



Quickly Advance Your Security Posture With Splunk Security Essentials

David Veuve | Principal Security Strategist

September 2017 | Washington, DC



Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. 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 functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, 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. © 2017 Splunk Inc. All rights reserved.

Personal Introduction

- ▶ **David Veuve**
Principal Security Strategist, Splunk
- ▶ SME for UEBA, Security, Architecture
- ▶ dveuve@splunk.com
- ▶ Former Splunk Customer
- ▶ Primary author of the Splunk Security Essentials app

▶ 2017 Talks:

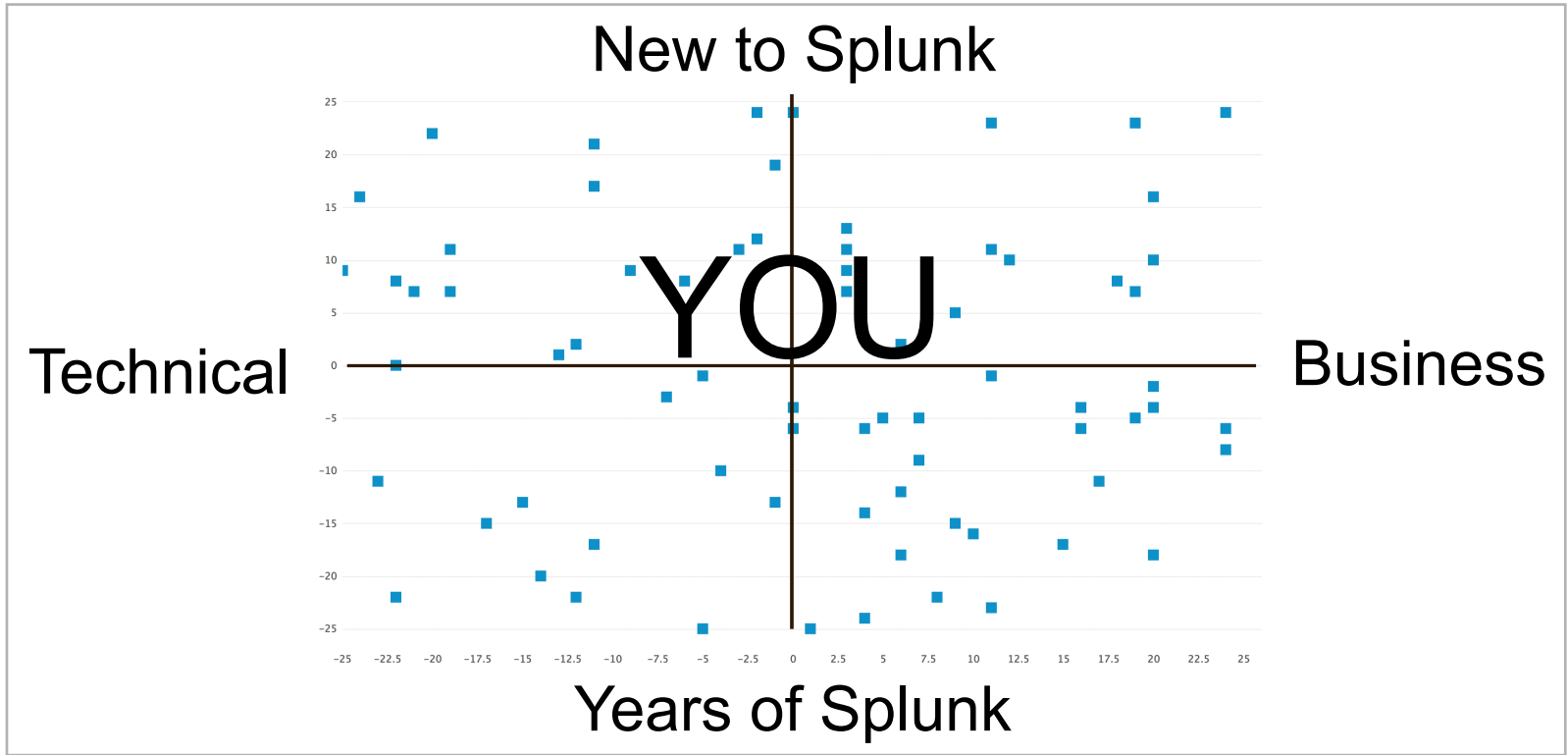
- Security Ninjutsu Part Four (Hi!)
- Searching FAST: Start Using tstats and other acceleration techniques
- Quickly Advance Your Security Posture with Splunk Security Essentials

▶ Prior Conf Talks:

- How to Scale Search from _raw to tstats
- Security Ninjutsu Part Three: .conf2016
- Security Ninjutsu Part Two: .conf 2015
- Security Ninjutsu Part One: .conf 2014
- Passwords are for Chumps: .conf 2014

Who Are You?

- ▶ Maybe a user of Splunk Security Essentials?
- ▶ All Levels of Splunk Experience
- ▶ Probably like Security



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1
10.2.1.1:5V1: - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03"
10.2.1.1:5V1: - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1

What Will You Get?

- ▶ Detect things better
- ▶ Learn about powerful free apps
- ▶ Only One Marketing Slide!

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K0-CU-01"
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-148"
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-5W-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D55L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=K0-CU-01"
137.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-148"

Agenda

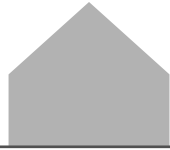
1. Splunk Security Essentials Overview
2. SSE Demo
3. End to End Scenario
4. Wrap Up



Splunk Security Essentials Overview

Technical Components for Successful Security Analytics

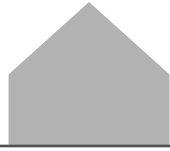
Alert Aggregation



Threat Detection

- ▶ Manage High Volume
- ▶ Track Entity Relationships
- ▶ Combination ML + Rules

Alert Creation



Simpler Detection

- ▶ Rules & Statistics
- ▶ Quick development
- ▶ Easy for analysts

ML Based Detection

- ▶ Detect unknown
- ▶ New vectors
- ▶ Heavy data science

Investigation

Investigative Platform

- ▶ Analyst Flexibility
- ▶ Provide access to data analysis solutions
- ▶ Record historical context for everything

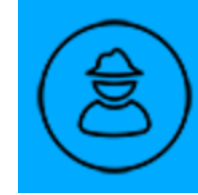
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15L9FF1ADFF3 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-5W-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.10.10.10

The Splunk Portfolio

Splunk Premium Solutions



Rich Ecosystem of Apps & Add-Ons



splunk > enterprise

splunk > cloud

splunk > Platform for Operational Intelligence



Mobile



IoT Devices



Network Wire Data



Hadoop



Relational Databases



Mainframe Data





Splunk Security Essentials

<https://splunkbase.splunk.com/app/3435/>

► Identify bad guys:

- 50+ use cases common in Security Analytics products, free on Splunk Enterprise
- Target external and insider threats
- Scales from small to massive companies
- Save from app, send hits to ES/UBA

Solve use cases you can today for free, then use Splunk UBA for advanced ML detection.

The screenshot displays the Splunk Security Essentials app interface. The top navigation bar includes 'Introduction', 'Use Cases', 'Assistants', 'Search', and 'Setup'. Below the navigation, there are tabs for 'All Examples (47 examples)', 'Access Domain (11 examples)', 'Data Domain (6 examples)', 'Endpoint Domain (20 examples)', 'Network Domain (9 examples)', and 'Threat Domain (3 examples)'. The main content area is titled 'Highlights' and features several use case cards, each with a small chart and a description:

- Authentication Against a New Domain Controller**: A common indicator for lateral movement is when a user starts logging into new domain controllers. Alert Volume: Medium. Examples: Demo Data, Live Data.
- Concentration of Hacker Tools by Filename**: It's uncommon to see filenames associated with attacker tools used in rapid succession on an endpoint. The first time, it's probably fine. The fourth or fifth file used should be suspicious. (MITRE CAR Reference). Alert Volume: Low. Examples: Demo Data, Live Data.
- Detect Data Exfiltration**: Find users who are exfiltrating data. Alert Volume: High. Examples: Demo Data, Accelerated Data.
- First Time Accessing a Git Repository**: Find users who accessed a git repository for the first time. Alert Volume: High. Examples: Demo Data, Live Data, Accelerated Data.
- First Time Accessing a Git Repository Not Viewed by Peers**: Find users who accessed a git repository for the first time, where their peer group also hasn't accessed it before. Alert Volume: Medium. Example: Demo Data.
- First Time Logon to New Server**: Find users who logged into a new server for the first time. Alert Volume: Very High. Examples: Demo Data, Live Data, Accelerated Data.
- Healthcare Worker Opening More Patient Records Than Usual**: If a healthcare worker (or someone associated, such as a DBA) views more patient records than normal, or more than their peers, then it could be a sign that their system is infected, or that they are exfiltrating patient data. Alert Volume: Low. Examples: Demo Data, Live Data.
- Increase in Pages Printed**: Find users who printed more pages than normal. Alert Volume: Medium. Examples: Demo Data, Live Data, Accelerated with Data Models.
- Anomalous New Listening Port**: New listening ports can be a sign of malware persistence, so detect them in your data! Alert Volume: Medium.
- Concentration of Discovery Tools by Filename**: It's uncommon to see filenames associated with host discovery tools used in rapid succession on an endpoint, except in very specific situations. The first time, it's probably fine. The fourth or fifth file used should be suspicious. (MITRE CAR Reference).

What about...

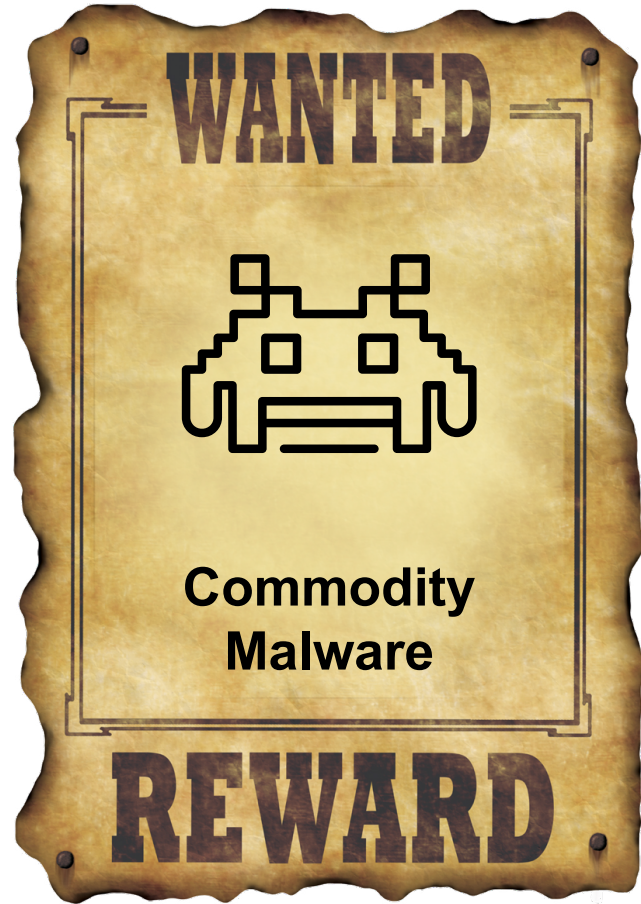
► Ransomware?

► Fraud?



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=5D15LAF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=5D95L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0
317.27.160.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D18SLBFF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0
189] "GET /cart.do?action=changequantity&itemId=EST-6&JSESSIONID=5D18SLBFF2ADFF9 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0
187] "GET /oldlink?item_id=EST-26&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=5D18SLBFF2ADFF9 HTTP 1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0
188] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0
189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0
188] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0
189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 3885 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" "0

What Can I Detect With Splunk Enterprise?



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD35L7FFGADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CW-01"
317.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FFIADFF3"
10.55.187.1 - [07/Jan 18:10:56:189] "GET /cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FFIADFF3"
10.55.187.1 - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FFIADFF3"
10.55.187.1 - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FFIADFF3"
10.55.187.1 - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FFIADFF3"
10.55.187.1 - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FFIADFF3"
10.55.187.1 - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FFIADFF3"
10.55.187.1 - [07/Jan 18:10:56:189] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD5SL9FFIADFF3 HTTP 1.1" 200 385 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL9FFIADFF3"

Splunk Security Essentials App Inventory

DOMAINS

- Access
- Data
- Endpoint
- Network
- Threat

DATA SOURCES

- Any Host Logs
- Electronic Medical Record System
- Email Logs
- Firewall
- Netflow
- Print Server Logs
- Salesforce Event Log File
- Source Code Repository Logs
- Splunk Notable Events

ALERT VOLUME

- Very Low
- Low
- Medium
- High
- Very High

“Say, aren’t those all recommended data sources for Splunk Security in general?”

Splunk Security Essentials

Types of Use Cases

Outlier(s)

2 Outlier(s)

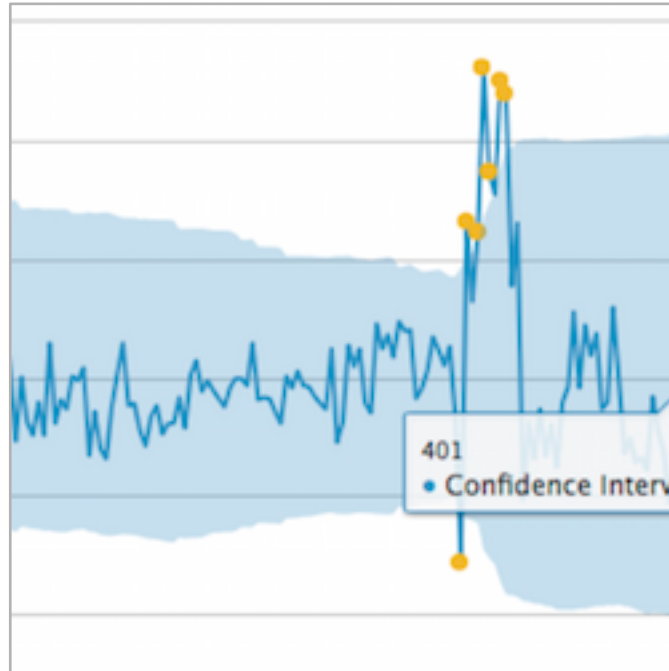
Raw Data and Outlier status

Year	Contract_interest_rate(%)	Initial_fees_and_charges(%)	
1981	14.85	2.57	15.40
1982	15.42	2.82	16.04
1978	8.51	0.46	8.58
1979	9.56	0.49	9.65
1980	12.06	1.23	12.33
1983	12.31	3.07	12.90
1984	11.84	3.35	12.48
1985	11.15	2.72	11.65
1986	9.79	2.21	10.18
1987	8.58	2.01	8.91

Dataset Preview

Adjustable_rate_loans(%)	Contract_interest_rate(%)
NA	8.51

First Time Seen
powered by stats



Time Series Analysis with
Standard Deviation

splunk> App: Splunk Security Essentials

Introduction Use Cases Assistants

Search

enter search here...

No Event Sampling v

General Security Analytics
Searches

Getting Started with Splunk Security Essentials

- ▶ Download from apps.splunk.com
- ▶ Browse use cases that match your needs
- ▶ Data Source Check shows other use cases for your existing data
- ▶ Evaluate free tools to meet gaps, such as Microsoft Sysmon
 - (links inside the app)

Use Case	Demo Data	Live Data	Accelerated Data
First Time Accessing a Git Repository	✓	!	!
First Time USB Usage	✓	!	!
First Time Logon to New Server	✓	✓	✓
Increase in # of Hosts Logged into	✓	✓	NA
Increase in Pages Printed	✓	!	NA
Increase in Source Code (Git) Downloads	✓	!	NA
Find Unusually Long CLI Commands	✓	!	NA
Processes with High Entropy Names	✓	✓	NA
Authentication Against a New Domain Controller	✓	!	NA
New Parent Process for cmd.exe or regedit.exe	✓	!	NA
Find Processes with Renamed Executables	✓	!	NA
Source IPs Communicating with Far More Hosts Than Normal	✓	✓	✓
New AD Domain Detected	✓	✓	NA
New Host with Suspicious cmd.exe / regedit.exe / powershell.exe Service Launch	✓	!	NA
New Path for a Common Filename with Process Launch	✓	✓	NA
Healthcare Worker Opening More Patient Records Than Usual	✓	!	NA
Remote PowerShell Launches	✓	✓	NA
Concentration of Hacker Tools by Filename	✓	✓	NA
Concentration of Hacker Tools by SHA1 Hash	✓	!	NA
Concentration of Discovery Tools by Filename	✓	✓	NA
Concentration of Discovery Tools by SHA1 Hash	✓	!	NA
Sources Sending Many DNS Requests	✓	✓	✓
Sources Sending a High Volume of DNS Traffic	✓	✓	✓
New Service Paths for Host	✓	✓	NA
New Suspicious Executable Launch for User	✓	✓	NA

Demo Scenario

Apply Splunk to Real Life Scenario

- ▶ **Actor:**
Malicious Insider (because it's hardest)
- ▶ **Motivation:**
Going to work for competitor
- ▶ **Target:**
Accounts, Opportunities, Contacts in Salesforce
- ▶ **Additional Target:**
Sales Proposals in Box
- ▶ **Exfiltration:**
Upload to a remote server

Malicious Insider



Chris Geremy
Director of Finance

** Photo of Splunker, I promise she is not a malicious insider*

Set Up Monitoring

▶ Ingest Salesforce Event Log File

- <https://splunkbase.splunk.com/app/1931/>

▶ Ingest Box Data

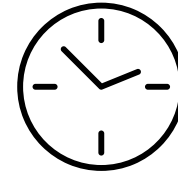
- <https://splunkbase.splunk.com/app/2679/>

▶ Install Splunk Security Essentials

- <https://splunkbase.splunk.com/app/3435/>

▶ Schedule Salesforce use cases

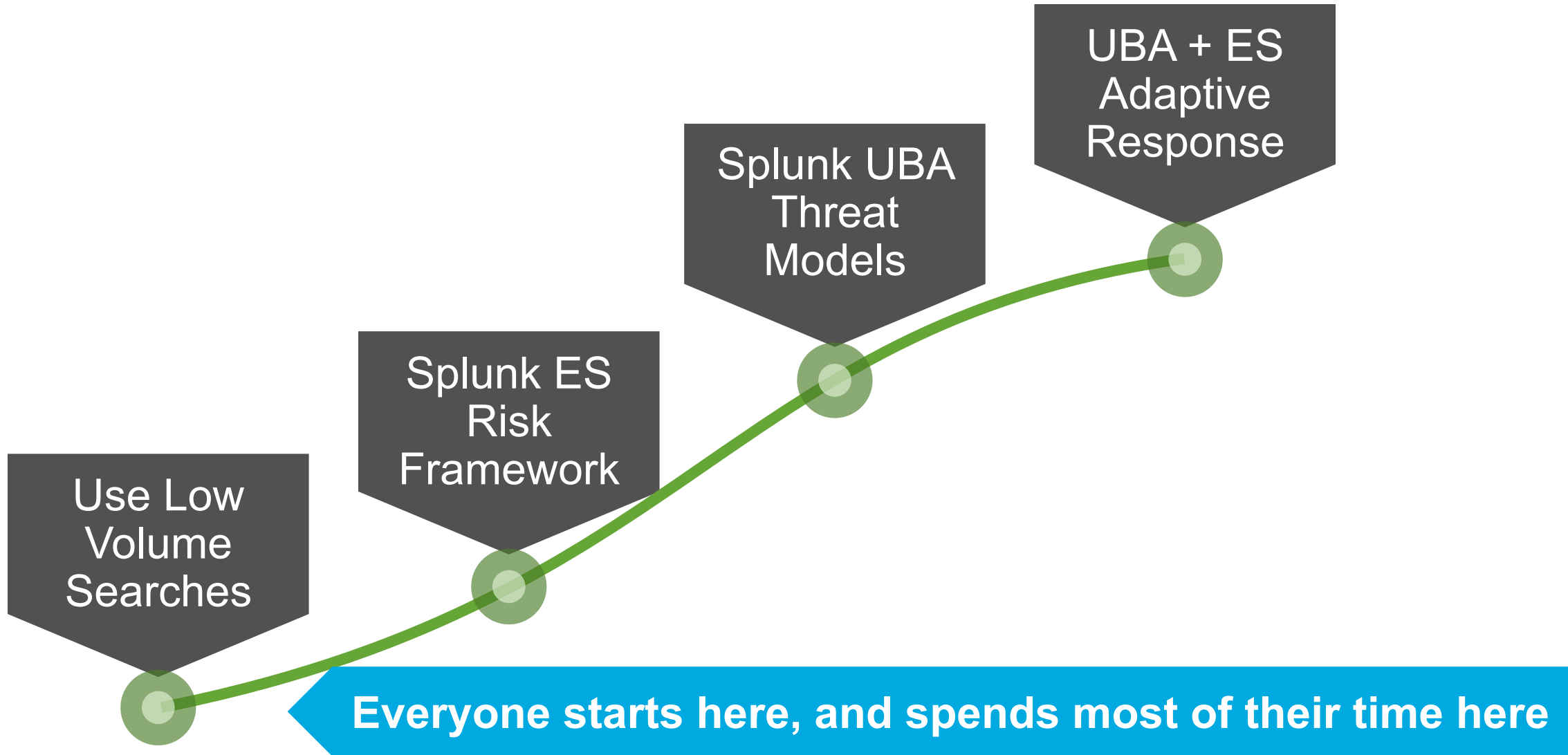
▶ Build a custom Box use case



About 1 Hour of Work

<p>2 Outlier(s)</p> <p>First Seen Use Case</p>	<p>New Application Accessing Salesforce.com API</p> <p>For many organizations, Salesforce.com contains the most critical information in their company. With Salesforce, you can use the API to pull information into third party apps. This search looks for new clients per user.</p> <p>Alert Volume: Low</p> <p>Examples:</p> <ul style="list-style-type: none"> • Demo Data • Live Data 	<p>2 Outlier(s)</p> <p>First Seen Use Case</p>	<p>New High Risk Event Types for Salesforce.com User</p> <p>Salesforce.com supports a variety of different event types in their event logs. This search detects users who suddenly query event types associated with data exfiltration</p> <p>Alert Volume: Medium</p> <p>Examples:</p> <ul style="list-style-type: none"> • Demo Data • Live Data
<p>2 Outlier(s)</p> <p>First Seen Use Case</p>	<p>New Tables Queried by Salesforce.com Peer Group</p> <p>Salesforce.com supports a simplified query language called SOQL. This search detects users who begin querying sensitive tables that have never been contacted by peer group.</p> <p>Alert Volume: Low</p> <p>Examples:</p> <ul style="list-style-type: none"> • Demo Data • Live Data 	<p>2 Outlier(s)</p> <p>First Seen Use Case</p>	<p>New Tables Queried by Salesforce.com User</p> <p>Salesforce.com supports a simplified query language called SOQL. This search detects users who begin querying new sensitive tables.</p> <p>Alert Volume: Low</p> <p>Examples:</p> <ul style="list-style-type: none"> • Demo Data • Live Data
<p>Time Series Use Case</p>	<p>Spike in Downloaded Documents Per User from Salesforce.com</p> <p>For many organizations, Salesforce.com contains the most critical information in their company. This use case tracks the number of documents downloaded per day per user (and is based on a real set of data collection).</p> <p>Alert Volume: Medium</p> <p>Examples:</p> <ul style="list-style-type: none"> • Demo Data • Live Data 	<p>Time Series Use Case</p>	<p>Spike in Exported Records from Salesforce.com</p> <p>For many organizations, Salesforce.com contains the most critical information in their company. This use case tracks the number of records exported per day (and is based on a real set of data collection).</p> <p>Alert Volume: Medium</p> <p>Examples:</p> <ul style="list-style-type: none"> • Demo Data • Live Data

Managing Alert Volume vs Value



130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-03" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.10.10

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.10.10

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.10.10

128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD35L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=KQ-CW-01" "Mozilla/5.0 (Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 14.1.10.10

Aggregate Alerting with ES Risk

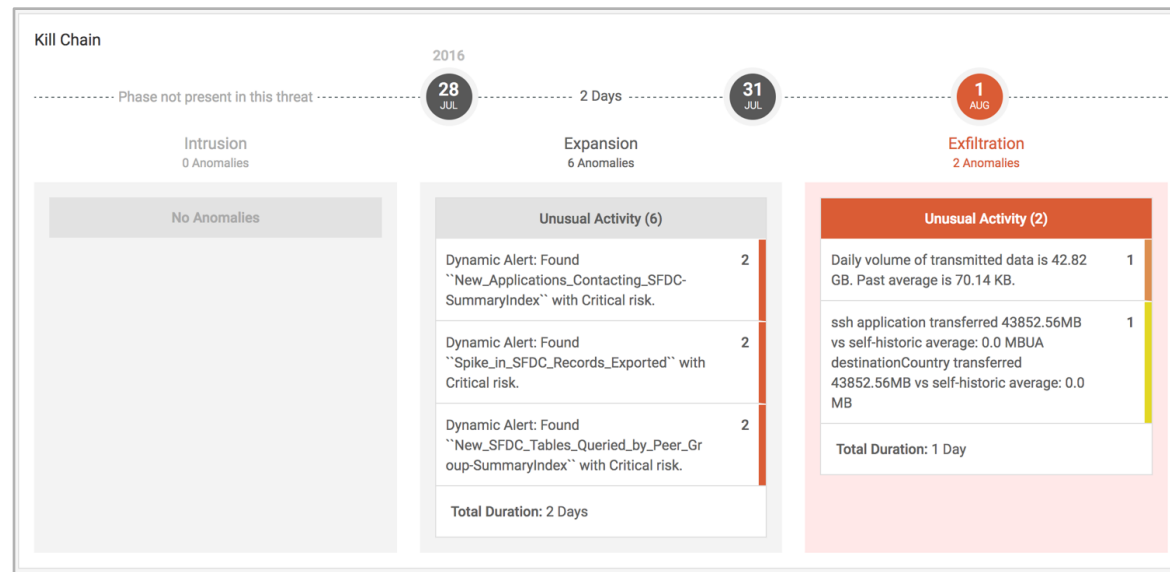
- ▶ Enterprise Security has a Risk Framework designed for aggregating low severity indicators

Risk Score By Object				
risk_object	risk_object_type	risk_score	source_count	count
aseykoski	user	480	2	6
jsmith	user	270	5	5
Hax0r	user	240	1	3
agasiewski	user	240	1	3
aseykoski@acmetech.com	user	240	1	3
cargento	user	240	1	3
dmsys	user	240	1	3
htrapper@acmetech.com	user	240	1	3
wohler	user	240	1	3
atria@c1z.at	user	120	1	3

« prev 1 2 next »

Apply Machine Learning With Splunk UBA

- ▶ Splunk UBA Threat Models leverage Data Science, Machine Learning
- ▶ Finds important, inter-related anomalies that analysts should actually view
- ▶ Support more advanced anomaly detections!



Respond With ES Adaptive Response

- ▶ High Confidence alerts from UBA fed into ES
- ▶ Take actions like
 - Box: “Change Permissions”
 - AD: “Reset Password” or “Disable Account”
 - PAN: Isolate Host

▶ 27 partners!

Adaptive Response Actions

Select actions to run.

[+ Add New Response Action](#)

▼ Reset User Password

User Name

Password

Action

Description:

UBA Threat: Unusual activity followed by data exfiltration by user Chris Geremy. User Chris Geremy involved in a sequence of events constituting a threat: user Chris Geremy first performed an unusual internal activity, followed by an unusually large data transfer to an external entity. This threat is a possible data exfiltration by user Chris Geremy to malicious domain.

Additional Fields	Value	Action
Action	Investigate the users involved. Check for recent changes in their role	▼
Application	ssh	▼
Modification Time	2016 Jul 31 8:00:00 PM	▼
Signature	Insider: Data Exfiltration by Suspicious User or Device	▼
Start Time	2016 Jul 28 10:33:50 AM	▼
Threat Category	Insider: Data Exfiltration by Suspicious User or Device	▼
User	Chris Geremy	▼

Correlation Search:

[Threat - UEBA Threat Detected \(Notable\) - Rule](#)

History:

[View all review activity for this Notable Event](#)

Contributing Events:

[View threat history](#)

Adaptive Responses: [🔗](#)

Response	Mode	Time	User	Status
Notable	saved	2017-03-16T19:05:30-0500	admin	✓ success
Risk Analysis	saved	2017-03-16T19:05:30-0500	admin	✓ success
Reset AD Password	saved	2017-03-16T19:05:39-0500	admin	✓ success

[View Adaptive Response Invocations](#)

ES + UBA + SSE Demo

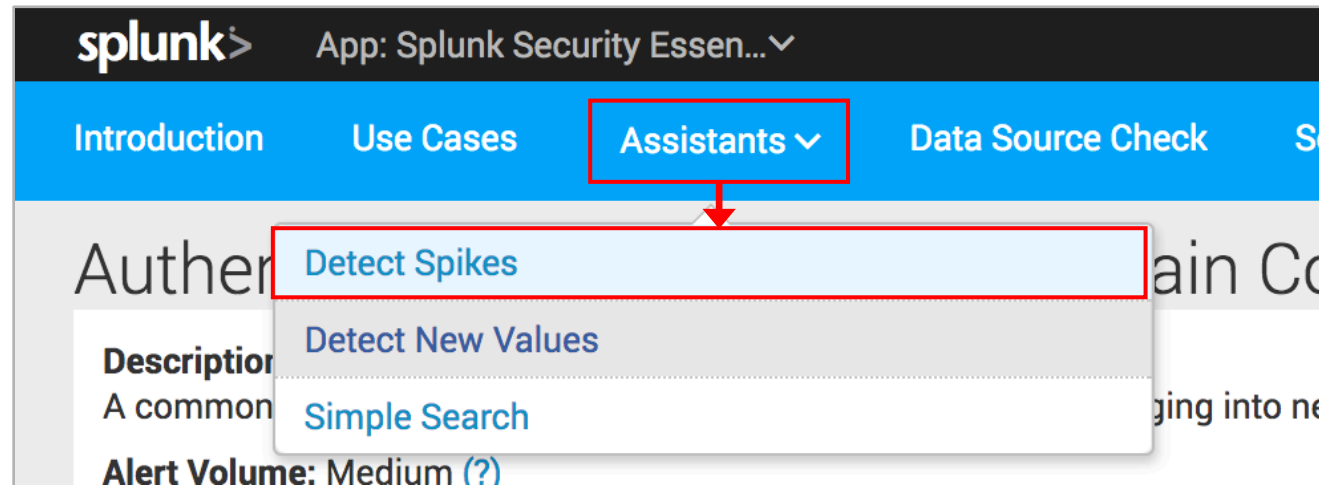
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD1SLAFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FI-SW-01"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD95L7FF6ADFF0 HTTP 1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-268product_id=KQ-CU-01"
137.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5L9FFIADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5L9FFIADFF3"
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD18SLBF2ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1408"
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD18SLBF2ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1408"
130.60.4 - - [07/Jan 18:10:57:123] "GET /category.screen?category_id=FLOWERS&JSESSIONID=SD18SLBF2ADFF9 HTTP 1.1" 200 3865 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1408"

But My Company Is So Custom

- ▶ Do you want to build your own detections like this?
- ▶ What if your environment is totally custom?
- ▶ No product has ever worked out of the box, and that's why you like Splunk, right?

We've got you.

Click Assistants, then "Detect Spikes"



The screenshot shows the Splunk web interface. At the top, the 'splunk' logo is followed by the application name 'App: Splunk Security Essen...'. Below this is a navigation bar with several tabs: 'Introduction', 'Use Cases', 'Assistants', 'Data Source Check', and 'Se...'. The 'Assistants' tab is highlighted with a red box, and a red arrow points down to a dropdown menu. This menu contains three options: 'Detect Spikes', 'Detect New Values', and 'Simple Search'. The 'Detect Spikes' option is also highlighted with a red box. Below the menu, the 'Description' section is partially visible, showing the text 'A common' and 'Alert Volume: Medium (?)'. The background of the interface is filled with a faint, repeating pattern of log data.

Use Case

- ▶ Our Malicious Insider, Jane Smith, also downloaded some proposals from Box
- ▶ Finding Box downloads spikes is easy, but we want focus on the Proposal Folder
- ▶ We will use the Detect Spikes assistant to help us



```
130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=GIFTS&SESSIONID=5D15L9FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=F1-SW-03"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&SESSIONID=5D35L7FF6ADFF0 HTTP 1.1" 404 322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=K9-CB-01"
137.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&SESSIONID=5D55L9FF1ADFF3"
137.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1182 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FLOWERS"
137.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1182 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FLOWERS"
137.27.160.0.0 - - [07/Jan 18:10:56:156] "GET /category.screen?category_id=FLOWERS&SESSIONID=5D55L9FF1ADFF3 HTTP 1.1" 200 1182 "http://buttercup-shopping.com/cart.do?action=remove&itemId=EST-1&product_id=FLOWERS"
```


- ▶ | inputlookup anonymized_box_logs.csv | search folder="PROPOSALS"
| bucket_time span=1d | stats count by user_time
- ▶ Looking for “count” by “user” with “6” standard deviations

Outlier(s) [↗](#)

1

Outlier(s)

Total Result(s) [↗](#)

114


Total Result(s)

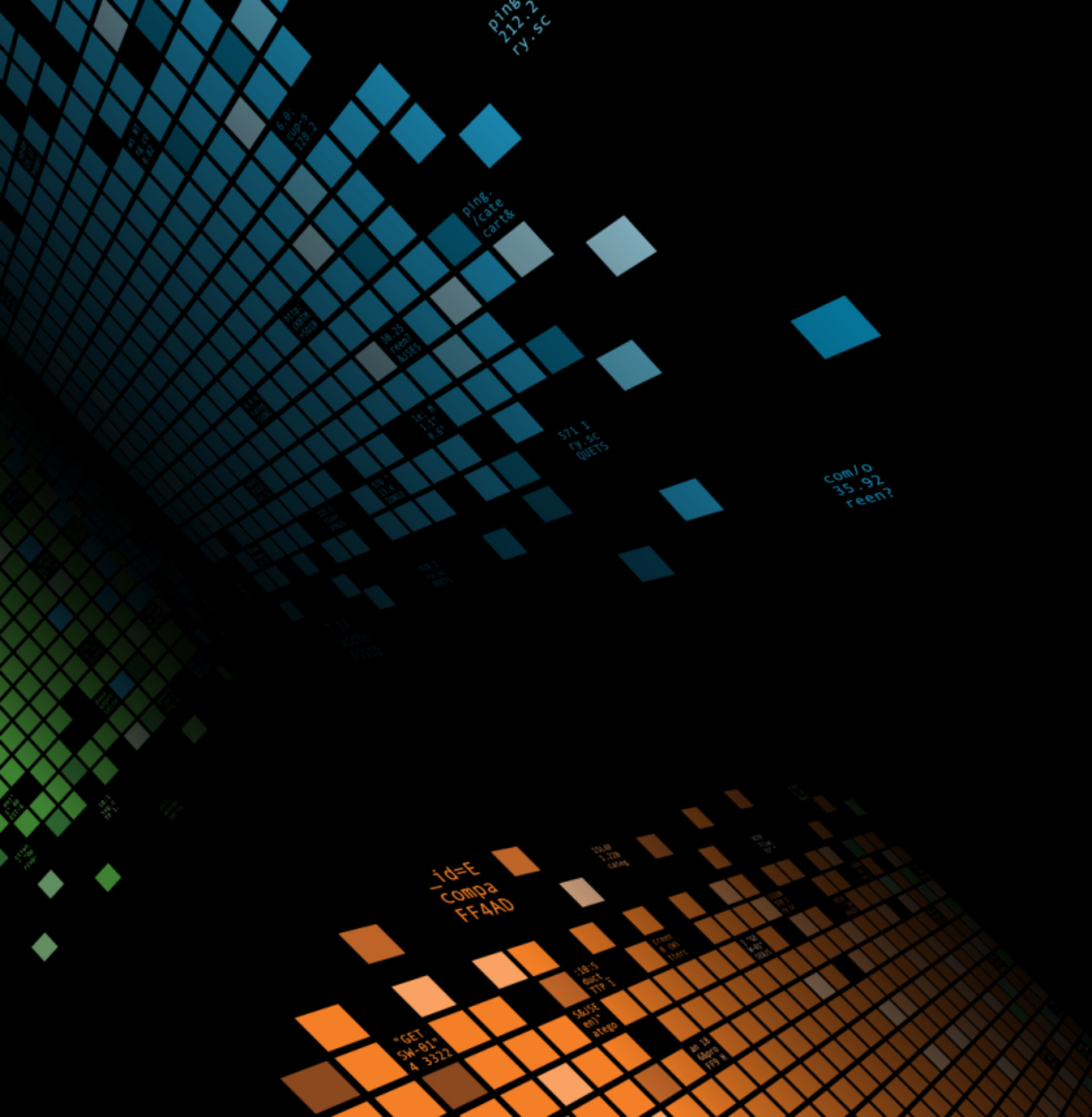
Raw Event(s)

Got Her!

Outliers Only [↗](#)

user	num_data_samples	count	avg	lowerBound
jsmith	15	112	3.071429	-14.61261





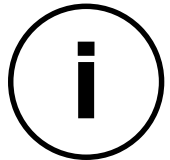
Wrap-Up

Splunk Security Portfolio



Enterprise Security Response

- OOB key security metrics
- Incident response workflow
- Adaptive response



Splunk Enterprise Detection

Realm of Known

- Log Aggregation
- Splunk Security Essentials
- Rules, statistics, correlation

Human-driven



Splunk UBA Detection

Realm of Unknown

- Risky behavior detection
- Entity profiling, scoring
- Kill chain, graph analysis

ML-driven

splunk>

.conf2017



What Did We Cover?

1. Splunk Security Essentials shows you new detection use cases
2. Ultimately it just uses Splunk Enterprise – Power of the Platform!
3. You can build your own use cases easily!
4. As you advance, look to ES or UBA to improve threat detection

1. Download Splunk Security Essentials
2. Try the Data Source Check dashboard
3. If you want to learn *how* -- attend Security Ninjutsu tomorrow!
4. If you want to build your own ML:
Security Ninjutsu tomorrow
Automating Threat Hunting w/ML tomorrow

What Next?



Thank You

Don't forget to **rate this session** in the
.conf2017 mobile app



I get to come back if you give me good ratings. Rate high, early, and often!