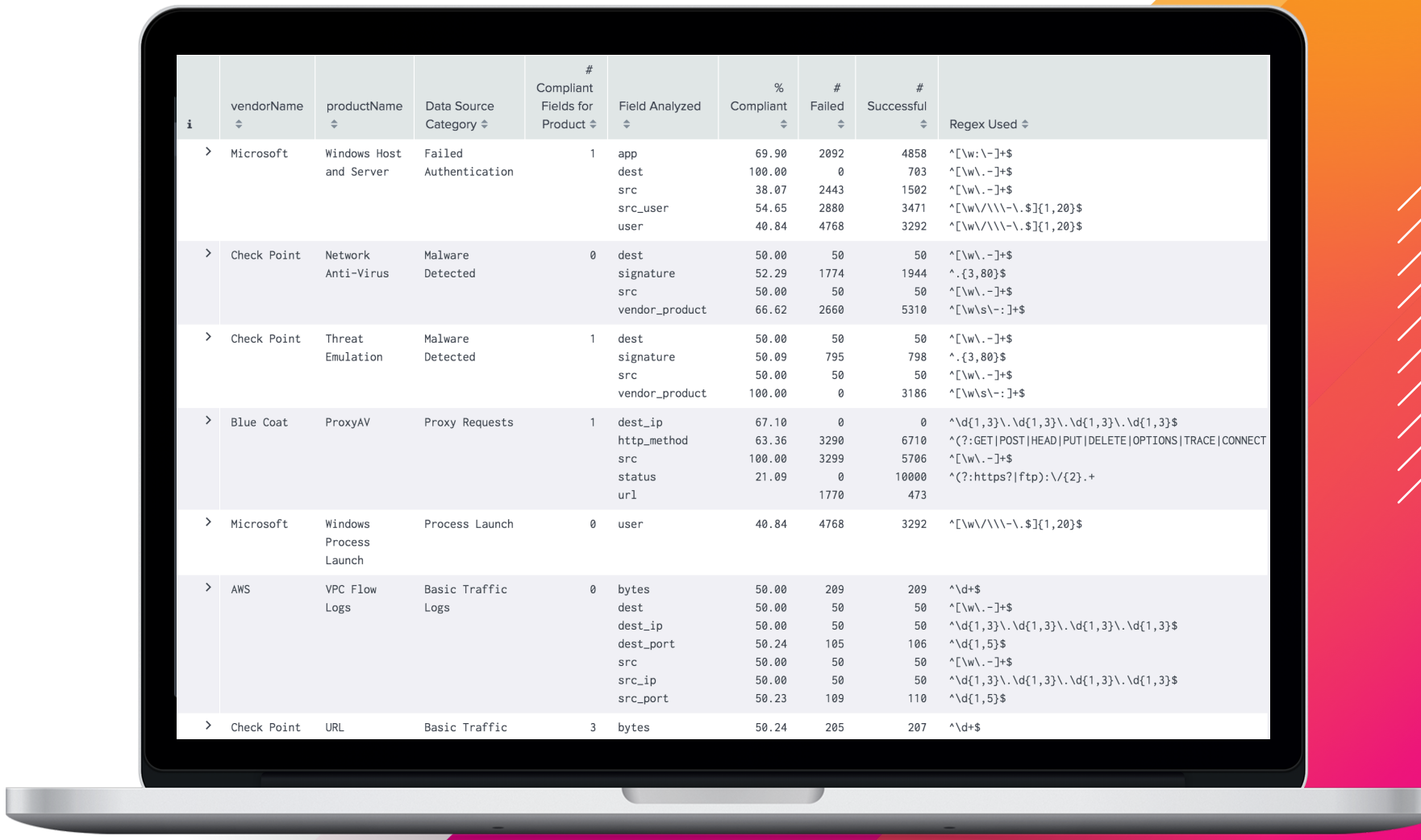
splunk> turn data into doing

© 2019 SPLUNK INC.

Track CIM Compliance

Ensure Data Formatting

SSE will analyze the most important CIM fields and evaluate whether your data matches.



vendorName	productName	Data Source Category	# Compliant Fields for Product	Field Analyzed	% Compliant	# Failed	# Successful	Regex Used
Microsoft	Windows Host and Server	Failed Authentication	1	app	69.90	2092	4858	^[\w:\-]+$
				dest	100.00	0	703	^[\w\.-]+$
				src	38.07	2443	1502	^[\w\.-]+$
				src_user	54.65	2880	3471	^[\w\/\\\-\.$]{1,20}$
				user	40.84	4768	3292	^[\w\/\\\-\.$]{1,20}$
Check Point	Network Anti-Virus	Malware Detected	0	dest	50.00	50	50	^[\w\.-]+$
				signature	52.29	1774	1944	^.{3,80}$
				src	50.00	50	50	^[\w\.-]+$
				vendor_product	66.62	2660	5310	^[\w\s\-:]+$
Check Point	Threat Emulation	Malware Detected	1	dest	50.00	50	50	^[\w\.-]+$
				signature	50.09	795	798	^.{3,80}$
				src	50.00	50	50	^[\w\.-]+$
				vendor_product	100.00	0	3186	^[\w\s\-:]+$
Blue Coat	ProxyAV	Proxy Requests	1	dest_ip	67.10	0	0	^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$
				http_method	63.36	3290	6710	^(?:GET|POST|HEAD|PUT|DELETE|OPTIONS|TRACE|CONNECT
				src	100.00	3299	5706	^[\w\.-]+$
				status	21.09	0	10000	^(?:https?|ftp):\/{2}.+
				url		1770	473	
Microsoft	Windows Process Launch	Process Launch	0	user	40.84	4768	3292	^[\w\/\\\-\.$]{1,20}$
AWS	VPC Flow Logs	Basic Traffic Logs	0	bytes	50.00	209	209	^\d+$
				dest	50.00	50	50	^[\w\.-]+$
				dest_ip	50.00	50	50	^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$
				dest_port	50.24	105	106	^\d{1,5}$
				src	50.00	50	50	^[\w\.-]+$
				src_ip	50.00	50	50	^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$
				src_port	50.23	109	110	^\d{1,5}$
Check Point	URL	Basic Traffic	3	bytes	50.24	205	207	^\d+$

splunk> turn data into doing

© 2019 SPLUNK INC.

© 2019 SPLUNK INC.

Hands-On



.conf19

splunk>

Home

Welcome to Splunk Security Essentials! Below you will find the primary areas where Splunk users get value from this app. Within each, you will see a guide showing you where to go, and what (if anything) you need to configure. The goal of this free app is to help you be more successful more quickly with Splunk for Security. If you run into any issues, check out the docs site or ask for help on Splunk Answers. Happy Splunking!

Demo Mode

Find Content

- Security Detection Basics
- Advanced Detection Content
- Prescriptive Content Recommendations
- Risk-Based Alerting Content

Learn

- Learn Splunk
- Learn Security
- Security Journey
- Data Onboarding Guides

Help Deploy

- Operationalize MITRE ATT&CK
- Monitor Data Ingest
- Automatically Generate Dashboards
- Deploy Content to your Environment
- Analyze CIM Compliance

Measure

- Justify New Data Sources via MITRE ATT&CK
- Document Your Deployed Content

splunk>enterprise App: Splunk Security Essentials ▾ Administrator ▾ 176 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Home | Security Content ▾ | Analytics Advisor ▾ | Security Operations ▾ | Data ▾ | Advanced ▾ | Documentation ▾ | Configuration | Splunk Security Essentials

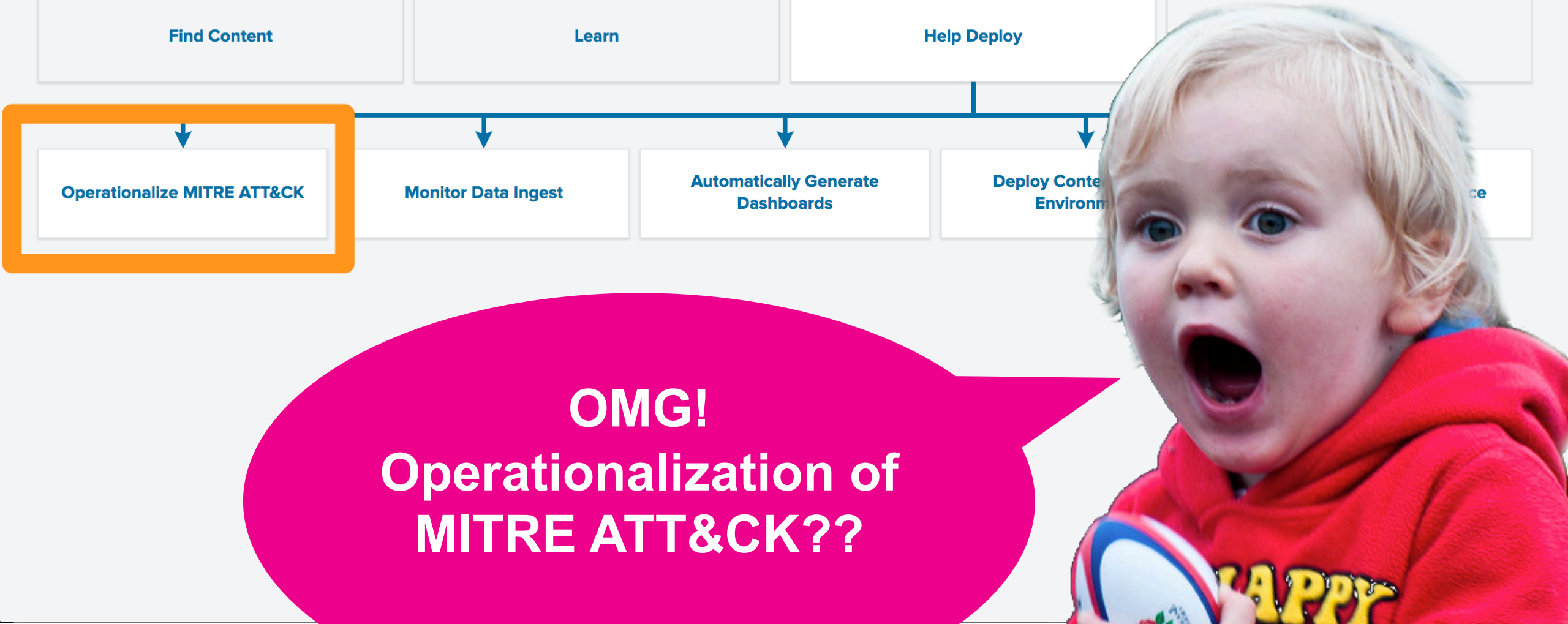
Home

Welcome to Splunk Security Essentials! Below you will find the primary areas where Splunk users get value from this app. Within each, you will see a guide showing you where to go, and what (if anything) you need to configure. The goal of this free app is to help you be more successful more quickly with Splunk for Security. If you run into any issues, check out the docs site or ask for help on Splunk Answers. Happy Splunking!

Demo Mode

Find Content | **Learn** | **Help Deploy**

- **Operationalize MITRE ATT&CK**
- **Monitor Data Ingest**
- **Automatically Generate Dashboards**
- **Deploy Conte… Environm…**




Vegetables first!
Make sure your data
is in good shape…

Data Availability

Find Content | Learn | Help

Operationalize MITRE ATT&CK | Monitor Data Ingest | Automatically Generate Dashboards | Deploy Content to your Environment | Analyze CIM Compliance

Monitor Data Ingest

There are many methods build for admins to help monitor data availability, but often fewer for users. This guide will help you with the configuration required and then point you to a dashboard built just for security users.

Setup Steps

Completion of these steps is required to get the value for this area.

✓	Configure enabled sources.	Launch w/ tour	In the app configuration, you can include / exclude different sources of content, allowing you to filter out Splunk solutions you might not own, or avoid seeing the free content from Splunk Security Essentials. Most users will leave this at the default settings.
?	Configure on the Data Inventory page.	Launch w/ tour	Data Source Categories use standardized searches to find data configured with the tags that are used in Splunk's Common Information Model. You can also add custom products that either don't match the Common Information Model, or mark that you have products you expect to add in the future.
✓	Configure on the Manage Bookmarks page.	Launch w/ tour	Tracking what content you have active is key to so much Splunk Security Essentials functionality (enriching the MITRE ATT&CK Matrix, guiding you to the right content, integrations with Splunk Enterprise Security, Risk-based Alerting, the Data Availability Dashboard). This can be accomplished through bookmarking (set status Implemented), but it's often easier to configure via Correlation Search Introspection on the Bookmarked Content dashboard.

Launch Feature

▭	Launch: Data Availability	Launch w/ tour	Splunk Security Essentials includes a machine-learning driven dashboard that tracks the typical data ingest latency of the products configured in SSE (effectively: how slow is typical for the logs). When a log source slows down, it will color code it, and you can click on it to see what detections are at risk for issue.

Data Availability

Data Availability

Model Health Warning

status

There are 34 products with fewer than thirty data points: AWS CloudTrail, AWS CloudWatch, AWS VPC Flow Logs, Azure Active Directory, Microsoft Office 365, Microsoft Sysmon, Microsoft Update Log, Microsoft Windows Application Log, Microsoft Windows Domain Controller, Microsoft Windows Host and Server, Microsoft Windows Powershell, Microsoft Windows Process Launch, Microsoft Windows System Log, Splunk ES Risk Framework, Stream ARP, Stream DHCP, Stream DNS, Stream HTTP, Stream ICMP, Stream LDAP, Stream SMB, Stream TCP, Stream UDP, Unknown

Data Latency by Product

This dashboard pulls a dataset from the configuration in the Data Inventory dashboard. A nightly search will run and over the past thirty days to determine how much latency is expected from each configured product. That data is pushed into a Machine Learning model and statistics are recorded. This dashboard then grabs data from the past four hours, calculates the current data lag, and feeds that through the ML model to determine if it is normal or not.

Vendor	Product	Index/Sourcetypes and Events	Summary	Minimum Lag Seen Per Product	Maximum Lag Seen Per Product (if different)	Number of Enabled Detections
AWS	CloudTrail	index=main sourcetype=aws:cloudtrail and events=23715	The latency observed is outside normal ranges	6467237		1
AWS	CloudWatch	index=main sourcetype=aws:cloudwatch and events=9938	The latency observed is outside normal ranges	6469299		0
AWS	VPC Flow Logs	index=main sourcetype=aws:cloudwatchlogs:vpcflow and events=142	The latency observed is outside normal ranges	6467312		0
Azure	Active Directory	index=main sourcetype=ms:aad:signin and events=537	The latency observed is outside normal ranges	6467649		3

Data Availability

Data Availability

Model Health Warning

status ⇕

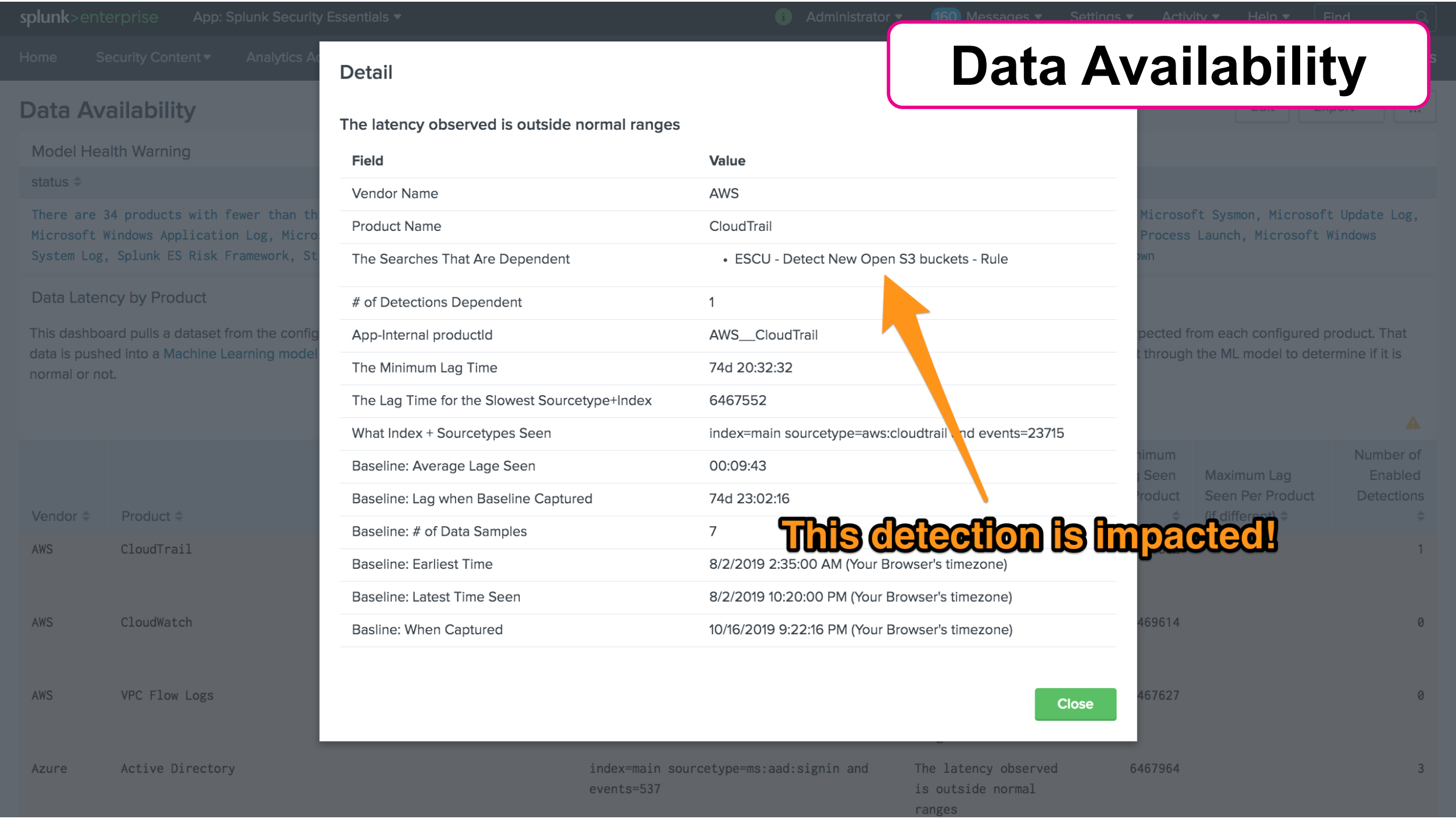
There are 34 products with fewer than thirty data points: AWS CloudTrail, AWS CloudWatch, AWS VPC Flow Logs, Azure Active Directory, Microsoft Office 365, Microsoft Sysmon, Microsoft Update Log, Microsoft Windows Application Log, Microsoft Windows Domain Controller, Microsoft Windows Host and Server, Microsoft Windows Powershell, Microsoft Windows Process Launch, Microsoft Windows System Log, Splunk ES Risk Framework, Stream ARP, Stream DHCP, Stream DNS, Stream HTTP, Stream ICMP, Stream LDAP, Stream SMB, Stream TCP, Stream UDP, Unknown

Data Latency by Product

This dashboard pulls a dataset from the configuration in the Data Inventory dashboard. A nightly search will run and over the past thirty days to determine how much latency is expected from each configured product. That data is pushed into a Machine Learning model and statistics are recorded. This dashboard then grabs data from the past four hours, calculates the current data lag, and feeds that through the ML model to determine if it is normal or not.

Click

Vendor ⇕	Product ⇕	Index/Sourcetypes and Events ⇕	Summary ⇕	Minimum Lag Seen Per Product ⇕	Maximum Lag Seen Per Product (if different) ⇕	Number of Enabled Detections ⇕
AWS	CloudTrail	index=main sourcetype=aws:cloudtrail and events=23715	The latency observed is outside normal ranges	6467237		1
AWS	CloudWatch	index=main sourcetype=aws:cloudwatch and events=9938	The latency observed is outside normal ranges	6469299		0
AWS	VPC Flow Logs	index=main sourcetype=aws:cloudwatchlogs:vpcflow and	The latency observed is outside normal	6467312		0
Azure	Active Directory	index=main sourcetype=ms:aad:signin and events=537	The latency observed is outside normal ranges	6467649		3



Data Availability

Detail

The latency observed is outside normal ranges

Field	Value
Vendor Name	AWS
Product Name	CloudTrail
The Searches That Are Dependent	• ESCU - Detect New Open S3 buckets - Rule
# of Detections Dependent	1
App-Internal productId	AWS__CloudTrail
The Minimum Lag Time	74d 20:32:32
The Lag Time for the Slowest Sourcetype+Index	6467552
What Index + Sourcetypes Seen	index=main sourcetype=aws:cloudtrail and events=23715
Baseline: Average Lage Seen	00:09:43
Baseline: Lag when Baseline Captured	74d 23:02:16
Baseline: # of Data Samples	7
Baseline: Earliest Time	8/2/2019 2:35:00 AM (Your Browser's timezone)
Baseline: Latest Time Seen	8/2/2019 10:20:00 PM (Your Browser's timezone)
Basline: When Captured	10/16/2019 9:22:16 PM (Your Browser's timezone)

Close

This detection is impacted!

splunk>enterprise App: Splunk Security Essentials ▾ Administrator ▾ 160 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Home | Security Content ▾ | Analytics Advisor ▾ | Security Operations ▾ | Data ▾ | Advanced ▾ | Documentation ▾

Data Availability

Data Availability

Model Health Warning

status ⇕

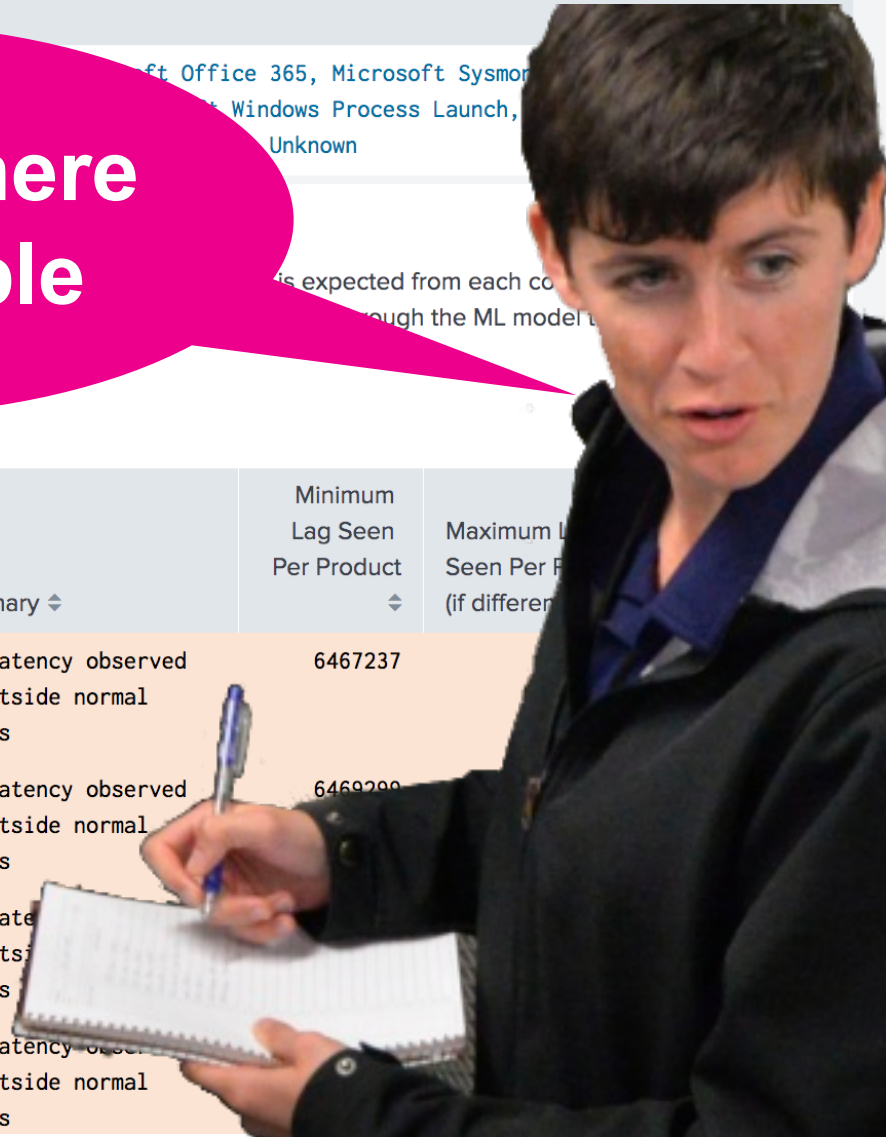
There are 34 products with fewer than thirty data points: AWS CloudTrail, AWS CloudWatch, AWS [illegible] ft Office 365, Microsoft Sysmon
Microsoft Windows Application Log, Microsoft Windows Domain Controller, Microsoft Windo[illegible] Windows Process Launch,
System Log, Splunk ES Risk Framework, Stream ARP, Stream DHCP, Stream DNS, Stream HT[illegible] Unknown

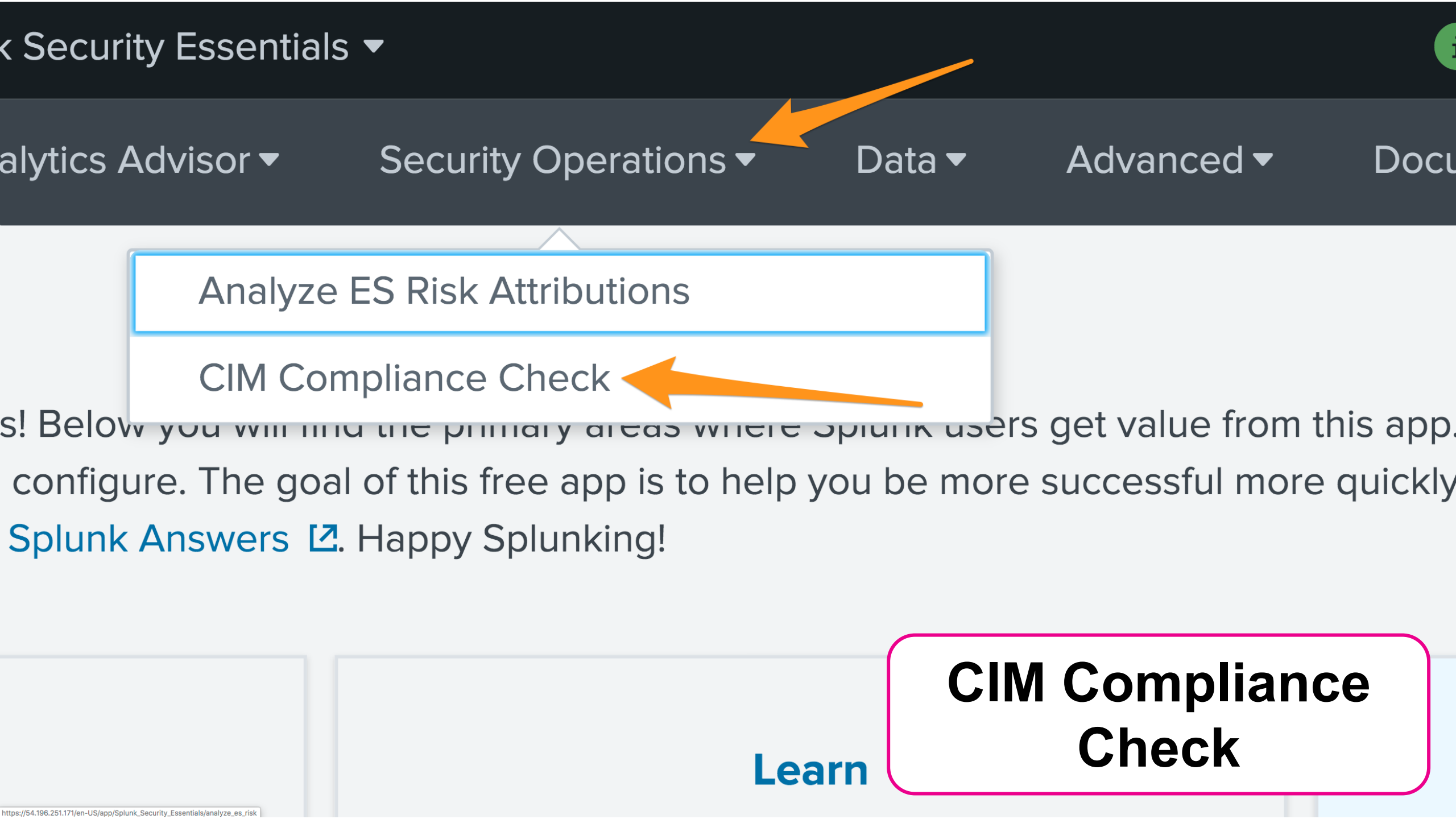
Data Latency by Product

This dashboard pulls a dataset from the configuration in the Data Inventory dashboard. A nightly [illegible] is expected from each co[illegible]
data is pushed into a Machine Learning model and statistics are recorded. This dashboard then gra[illegible] ough the ML model t[illegible]
normal or not.

Told you there was trouble

Vendor ⇕	Product ⇕	Index/Sourcetypes and Events ⇕	Summary ⇕	Minimum Lag Seen Per Product ⇕	Maximum L[illegible] Seen Per P[illegible] (if differen[illegible]
AWS	CloudTrail	index=main sourcetype=aws:cloudtrail and events=23715	The latency observed is outside normal ranges	6467237	
AWS	CloudWatch	index=main sourcetype=aws:cloudwatch and events=9938	The latency observed is outside normal ranges	6469299	
AWS	VPC Flow Logs	index=main sourcetype=aws:cloudwatchlogs:vpcflow and events=142	The late[illegible] is outsi[illegible] ranges		
Azure	Active Directory	index=main sourcetype=ms:aad:signin and events=537	The latency [illegible] is outside normal ranges		




k Security Essentials
alytics Advisor
Security Operations
Data
Advanced
Docu
Analyze ES Risk Attributions
CIM Compliance Check
s! Below you will find the primary areas where Splunk users get value from this app.
configure. The goal of this free app is to help you be more successful more quickly
Splunk Answers . Happy Splunking!
Learn
CIM Compliance Check

CIM Compliance Check

CIM Compliance Check

Introduction

Welcome to the Common Information Model Compliance Check dashboard. This dashboard builds on top of the Data Inventory introspection to show you what fields are CIM compliant. It aggregates those fields per-product, and tells you how those products are doing. CIM compliance is performed by checking common field values against a regular expression, also shown. Important note: this looks for the most common CIM fields used for most security content, but doesn't check all CIM fields.

If you're new to Splunk's Common Information Model, consider reading Splunk Docs. If you would like to go deeper into assessing the CIM compliance of your data, we highly recommend SA-cim_validator -- this functionality is a simplified version of what Splunk's Vladimir Skoryk has built there.

Products

i	vendorName	productName	Data Source Category	# Compliant Fields for Product	Field Analyzed	% Compliant	# Failed	# Successful	Regex Used
>	Microsoft	Office 365	Outgoing Messages	3	dest	59.13	85	123	^[\w\.-]+$
					message_id	100.00	0	208	^[\w\.-]+$
					recipient	100.00	0	208	^[\w\/\\\-\.$]{1,20}$
					src	61.54	80	128	
					src_user	0.00	208	0	
					subject	100.00	0	208	
>	Stream	DNS	DNS Queries	5	dest_port	64.85	3267	6027	^\d{1,5}$
					message_type	100.00	0	17316	^[\w\.-]+$
					query	100.00	0	17324	^[a-z0-9]+$
					query_count	100.00	0	0	
					query_type	52.81	0	314	
					src	100.00	4534	5074	
					transaction_id	100.00	0	627	
					transport		0	9294	
>	Azure	Active Directory	Successful Authentication	0	app	1.68	528	9	^[\w:\-]+$
					src	56.98	231	306	^[\w\.-]+$
					user	0.00	537	0	^[\w\/\\\-\.$]{1,20}$

Products

CIM Compliance Check

i	vendorName	productName	Data Source Category	# Compliant Fields for Product	Field Analyzed	% Compliant		
⌄	Microsoft	Office 365	Outgoing Messages	3	dest	59.13		
					message_id	100.00		
					recipient	100.00		
					src	61.54	80	128
					src_user	0.00	208	0
					subject	100.00	0	208

field	count	distinct_count	values
dest	208	4	[{"value":"null","count":122}, {"value":"18.224.52.126","count":84}, {"value":"34.217.56.192","count":1}, {"value":"74.6.137.64","count":1}]
message_id	208	98	[{"value":"<BY5PR17MB336878F267001965F65A8EE8DBDF0@BY5PR17MB3368.namprd17.prod.outlook.com>","count":10}, {"value":"<CY4PR17MB120684388A62BD6EFCCB6D98BFDF0@CY4PR17MB1206.namprd17.prod.outlook.com>","count":10}, {"value":"<SN6PR17MB2061F1AC442084A4C7233271BCDF0@SN6PR17MB2061.namprd17.prod.outlook.com>","count":10}, {"value":"<20190801002228.895A44212A@mx2.cazadoresseguridad.com.ar>","count":3}, {"value":"<BY5PR17MB3368019555F689B9A7E5F04DDBDF0@BY5PR17MB3368.namprd17.prod.outlook.com>","count":3}, {"value":"<CY4PR17MB12067D092679F0CE9AFDAB99BFDF0@CY4PR17MB1206.namprd17.prod.outlook.com>","count":3}, {"value":"<0100016c4a50ef52-3cbc33e3-42ac-4be6-a7b2-c7e3f90907c0-000000@email.amazonses.com>","count":2}, {"value":"<0101016c4a501804-8a9c2f52-0280-43b5-8f48-adf60ad0b0db-000000@us-west-2.amazonses.com>","count":2}, {"value":"<0101016c4a5136d4-e6a0d277-7f42-458e-8c96-51c4a725e794-000000@us-west-2.amazonses.com>","count":2}, {"value":"<0ca0a3f0bbef4b6bb82109bff3d33c32-JVKUGUBNKBZG6ZBNIJHDE7CPGM3DKQLENVUW4UDPOJ2GC3D4J4ZTMNKBMRWWS3SHMVXGK4TJMN6FG3LUOA======@microsoft.com>","count":2}, {"value":"<1143724797.893866.1564658937211.JavaMail.app@ltx1-app9401.prod.linkedin.com>","count":2}, {"value":"<1397551089.1292658.1564698044664.JavaMail.app@ltx1-app7686.prod.linkedin.com>","count":2}, {"value":"<1b135cbf-54cd-7c46-17c1-04193861f893@gmail.com>","count":2}, {"value":"<2017997986.99701128.1564671771944.JavaMail.rocketman@push-dispatcher34.snc1>","count":2}, {"value":"<201906241452.x5OEqksu016648@znet.kiev.ua>","count":2}, {"value":"<20190731122854.03FC01261BBF@mail.telkomcel.tl>","count":2}, {"value":"<20190801002155.3525D4016A@mx2.cazadoresseguridad.com.ar>","count":2}, {"value":"<20190801002311.A5B654370F@mx2.cazadoresseguridad.com.ar>","count":2}, {"value":"<20190801002315.171AD450EC@mx2.cazadoresseguridad.com.ar>","count":2}, {"value":"<20190801002350.32CCD45190@mx2.cazadoresseguridad.com.ar>","count":2}, {"value":"<20190801061019.88DAD348278@mymail.ipnet.co.id>","count":2}, {"value":"<20190801063445.ED37134C646@mymail.ipnet.co.id>","count":2}, {"value":"<20190801063454.CCACC34C652@mymail.ipnet.co.id>","count":2}, {"value":"<20190801072037.9E15D351181@mymail.ipnet.co.id>","count":2}, {"value":"<20190801075338.52F9F356BFA@mymail.ipnet.co.id>","count":2}, {"value":"<2068122113.97343635.1564660805421.JavaMail.rocketman@push-dispatcher39.snc1>","count":2}, {"value":"<29984e32-98f6-4909-96f5-891750f374d4@SN1NAM02FT062.eop-nam02.prod.protection.outlook.com>","count":2}, {"value":"<3dbdb2b6-8e61-44a4-aded-6b076d91c79a@www.fastmail.com>","count":2}, {"value":"<566935865.1063547.1564667069582.JavaMail.app@ltx1-app6466.prod.linkedin.com>","count":2}, {"value":"<593627679.105573941.1564664720879.JavaMail.rocketman@push-dispatcher16.snc1>","count":2},

Products

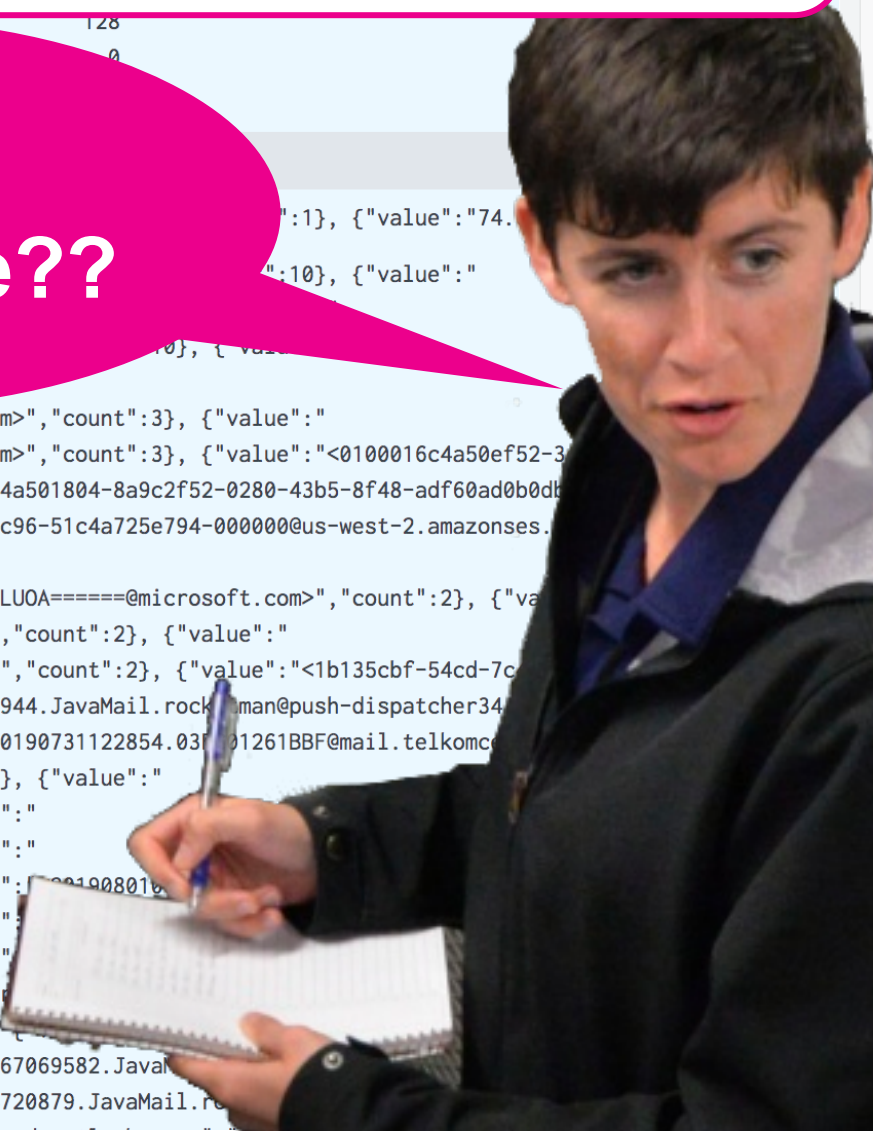
i	vendorName	productName	Data Source Category	# Compliant Fields for Product	Field Analyzed	% Compliant
⌄	Microsoft	Office 365	Outgoing Messages	3	dest	59.13
					message_id	100.00
					recipient	100.00
					src	
					src_us	

field	count	distinct_count	values
dest	208	4	[{"value":"null","count":122}, :1}, {"value":"74.
message_id	208	98	[{"value":"<BY5PR17MB336878F267 :10}, {"value":"

<CY4PR17MB120684388A62BD6EFCCB6D98
<SN6PR17MB2061F1AC442084A4C7233271BCDF
<20190801002228.895A44212A@mx2.cazadoresseguri
<BY5PR17MB3368019555F689B9A7E5F04DDBDF0@BY5PR17MB3368.namprd17.prod.outlook.com>","count":3}, {"value":"
<CY4PR17MB12067D092679F0CE9AFDAB99BFDF0@CY4PR17MB1206.namprd17.prod.outlook.com>","count":3}, {"value":"<0100016c4a50ef52-3
a7b2-c7e3f90907c0-000000@email.amazonses.com>","count":2}, {"value":"<0101016c4a501804-8a9c2f52-0280-43b5-8f48-adf60ad0b0db
2.amazonses.com>","count":2}, {"value":"<0101016c4a5136d4-e6a0d277-7f42-458e-8c96-51c4a725e794-000000@us-west-2.amazonses.
{"value":"<0ca0a3f0bbef4b6bb82109bff3d33c32-
JVKUGUBNKBZG6ZBNIJHDE7CPGM3DKQLENVUW4UDPOJ2GC3D4J4ZTMNKBMRWWS3SHMVXGK4TJMN6FG3LUOA======@microsoft.com>","count":2}, {"va
<1143724797.893866.1564658937211.JavaMail.app@ltx1-app9401.prod.linkedin.com>","count":2}, {"value":"
<1397551089.1292658.1564698044664.JavaMail.app@ltx1-app7686.prod.linkedin.com>","count":2}, {"value":"<1b135cbf-54cd-7c
04193861f893@gmail.com>","count":2}, {"value":"<2017997986.99701128.1564671771944.JavaMail.rock man@push-dispatcher34
{"value":"<201906241452.x5OEqksu016648@znet.kiev.ua>","count":2}, {"value":"<20190731122854.03 01261BBF@mail.telkomc
{"value":"<20190801002155.3525D4016A@mx2.cazadoresseguridad.com.ar>","count":2}, {"value":"
<20190801002311.A5B654370F@mx2.cazadoresseguridad.com.ar>","count":2}, {"value":"
<20190801002315.171AD450EC@mx2.cazadoresseguridad.com.ar>","count":2}, {"value":"
<20190801002350.32CCD45190@mx2.cazadoresseguridad.com.ar>","count":2}, {"value":
{"value":"<20190801063445.ED37134C646@mymail.ipnet.co.id>","count":2}, {"value":
{"value":"<20190801072037.9E15D351181@mymail.ipnet.co.id>","count":2}, {"value":
{"value":"<2068122113.97343635.1564660805421.JavaMail.rocketman@push-dispatcher
891750f374d4@SN1NAM02FT062.eop-nam02.prod.protection.outlook.com>","count":2},
6b076d91c79a@www.fastmail.com>","count":2}, {"value":"<566935865.1063547.1564667069582.Java
app6466.prod.linkedin.com>","count":2}, {"value":"<593627679.105573941.1564664720879.JavaMail.r

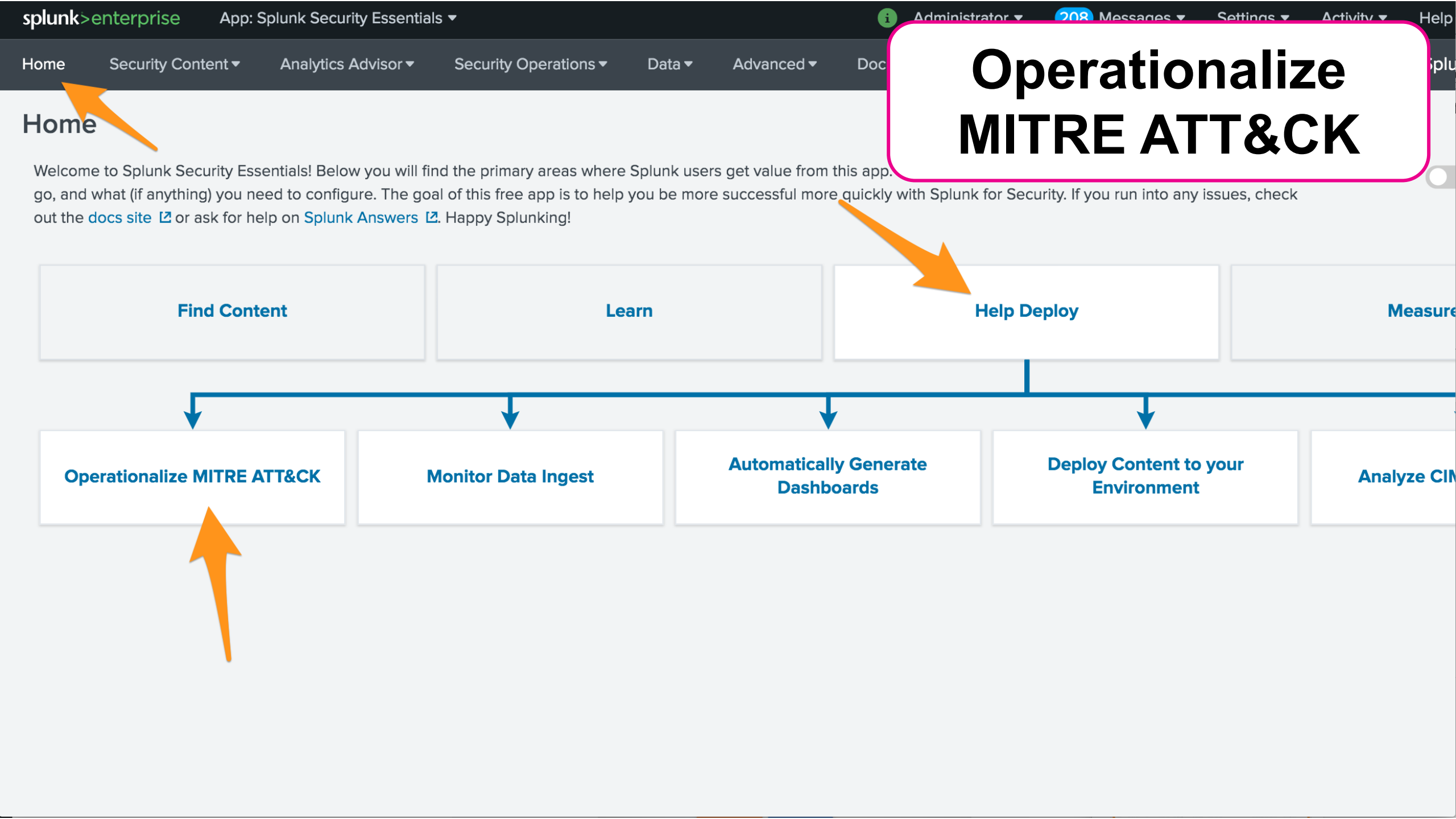
CIM Compliance Check

Are You Kidding Me??



© 2019 SPLUNK INC.




splunk>enterprise
App: Splunk Security Essentials
Administrator
208 Messages
Settings
Activity
Help
Home
Security Content
Analytics Advisor
Security Operations
Data
Advanced
Operationalize MITRE ATT&CK
Home
Welcome to Splunk Security Essentials! Below you will find the primary areas where Splunk users get value from this app.
go, and what (if anything) you need to configure. The goal of this free app is to help you be more successful more quickly with Splunk for Security. If you run into any issues, check
out the docs site or ask for help on Splunk Answers. Happy Splunking!
Find Content
Learn
Help Deploy
Measure
Operationalize MITRE ATT&CK
Monitor Data Ingest
Automatically Generate Dashboards
Deploy Content to your Environment
Analyze CIM

© 2019 SPLUNK INC.

MITRE ATT&CK Throughout App

Utilization Made Easier

Enrich Enterprise Security



ATT&CK Descriptions in Incident Review and risk framework

MITRE Threat Groups



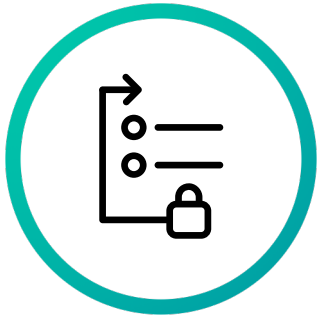
View which detections handle techniques used by which Threat Groups, w/ MITRE's evidence

MITRE-based Content Advice



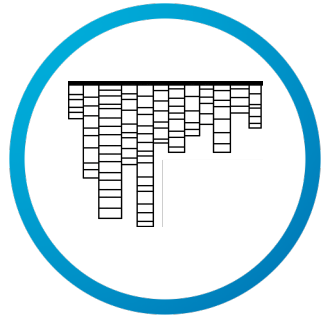
Content Recommendations tied to techniques popular amongst many threat groups

Analyze ES Risk w/ ATT&CK



Drilldown to a customized ATT&CK Matrix, correlate risky events across Tactics, Techniques

View Your ATT&CK Coverage



ATT&CK Matrix highlighting gaps and showing content you can enable for free with existing data

splunk> .conf19

© 2019 SPLUNK INC.

MITRE ATT&CK Throughout App

Utilization Made Easier

Enrich Enterprise Security



ATT&CK Descriptions in Incident Review and risk framework

MITRE Threat Groups



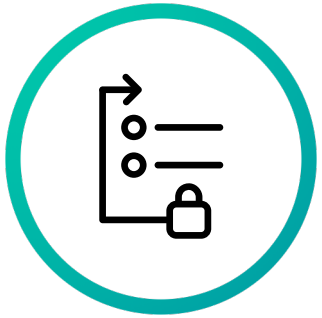
View which detections handle techniques used by which Threat Groups, w/ MITRE's evidence

MITRE-based Content Advice



Content Recommendations tied to techniques popular amongst many threat groups

Analyze ES Risk w/ ATT&CK



Drilldown to a customized ATT&CK Matrix, correlate risky events across Tactics, Techniques

View Your ATT&CK Coverage



ATT&CK Matrix highlighting gaps and showing content you can enable for free with existing data

Operationalize MITRE ATT&CK

If you are orienting your security environment, you're in luck (particularly if you use Splunk Enterprise Security). This app contains a we

Analyze ES Risk Attributions

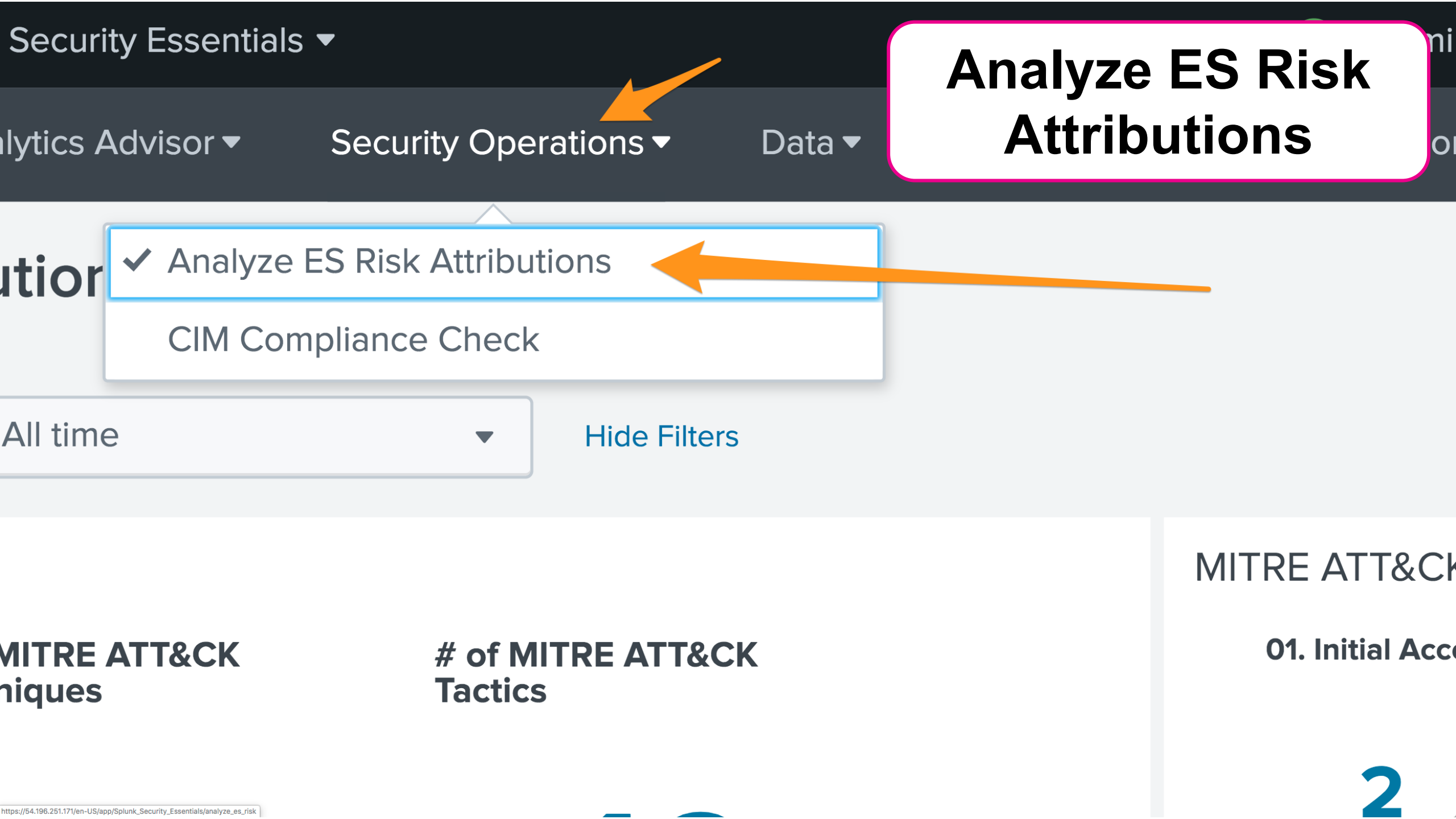
Setup Steps

Completion of these steps is required to get the value for this area.

✓	Configure enabled sources.	Launch w/ tour	In the app configuration, you can include / exclude different sources of co seeing the free content from Splunk Security Essentials. Most users will le
?	Configure on the Data Inventory page.	Launch w/ tour	Data Source Categories use standardized searches to find data configured with the tags that are used in Splunk's Common Information Model. You can also add custom products that either don't match the Common Information Model, or mark that you have products you expect to add in the future.
✓	Configure on the Manage Bookmarks page.	Launch w/ tour	Tracking what content you have active is key to so much Splunk Security Essentials functionality (enriching the MITRE ATT&CK Matrix, guiding you to the right content, integrations with Splunk Enterprise Security, Risk-based Alerting, the Data Availability Dashboard). This can be accomplished through bookmarking (set status Implemented), but it's often easier to configure via Correlation Search Introspection on the Bookmarked Content dashboard.
!	Configure ES Integration.	Launch w/ tour	Assuming that you have ES in your environment, Splunk Security Essentials can push MITRE ATT&CK and Kill Chain attributions to the Incident Review dashboard, along with raw searches of index=risk or index=notable. Just configure the ES Integration in the system config menu.

Launch Features

	Launch: Analytics Advisor MITRE ATT&CK Framework	Launch w/ tour	The Analytics Advisor dashboards are designed to help you understand what content you might want to deploy inside of Splunk based on the content you already have and the data that's present in your environment. The MITRE ATT&CK Overview dashboard even includes a customized MITRE ATT&CK Matrix that shows your level of coverage on MITRE ATT&CK while letting you filter for the data you have in the environment, or the threat groups that target you.
	Launch: Analyze ES Risk Attributions	Launch w/ tour	Risk-based Alerting is all oriented towards aggregating risky events. This dashboard looks at the content in the ES Risk Framework with out-of-the-box Risk aggregations. It also includes a customized MITRE ATT&CK Matrix based on your search filters, letting you see what techniques have been seen against a particular user, host, or network.
	Launch: MITRE ATT&CK-based Content Recommendations	Launch w/ tour	With an understanding of what data you have, you can specify the types of security concerns you're facing and then use MITRE ATT&CK to filter for the Splunk content related to MITRE Techniques that are associated with many different threat groups.
	Launch: Advanced Content		Splunk Security Essentials has a wealth of advanced security content and a list of all of Splunk's Security Content, complete with a mapping to popular frameworks like MITRE ATT&CK and the Kill Chain. Explore all of our content.


Security Essentials
Analyze ES Risk Attributions
lytics Advisor
Security Operations
Data
utior
Analyze ES Risk Attributions
CIM Compliance Check
All time
Hide Filters
MITRE ATT&CK
niques
# of MITRE ATT&CK Tactics
MITRE ATT&CK
01. Initial Acc
2

Analyze ES Risk Attributions

System-wide Metrics

# of Detections

13

# of MITRE ATT&CK Techniques

14

# of MITRE ATT&CK Tactics

10

% of MITRE ATT&CK Techniques

6

Average Risk Object Score

48

 # Risk Objects

45

MITRE ATT&CK Tacti

01. Initial Access

2

05. Defense Evasion

8

06. Credential Access

8

07. Discovery

3

08. Lateral Movement

0

09. Collection

0

10. Command and Cont...

0

11. Exfiltration

2

12. Impact

0

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Valid Accounts	Command-Line Interface	New Service	New Service	Scripting	Credential Dumping	Network Service Scanning			Exfiltration Over Command and Control Channel	Commonly Used Port	
	Scripting	Valid Accounts	Valid Accounts	Indicator Removal on Host	Brute Force						
	PowerShell			Valid Accounts							
	User Execution										

Count of Risk Object Attributions by MITRE ATT&CK Tactic

400

Count of Risk Object Attributions by MITRE ATT&CK Technique

400

Analyze ES Risk Attributions

% of MITRE ATT&CK Techniques	Average Risk Object Score	# Risk Objects
6	48	45

MITRE ATT&CK Tactics

01. Initial Access	02. Execution	03. Persistence	04. Privilege Escalation
2	29	14	2
05. Defense Evasion	**06. Credential Access**	**07. Discovery**	**08. Lateral Movement**
8	8	3	0
09. Collection	**10. Command and Cont...**	**11. Exfiltration**	**12. Impact**
0	0	2	0

How many risk events for each MITRE ATT&CK Tactic

MITRE ATT&CK Matrix

Initial Access	Execution				Collection	Exfiltration	Command and Control	Impact
Valid Accounts	Command-Line Interface					Exfiltration Over Command and Control Channel	Commonly Used Port	
	Scripting							
		Accounts	Accounts	Removal on Host				
	PowerShell			Valid Accounts				
	User Execution							

Count of Risk Object Attributions by MITRE ATT&CK Tactic

400

Count of Risk Object Attributions by MITRE ATT&CK Technique

400

Analyze ES Risk Attributions

% of MITRE ATT&CK Techniques

6

Average Risk Object Score

48

Risk Objects

45

MITRE ATT&CK Tactics

01. Initial Access	02. Execution	03. Persistence	04. Privilege Escalation
2	29	14	2

05. Defense Evasion	06. Credential Access	07. Discovery	08. Lateral Movement
8	8	3	0

12. Impact

0

Customized MITRE ATT&CK Matrix

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Valid Accounts	Command-Line Interface	New Service	New Service	Scripting	Credential Dumping	Network Service Scanning			Exfiltration Over Command and Control Channel	Commonly Used Port	
	Scripting	Valid Accounts	Valid Accounts	Indicator Removal on Host	Brute Force						
	PowerShell			Valid Accounts							
	User Execution										

400

400

Analyze ES Risk Attributions

Aggregate Risk Attribution Scores by Analytic

		Score	ATT&CK Tactics
		3840	
Rule		3168	
Threat - RR - Suspicious activity or known framework detected - Combined - Rule		3024	
Threat - RR - Suspisious Process or DLL detected - Combined - Rule		1760	
ESCU - Malicious PowerShell Process - Encoded Command - Rule		960	Execution
Threat - RR - Suspicious service or registry change detected - Combined - Rule		576	
Threat - Threat List Activity - Rule		560	
ESCU - Create local admin accounts using net.exe - Rule		520	Execution Persistence
Access - Brute Force Access Behavior Detected - Rule		480	Credential Access
Threat - UEBA Threat Detected - Rule		480	

Aggregate Risk Attribution Scores by Risk Object

Scroll Down

risk_object	sparkline	Score	ATT&CK Tactics
agrady-l		4180	
agrady		4072	
FYODOR-L.froth.ly		1040	Credential Access Defense Evasion Execution Persistence
BudStoll		898	
bstoll-l		848	
JeremiahWortoski		784	
jwortoski-l		784	
136.0.0.125		400	
FyodorMalteskesko		364	
fmaltekesko-l		364	

A variety of aggregation methods

Watch-listed Objects with Risk Attributions

Fullname	count	Score	Manager	Identities	Roles	BU	Analytics	Tactics	Techniques
Bud Stoll	26	1826	fyodor	AzureAD\BudStoll BudStoll bstoll bstoll@froth.ly	americas privileged technical watchlist	americas	ESCU - Malicious PowerShell Process - Encoded Command - Rule Endpoint - Code42 Rule Match - Rule Threat - RR - Command and Control Activity Detected - Combined - Rule Threat - RR - Malware detected by Windows Defender - Combined - Rule	Execution	PowerShell Scripting

Analyze ES Risk Attributions

Edit | Export | ...

Search Criteria

agrady | All time | Hide Filters

Analyze ES Risk Attributions

Enter agrady Hit Enter

System-wide Metrics

# of Detections	# of MITRE ATT&CK Techniques	# of MITRE ATT&CK Tactics
13	14	

% of MITRE ATT&CK Techniques	Average Risk Object Score	
6	48	45

MITRE ATT&CK Tacti

01. Initial Access			
0	5	1	0
05. Defense Evasion	**06. Credential Access**	**07. Discovery**	**08. Lateral Movement**
0	0	0	0
09. Collection	**10. Command and Cont...**	**11. Exfiltration**	**12. Impact**
0	0	0	0

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
	Command-Line Interface			Scripting							
	Scripting										
	PowerShell										

Scroll Up

Count of Risk Object Attributions by MITRE ATT&CK Tactic

Count of Risk Object Attributions by MITRE ATT&CK Technique

Analyze ES Risk Attributions

Edit | Export | ...

Search Critera

agrady

ters

Focused to: agrady

Analyze ES Risk Attributions

System-wide Me

# of Detections		&CK
13	14	10
% of MITRE ATT&CK Techniques	Average Risk Object Score	# Risk Objects
6	48	45

MITRE ATT&CK Tacti

01. Initial Access			
0	5	1	0
05. Defense Evasion	06. Credential Access	07. Discovery	08. Lateral Movement
0	0	0	0
09. Collection	10. Command and Cont...	11. Exfiltration	12. Impact

Focused MITRE ATT&CK Matrix

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
	Command-Line Interface			Scripting							
	Scripting										
	PowerShell										

© 2019 SPLUNK INC.

MITRE ATT&CK Throughout App

Utilization Made Easier

Enrich Enterprise Security



ATT&CK Descriptions in Incident Review and risk framework

MITRE Threat Groups



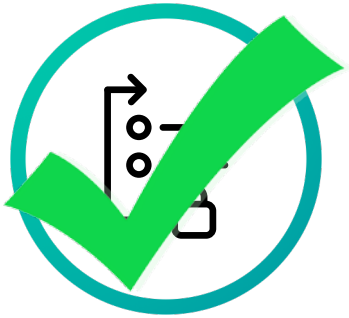
View which detections handle techniques used by which Threat Groups, w/ MITRE's evidence

MITRE-based Content Advice



Content Recommendations tied to techniques popular amongst many threat groups

Analyze ES Risk w/ ATT&CK



Drilldown to a customized ATT&CK Matrix, correlate risky events across Tactics, Techniques

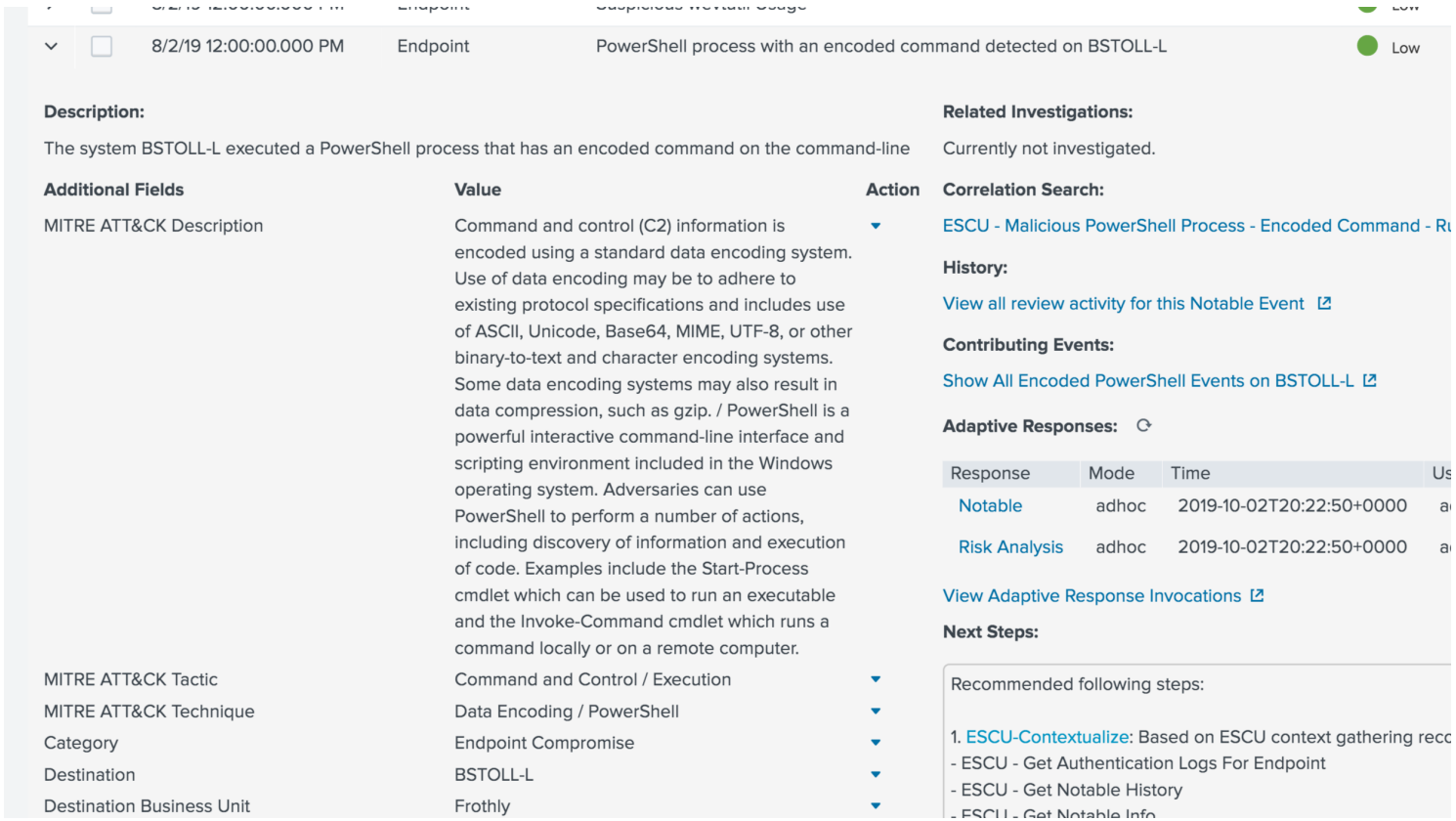
View Your ATT&CK Coverage



ATT&CK Matrix highlighting gaps and showing content you can enable for free with existing data

© 2019 SPLUNK INC.

Push MITRE Techniques and Tactics into ES



splunk> .conf19

© 2019 SPLUNK INC.

MITRE ATT&CK Throughout App

Utilization Made Easier

Enrich Enterprise Security



ATT&CK Descriptions in Incident Review and risk framework

MITRE Threat Groups



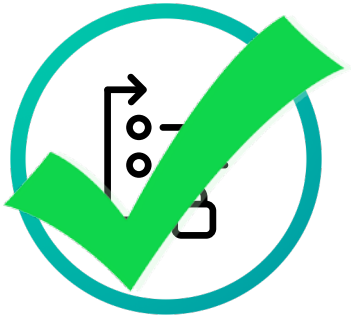
View which detections handle techniques used by which Threat Groups, w/ MITRE's evidence

MITRE-based Content Advice



Content Recommendations tied to techniques popular amongst many threat groups

Analyze ES Risk w/ ATT&CK



Drilldown to a customized ATT&CK Matrix, correlate risky events across Tactics, Techniques

View Your ATT&CK Coverage



ATT&CK Matrix highlighting gaps and showing content you can enable for free with existing data

splunk> .conf19

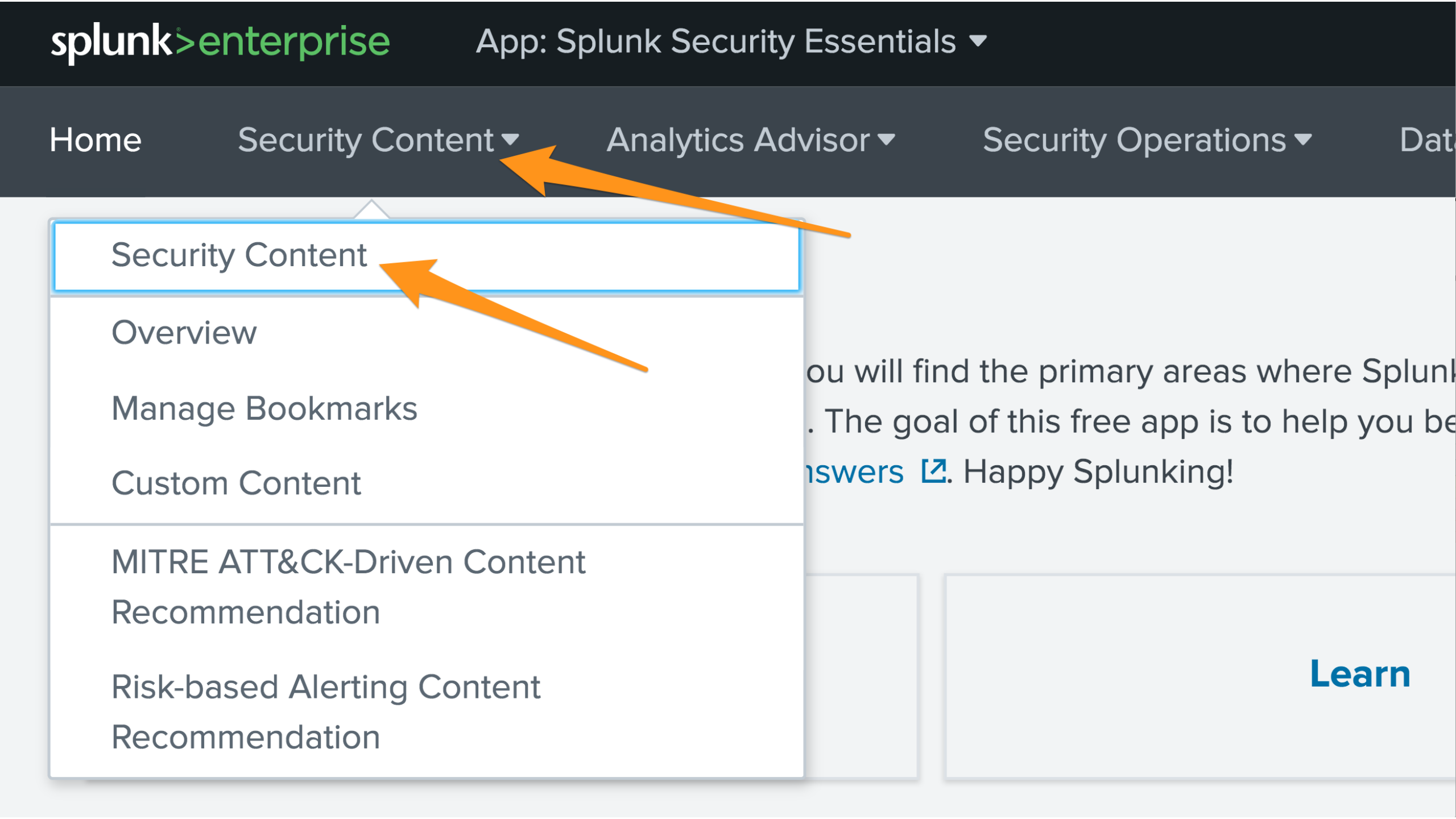
© 2019 SPLUNK INC.

Okay, that's a lot of MITRE ATT&CK…

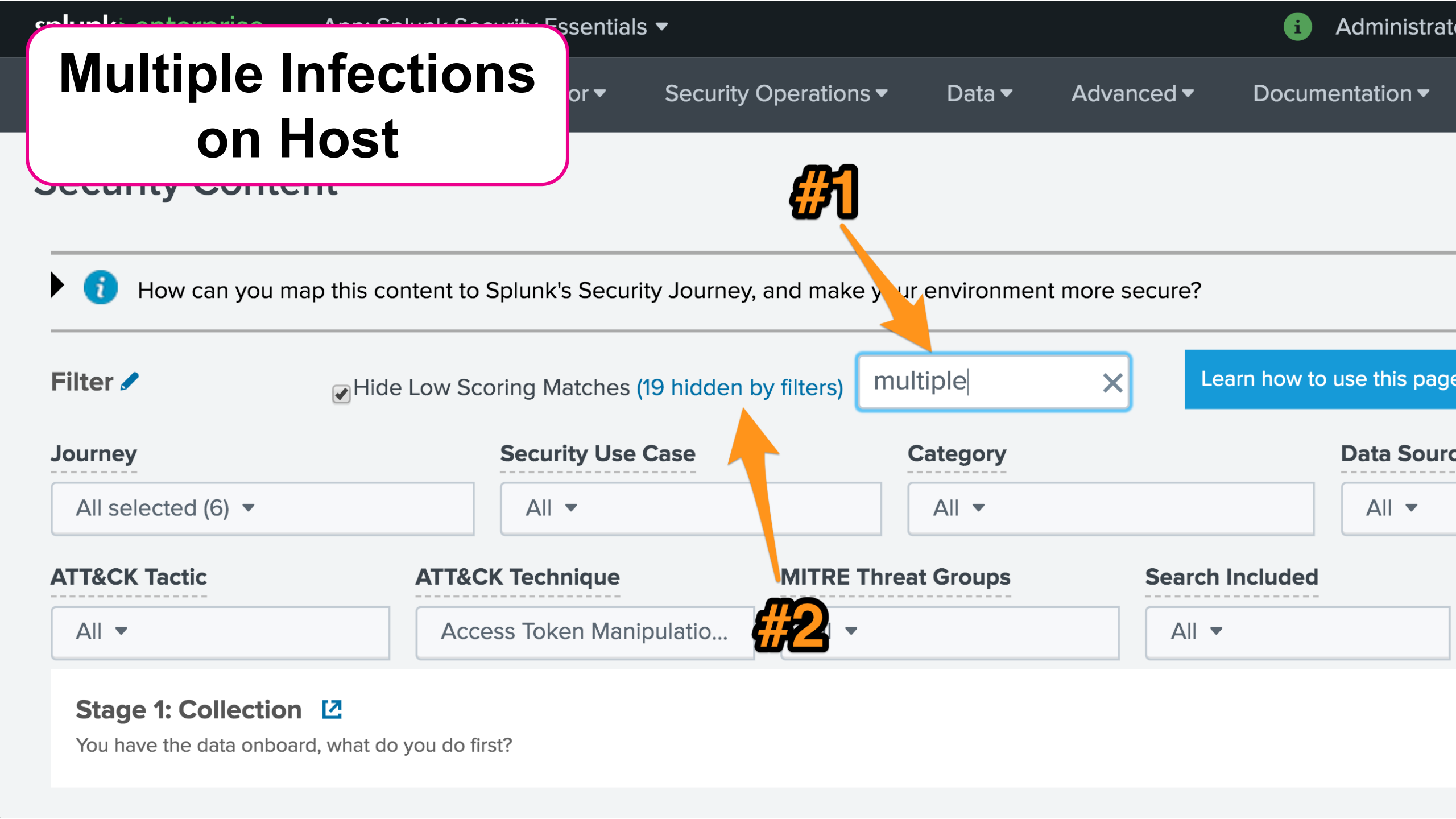
© 2019 SPLUNK INC.

… but can you deploy a real detection?




splunk>enterprise
App: Splunk Security Essentials
Home
Security Content
Analytics Advisor
Security Operations
Dat
Security Content
Overview
Manage Bookmarks
Custom Content
MITRE ATT&CK-Driven Content Recommendation
Risk-based Alerting Content Recommendation
ou will find the primary areas where Splunk
. The goal of this free app is to help you be
nswers
. Happy Splunking!
Learn

Multiple Infections on Host



Multiple Infections on Host

Security Journey, and make your environment more secure?

Hide Low Scoring Matches

multiple

Learn how to use this page

Journey: All selected (6)

Security Use Case: All

Category: All

Data Sourc: All

ATT&CK Tactic: All

ATT&CK Technique: All

MITRE Threat Groups: All

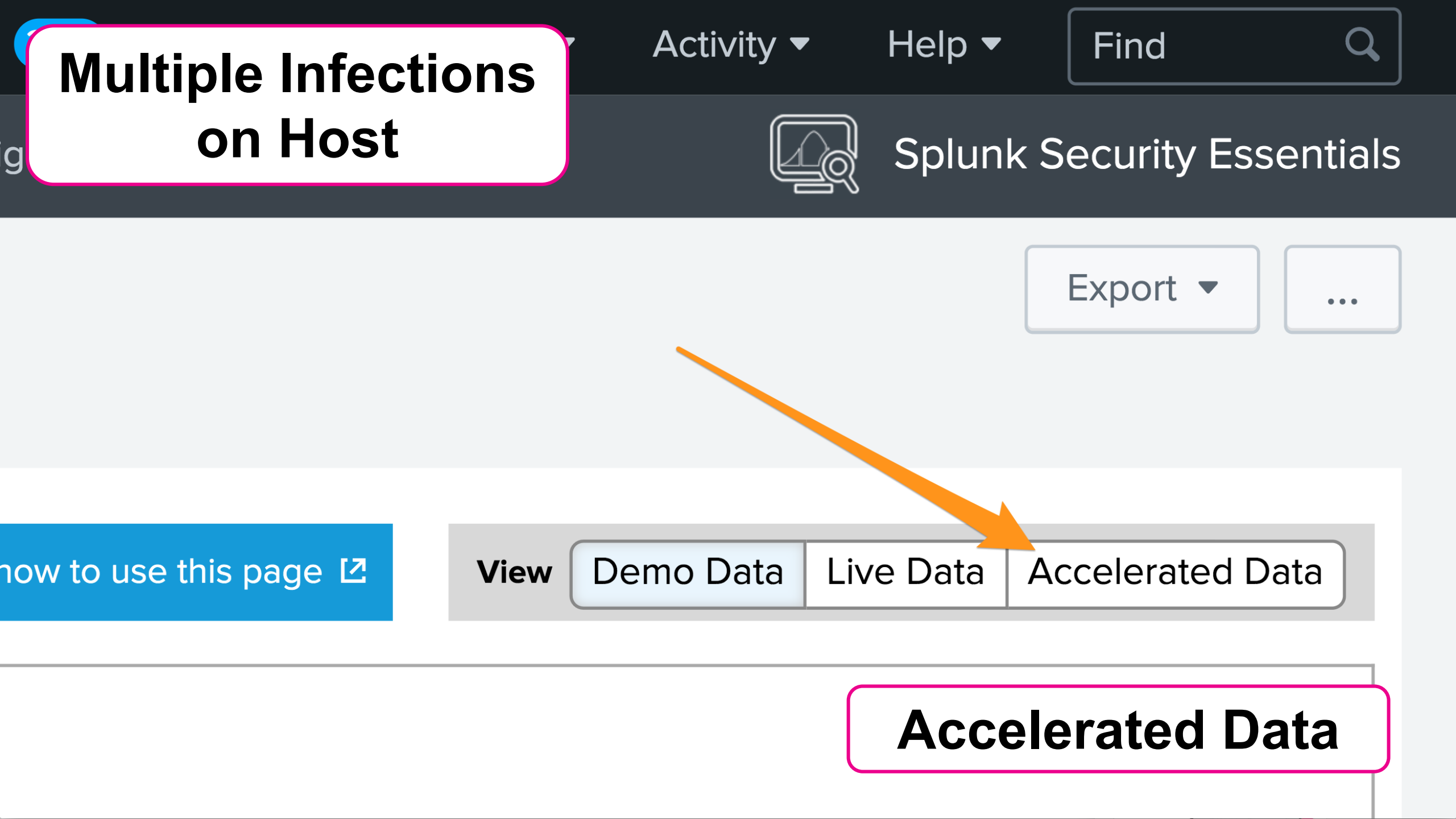
Search Included: All

Stage 1: Collection

You have the data onboard, what do you do first?

Multiple Infections on Host

Finds hosts that have logged multiple different infections in a short period of time.


Multiple Infections on Host
Activity
Help
Find
Splunk Security Essentials
Export
...
how to use this page
View
Demo Data
Live Data
Accelerated Data
Accelerated Data

Multiple Infections on Host (Accelerated Data)

Kill Chain Phases

ces

r Anti-Malware

Data Check	Status	Open in Search	Resolution (if needed)
Must have accelerated data in your Malware Data Model	✓	Open in Search	Add data to the Malware Data Model using the Technology Add-on for your anti-malware product (look on Splunkbase) and then accelerate that data model.

Schedule in ES

Enter a search

```
| tstats summariesonly=t allow_old_summaries=t count values(Malware_Attacks.signature) as signature values(Malware_Attacks.category) as category values(Malware_Attacks.action
    ) as action from datamodel=Malware by _time span=1m Malware_Attacks.dest
| rename Malware_Attacks.* as *
| transaction maxpause=1h dest
| where eventcount >=3 AND duration>240
```

All time

✓ 21 events (1/1/70 12:00:00.000 AM to 10/17/19 6:05:40.000 AM)

Job ▾ Smart Mode ▾

Detect New Values | Line-by-Line SPL Documentation

Schedule in ES

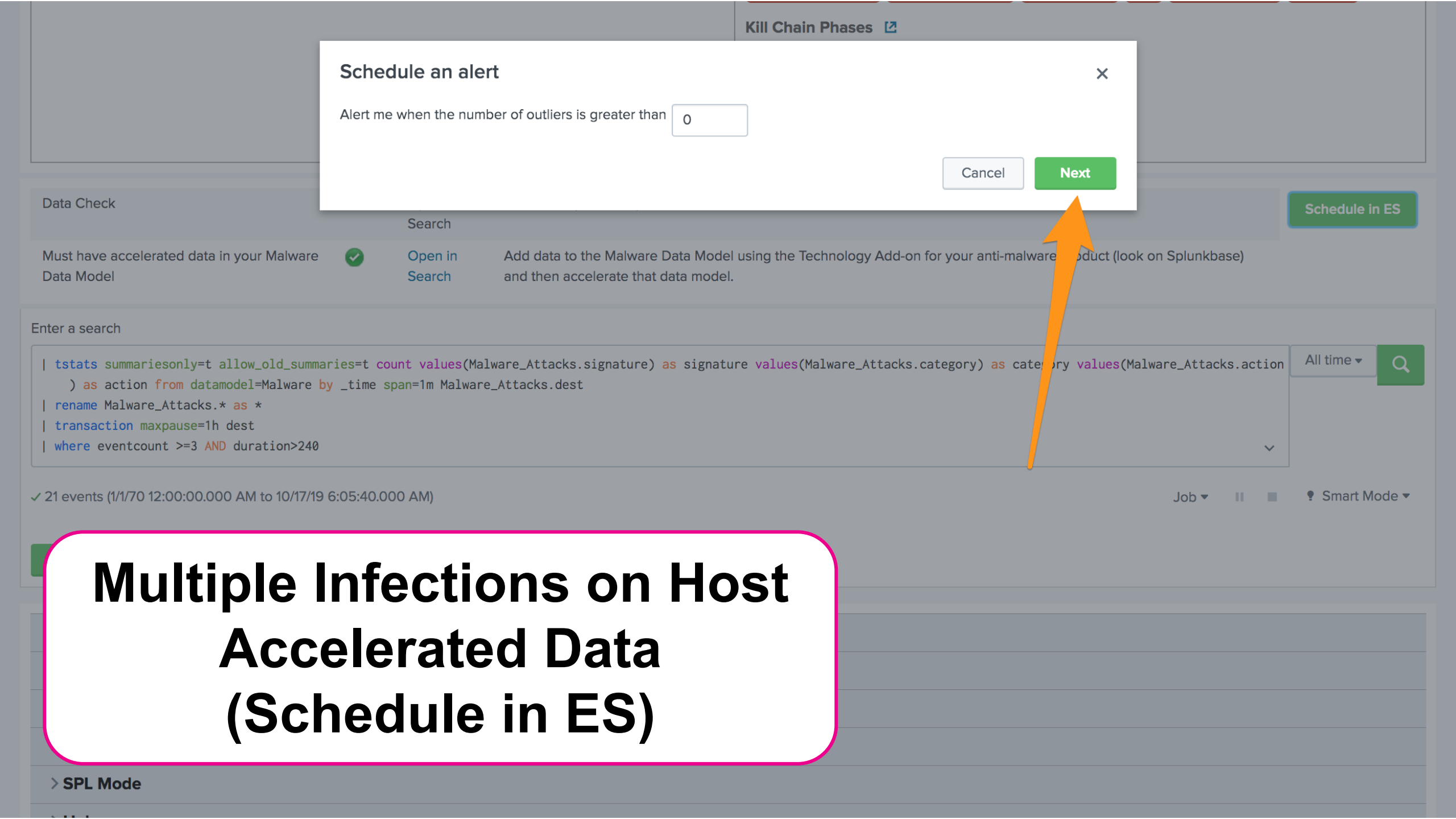
> Recommended Phantom Playbooks

> How to Implement

> Known False Positives

> How To Respond

> SPL Mode



Multiple Infections on Host Accelerated Data (Schedule in ES)

Kill Chain Phases

Data Check

Must have accelerated data in your Malware Data Model

Enter a search

```
| tstats summariesonly=t allow_old_summ
    ) as action from datamodel=Malware
| rename Malware_Attacks.* as *
| transaction maxpause=1h dest
| where eventcount >=3 AND duration>240
```

✓ 21 events (1/1/70 12:00:00.000 AM to 10/17/19

Detect New Values | Line-by-Line SPL D

alware_Attacks.action | All time | Job | Smart Mode

> Recommended Phantom Playboo
> How to Implement
> Known False Positives
> How To Respond
> SPL Mode

Save As Alert

Settings

Search: | tstats summariesonly=t allow_old_summaries=t count values(Malware_Attacks.signature) as signature values(Malware_Attacks.category) as

Title: Multiple_Infections_on_Host David

Description: Generated by the Splunk Security Essentials app at Thu, 17 Oct 2019 06:08:30 GMT

Alert type: Scheduled | Real-time

Run on Cron Schedule

Time Range: All time

Cron Expression: 37 1 * * *

e.g. 00 18 *** (every day at 6PM). Learn More

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Number of Results

Cancel | Save

Add Your Name (Avoid Duplicates)

Kill Chain Phases

Data Check

Schedule in ES

Must have accelerated data in your Malware Data Model

k on Splunkbase)

Enter a search

```
| tstats summariesonly=t allow_old_summ
    ) as action from datamodel=Malware
| rename Malware_Attacks.* as *
| transaction maxpause=1h dest
| where eventcount >=3 AND duration>240
```

alware_Attacks.action

All time

✓ 21 events (1/1/70 12:00:00.000 AM to 10/17/19

Job

Smart Mode

Detect New Values

Line-by-Line SPL D

Recommended Phantom Playboo

How to Implement

Known False Positives

How To Respond

SPL Mode

Alert has been saved

You can view your alert, or continue editing it.

Enabling ES Correlation Search

ES Correlation Search Enabled! We recommend you click here to continue editing the Notable Event to customize the display fields.

Continue Editing

View Alert



Administrator 336 Messages Settings Activity Help Find

Audit Search Configure Enterprise Security

-down search in a notable event or links in an

Essentials app at Thu, 17 Oct 2019

Manual

_summaries=t count
as signature
as category
action from datamodel=Malware by
est

Back to Content Management Save

© 2019 SPLUNK INC.

You've Now Checked Your Data Latency

You've At Least Identified Missing CIM Fields

You've Pushed MITRE ATT&CK to ES

You've Analyzed High Risk Entities

You've Enabled New Detections

I Bet You Feel Pretty Great!

© 2019 SPLUNK INC.

But How Will You Make This Guy Happy?



© 2019 SPLUNK INC.

Measure Success

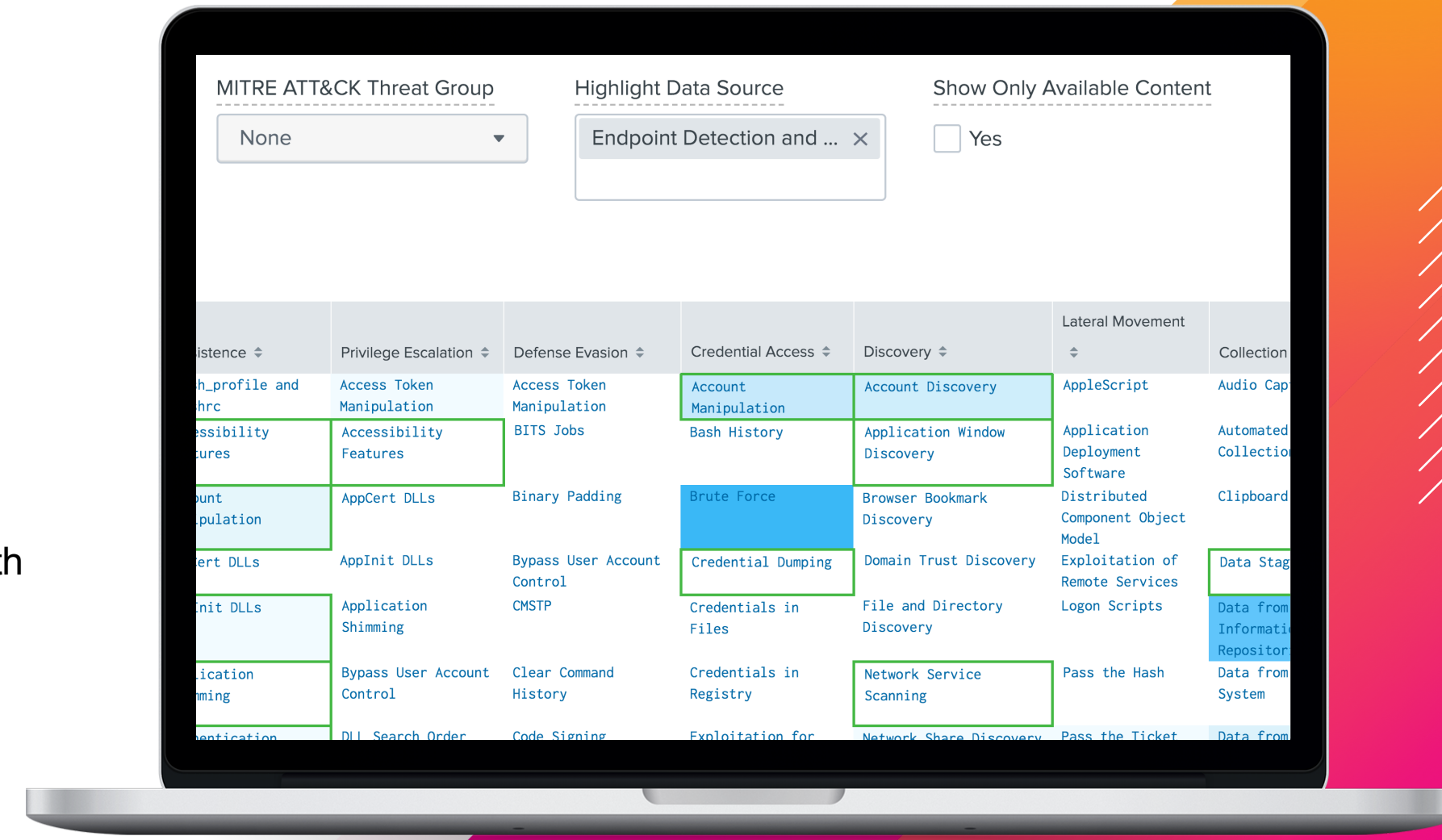


.conf19

splunk>

Justify New Data

Show what industry-standard capabilities you would have with new data onboard



© 2019 SPLUNK INC.

splunk> turn data into doing

© 2019 SPLUNK INC.

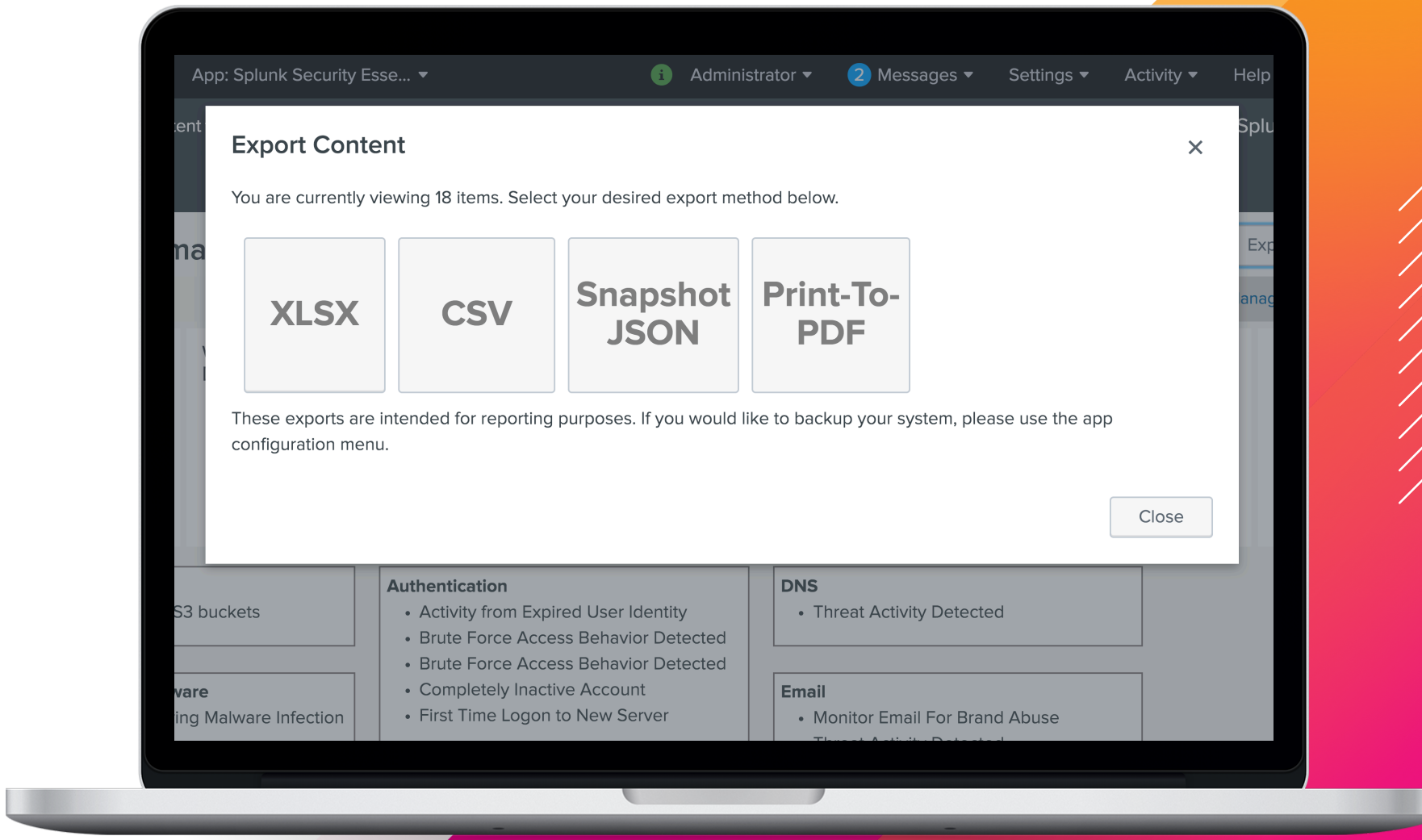


Make Auditors Happy with Excel or PDF Exports of your Enabled Content

splunk> turn data into doing

Export Enabled or Bookmarked Content

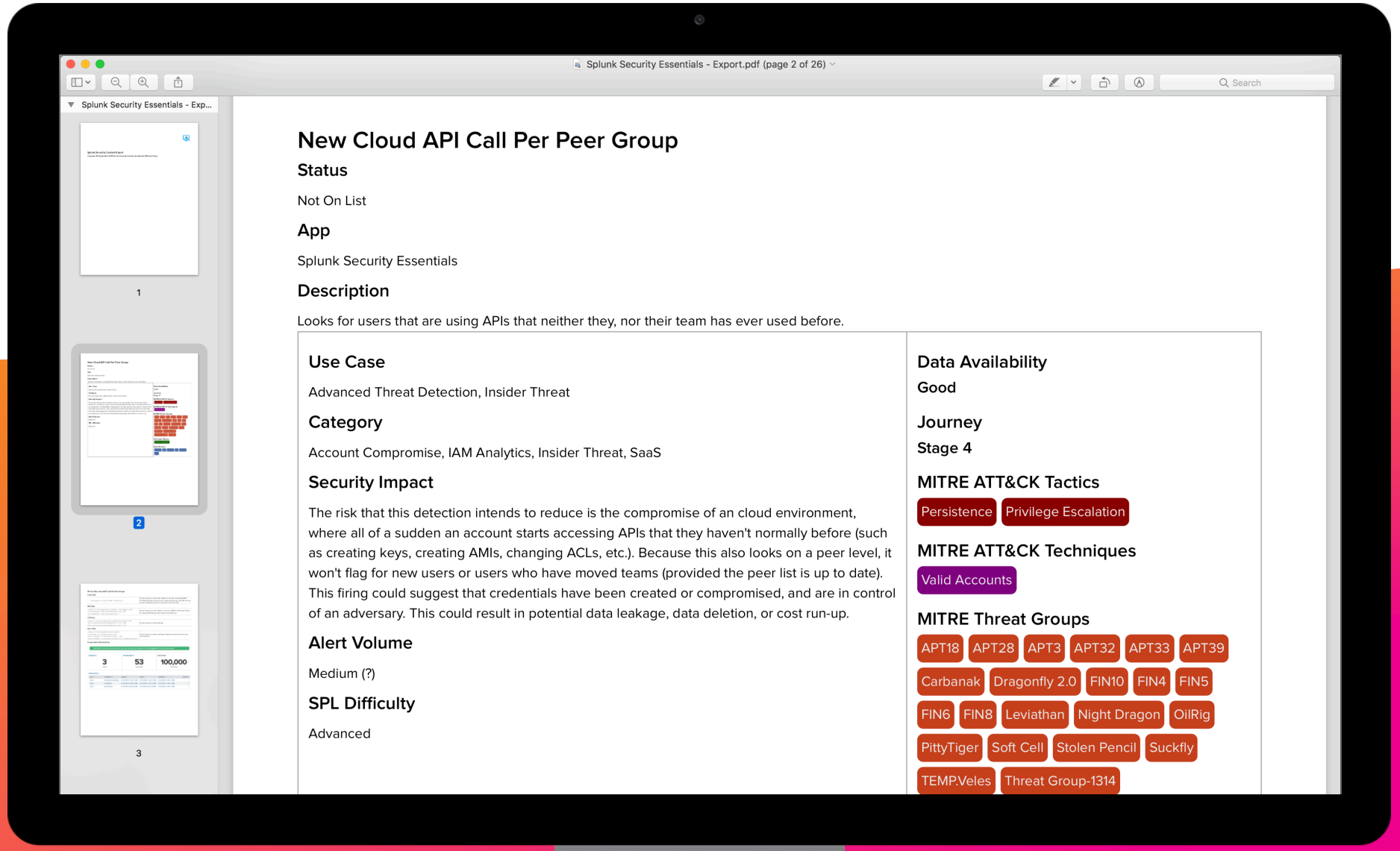
Generate dense Excel docs, or descriptive PDF exports that can include screenshots, SPL, and your deployment notes



splunk> turn data into doing

© 2019 SPLUNK INC.

© 2019 SPLUNK INC.



splunk> turn data into doing

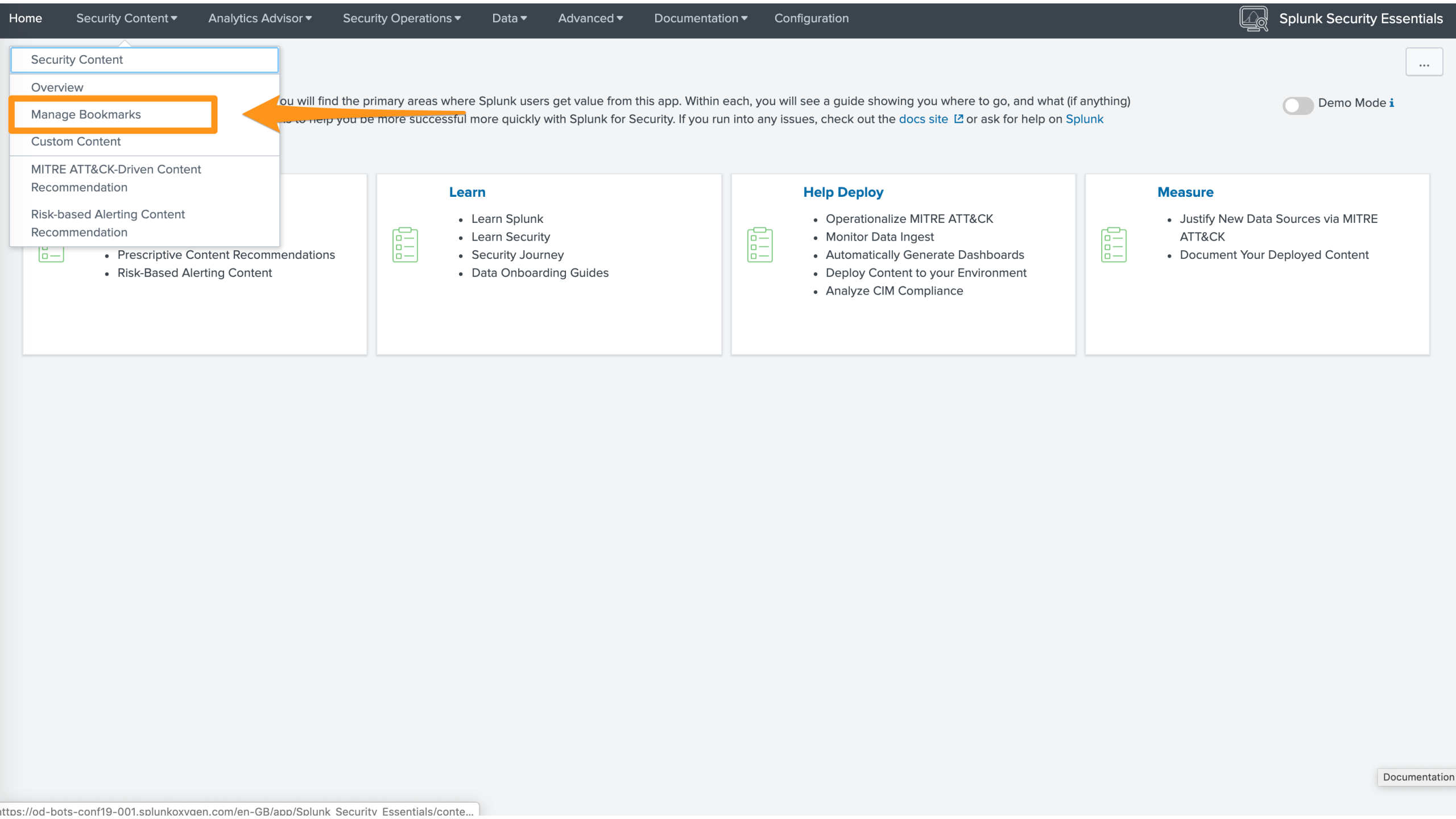
© 2019 SPLUNK INC.

Hands-On



.conf19

splunk>


Home
Security Content
Analytics Advisor
Security Operations
Data
Advanced
Documentation
Configuration
Splunk Security Essentials
Security Content
Overview
Manage Bookmarks
Custom Content
MITRE ATT&CK-Driven Content Recommendation
Risk-based Alerting Content Recommendation
...
ou will find the primary areas where Splunk users get value from this app. Within each, you will see a guide showing you where to go, and what (if anything)
is to help you be more successful more quickly with Splunk for Security. If you run into any issues, check out the docs site or ask for help on Splunk
Demo Mode
Prescriptive Content Recommendations
Risk-Based Alerting Content
Learn
Learn Splunk
Learn Security
Security Journey
Data Onboarding Guides
Help Deploy
Operationalize MITRE ATT&CK
Monitor Data Ingest
Automatically Generate Dashboards
Deploy Content to your Environment
Analyze CIM Compliance
Measure
Justify New Data Sources via MITRE ATT&CK
Document Your Deployed Content
Documentation

© 2019 SPLUNK INC.

Manage Bookmarks

Export ... Correlation Search Introspection Manage List Add Bookmark

Bookmarked	Waiting on Data	Ready For Deployment	Implementation Issues	Needs Tuning	Fully Implemented	Custom
37	0	0	0	0	37	0

AWS
- AWS Config Violation
- AWS Guard Duty Alert
- Detect New Open S3 buckets
- Many Unauthorized AWS Operations

Anti-Virus or Anti-Malware
- Host With A Recurring Malware Infection
- RR - Command and Control Activity Detected - Combined
- RR - Credential Theft Tool Detected - Combined
- RR - Discovery tool or technique detected - Combined
- RR - Malware detected by Windows Defender - Combined
- RR - Suspicious CLI command related to information gathering - Combined
- RR - Suspicious service or registry change detected - Combined
- RR - Suspisious Process or DLL detected - Combined

Audit Trail
- AWS Config Violation
- AWS Guard Duty Alert
- Detect New Open S3 buckets
- Many Unauthorized AWS Operations

Authentication
- Activity from Expired User Identity
- Brute Force Access Behavior Detected

DNS
- Detect hosts connecting to dynamic domain providers
- RR - DDNS Activity Detected - System
- Threat Activity Detected

Email
- Monitor Email For Brand Abuse
- Threat Activity Detected

Endpoint Detection and Response
- Create local admin accounts using net.exe
- Indicator of mimikatz Activity
- Malicious PowerShell Process - Encoded Command
- Prohibited Process Detected
- RR - Process Discrepancy Detected - System
- RR - Suspicious CLI command - Combined
- RR - Suspicious activity or known framework detected - Combined
- RR - Suspicious activity related to escalation of privs has been detected - Combined
- RR - USB Insertion with 1st time seen Serial Number - Combined
- RR - USB Insertion with 1st time seen Vendor ID - Combined
- Suspicious wevtutil Usage
- Threat Activity Detected

IDS or IPS
- Vulnerability Scanner Detected (by targets)

Web Proxy
- Threat Activity Detected

Windows Security

Documentation

Manage Bookmarks

Export | ...

elation Search Introspection | Manage List | Add Bookmark

Bookmarked	Waiting on Data	nplemented	Custom
37	0	37	0

AWS
- AWS Config Violation
- AWS Guard Duty Alert
- Detect New Open S3 buckets
- Many Unauthorized AWS Operations

Anti-Virus or Anti-Malware
- Host With A Recurring Malware Infection
- RR - Command and Control Activity Detected - Combined
- RR - Credential Theft Tool Detected - Combined
- RR - Discovery tool or technique detected - Combined
- RR - Malware detected by Windows Defender - Combined
- RR - Suspicious CLI command related to information gathering - Combined
- RR - Suspicious service or registry change detected - Combined
- RR - Suspisious Process or DLL detected - Combined

Audit Trail
- AWS Config Violation
- AWS Guard Duty Alert
- Detect New Open S3 buckets
- Many Unauthorized AWS Operations

Authentication
- Activity from Expired User Identity
- Brute Force Access Behavior Detected

DNS
- Detect hosts connecting to dynamic domain providers
- RR - DDNS Activity Detected - System
- Threat Activity Detected

Email
- Monitor Email For Brand Abuse
- Threat Activity Detected

Endpoint Detection and Response
- Create local admin accounts using net.exe
- Indicator of mimikatz Activity
- Malicious PowerShell Process - Encoded Command
- Prohibited Process Detected
- RR - Process Discrepancy Detected - System
- RR - Suspicious CLI command - Combined
- RR - Suspicious activity or known framework detected - Combined
- RR - Suspicious activity related to escalation of privs has been detected - Combined
- RR - USB Insertion with 1st time seen Serial Number - Combined
- RR - USB Insertion with 1st time seen Vendor ID - Combined
- Suspicious wevtutil Usage
- Threat Activity Detected

IDS or IPS
- Vulnerability Scanner Detected (by targets)

Web Proxy
- Threat Activity Detected

Windows Security

Export Content

You are currently viewing 37 items. Select your desired export method below.

XLSX | CSV | Snapshot JSON | Print-To-PDF

Close

Manage Bookmarks

Export | ...

Correlation Search Introspection | Manage List | Add Bookmark

Bookmarked	Waiting on Data	Ready F... Deployr...	Fully Implemented	Custom
37	0		37	0

AWS
- AWS Config Violation
- AWS Guard Duty Alert
- Detect New Open S3 buckets
- Many Unauthorized AWS Operations

Anti-Virus or Anti-Malware
- Host With A Recurring Malware Infection
- RR - Command and Control Activity Detected - Combined
- RR - Credential Theft Tool Detected - Combined
- RR - Discovery tool or technique detected - Combined
- RR - Malware detected by Windows Defender - Combined
- RR - Suspicious CLI command related to information gathering - Combined
- RR - Suspicious service or registry change detected - Combined
- RR - Suspisious Process or DLL detected - Combined

AWS
- AWS Config Violation
- AWS Guard Duty Alert
- Detect New Open S3 buckets
- Many Unauthorized AWS Operations

Authentication
- Activity from Expired User Identity
- Brute Force Access Behavior Detected

DNS
- Detect hosts connecting to dynamic domain providers
- RR - DDNS Activity Detected - System
- Threat Activity Detected

- Monitor Email For Brand Abuse
- Threat Activity Detected

Endpoint Detection and Response
- Create local admin accounts using net.exe
- Indicator of mimikatz Activity
- Malicious PowerShell Process - Encoded Command
- Prohibited Process Detected
- RR - Process Discrepancy Detected - System
- RR - Suspicious CLI command - Combined
- RR - Suspicious activity or known framework detected - Combined
- RR - Suspicious activity related to escalation of privs has been detected - Combined
- RR - USB Insertion with 1st time seen Serial Number - Combined
- RR - USB Insertion with 1st time seen Vendor ID - Combined
- Suspicious wevtutil Usage
- Threat Activity Detected

IDS or IPS
- Vulnerability Scanner Detected (by targets)

Web Proxy
- Threat Activity Detected

Windows Security

Choose Content to Include

In addition to the key default descriptions and tags, choose additional content you'd like to include in the export:

- [x] Bookmark Details
- [x] SPL (where available)
- [x] Demo Screenshots (where available)
- [x] Enhance Color (uncheck for black-and-white printing)

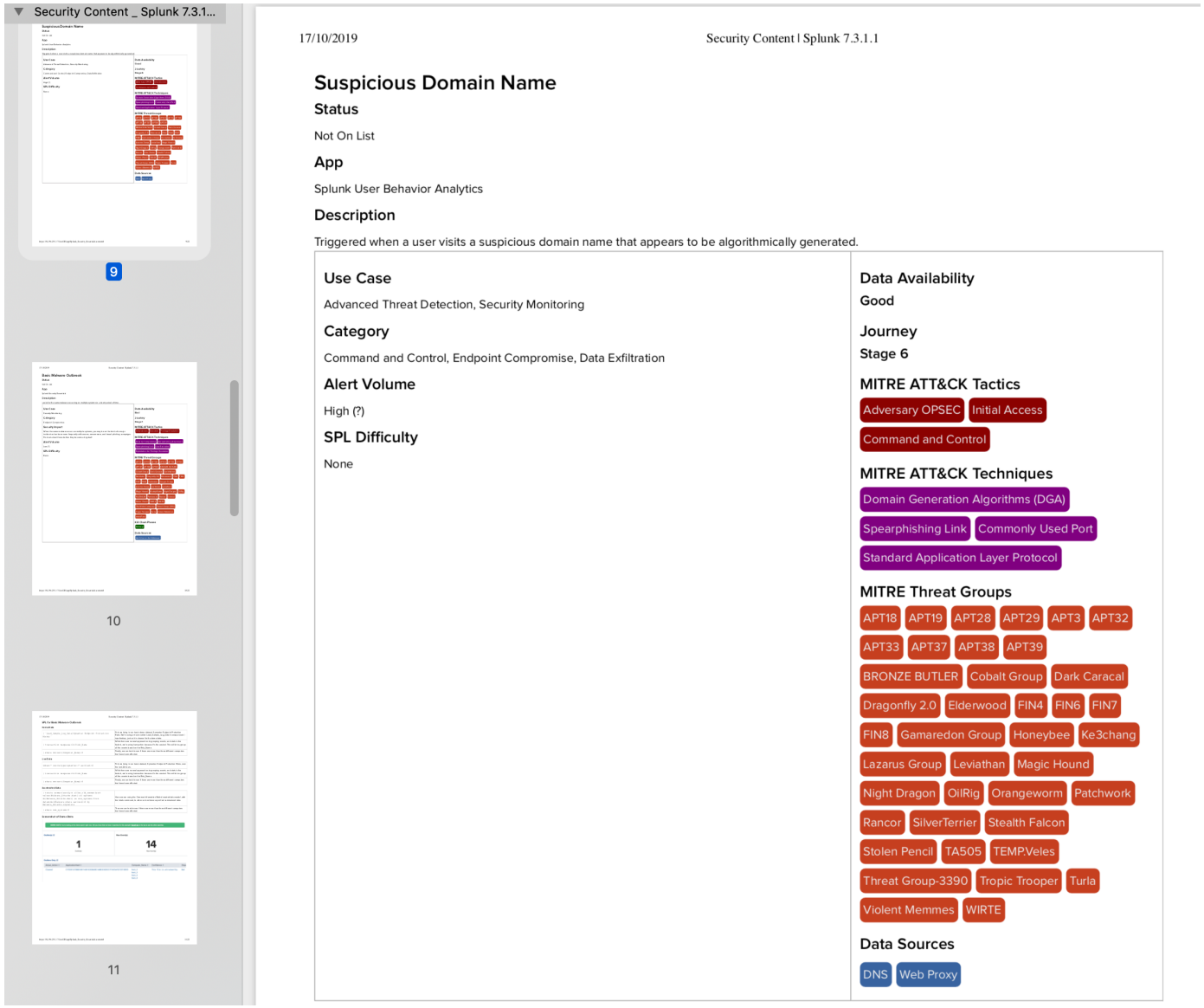
Note: printed or PDF-exported documents look best when generated with Google Chrome.

Generate

© 2019 SPLUNK INC.

PDF Export

Includes status, screenshots, SPL, and your deployment notes



splunk> .conf19

© 2019 SPLUNK INC.

Next Steps



.conf19

splunk>

© 2019 SPLUNK INC.

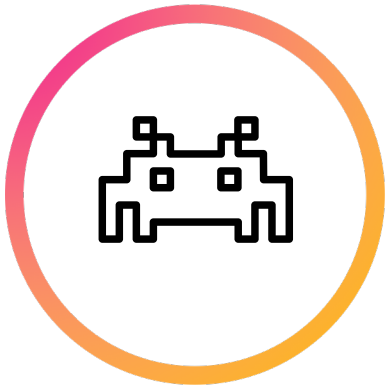
Splunk Security Essentials is the free Splunk app that makes security easier.

© 2019 SPLUNK INC.

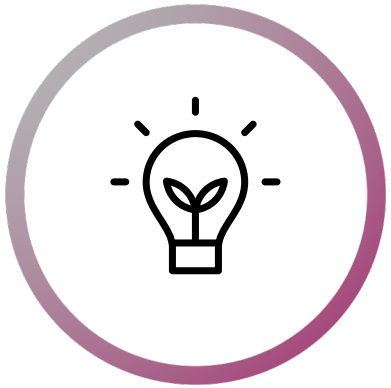
Four Pillars

Four ways in which SSE has delivered value to users

Finding Content



Learning Splunk Security



Improve Production



Measure Your Success



© 2019 SPLUNK INC.

Testimonials

"I got the security essentials tool loaded and did a basic overview with the SOC. They lit up like christmas trees."

Security Tools Engineer, Fortune 100 Healthcare

"I can take the content library off my list of projects for this year. It's already built! "

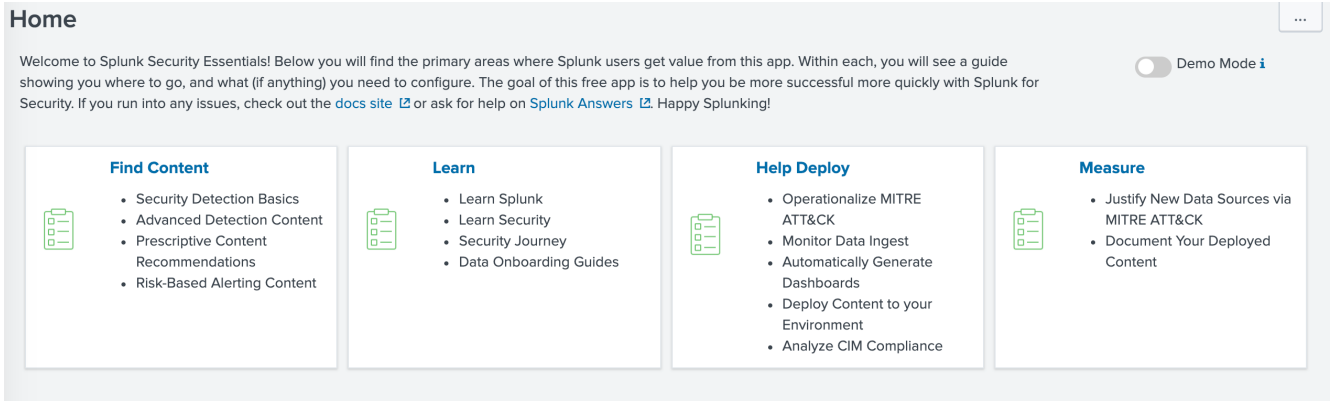
Director of Security, Small Financial Services

© 2019 SPLUNK INC.

Key Takeaways

Security Essentials helps you in multiple ways.

1. Security Essentials has evolved to being a key app for Splunk in security.
2. Helps you operationalize and measure the content you are deploying.
3. New app guide helps you choose your adventure.

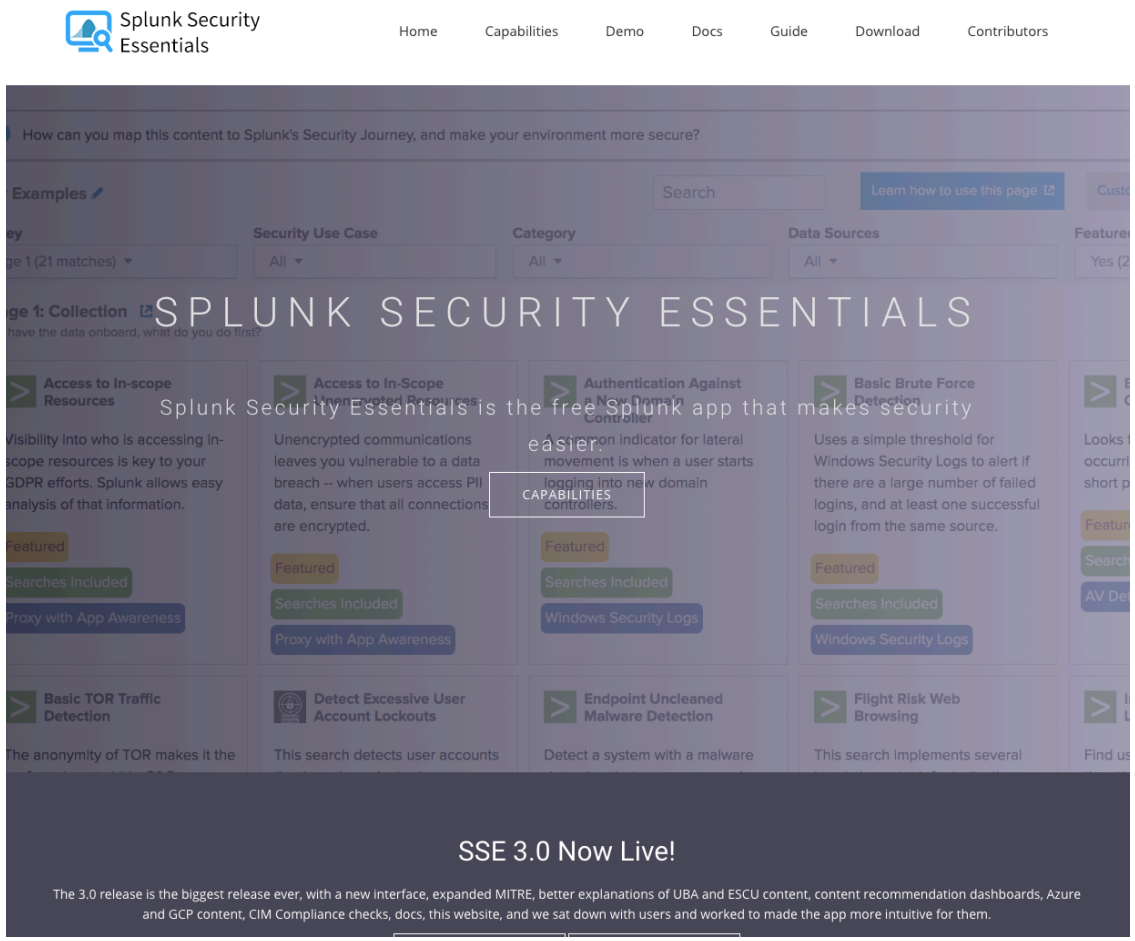


splunk> .conf19

© 2019 SPLUNK INC.

Security Essentials now has it's own website

Contains all content, documentation and an online demo environment.



https://www.splunksecurityessentials.com

splunk> .conf19

© 2019 SPLUNK INC.



Visit the Security Essentials booth at **source=*Pavilion** to see everything in action.

© 2019 SPLUNK INC.

Please rate this talk!

© 2019 SPLUNK INC.



splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION