Full Speed Ahead With Risk-Based Alerting (RBA)

Jim Apger

Staff Security Strategist | Splunk

Kyle Champlin

Principal Product Manager | Splunk

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.

Agenda

1) More MITRE ATT&CK

Improvements

2) Threat Objects and SOAR

Introduction

3) Customer Win

Compelling

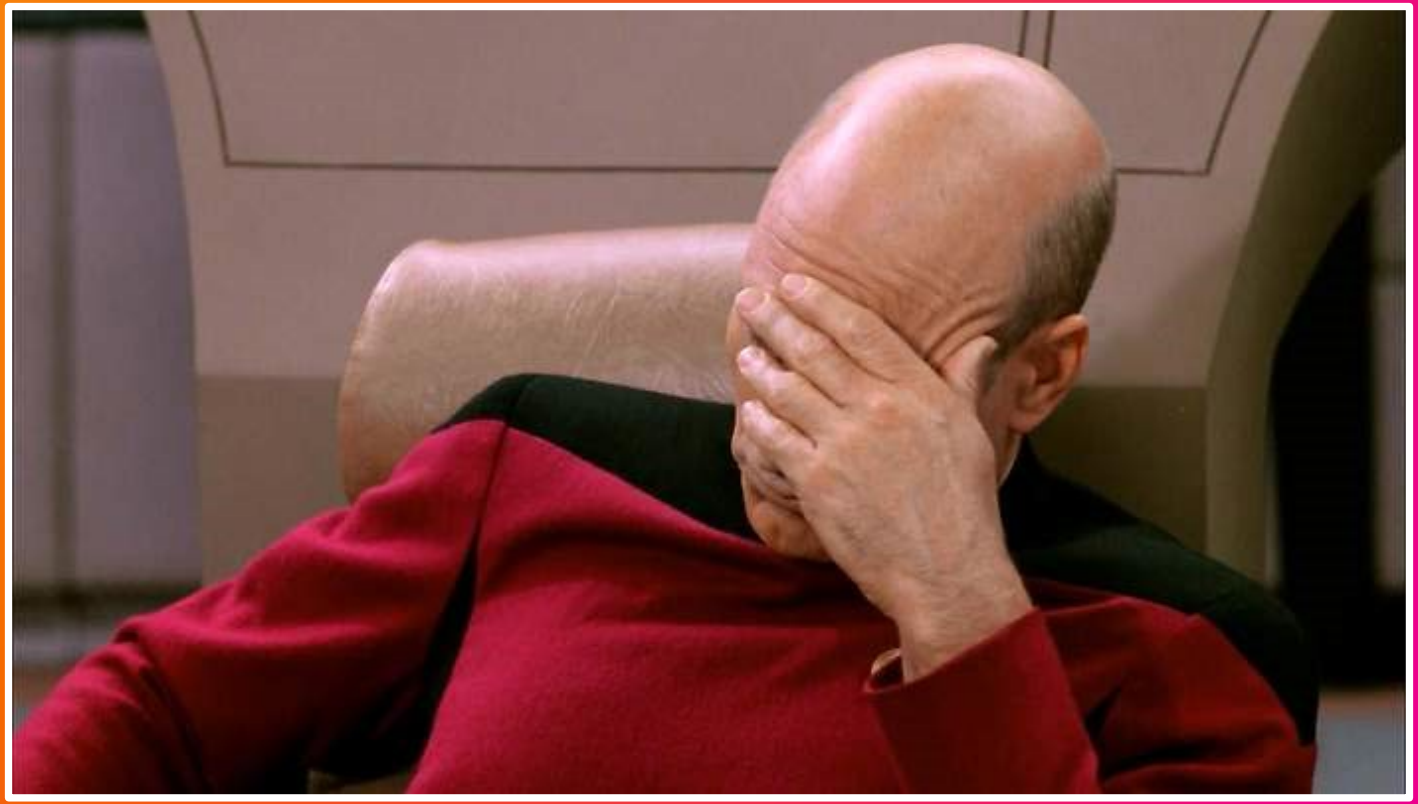
4) Enterprise Security

Acceleration

Jim Apger

Staff Security Strategist | Splunk

splunk> .conf20



ALERT FATIGUE

facepalm

ALERT SUPRESSION

double facepalm

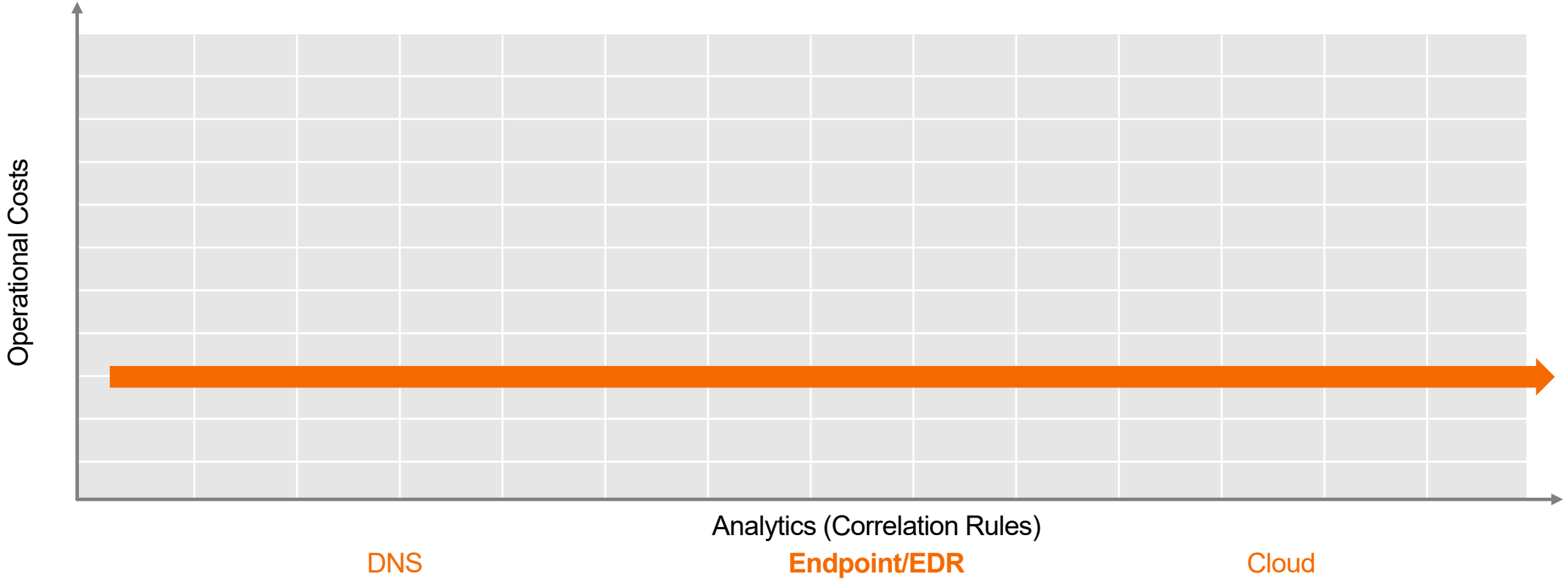
The Business of SOC

Traditional Approach

"Highly illogical." — Spock

The Business of SOC

RBA



"Logic is the beginning of wisdom, not the end." — Spock

RBA Milestones

3-Year Journey

Early Adopters

2018

Risk Rules

Risk Scoring

MITRE ATT&CK

Risk Index

Risk Notables

.Conf18 talk

Accelerated Adoption

2019

SA-RBA Reference App

(4) .Conf19 talks

SANS and ISC2 talks

Evolution

2020

MITRE ATT&CK

Threat Objects

SOAR

Attack Web Viz

Turnkey Enterprise Security

2020

PM Updates

MITRE ATT&CK

Map to Technique

```
|eval mitre_technique_id="T1170"
|lookup mitredict mitre_technique_id OUTPUTNEW mitre_tactic_id
|eval risk_message="Possible use mshta.exe to proxy execution of
    VBScript through a trusted Windows utility. Image=".Image.".
    parent_process_path:".parent_process_path
|eval testmode=0
|eval threat_object=Image
|eval threat_object_type="commandline"
`risk_score_system(src,5)`
`risk_score_user(user,5)`
```

MITRE ATT&CK

Add ATT&CK Context

```
|
|eval mitre_technique_id="T1170"
|lookup mitredict mitre_technique_id OUTPUTNEW mitre_tactic_id
|eval risk_message="Possible use mshta.exe to proxy execution of
    VBScript through a trusted Windows utility. Image=".Image.".
    parent_process_path:".parent_process_path
|eval testmode=0
|eval threat_object=Image
|eval threat_object_type="commandline"
`risk_score_system(src,5)`
`risk_score_user(user,5)`
```

MITRE ATT&CK

```
|inputlookup mitredict|search mitre_technique_id="T1546.011"|transpose
```

https://rbaallday.com

-OR-

MITRE **Supporting Add on for MITRE**

-OR-

https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json

MITRE ATT&CK

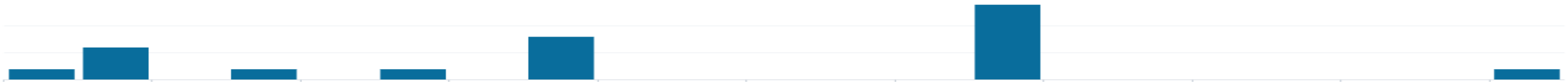
mitre_description	Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by application shims. The Microsoft Windows App Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over ti feature allows developers to apply fixes to applications (without rewriting code) that were created for Windows XP so that it will work with Windows 10. 2017) Within the framework, shims are created to act as a buffer between the program (or more specifically, the Import Address Table) and the Windows OS. When referenced to determine if the program requires the use of the shim database (.sdb). If so, the shim database uses hooking to redirect the code as neces A list of all shims currently installed by the default Windows installer (sdbinst.exe) is kept in: * <code>%WINDIR%\AppPatch\sysmain.sdb</code> and * <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\installedsdb</code> Custom databases are stored in: * <code>%WINDIR%\AppPatch\custom & %WINDIR%\AppPatch\AppPatch64\Custom</code> and * <code>hklm\software\microsoft\windows nt\currentversion\appcompatflags\custom</code> To keep shims secure, Windows designed them to run in user mode so they cannot modify the kernel and you must have administrator privileges to install a [Bypass User Access Control](https://attack.mitre.org/techniques/T1548/002) (UAC and RedirectEXE), inject DLLs into processes (InjectDLL), disable Data Structure Exception Handling (DisableSEH), and intercept memory addresses (GetProcAddress). Utilizing these shims may allow an adversary to perform several malicious acts such as elevate privileges, install backdoors, disable defenses like Wind Application Shimming) Shims can also be abused to establish persistence by continuously being invoked by affected programs.
mitre_detection	There are several public tools available that will detect shims that are currently available (Citation: Black Hat 2015 App Shim): * Shim-Process-Scanner - checks memory of every running process for any shim flags * Shim-Detector-Lite - detects installation of custom shim databases * Shim-Guard - monitors registry for any shim installations * ShimScanner - forensic tool to find active shims in memory * ShimCacheMem - Volatility plug-in that pulls shim cache from memory (note: shims are only cached after reboot) Monitor process execution for sdbinst.exe and command-line arguments for potential indications of application shim abuse.

MITRE ATT&CK

mitre_software_name	ShimRat SDBot
mitre_software_platform	Windows Windows
mitre_software_type	malware malware
mitre_software_url	https://attack.mitre.org/software/S0444 https://attack.mitre.org/software/S0461
mitre_tactic	privilege-escalation persistence
mitre_tactic_id	TA0004 TA0003
mitre_technique	Application Shimming
mitre_technique_id	T1546.011
mitre_threat_group_aliases	FIN7
mitre_threat_group_name	FIN7
mitre_threat_group_url	https://attack.mitre.org/groups/G0046
mitre_url	https://attack.mitre.org/techniques/T1546/011

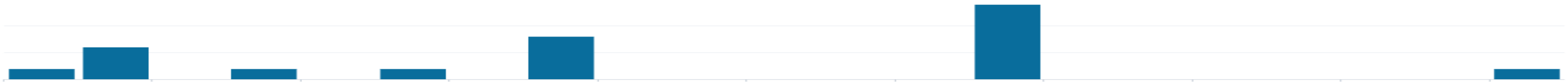
MITRE ATT&CK

Slow-and-Low



MITRE ATT&CK

Improved Detections!

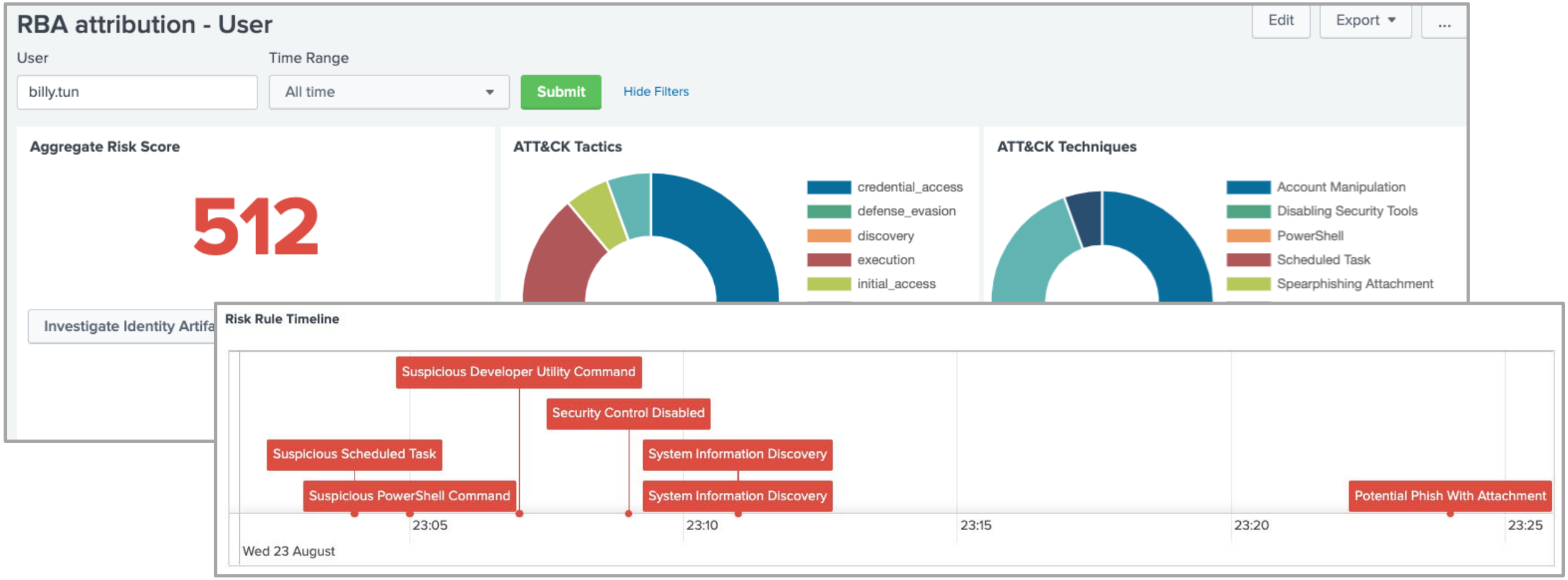


days or even weeks

billy.tun	RBA: ATT&CK Tactic threshold exceeded (>=3) over previous 7 days for user=billy.tun spanning 6 Risk Rules, 5 ATT&CK tactics, and 6 ATT&CK techniques	High

MITRE ATT&CK

Investigation



IOCs as Threat Objects

Domain

URL

Command

Protocol

IP

Registry

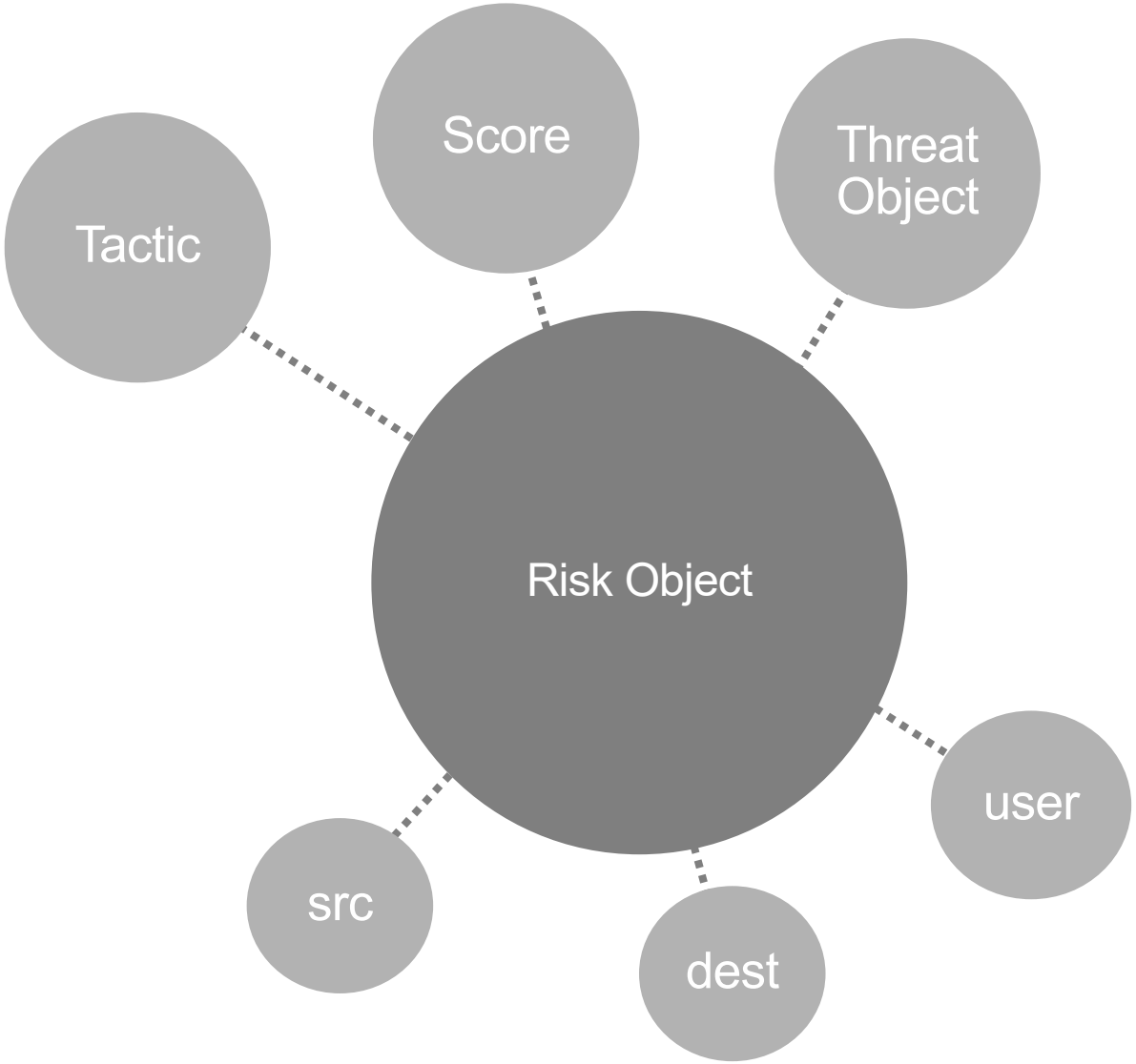
Filehash

Username

Threat Objects

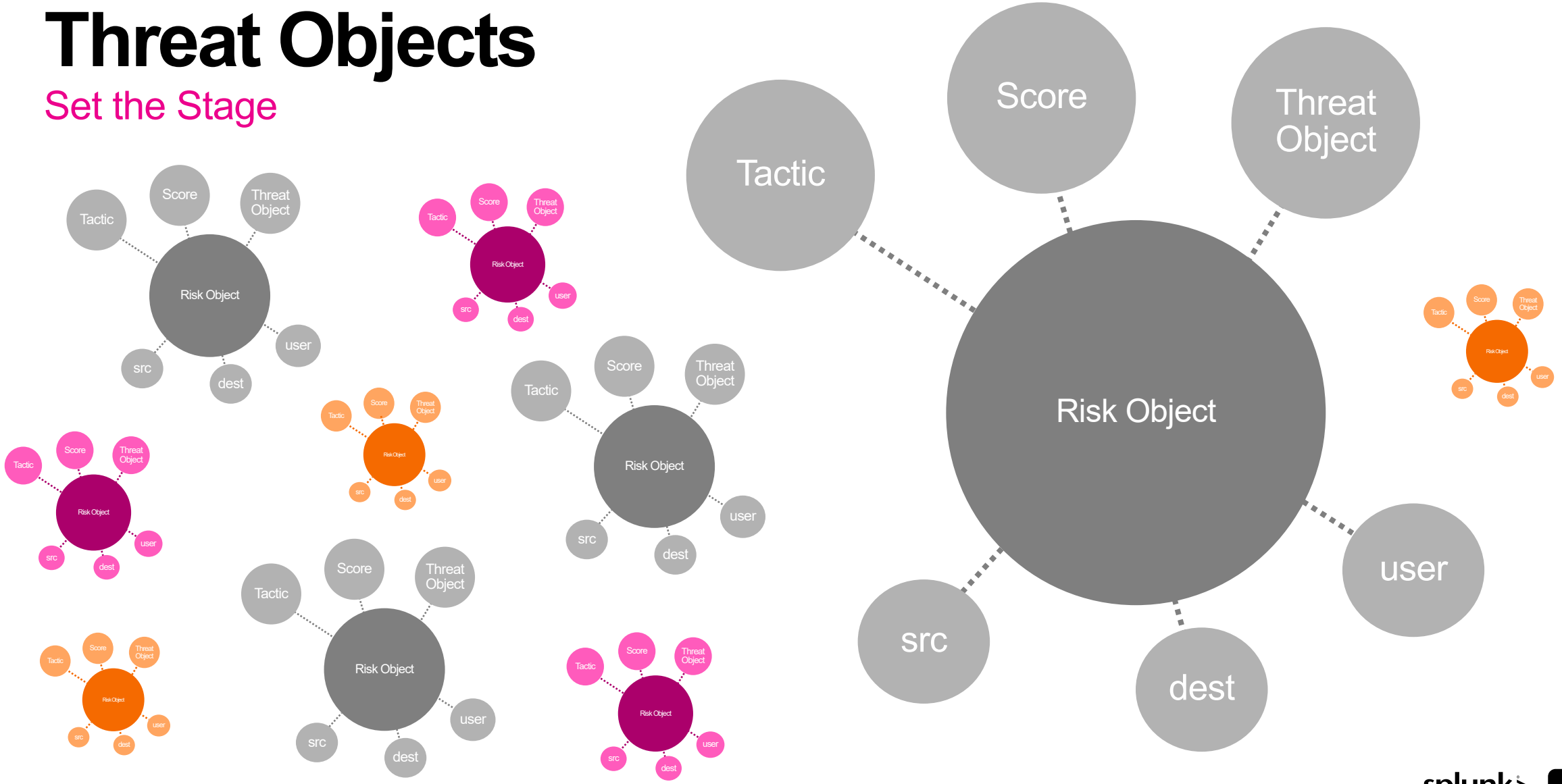
Per Risk Rule

```
| eval threat_object = process_name
| eval threat_object_type = "cmdline"
```



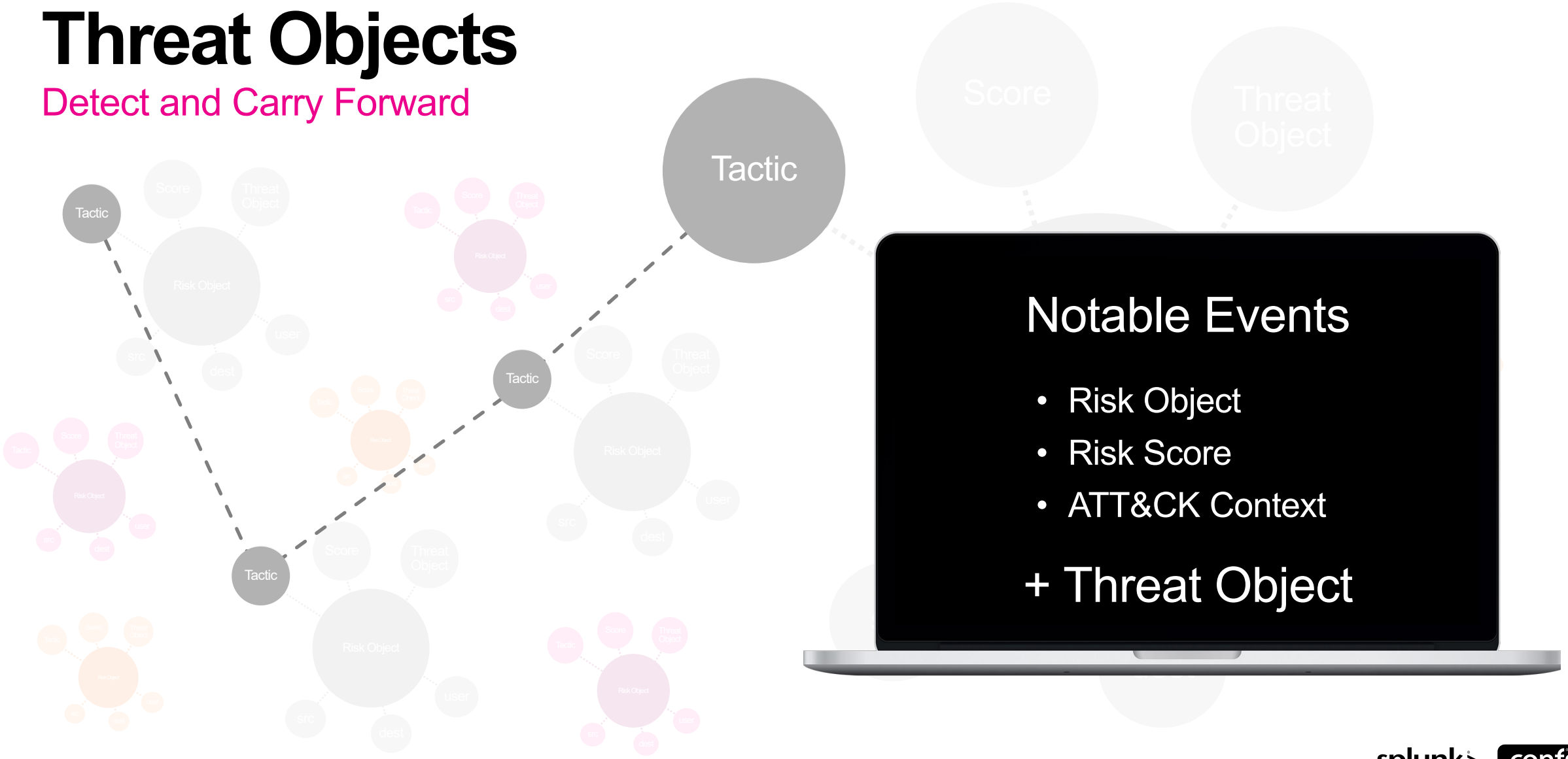
Threat Objects

Set the Stage



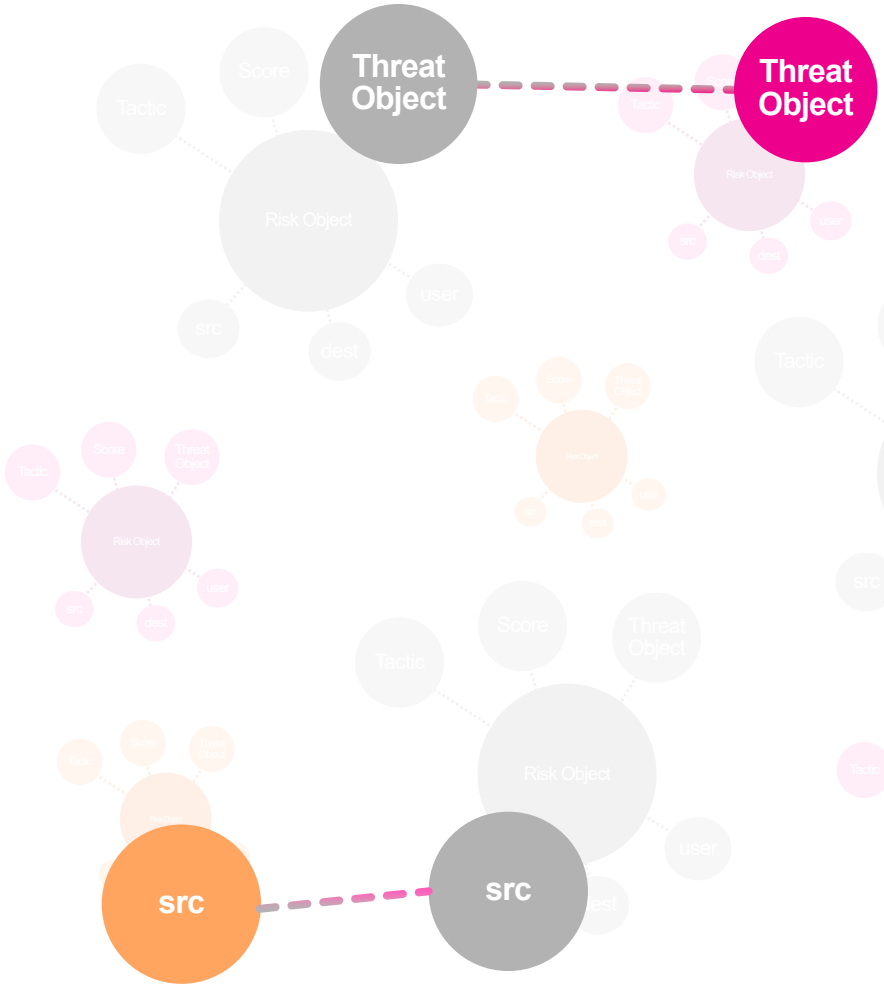
Threat Objects

Detect and Carry Forward



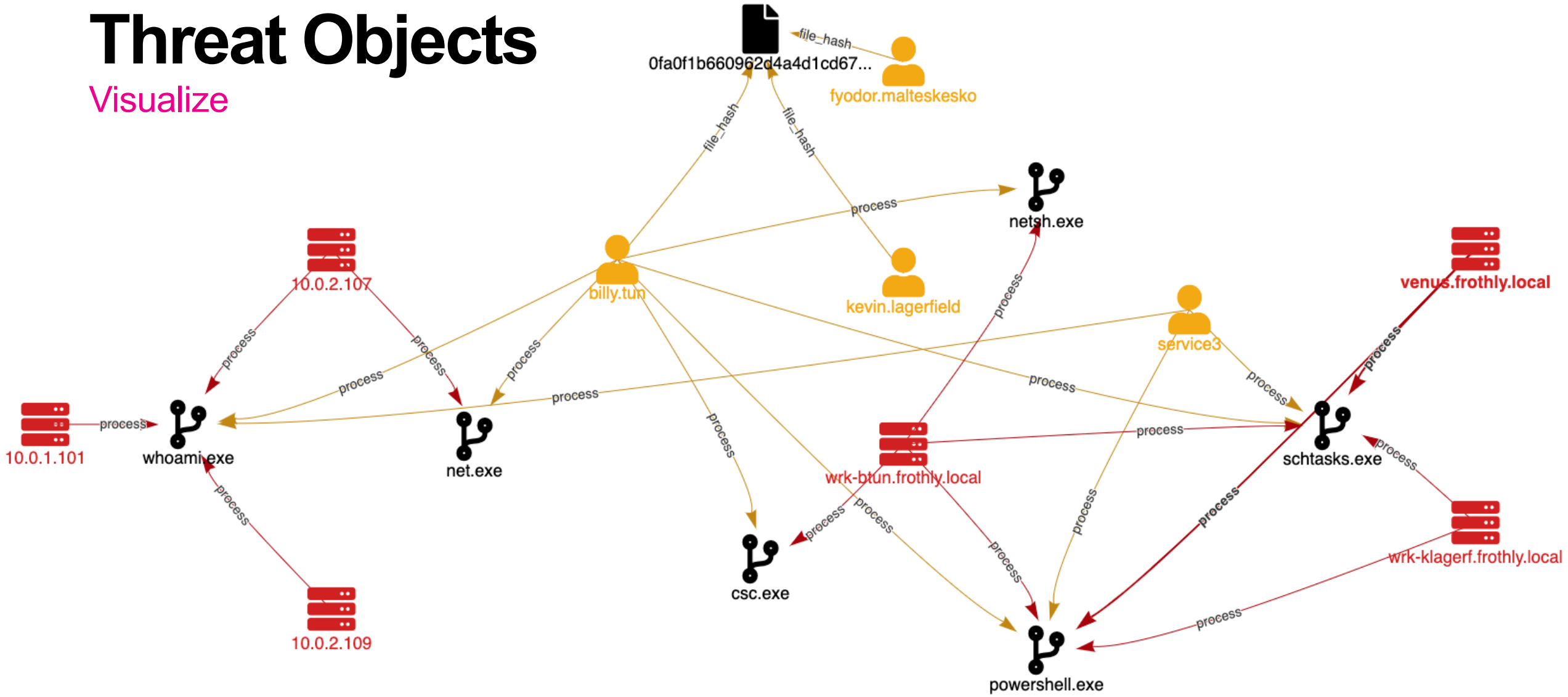
Threat Objects

Related Objects



Threat Objects

Visualize



"Fascinating." -- Spock

Threat Objects

Risk Notables Into Phantom

splunk>phantom

rba-phantom-public version 4.9.34514 | Ford Prefect

Sources

Events | Indicators | Cases | Tasks

Search by event names or ID

Show | Select a filter | + EVENT | IMPORT

Top Events
5
notable

Severity
Critical 1
High 0
Medium 2
Low 2
Informational 0

Status
New 5
Open 0
Closed 0

Top Owners

Dynamic Updates | Show Stats

ID	NAME	LABEL	OWNER	STATUS	SEVERITY	SENSITIVITY	ARTIFACTS	CREATED	OPENED
21	RBA: Threat - RIR - 7 day ATT&CK Tactic threshold exceeded - Rule: wrk-btun.frothly.local	notable		New	CRITICAL	TLP AMBER	14	Yesterday at 6:49 pm	
20	RBA: Threat - RIR - 7 day ATT&CK Tactic threshold exceeded - Rule: venus.frothly.local	notable		New	LOW	TLP AMBER	4	Yesterday at 6:49 pm	
19	RBA: Threat - RIR - 24 hour risk threshold exceeded - Rule: wrk-btun.frothly.local	notable		New	MEDIUM	TLP AMBER	14	Yesterday at 6:49 pm	
18	RBA: Threat - RIR - 7 day ATT&CK Tactic threshold exceeded - Rule: service3	notable		New	MEDIUM	TLP AMBER	5	Yesterday at 6:49 pm	
17	RBA: Threat - RIR - 24 hour risk threshold exceeded - Rule: service3	notable		New	LOW	TLP AMBER	5	Yesterday at 6:49 pm	

Threat Objects

Automation

splunk>phantom

INVESTIGATION

notable CRITICAL ID: 21

RBA: Threat - RIR - 7 day ATT&CK Tactic threshold exceeded - Rule: wrk-btun.frothly.local

Owner Select... Status New

Playbooks Run:	7	Created:	Yesterday at 6:49 pm	Authorized:	
Actions Run:	7	Activity Start:	Yesterday at 6:49 pm		
Artifacts:	14	Last Updated:	Yesterday at 6:49 pm		
		SLA:	Exceeded by 6 hours		

Activity | Workbook | Guidance | Timeline | Artifacts | Evidence | Files | Approvals | Reports

Recent Activity

automation Yesterday at 6:49 pm

- RBA Prep 2.0
  - fetch_risk_rules
  - update_artifact_sev_crit
    1 action failed for app Phantom
- RBA Prep 2.0
- RBA Investigate
- RBA Investigate - ip
- RBA Investigate - domain
- RBA Investigate - process
- RBA Response

ARTIFACTS (14)

ID	LABEL	NAME	SEVERITY	CREATED BY	TAGS
175	risk_rule	Threat Intel File Activity	INFORMATION...		execution
174	risk_rule	Suspicious Scheduled Task	INFORMATION...		persistence
173	risk_rule	Suspicious SSL Certificate	INFORMATION...		defense_evasion
172	risk_rule	Suspicious PowerShell Comma...	INFORMATION...		execution
171	risk_rule	Suspicious PowerShell Comma...	INFORMATION...		execution
170	risk_rule	Suspicious PowerShell Comma...	INFORMATION...		execution
169	risk_rule	Suspicious Developer Utility Co...	INFORMATION...		execution
168	risk_rule	Security Control Disabled	INFORMATION...		defense_evasion
167	risk_rule	Long Network Connection	INFORMATION...		command_and_control
166	risk_rule	Long Network Connection	INFORMATION...		command_and_control

splunk> .conf20

Professional Services

*"As a security practitioner and network defender, the RBA methodology is **dramatically streamlining the amount of effort** security analysts spend triaging security alerts, and finally giving them the opportunity to zero in on high fidelity, high confidence risk alerts that are absolutely worth their time and effort."*

– Marquis Montgomery, Principal Security Architect, Global Security Services at Splunk

Average Event Abandonment

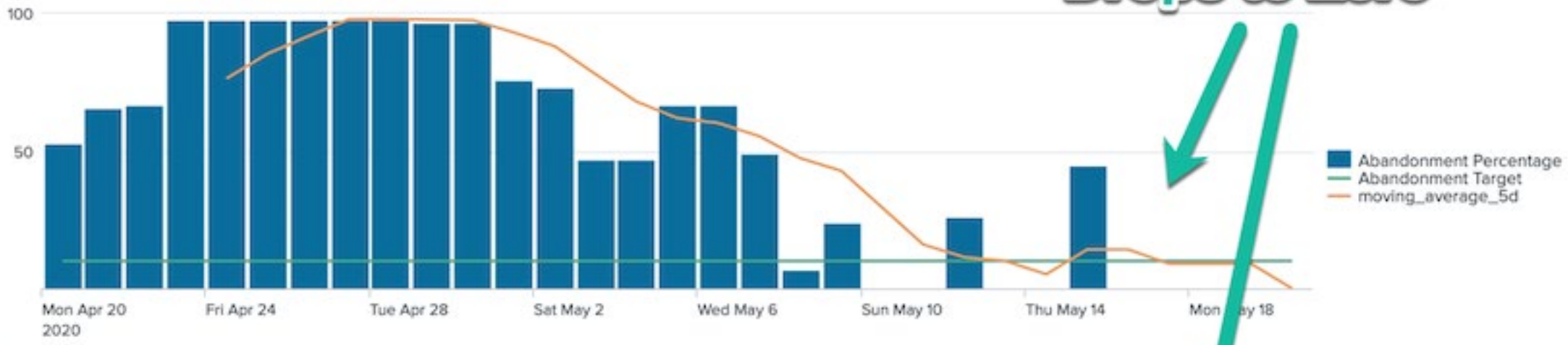
RBA Goes Live in Production

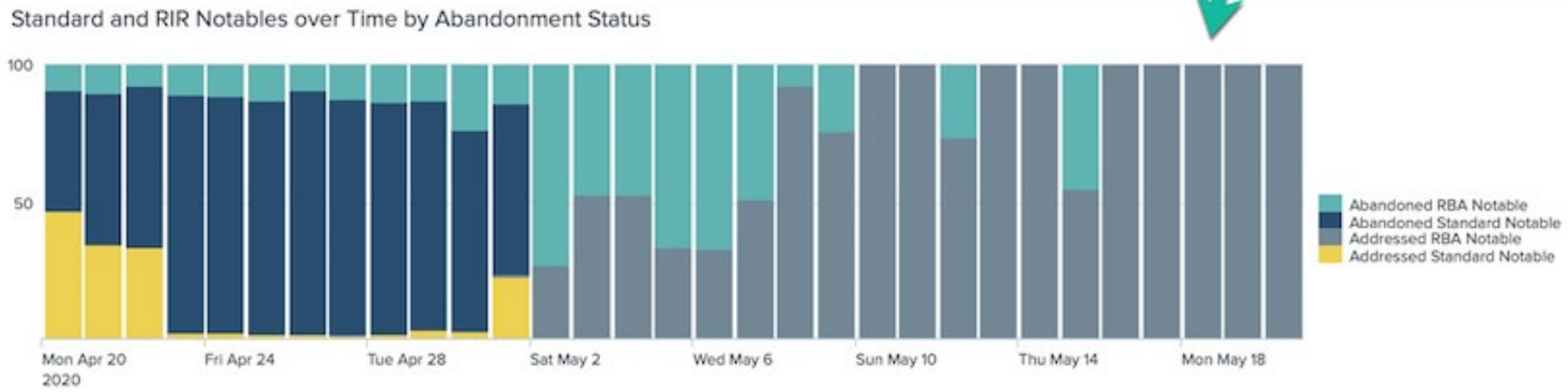
Further Notable Reduction after Tuning

Notable Event Trends

Provided by Viasat and the Viasat CSOC

Notable Abandonment Drops to Zero



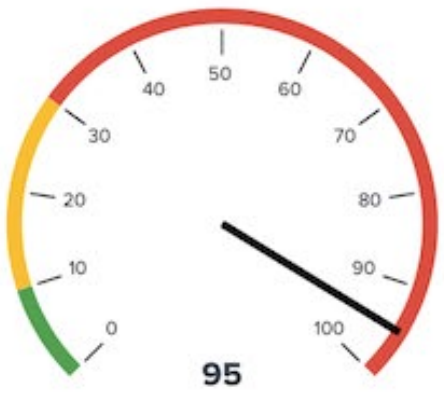


Provided by Viasat and the Viasat CSOC

Mar 2020

Hide Filters

Average Event Abandonment



Only Critical and High Notables Addressed, Resulting in High Abandonment Rate

Notable Event Trends

Thousands of Notable Events Every Day

Provided by Viasat and the Viasat CSOC

splunk> .conf20

Jun 2020

Hide Filters

Average Event Abandonment

Notable Abandonment Below 10% Target

Notable Event Trends

Daily Notables Reduced by 10x

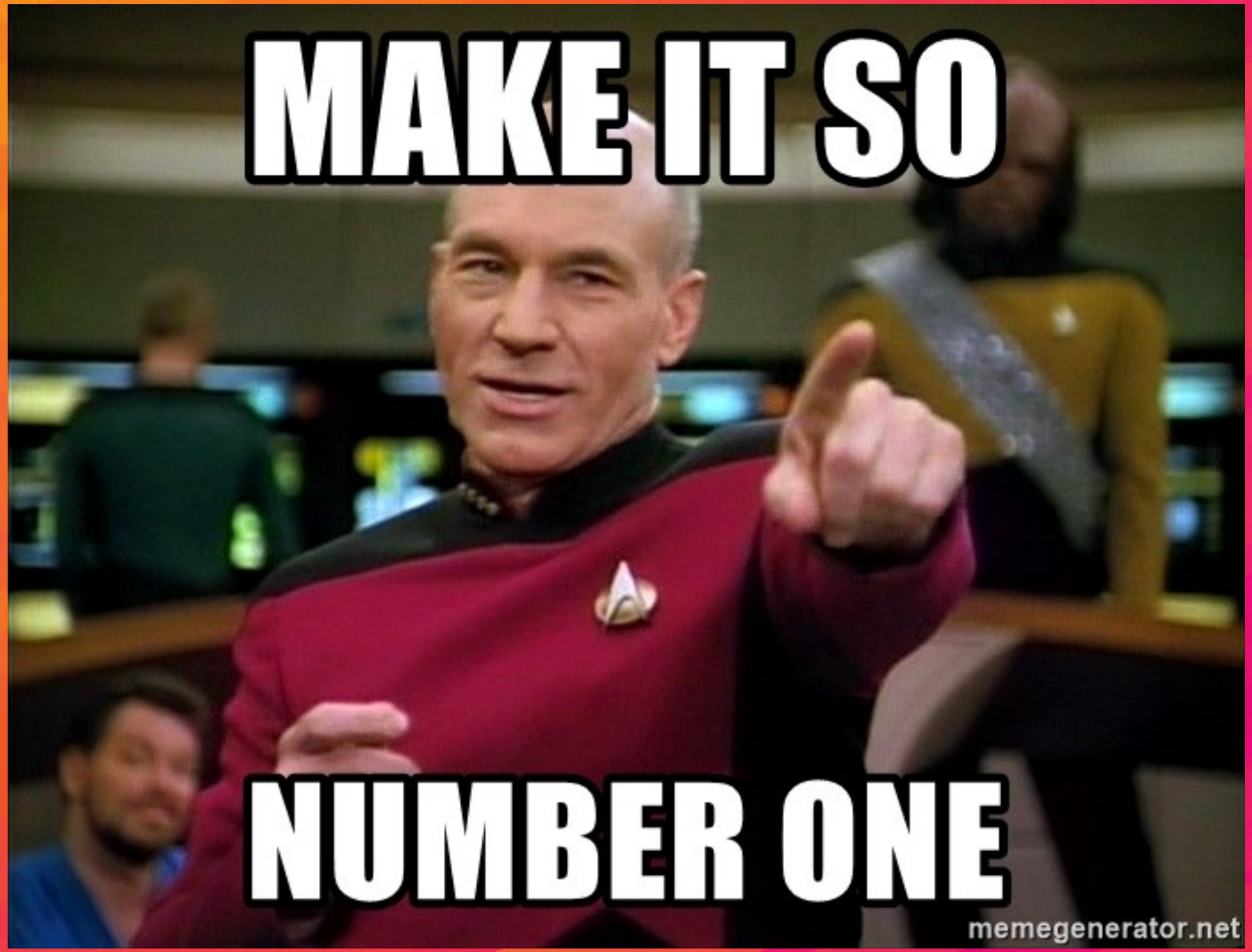
More RBA Content

RBA/Phantom Content Links in the Speaker Notes

Kyle Champlin

Principal Product Manager | Splunk

Charts and Tables



Risk Based Alerting

Is It Right For Me?

Do you suffer from any of these symptoms?

- alert fatigue, ballooning allow/deny lists, situational numbness

Are you

- An existing ES user who wants to get ES more "operationalized”?
- Brand new ES customers who would benefit from a more turn-key SIEM experience?
- A smaller SOC team that wants a solution that will mature and grow with them?

Risk Based Alerting

What Are We Doing In ES?

- Shipped out-of-box Correlation Searches mapped to MITRE ATT&CK annotations (ESCU inclusive!)
- Shipped out-of-box Correlation Searches that deploy the new "Risk" adaptive response action (existing and new, ESCU inclusive!)
- Shipped out-of-box dashboards and panels that provide a risk-centric investigative experience
- Shipped new Correlation Searches that mine the risk index for notables (risk incident rules)

SA-RBA to ES

Map to Technique

```
|eval mitre_technique_id="T1170"
|lookup mitredict mitre_technique_id OUTPUTNEW mitre_tactic_id
|eval risk_message="Possible use mshta.exe to proxy execution of
    VBScript through a trusted Windows utility. Image=".Image.".
    parent_process_path:".parent_process_path
|eval testmode=0
|eval threat_object=Image
|eval threat_object_type="commandline"
`risk_score_system(src,5)`
`risk_score_user(user,5)`
```

Risk Annotations

Annotate correlation searches directly in the CS editor

ATT&CK techniques are pre-populated

Search

```
| from datamodel:"Authentication"."Authentication" | stats values(tag) as tag,values(app) as app,count(eval('action'=="failure")) as failure,count(eval('action'=="success")) as success by src | search success>0 | `mltk_apply_upper("app:failures_by_src_count_1h", "high", "failure")`
```

Annotations

CIS 20: Type an attribute and press enter

Kill Chain: Type an attribute and press enter

MITRE ATT&CK: Brute Force × Password Policy Discovery ×

NIST: .bash_profile and .bashrc

/etc/passwd and /etc/shadow

Risk Annotations

Search | from datamodel:"Authentication"."Authentication" | stats values(tag) as

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Intelligence Downloads

New

Data inputs » Intelligence Downloads

Showing 1-1 of 1 item

MITRE

25 per page

Name	Description	Interval	Type	URL	Weight	Debug	Status	Actions
mitre_attack	MITRE ATT&CK framework	86400	mitre_attack	https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json	60	False	Enabled | Disable	Clone

Kill Chain: Type an attribute and press enter

MITRE ATT&CK: Brute Force × Password Policy Discovery ×

NIST: .bash_profile and .bashrc

/etc/passwd and /etc/shadow

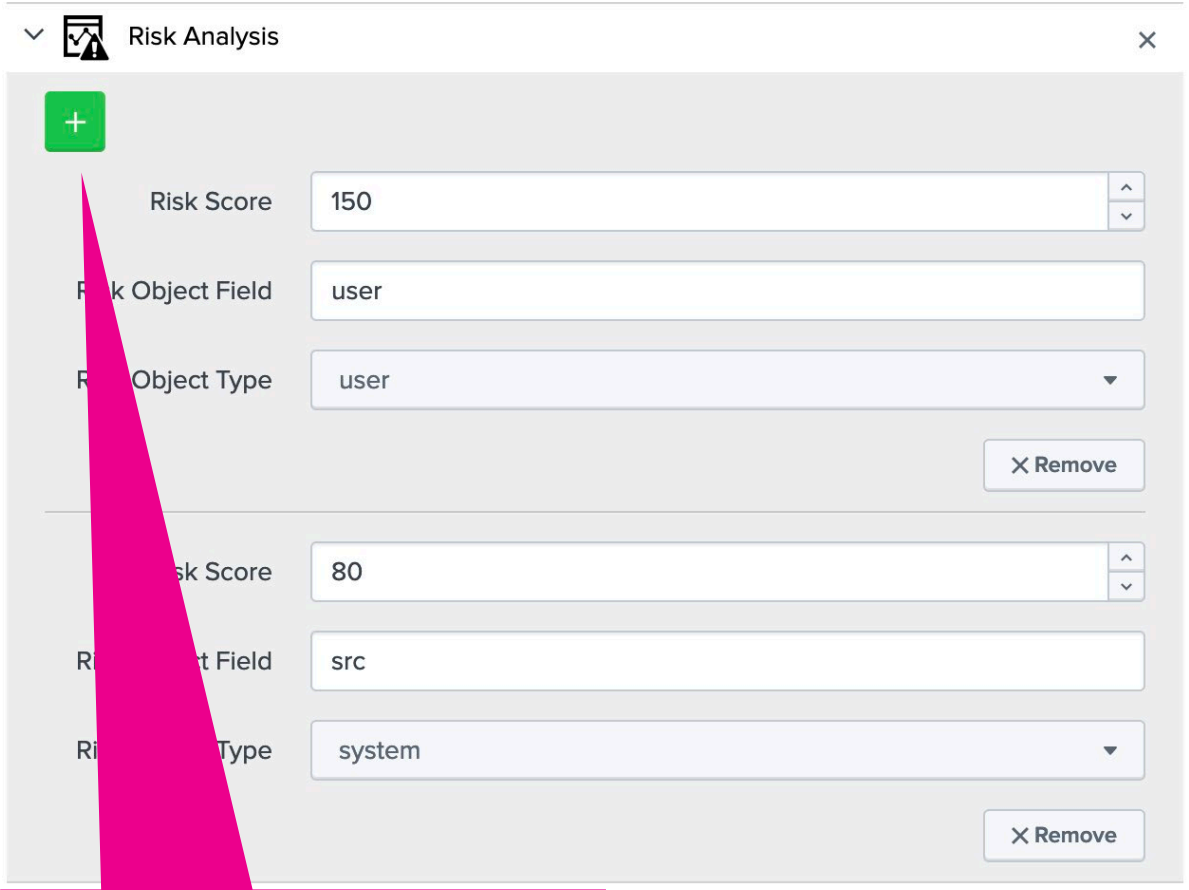
Always kept up to date with the latest from MITRE

SA-RBA to ES

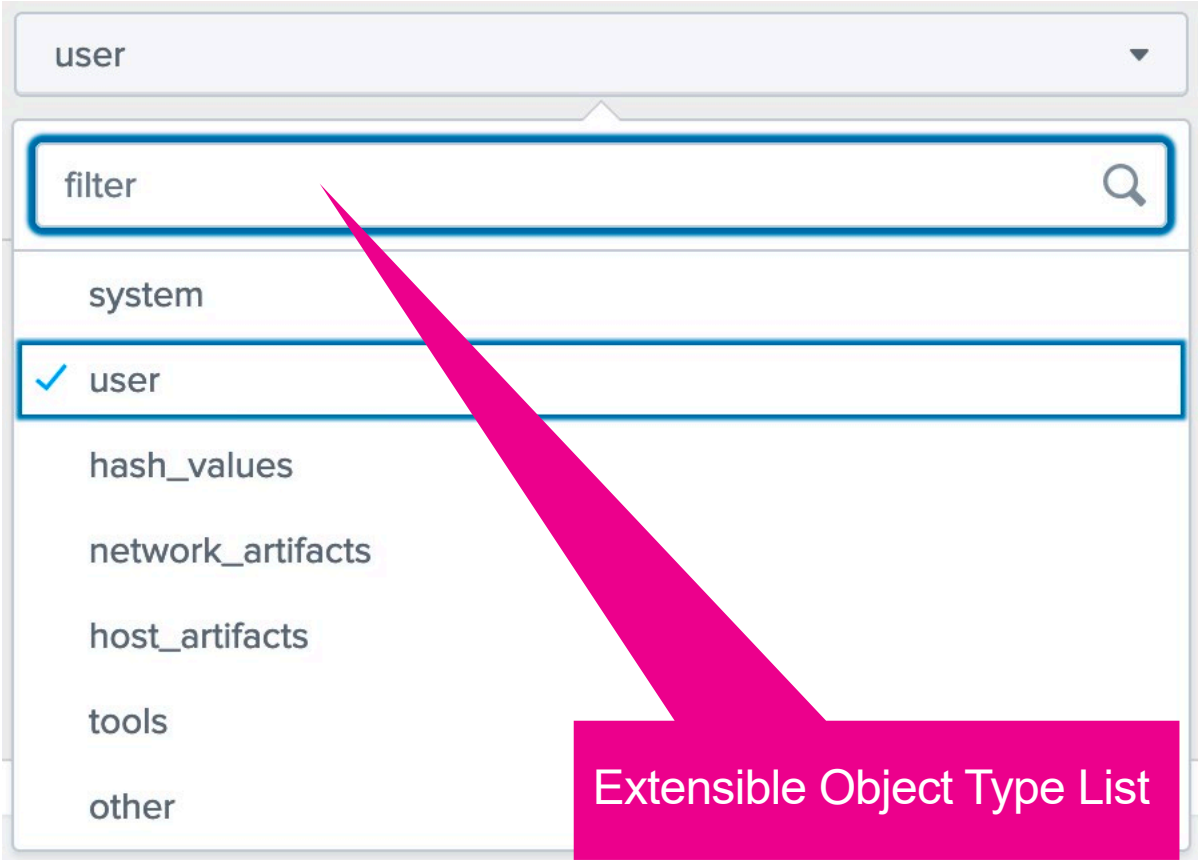
Dynamic Scoring & Multiple Risk Objects

```
|
|eval mitre_technique_id="T1170"
|lookup mitredict mitre_technique_id OUTPUTNEW mitre_tactic_id
|eval risk_message="Possible use mshta.exe to proxy execution of
    VBScript through a trusted Windows utility. Image=".Image.".
    parent_process_path:".parent_process_path
|eval testmode=0
|eval threat_object=Image
|eval threat_object_type="commandline"
`risk_score_system(src,5)`
`risk_score_user(user,5)`
```

Risk Action



Score multiple objects per correlation



Extensible Object Type List

splunk> .conf20

Risk Factors

Risk Factor Editor
< Back to Content Management

Search for Risk Factors
Sort By Name
Show Disabled
Add Risk Factor
47 Insufficient facts always invi...
Addition
100 Test Factor
Addition

Enable
Name
Insufficient facts always invite danger
Description
My First Risk Factor
Operation Group
Addition
Factor
47
Conditions
Simple Advanced
Field # 1 Risk Event Field
src_ip
Comparator
is equal to
Compare against field
Value
evil

Namespace
SA-ThreatIntelligence
Similar Risk Factors

Clone Save Save All

Create simple or advanced matching lconditions, as well as stack conditions w/in a single factor

Manage your risk factors

SA-RBA to ES

Threat Object Support

```
|
|eval mitre_technique_id="T1170"
|lookup mitredict mitre_technique_id OUTPUTNEW mitre_tactic_id
|eval risk_message="Possible use mshta.exe to proxy execution of
    VBScript through a trusted Windows utility. Image=".Image.".
    parent_process_path:".parent_process_path
|eval testmode=0
|eval threat_object=Image
|eval threat_object_type="commandline"
`risk_score_system(src,5)`
`risk_score_user(user,5)`
```

Updated Risk Data Model

EXTRACTED

annotations	String
annotations._all	String
annotations._frameworks	String
annotations.cis20	String
annotations.kill_chain_phases	
annotations.mitre_attack	
annotations.mitre_attack.mitre_description	
annotations.mitre_attack.mitre_detection	String
annotations.mitre_attack.mitre_tactic	String
annotations.mitre_attack.mitre_tactic_id	String
annotations.mitre_attack.mitre_technique	String
annotations.mitre_attack.mitre_technique_id	String
annotations.nist	String
creator	String
risk_object_bunit	String
risk_object_category	String
risk_object_priority	
savedsearch_description	S
tag	S
threat_object	String

Additional MITRE ATT&CK enrichment

Risk & Threat Object Support

CALCULATED

description	String
object	String
object_type	String
risk_score	Number
threat_object_type	String
risk_factor_add	Number
risk_factor_add_matched	Number
risk_factor_mult	Number
risk_factor_mult_matched	
_risk_score	

Scores are calculated via factors during DMA

SA-RBA to ES

Auto-Enrichment Of ATT&CK data

```
|
|eval mitre_technique_id="T1170"
|lookup mitredict mitre_technique_id OUTPUTNEW mitre_tactic_id
|eval risk_message="Possible use mshta.exe to proxy execution of
    VBScript through a trusted Windows utility. Image=".Image.".
    parent_process_path:".parent_process_path
|eval testmode=0
|eval threat_object=Image
|eval threat_object_type="commandline"
`risk_score_system(src,5)`
`risk_score_user(user,5)`
```

Updated Risk Data Model

List ▾ Format 20 Per Page ▾ < Prev 1 2 3 4

< Hide Fields All Fields

SELECTED FIELDS
- host 1
- source 7
- sourcetype 1

INTERESTING FIELDS
- annotations 3
- annotations._all 5
- annotations._frameworks 1
- annotations.mitre_attack 5
- annotations.mitre_attack.mitre_description 4
- annotations.mitre_attack.mitre_detection 4
- annotations.mitre_attack.mitre_platform 4
- annotations.mitre_attack.mitre_software_name 63
- annotations.mitre_attack.mitre_software_platform 6
- annotations.mitre_attack.mitre_software_type 2
- annotations.mitre_attack.mitre_software_url 63
- annotations.mitre_attack.mitre_tactic 3
- annotations.mitre_attack.mitre_tactic_id 3
- annotations.mitre_attack.mitre_techn

Time	Event
8/27/20 11:40:15.000 PM	1598586012, search_name="Network - Unroutable Host Activity - Rule", annotations="{\"mitre_attack\": [\" 1", annotations._frameworks="mitre_attack", annotations.mitre_attack="T1041", bogon_ip="0.9.114.104", de nfinity", info_min_time="0.000", risk_object="16.108.183.163", risk_object_type="system", risk_score="80 s when activity to or from a host that is unroutable is detected.", orig_sourcetype="stream:http", src="16.108.1

Event Actions ▾

Type	Field	Value	Actions
Selected	host ▾	soln-esnightly1	
	source ▾	Network - Unroutable Host Activity - Rule	
	sourcetype ▾	stash	
Event	annotations ▾	{"mitre_attack": ["T1041"]}	
	annotations._all ▾	T1041	
	annotations._frameworks ▾	mitre_attack	
	annotations.mitre_attack ▾	T1041	
	annotations.mitre_attack.mitre_description ▾	Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.	
	annotations.mitre_attack.mitre_detection ▾	Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used. (Citation: University of Birmingham C2)	
	annotations.mitre_attack.mitre_platform ▾	Linux	
		macOS	

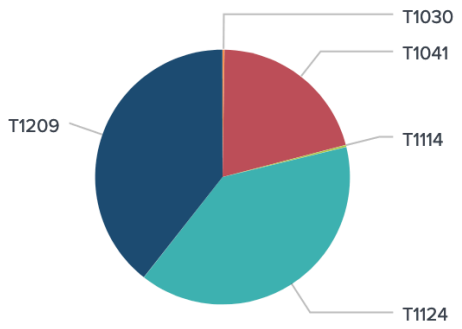
Risk events are now auto-enriched for any data model searches and risk index searches

.conf20

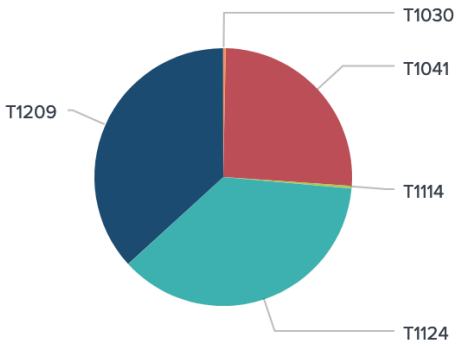
Updated Risk Analysis Dashboard Panels

Risk Modifiers Over Time

Risk Modifiers By Annotations



Risk Score By Annotations



Risk Score By Object

risk_object	t_type	risk_score	source	count
127.0.0			1	6
arn:aws		160.0	1	2
1.2.3.4		140.0	2	2
i-0aa0c		120.0	1	2
i-0b61b		120.0	1	2
i-0b77550d0486c75c8	system	120.0	1	2
BudStoll	user	100.0	1	2
0.105.125.21	system	80.0	1	1

New panels showing risk modifiers by ATT&CK technique

ost Active Sources

source	risk_score	risk_objects	count
Endpoint - Should Timesync Host Not Syncing - Rule	9360.0	156	156
Network - Unroutable Host Activity - Rule	6560.0	82	82
Audit - Personally Identifiable Information Detection - Rule	480.0	1	6
Threat - AWS Guard Duty Alert - Rule	360.0	3	6
Threat - Many Unauthorized AWS Operations - Rule	160.0	1	2
Endpoint - Code42 Rule Match - Rule	100.0	1	2
Endpoint - Host Sending Excessive Email - Rule	80.0	1	1

Thank You

"Live long, and prosper." — Spock

Please provide feedback via the

SESSION SURVEY