

.conf19

splunk®>

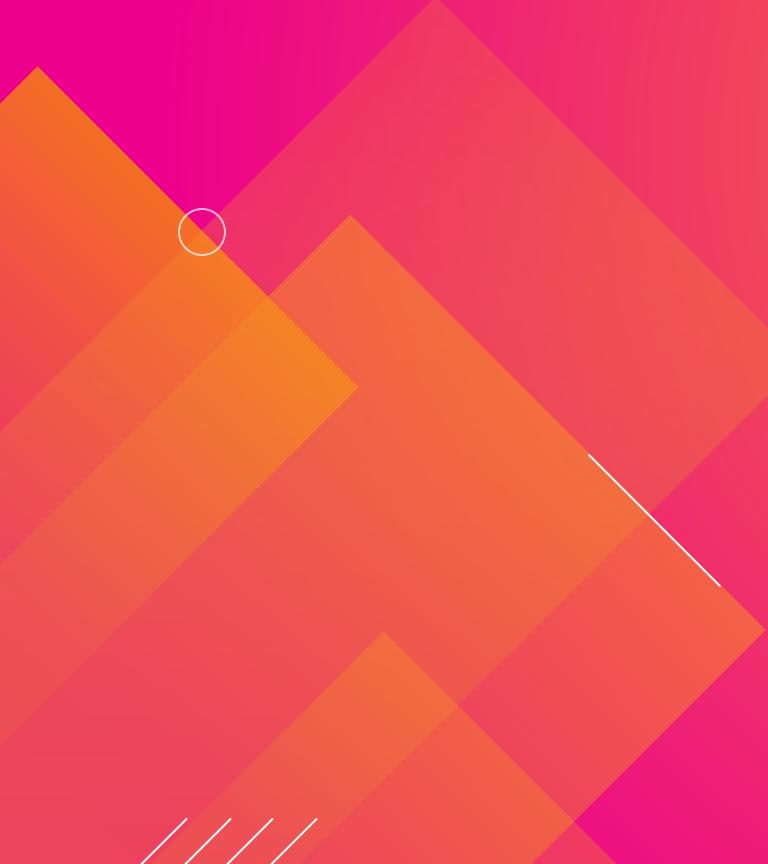
Enterprise Security Biology III:

Incident Review Framework

John Stoner | Principal Security Strategist

October 2019

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 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.



John Stoner

Principal Security Strategist
@stonerpsu

20+ years kicking around databases, ISPs and cyber

4.5 years at Splunk

Creator of SA-Investigator

Co-editor and author Hunting with Splunk: The Basics blogs

Assist in steering the BOTS ship

Developed APT Scenario for BOTS IV

Develop workshops on hunting and investigating with Splunk

Agenda

Incident Management Framework

Enterprise Security Frameworks

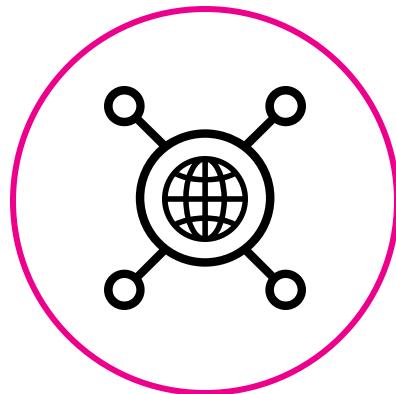
Correlation Searches

Notables

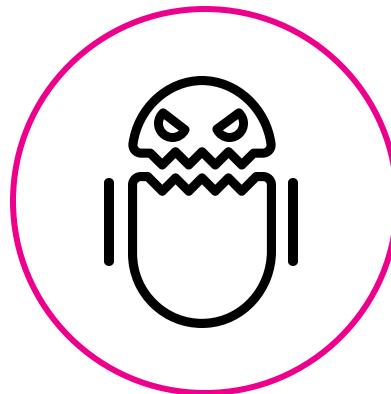
Incident Review

Event Sequencing & Audit

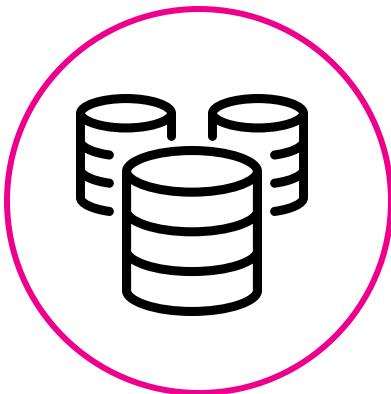
Enterprise Security Frameworks



Threat
Intelligence



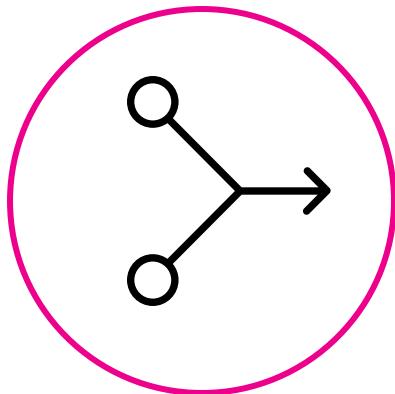
Incident
Management



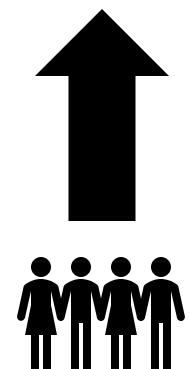
Asset &
Identity



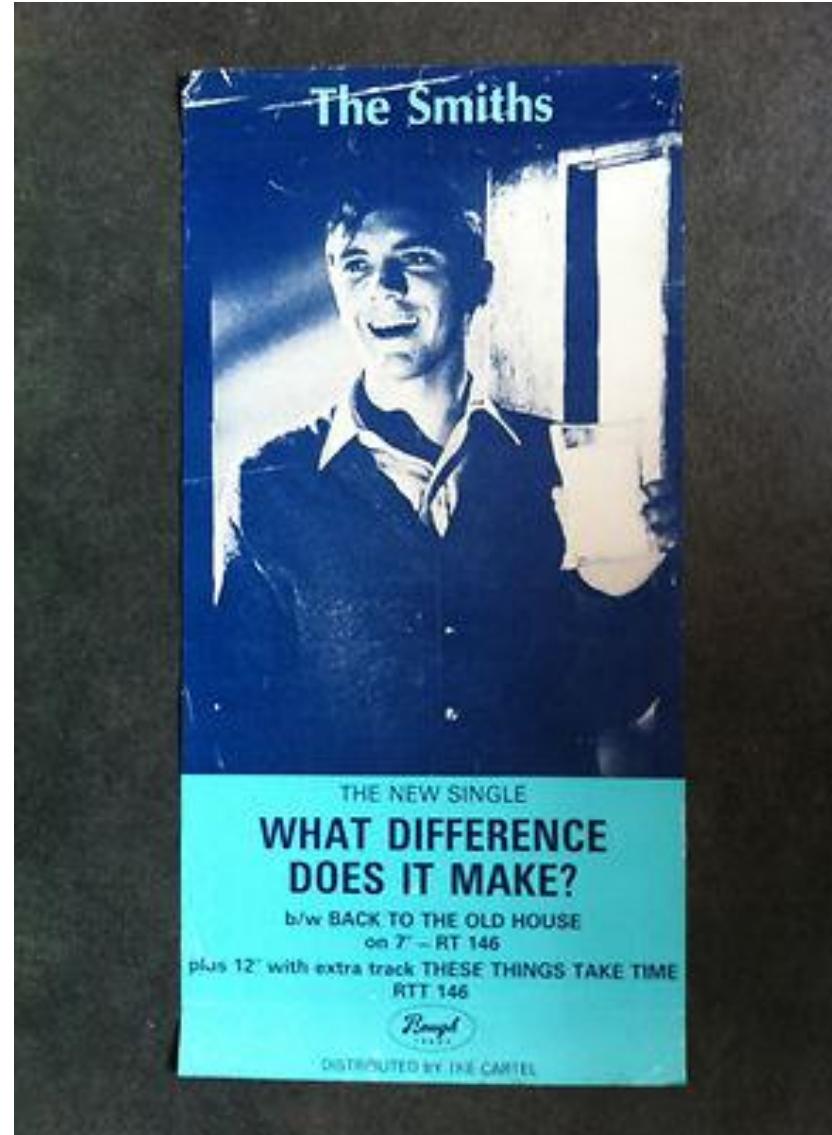
Risk



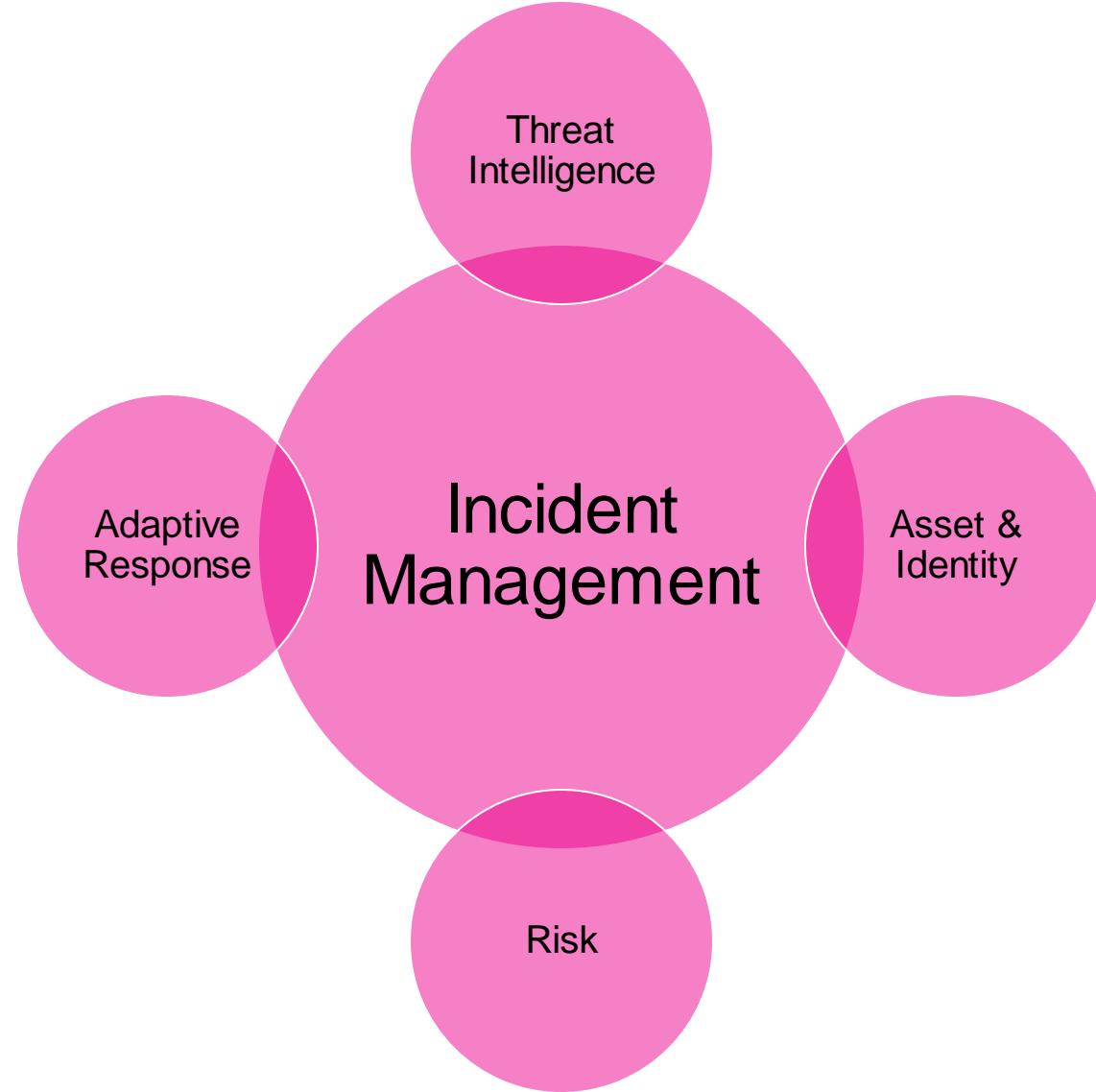
Adaptive
Response



Incident Management aka Notable Event Framework



Central to Enterprise Security



Why Should I Care About IM Framework?

Practical Application of Context

8/23/17 2:59:57.000 PM Threat Threat Activity Detected (nc.exe) Low New unassigned

Additional Fields	Value
Destination	160.153.91.7
Destination Expected	false
Destination PCI Domain	untrust
Destination Requires Antivirus	false
Destination Should Time Synchronize	false
Destination Should Update	false
Source	10.0.2.109
Source Category	workstation
Source City	windows
Source Country	San Francisco
Source DNS	US
Source IP Address	wrk-klagerf.frothly.local
Source Expected	10.0.2.109
Source MAC Address	false
Source NT Hostname	00:0c:29:f5:5e:8e
Source Owner	wrk-klagerf
Source PCI Domain	Kevin Lagerfeld
Source Requires Antivirus	untrust
Source Should Time Synchronize	TRUE
Source Should Update	false
Threat Category	undefined
Threat Collection	file
Threat Group	undefined
Threat Match Field	file_name
Threat Match Value	nc.exe

Description:
Threat activity (nc.exe) was discovered in the "file_name" field based on threat intelligence available in the file collection

Related Investigations:
Investigation (No Permission)

Action

Correlation Search:

- Threat - Threat List Activity - Rule

History:

- View all review activity for this Notable Event

Contributing Events:

- View all threat activity involving file_name="nc.exe"

Original Event:

```
08/23/2017 21:59:57 +0000, search_name="Threat - File Name Matches - Threat Gen", search_now=1505071997.000, info_search_time=1505071997.110, dest="160.153.91.7", file_name="nc.exe", info_max_time="1503547198.000000", info_min_time="1503521597.000000", info_search_time="1503525597.000000", orig_sourcetype="stream:ftp", src="10.0.2.109", tag="", threat_collection=file, threat_description="This file was detected and reported by John Stoner in the FRPCENK report", threat_match_field=file_name, threat_match_value="nc.exe"
```

Adaptive Responses:

Response	Mode	Time	User	Status
Risk Analysis	adhoc	2017-09-10T12:33:20-0700	system	✓ success
Notable	adhoc	2017-09-10T12:33:19-0700	system	✓ success

Next Steps:

No Next Steps defined.

Our Goal Today?

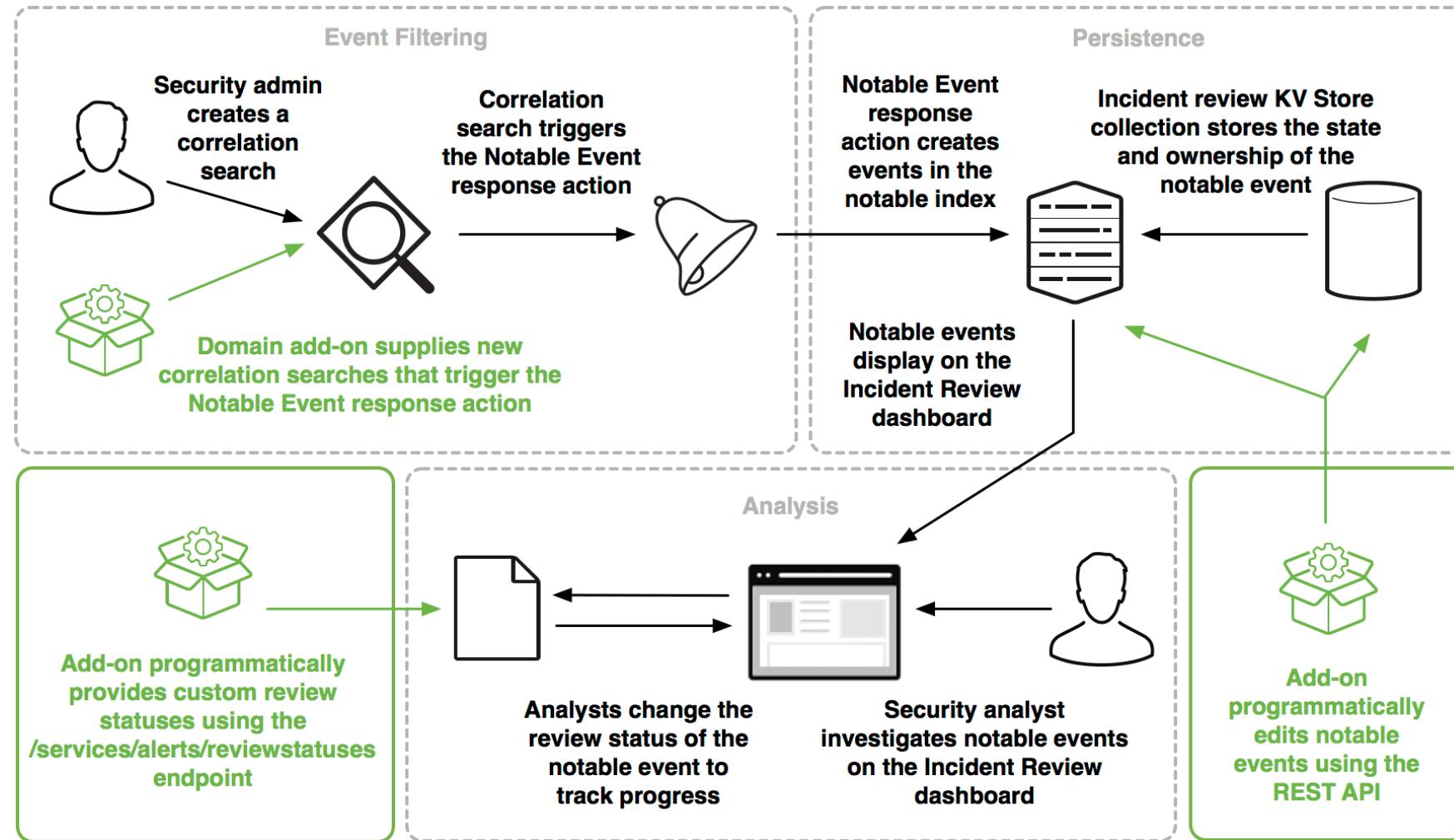
Better understand how
Splunk processes
notable events in
Enterprise Security

Better Insight =
Better Understanding =
Better Troubleshooting =
More Effective Use



Notable Event Framework

<http://dev.splunk.com/view/enterprise-security/SP-CAAAFA9>

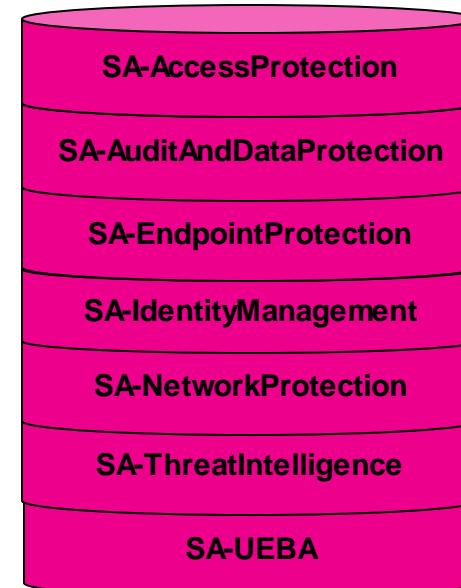
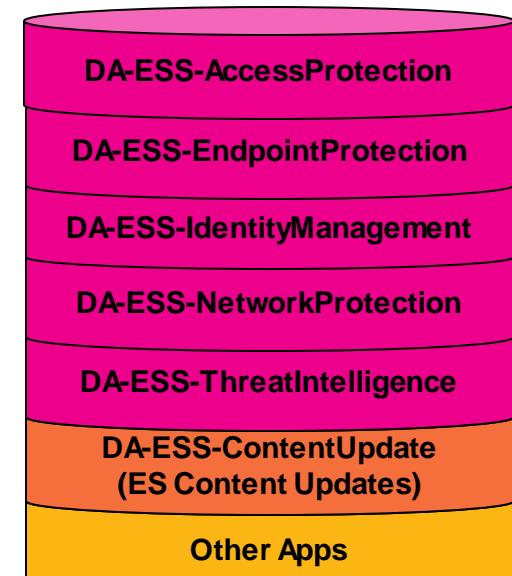


Notable Event Framework

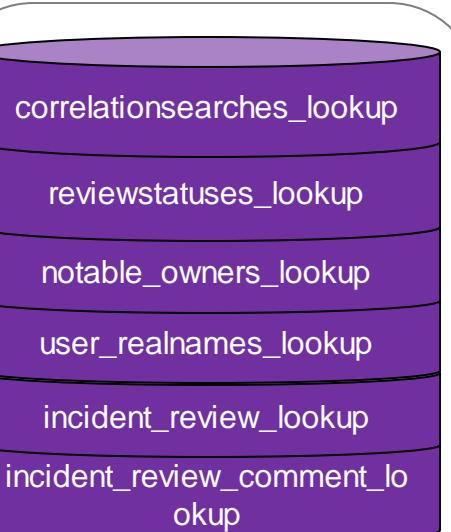
./savedsearches.conf



Enterprise Security



Adaptive Response Action



Incident Management Data Model

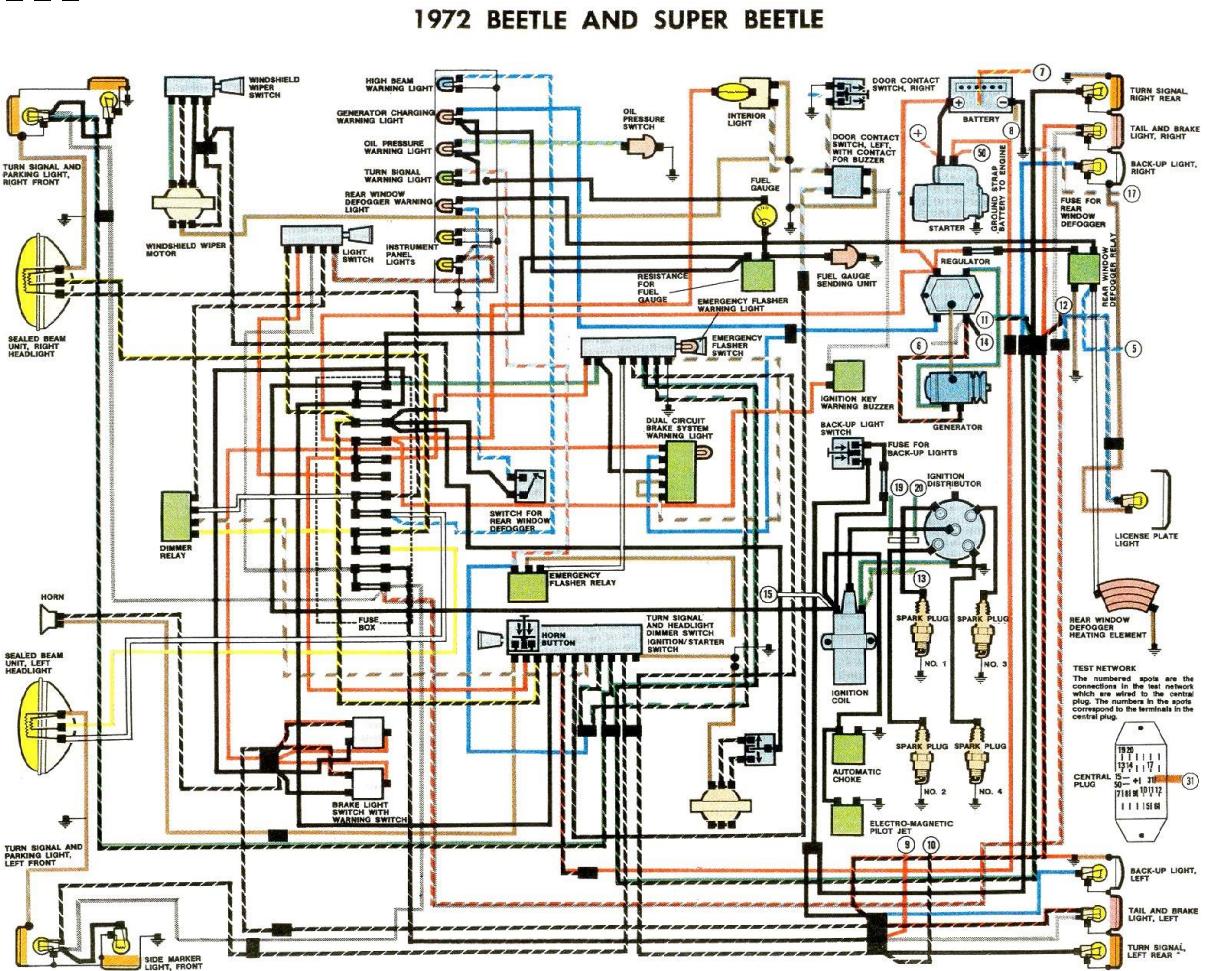
index=Notable

log_review.conf

Incident Review

Other Actions (Risk, Phantom, Cisco)

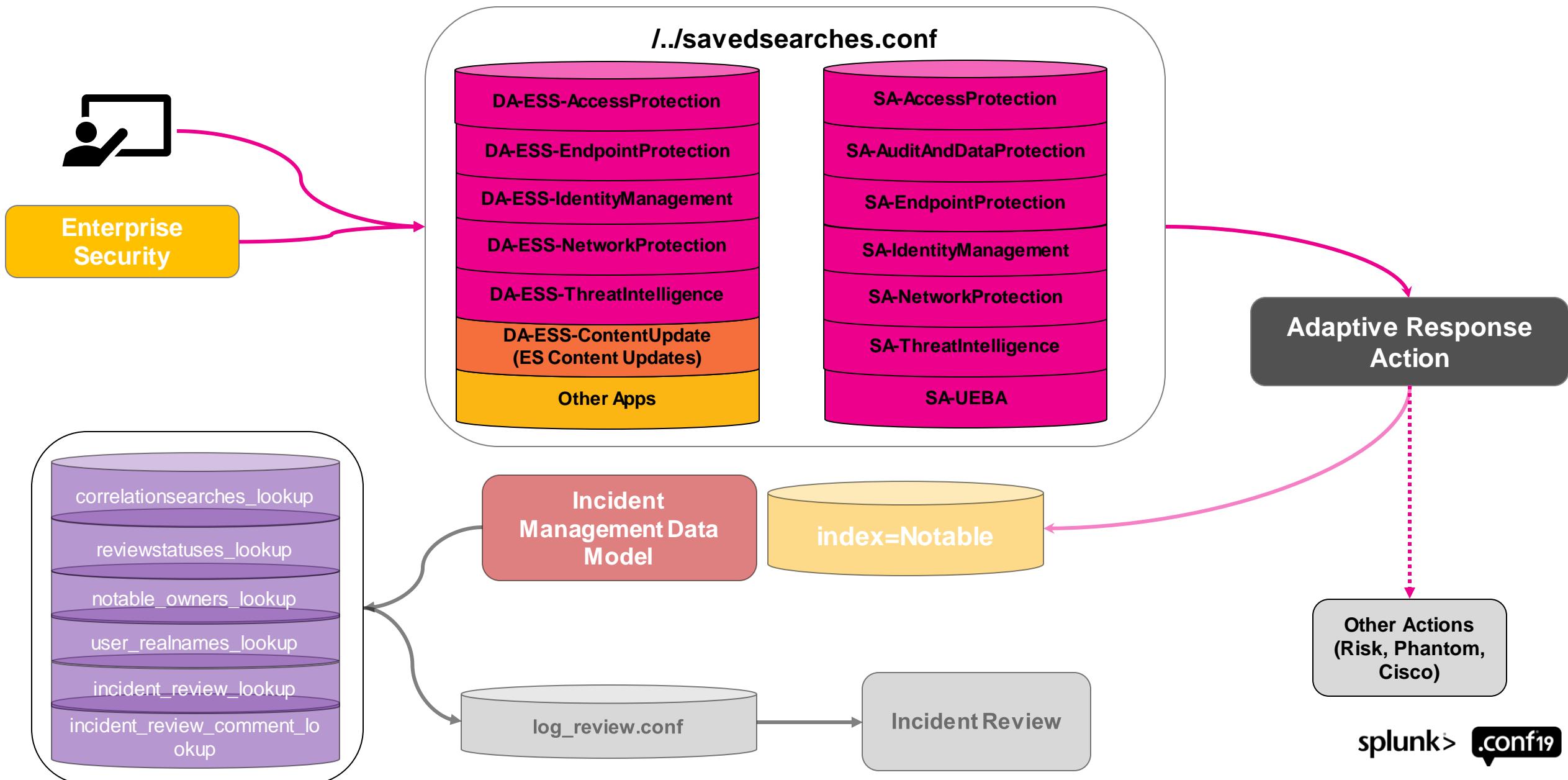
Why This Presentation...





Correlation Searches

Notable Event Framework



savedsearches.conf v. correlationsearches.conf

correlationsearches.conf was deprecated in ES4.6
confcheck_es_correlationmigration.py

Threat - Correlation Searches - Lookup Gen

All searches including correlation are found in savedsearches.conf

- action.correlationsearch.enabled=1

Search ▾

Configure ▾

SA-Investigat

All Configurations

CIM Setup

UBA Setup

General >

Content Management

Data Enrichment >

Incident Management >

Content Management

Create New Content ▾

Manage knowledge objects and other content specific to Splunk Enterprise Security, such as correlation searches, lookups, investigations, key indicators, glass tables, and reports.

[Back to ES Configuration](#)

	Name	Type	App	Next Scheduled Time	Actions
<input type="checkbox"/>	Attempt To Add Certificate To Untrusted Store	Correlation Search	ES Content Updates		Enable Disabled
<input type="checkbox"/>	AWS Cloud Provisioning From Previously Unseen IP Address	Correlation Search	ES Content Updates		Enable Disabled
<input type="checkbox"/>	Create local admin accounts using net.exe	Correlation Search	ES Content Updates	disabled = 0	Enable Disabled
<input type="checkbox"/>	Deleting Shadow Copies	Correlation Search	ES Content Updates	realtime_schedule = 0	Enable Disabled
<input type="checkbox"/>	Detect New Local Admin account	Correlation Search	ES Content Updates	Aug 14, 2019 9:00 AM GMT	Enabled Disable
<input type="checkbox"/>	Detect Unauthorized Assets by MAC address	Correlation Search	ES Content Updates		Enable Disabled
<input type="checkbox"/>	RunDLL Loading DLL By Ordinal	Correlation Search	ES Content Updates		Enable Disabled
<input type="checkbox"/>	Scheduled tasks used in BadRabbit ransomware	Correlation Search	ES Content Updates		Enable Disabled

Guided Search Briefly

Mode

Guided

Manual

Guided Search Editor X

● Data ○ Filter ○ Aggregate ○ Analyze ○ Done

Data source Data Model Lookup File

Data Model Network_Traffic ▾

Dataset All_Traffic ▾

Summaries only ? Yes No

Time Range Last 15 minutes ▾

▼ Preview

```
| from datamodel:"Network_Traffic"."All_Traffic"
```

Cancel Next >

Guided Search Editor

Data Filter Aggregate Analyze Done

Create or edit aggregates to obtain statistics on the data.

Aggregate

- sum (All_Traffic.bytes_out) as
- sum (All_Traffic.bytes_in) as
- values (All_Traffic.action) as

+ Add a new aggregate

Split-by

by All_Traffic.app as Alias

+ Add a new split-by

Preview

```
| tstats summariesonly=true allow_old_summaries=true sum(All_Traffic.bytes_out),sum(All_Traffic.bytes_in),values(All_Traffic.action) from datamodel="Network_Traffic"."All_Traffic" by "All_Traffic.app"
```

Cancel < Next >

Guided Search Editor



Filter

Field Select a field ▾

C sum(All_Traffic.bytes_out)

sum(All_Traffic.bytes_in)

values(All_Traffic.action)

All_Traffic.app

> Preview

Cancel

<

Next >

Content Management

Statistics

Content Management

Manage knowledge objects and other content specific to Splunk Enterprise Security, such as correlation searches, lookups, investigations, key indicators, glass tables, and reports.

[Create New Content ▾](#)

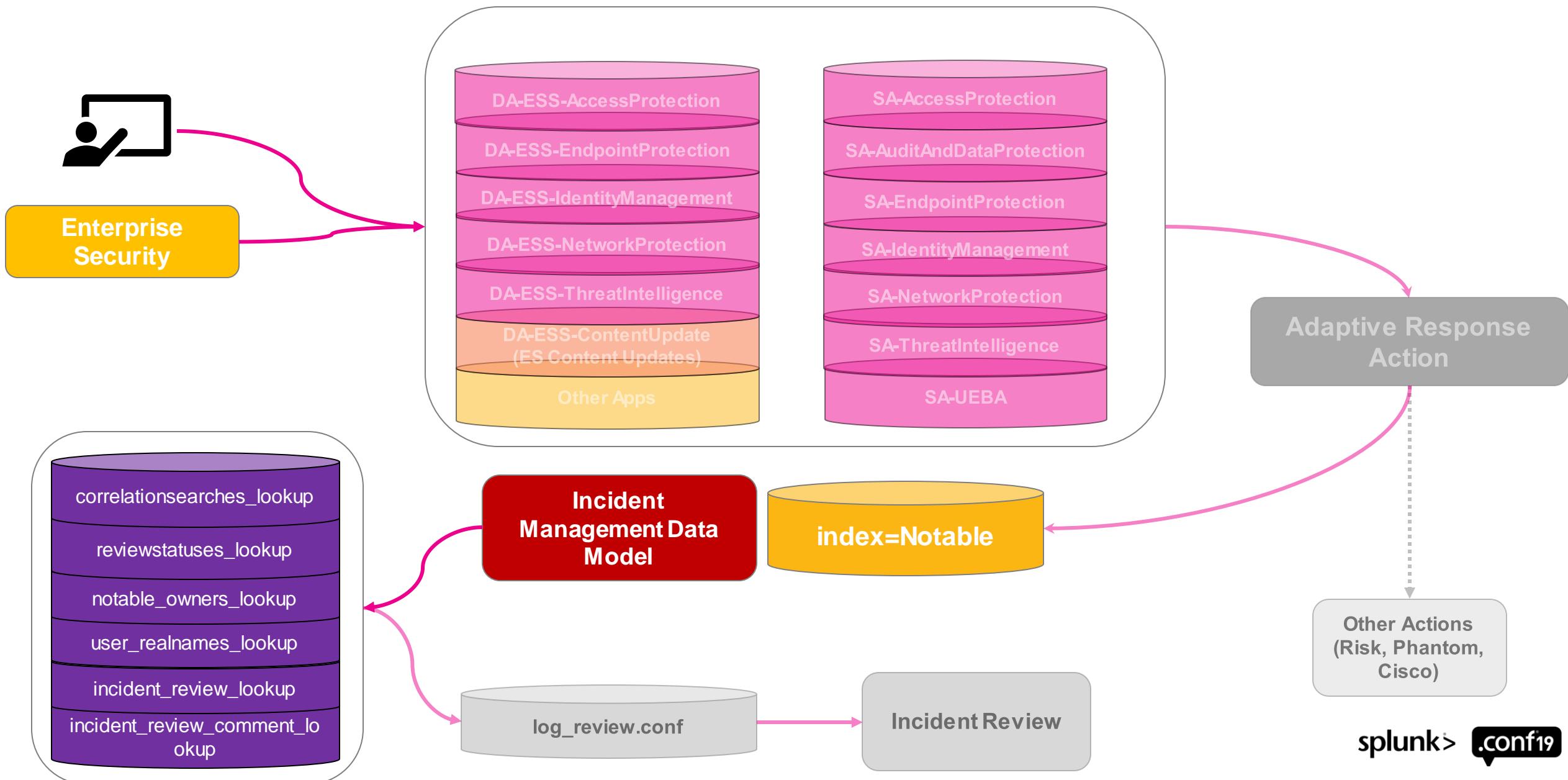
[Back to ES Configuration](#)

Edit selection ▾		Type: Correlation Search ▾	App: All ▾	Status: Enabled ▾	filter	Clear filters	25 per page ▾
9 Objects	Name	Type	App	Next Scheduled Time	Actions		
<input type="checkbox"/>	<input type="checkbox"/> i Detect New Local Admin account	Correlation Search	ES Content Updates	Sep 9, 2019 6:32 AM PDT	Enabled Disable		
<p>This search looks for newly created accounts that have been elevated to local administrators.</p> <p>The index has no events from the past 24 hours.</p> <p>Statistics</p> <ul style="list-style-type: none"> Avg. Event Count ... 1.333 Avg. Result Count .. 1.333 Avg. Run Time 0:00:02 Invocations 24 Skipped 0 Success 24 Update Time Sep 9, 2019 8:30:00 AM <p>Lookups</p> <ul style="list-style-type: none"> ✓ mitre_attack ↗ 							
<input type="checkbox"/>	> Detection of DNS Tunnels	Correlation Search	ES Content Updates	Sep 9, 2019 6:34 AM PDT	Enabled Disable		



Responses – Notables

Notable Event Framework



Incident Management Data Model

Events

- Notable Events (Metadata Only)

Searches

- Notable Events
- Suppressed Notable Events
- Incident Review
- Correlation Search Lookups
 - Correlation Searches
 - Notable Owners
 - Review Statuses
 - Security Domains
 - Urgencies
- Notable Event Suppressions
 - Suppression Audit
 - Expired Suppressions
 - Suppression Eventtypes

Incident Management

Incident_Management

[Edit ▾](#) [Download](#) [Pivot](#) [Documentation ↗](#)

[◀ All Data Models](#)

⚠ This Data Model cannot be edited because it is accelerated. Disable acceleration in order to edit the Data Model.

Datasets	Notable Events
EVENTS	Notable_Events
Notable Events (Metadata Only)	BASE SEARCH
SEARCHES	`notable` search NOT `suppression`
	Search
	EXTRACTED
	_time Time
	owner String
	owner_realname String
	rule_name String
	security_domain String
	source String
	status String
	status_group String
	tag String
	urgency String
	CALCULATED
	dest String
	src String
	Eval Expression
	Eval Expression

Notable Events

Suppressed Notable Events

Incident Review

Correlation Search Lookups

- Correlation Searches
- Notable Owners
- Review Statuses
- Security Domains
- Urgencies

Notable Event Suppressions

- Suppression Audit
- Expired Suppressions
- Suppression Eventtypes

index=notable

| from datamodel:"Incident_Management.Notable_Events"

ˋnotableˋ

```
1567951985, search_name="Threat - Threat List Activity - Rule", ppf_cell="", ppf_cell="file_name", ppf_cell="nc.exe", orig_raw="08/23/2017 21:59:57 +0000, search_name=\"Threat - File Name Matches - Threat Gen\", search_now=1505071997.000, info_search_time=1505071997.110, dest=\"160.153.91.7\", file_name=\"nc.exe\", info_max_time=\"1503547198.000000\", info_min_time=\"1503521597.000000\", info_search_time=\"1503525597.000000\", orig_sourcetype=\"stream:ftp\", src=\"10.0.2.109\", tag "\", threat_collection=file, threat_description=\"This file was detected and reported by John Stoner in the FRPCENK report\", threat_match_field=file_name, threat_match_value=\"nc.exe\"", dest="160.153.91.7", info_max_time="1567951680.000000000", info_min_time="1483257600.000000000", info_search_time="1567951982.621676000", risk_object="nc.exe", risk_object_type="other", orig_source="Threat - File Name Matches - Threat Gen", src="10.0.2.109", threat_category="undefined", threat_collection="file", threat_group="undefined", threat_match_field="file_name", threat_match_value="nc.exe"
```

Incident Review

| from datamodel:"Incident_Management.Incident_Review"

_time ▾	host	source	sourcetype	comment	owner	reviewer	rule_id	security_domain	status_label	status_group	tag	urgency
2019-09-09 06:28:49.585				Running through investigative steps...	abluebird	admin	C8A9AB2D-487E-49CB-99D8-A570ABDD07AF@notable@197aa4ceabf8bb5985d541cc66e9017b		In Progress		Open	

| `incident_review`

_time ▾	comment	owner	owner_realname	reviewer	reviewer_realname	rule_id
2019-09-09 06:28:49.585	Running through investigative steps...	abluebird	Alice Bluebird	admin	Administrator	C8A9AB2D-487E-49CB-99D8-A570ABDD07AF@notable@197aa4ceabf8bb5985d541cc66e9017b

rule_name	status	status_default	status_description	status_end	status_group	status_label	time	urgency
Threat Activity Detected	2	false	Investigation or response is in progress.	false	Open	In Progress	09/09/2019 06:28:49	

Incident Review

i		Time	Security Domain	Title	Urgency	Status	Owner	Actions
▼	□	9/8/19 7:13:05.000 AM	Threat	Threat Activity Detected (nc.exe)	Low	In Progress	Alice Bluebird	▼

Description:
Threat activity (nc.exe) was discovered in the "file_name" field based on threat intelligence available in the file collection

Additional Fields

	Value	Action
Destination	160.153.91.7 0	▼
Source	10.0.2.109 0	▼
Source DNS	wrk-klagerf.frothly.local	▼
Threat Category	undefined	▼
Threat Collection	file	▼
Threat Group	undefined	▼
Threat Match Field	file_name	▼
Threat Match Value	nc.exe	▼

Related Investigations:
Currently not investigated.

Correlation Search:
[Threat - Threat List Activity - Rule ↗](#)

History:

2019 Sep 9 9:28:49 AM	Administrator
Running through investigative steps...	

incident_review

notable`

Contributing Events:
[View all threat activity involving file_name="nc.exe" ↗](#)

Original Event:

```
08/23/2017 21:59:57 +0000, search_name="Threat - File Name Matches - Threat Gen", search_now=1505071997.000, info_search_time=1505071997.110, dest="160.153.91.7", file_name="nc.exe", info_max_time="1503547198.000000", info_min_time="1503521597.000000", info_search_time="1503525597.000000", orig_sourcetype="stream:ftp", src="10.0.2.109", tag="", threat_collection=file, threat_description="This file was detected and reported by John Stoner in the FRPCENK report", threat_match_field=file_name, threat_match_value="nc.exe"
```

Another Example

Detect New Local Admin Account - Notable

1503548335, search_name="ESCU - Detect New Local Admin account - Rule", EventCode="4720 4732", Group_Name="Administrators", Message="A member was added to a security-enabled local group.

Subject:

Security ID:	FROTHLY\\service3
Account Name:	service3
Account Domain:	FROTHLY
Logon ID:	0x927DF4B

Member:

Security ID:	FROTHLY\\svcvnc
Account Name:	-

<snip>

Additional Information:

Privileges -, Security_ID="BUILTIN\Administrators FROTHLY\\service3 FROTHLY\\svcvnc", orig_time="1503548335", description="Adversaries may steal the credentials of a specific user or service account using Credential Access techniques or capture credentials earlier in their reconnaissance process through social engineering for means of gaining Initial Access.", dest="mercury.frothly.local", identifier="T1078", info_max_time="1568031720.00000000", info_min_time="1483257600.00000000", info_search_time="1568032322.654381000", src_user="service3", tactic="Initial Access, Persistence, Privilege Escalation, Defense Evasion", technique="Valid Accounts", user="svcvnc"

9/9/19 5:32:08.000 AM Access New local admin account svcvnc created by service3.

Description:
The new user account svcvnc was created on mercury.frothly.local by service3.

Additional Fields	Value	Action	Correlation Search:
Event Code	4720 4732	▼	ESCU - Detect New Local Admin account - Rule ↗
Group Name	Administrators	▼	
Message	A member was added to a security-enabled local group. Subject: Security ID: FROTHLY\service3 Account Name: service3 Account Domain: FROTHLY Logon ID: 0x927DF4B Member: Security ID: FROTHLY\svcvnc Account Name: - Group: Security ID: BUILTIN\Administrators Group Name: Administrators Group Domain: Builtin Additional Information: Privileges: - A user account was created. Subject: Security ID: FROTHLY\service3 Account Name: service3 Account Domain: FROTHLY Logon ID: 0x927DF4B New Account: Security ID: FROTHLY\svcvnc Account Name: svcvnc Account Domain: FROTHLY Attributes: SAM Account Name: svcvnc Display Name: <value not set> User Principal Name: - Home Directory: <value not set> Home Drive: <value not set> Script Path: <value not set> Profile Path: <value not set> User Workstations: <value not set> Password Last Set: <never> Account Expires: <never> Primary Group ID: 513 Allowed To Delegate To: - Old UAC Value: 0x0 New UAC Value: 0x15 User Account Control: Account Disabled 'Password Not Required' - Enabled 'Normal Account' - Enabled User Parameters: <value changed, but not displayed> SID History: - Logon Hours: <value not set> Additional Information: Privileges -	▼	

Related Investigations:
Currently not investigated.

History:

2019 Sep 9 10:03:21 AM	Administrator
Waiting for review...	

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

Adaptive Responses: ⓘ

Response	Mode	Time	User	Status
Notable	saved	2019-09-09T05:32:05-0700	admin	✓ success
Risk Analysis	saved	2019-09-09T05:32:05-0700	admin	✓ success

[View Adaptive Response Invocations ↗](#)

Next Steps:

Recommended following steps:

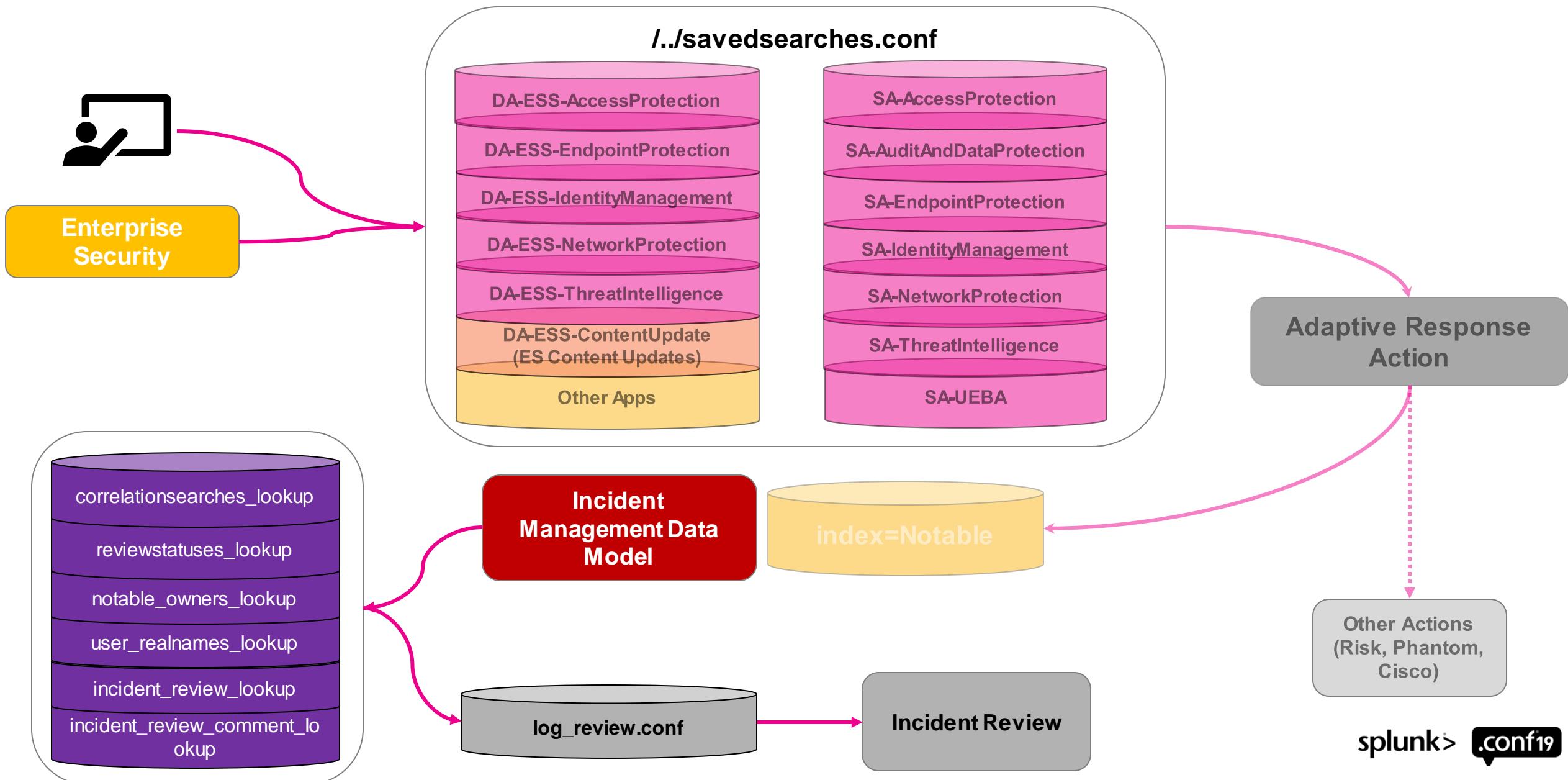
- ESCU-Contextualize:** Based on ESCU context gathering recommendations:
 - ESCU - Get Authentication Logs For Endpoint
 - ESCU - Get Notable History
 - ESCU - Get Notable Info
 - ESCU - Get Risk Modifiers For Endpoint
 - ESCU - Get Risk Modifiers For User
 - ESCU - Get User Information from Identity Table
- ESCU-Investigate:** Based on ESCU investigate recommendations:

incident_review



Incident Review

Notable Event Framework

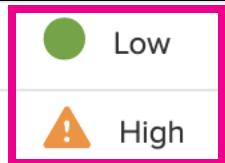


Urgency Calculation

severity						priority	urgency
low						medium	low
low						high	medium
low						critical	medium
medium						unknown	low
medium						low	low
medium						medium	medium
medium						high	high
medium						critical	high
high						unknown	medium
high						.	medium
high	ip ▲	mac ▲	nt_host ▼	dns ▲	owner ▲	priority ▲	high
high	10.0.2.107	00:0c:29:6f:d0:2f	wrk- btun	wrk- btun.frothly.local	Billy Tun	low	critical
critical	10.0.1.101	venus	venus	venus.frothly.local	Fyodor Malteskesko	high	high

PowerShell process with an encoded command detected on wrk-btun.frothly.local

PowerShell process with an encoded command detected on venus.frothly.local



Customizing Incident Review - log_review.conf

```
[root@OD-FM-CONF-NA-i-072e4f10e55fe412a default]# cat log_review.conf
[notable_editing]
allow_urgency_override = true

[comment]
minimum_length = 20
is_required = false

[incident_review]
default_earliest = -24h@h
default_latest = now

table_attributes = [{"field": "_time", "label": "Time"}, \
                    {"field": "security_domain", "label": "Security Domain"}, \
                    {"field": "rule_title", "label": "Title"}, \
                    {"field": "urgency", "label": "Urgency"}, \
                    {"field": "status_label", "label": "Status"}, \
                    {"field": "owner_realname", "label": "Owner"}]

event_attributes = [{"field": "action", "label": "Action"}, \
                     {"field": "app", "label": "Application"}, \
                     {"field": "bytes_in", "label": "Bytes In"}, \
                     {"field": "bytes_out", "label": "Bytes Out"}, \
                     {"field": "category", "label": "Category"}, \
                     {"field": "change_type", "label": "Change Type"}, \
```

Customizing Incident Review

Config -> Incident Management -> Incident Review Settings

Notable Events

Allow Overriding of
Urgency



Allows analysts to override and replace the calculated urgency of a notable

Comments

Required



Required: An analyst must provide a comment when editing a notable event.

Minimum Length

20

Minimum length of a comment if required.

Incident Review - Default Time Range

Earliest Time

0

Set a default time range of events to search. Type an earliest time using relative time modifiers.

Latest Time

now

Type a latest time using relative time modifiers.

Adding Fields to Incident Review

Incident Review - Event Attributes

List of available attributes for notable event details.

Label	Field	Action
Description - ATT&CK	description	Edit Remove
Identifier - ATT&CK	identitier	Edit Remove
Tactic - ATT&CK	tactic	Edit Remove
Technique - ATT&CK	technique	Edit Remove
Message	Message	Edit Remove
Command	cmdline	Edit Remove
Parent Process	parent_process	Edit Remove

Correlation Search Example

Process Execution via WMI

```
index=botsv2 (sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR tag=process)
parent_process_name=*WmiPrvSE.exe | stats count min(_time) as firstTime max(_time) as lastTime by dest, user, parent_process, process, parent_process_name, process_name | `ctime(firstTime)` `ctime(lastTime)` | eval identifier= "T1047" | lookup mitre_attack id AS identifier OUTPUT tactic technique description
```

9/3/19 12:33:26.000 PM Endpoint Process launched via WMI on wrk-klagerf.frothly.local ! High New

Description:
This search looks for child processes of WmiPrvSE.exe, which indicates that a process was launched via WMI.

Additional Fields	Value
ATT&CK Description	Windows Management Instrumentation (WMI) is a Windows administration feature that provides a uniform environment for local and remote access to Windows system components. It relies on the WMI service for local and remote access and the server message block (SMB) and Remote Procedure Call Service (RPCS) for remote access. RPCS operates over port 135.
Destination	wrk-klagerf.frothly.local 40
Destination Category	workstation
Destination City	windows
Destination Country	San Francisco
Destination DNS	US
Destination IP Address	wrk-klagerf.frothly.local
Destination MAC Address	10.0.2.109
Destination NT Hostname	00:0c:29:f5:5e:8e
Destination Owner	wrk-klagerf
First Time of Activity	Kevin Lagerfield
ATT&CK Identifier	08/23/2017 20:55:13
Last Time of Activity	T1047
Process	08/23/2017 20:55:13
	C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc
	WwBSAGUARgBdAC4AQQBTAHMARQBNAGIATABZA
	C4ARwBIAFQAVABZAHAAZQAOAcCauwB5AHMAdAB
	IAG0ALgBNAGEAbgBhAGcAZQtAGUAAbgB0AC4AQQ
	B1AHQAbwBtAGEAdAbpAG8AbgAuAEEAbQBzAGkAV
	QB0AGkAbAbzACcAKQB8AD8AewAkAF8AfQB8ACUA
	ewAkAF8ALgBHAEUAdABGAEkARQB8AGQAKAAnAG
	EAbQBzAGkASQBuiAGkAdABGAGEAaQB8sAGUZAAn
	ACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAdA
	BhAHQAaQBiACcAKQAUAFMARQB0AFYAYQBMAHUA

Related Investigations:
Currently not investigated.

Action **Correlation Search:**
[ESCU - Process Execution via WMI - Rule](#)

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

Adaptive Responses: (1)

Response	Mode	Time	User	Status
Risk Analysis	saved	2019-09-03T12:33:24-0700	admin	✓ success
Notable	saved	2019-09-03T12:33:23-0700	admin	✓ success

[View Adaptive Response Invocations](#)

Next Steps:

Recommended following steps:

- ESCU-Contextualize:** Based on ESCU context gathering recommendations:
 - ESCU - Get Authentication Logs For Endpoint - Rule
 - ESCU - Get Notable History - Rule
 - ESCU - Get Notable Info - Rule
 - ESCU - Get Risk Modifiers For Endpoint - Rule
 - ESCU - Get Risk Modifiers For User - Rule
 - ESCU - Get User Information from Identity Table - Rule
- ESCU-Investigate:** Based on ESCU investigate recommendations:
 - ESCU - Get Process Info - Rule
 - ESCU - Get Sysmon WMI Activity for Host - Rule

Notable Event Suppression

Incident Review & Configure -> Notable Event Suppressions

Notable Event Suppressions

[Create New Suppression](#)

Show 25 entries Search:

Label	Description	Start Time	Expiration Time
Detect_New_Local_Admin_Account	Look at throttling this.	Tue Sep 03 2019 00:00:00 GMT-0400 (Eastern Daylight Time)	Wed Sep 04 2019 00:00:00 GMT-0400 (Eastern Daylight Time)
Malicious_PowerShell_Process_-_Encoded_Command	Need to revise and review the freq throttling this.		MT-0400 (Eastern Daylight Time)
Suspicious_wvtutil_Usage	Need to revise and review the freq throttling this.		MT-0400 (Eastern Daylight Time)

Add Event to Investigation

- Build Event Type
- Extract Fields
- Run Adaptive Response Actions
- Share Notable Event
- Suppress Notable Events**
- Show Source

Suppress Notable Events

Suppression Name: Malicious_PowerShell_Process_-Encoded_Command

Description (optional):

Suppress From: 09/04/2019 To: []

Selected Fields: dest user process_name

Search Preview: `get_notable_index` source="ESCU - Malicious PowerShell Process - Encoded Command - Rule" dest="wrk-btn.frothly.local" _time>=1567569600

Cancel Save

Notable Event Suppression

The screenshot shows a Splunk search interface with the following details:

Search bar query: `get_notable_index` source="ESCU - Malicious PowerShell Process - Encoded Command - Rule" dest="wrk-klagerf .frothly.local" _time>=1567483200 _time<=1567656000 | table _time eventtype

Results summary: ✓ 14 events (9/2/19 9:00:00.000 PM to 9/4/19 9:00:01.000 PM) No Event Sampling ▾

Job controls: Job ▾, II, ■, ↗, +, ↓, Smart Mode ▾

Table navigation: Events, Patterns, Statistics (14), Visualization

Table sorting: 10 Per Page ▾, Format, Preview ▾, _time ▾, eventtype ▾, tag ▾

Table data (Rows 1-3 shown):

_time	eventtype	tag
2019-09-04 05:42:15	modnotable_results notable notable_suppression-Malicious_PowerShell_Process_-_Encoded_Command	modaction_result watchlist
2019-09-04 03:42:14	modnotable_results notable notable_suppression-Malicious_PowerShell_Process_-_Encoded_Command	modaction_result watchlist



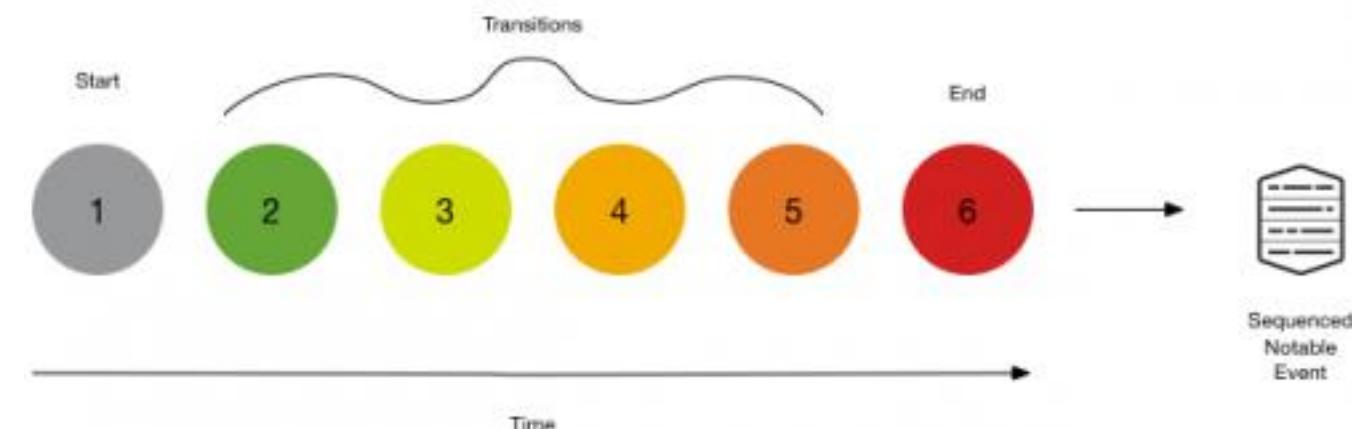
Event Sequencing and Audit

Event Sequencing

Group correlation searches into batches of events, either in a specific sequence, by specific attributes, or both

The Event Sequencing Engine runs as a indexed real-time search and listens for incoming notable events and risk modifiers that are triggered by correlation searches

Stored in the sequence_templates.conf file



Initial Configuration

Requires the edit_sequence_template capability

- ES assigns the capability to the ess_admin role

General Settings

Configuration settings for Splunk Enterprise Security by app.

[**< Back to ES Configuration**](#)

Event Sequencing Engine	Enable	Disable	SplunkEnterpriseSecuritySuite
	Enables the main Event Sequencing Engine		

Content Management

Manage knowledge objects and other content specific to Splunk Enterprise Security, such as correlation searches, lookups, investigations, key indicators, glass tables, and reports.

[Back to ES Configuration](#)

3 Objects

Edit selection ▾

Type: Sequence Template ▾

App: All ▾

Status: All ▾

filter



Clear filters

<input type="checkbox"/>	<input type="checkbox"/> i Name	Type	App	Next Scheduled Time	
<input type="checkbox"/>	Taedonggang APT	Sequence Template	ES Content Updates		Enabled Disable
<input type="checkbox"/>	Taedonggang APT - Foothold	Sequence Template	Enterprise Security		Enabled Disable
<input type="checkbox"/>	Taedonggang APT - Indicator Removal	Sequence Template	Enterprise Security		Enabled Disable

Create New Content ▾

Analytic Story

Correlation Search

Data Model

Key Indicator Search

Managed Lookup

Panel

Saved Search

Search-Driven Lookup

Sequence Template

Sequence Template

Name Taedonggang APT - Indicator Removal

Description The following actions have been seen previously in Frothly's environment and have been attributed to Taedonggang APT. These actions indicate evasion through removing indicators of activities within Frothly.

App Enterprise Security

Defines the app in which the .conf entries will be created.

Start

Correlation Search [?](#) ESCU - Process Execution via WMI - Rule

Expression [?](#) 'index'="notable"

Field value should be enclosed in single quotes, and the matching value enclosed in double quotes. Ex:
'host' = "127.0.0.1"

State [?](#)

Field	Label
user	user
dest	dest
process	process

Field	Label
user	user
dest	dest
process	process

+ Add State

Transitions

Enforce Ordering

Enforces chronological order of transitions, otherwise just checks for existence. Saving state on transitions is disabled when ordering is disabled.

Aggregate Matches

Keep accumulating matched events that may occur multiple times while template is running.
Accumulated events will be added to the final sequenced event.

Encoded PowerShell

Title Encoded PowerShell

Correlation Search [?](#) ESCU - Malicious PowerShell Process - Encoded Command - Rule

Expression [?](#) 'dest'="\$dest\$"

Field value should be enclosed in single quotes, and the matching value enclosed in double quotes.

Ex: 'host' = "127.0.0.1"

Utilization of wevtutil.exe

Title Utilization of wevtutil.exe

Correlation Search [?](#) ESCU - Suspicious wevtutil Usage - Rule

Expression [?](#) 'dest'="\$dest\$"

Field value should be enclosed in single quotes, and the matching value enclosed in double quotes.

Ex: 'host' = "127.0.0.1"

+ Add Transition

End

Correlation Search [?](#) ESCU - Windows Event Log Cleared - Rule

Expression [?](#) 'dest'="\$dest\$"

Field value should be enclosed in single quotes, and the matching value enclosed in double quotes. Ex:
'host' = "127.0.0.1"

Time Limit [?](#) 2 hour(s)

Actions

[▼ Sequenced Event](#)

Event Title Strong Indication of Taedonggang APT TTPs to Remove Indicators on \$dest_ip\$
Supports state token substitution.

Event Description This is a known set of TTPs indicative of Taedonggang APT removing indicators from i
Supports state token substitution.

Urgency Critical

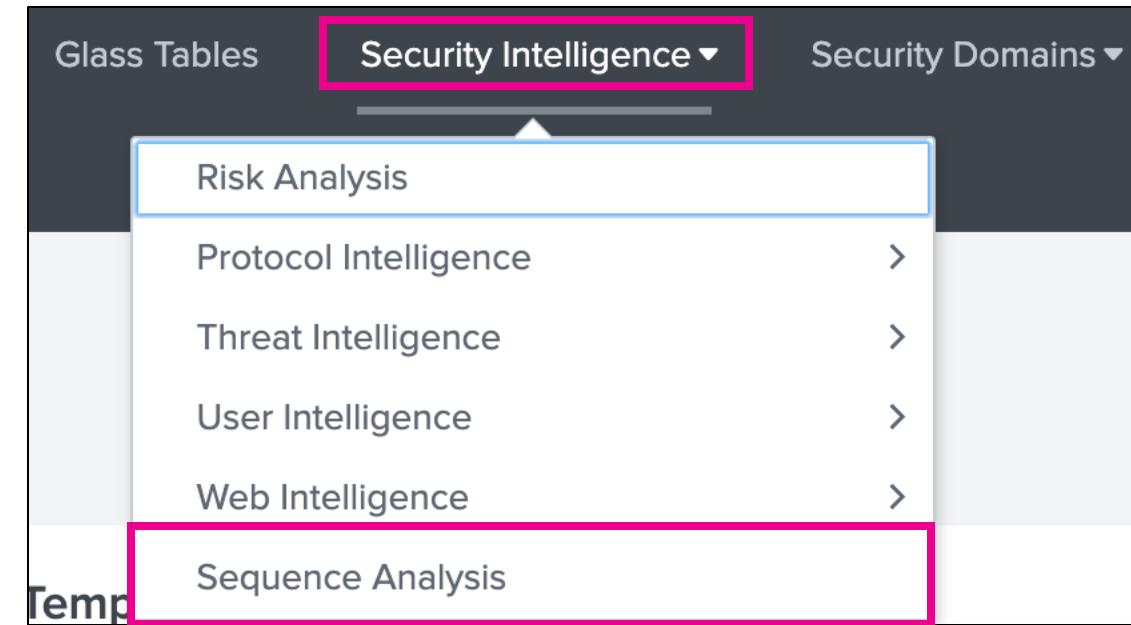
Security Domain Endpoint

Output Fields

user	\$user\$	X
dest	\$dest\$	X
process	\$process\$	X

+ Add Field

The value field can be populated with either static values or saved state tokens from transitions.



Sequence Analysis

View the running list of attack templates.

[◀ Back to Content Management](#)

50 Objects

Showing: All ▾

Showing: Last 24 Hours ▾

◀ Prev 1 2 3 4 5 Next ▶

i	Attack Template ▾	Start Time ▾	Last Activity Time ▾	Status ▾	Actions
>	Taedonggang APT - Foothold	Mon Sep 02 2019 13:33:09 GMT-0400 (Eastern Daylight Time)	6 hours ago	expired	Edit sequence
>	Taedonggang APT - Indicator Removal	Mon Sep 02 2019 18:34:20 GMT-0400 (Eastern Daylight Time)	6 hours ago	expired	Edit sequence
>	Taedonggang APT	Mon Sep 02 2019 18:33:09 GMT-0400 (Eastern Daylight Time)	6 hours ago	expired	Edit sequence
>	Taedonggang APT	Mon Sep 02 2019 23:33:09 GMT-0400 (Eastern Daylight Time)	6 hours ago	expired	Edit sequence
>	Taedonggang APT - Indicator Removal	Tue Sep 03 2019 03:34:27 GMT-0400 (Eastern Daylight Time)	7 hours ago	running	Edit sequence

State Data

user FROTHLY\service3
 dest venus.frothly.local
 dest_dns dest_ip dest_nt_host

Transitions

Title	Time	State
start	Tue Sep 03 2019 13:33:19 GMT-0400 (Eastern Daylight Time)	Matched
Encoded PowerShell	Tue Sep 03 2019 13:42:12 GMT-0400 (Eastern Daylight Time)	Matched
Utilization of wevtutil.exe		Awaiting Matches
end		Awaiting Matches

State Data

dest_dns user FROTHLY\billy.tun
 dest_nt_host dest_ip

Transitions

Title	Time	State
start	Mon Sep 02 2019 13:33:21 GMT-0400 (Eastern Daylight Time)	Matched
Encoded PowerShell		No match found
Utilization of wevtutil.exe		No match found
end		No match found

Expiration Date

This sequence instance expired at Mon Sep 02 2019 21:33:21 GMT-0400 (Eastern Daylight Time)

9/4/19 10:07:05.000 AM Endpoint Strong Indication of Taedonggang APT TTPs to Remove Indicators on 10.0.2.109 ⚠ Critical

Sequenced Event Description:
This is a known set of TTPs indicative of Taedonggang APT removing indicators from a compromised system. These TTPs have previously been used to targeted Froth.ly. Escalate this to Alice upon immediate alert.

Template Title: Taedonggang APT - Indicator Removal

Template Description:
The following actions have been seen previously in Frothly's environment and have been attributed to Taedonggang APT. These actions indicate evasion through removing indicators of activities within Frothly.
[View events](#)

Transitions:

Stage	Time	Match
start	Sep 4, 2019 9:33 AM	Process launched via WMI on wrk-klagerf.frothly.local View original events
Encoded PowerShell	Sep 4, 2019 9:42 AM	PowerShell process with an encoded command detected on wrk-klagerf.frothly.local View original events
Utilization of wevtutil.exe	Sep 4, 2019 10:02 AM	Suspicious wevtutil Usage View original events
end	Sep 4, 2019 10:06 AM	Windows Event Log Cleared on OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com View original events

Additional Fields

Destination	Value
Destination Category	wrk-klagerf.frothly.local 40
Destination City	workstation
Destination Country	windows
Destination DNS	San Francisco
Destination IP Address	US
Destination MAC Address	wrk-klagerf.frothly.local
Destination NT Hostname	10.0.2.109
Destination Owner	00:0c:f5:5e:8e
End Time	wrk-klagerf
Process	Kevin Lagerfield
Start Time	Sep 4, 2019 2:33 PM
User	C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc
	WwBSAGUARqBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBIAFQAVABZAHAAZQoACcAUwB5AHMAdABIAGOALqBNA

2019-09-04 03:42:14	ESCU - Malicious PowerShell Process - Encoded Command - Rule	wrk-klagerf.frothly.local	modnotable_results notable notable_suppression-Malicious_PowerShell_Process_-Encoded_Command
---------------------	--	---------------------------	---

Transitions:

Stage	Time	Match
start	Sep 4, 2019 2:33 AM	Process launched via WMI on wrk-klagerf.frothly.local View original events
Encoded PowerShell	Sep 4, 2019 3:42 AM	PowerShell process with an encoded command detected on wrk-klagerf.frothly.local View original events
Utilization of wevtutil.exe	Sep 4, 2019 3:02 AM	Suspicious wevtutil Usage View original events
end	Sep 4, 2019 4:06 AM	Windows Event Log Cleared on OD-FM-NA-i-00d3cc13d300ce9d5.amazonaws.com View original events
Additional Fields		Value
Destination		wrk-klagerf.frothly.local 40

2019-09-04 03:02:29	ESCU - Suspicious wevtutil Usage - Rule	wrk-klagerf.frothly.local	modnotable_results notable notable_suppression-Suspicious_wevtutil_Usage
---------------------	---	---------------------------	---

Testing Your Event Templates

`execute_sequence_template(*template_name*, false)`

```
{ [-]  
  dest: wrk-klagerf.frothly.local  
  end_time: 1567690399  
  events_spl: earliest=1567683199.0 latest=1567685164.0 `event_seq_events` | search event_id="C8A9AB2D-487E-49CB-99D8-A570A  
  orig_rid: 0f7b2bab-4c82-4798-966c-4453a824f4df  
  orig_sid: 1567690579.3925  
  process: C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc  
  WwBSAGUARgBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBlAFQAVABZAHAAZQAOACcAUwB5AHMAdABLAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBt  
  rid: 0f7b2bab-4c82-4798-966c-4453a824f4df  
  rule_description: This is a known set of TTPs indicative of Taedonggang APT removing indicators from a compromised system  
  rule_title: Strong Indication of Taedonggang APT TTPs to Remove Indicators on $dest_ip$  
  security_domain: endpoint  
  start_time: 1567683199  
  template_description: The following actions have been seen previously in Frothly's environment and have been attributed to  
  template_name: Taedonggang APT - Indicator Removal  
  transition_matches: [{"stage": "start", "matches": [{"event_time": 1567683199.0, "reason": "start_match", "event_title": "Indicator Removal"}]}]  
  urgency: critical  
  user: FROTHLY\service3  
}
```

Incident Review Audit

Incident Review Audit

[Edit](#) [Export](#) ...

Review Activity By Reviewer

count

time

Alice Bluebird
Kevin Lagerfield

Top Reviewers

reviewer_realname	sparkline	count	firstTime	lastTime
Alice Bluebird		45	09/01/2017 11:37:45	09/01/2017 11:47:17
Kevin Lagerfield		1	06/21/2017 08:37:09	06/21/2017 08:37:09

Notable Events By Status - Last 48 Hours

status

New
Resolved
Closed
Pending
In Progress
Unassigned

count

critical
high
informational
low
medium

Notable Events By Owner - Last 48 Hours

owner

unassigned
ablubird
admin
klagerfield

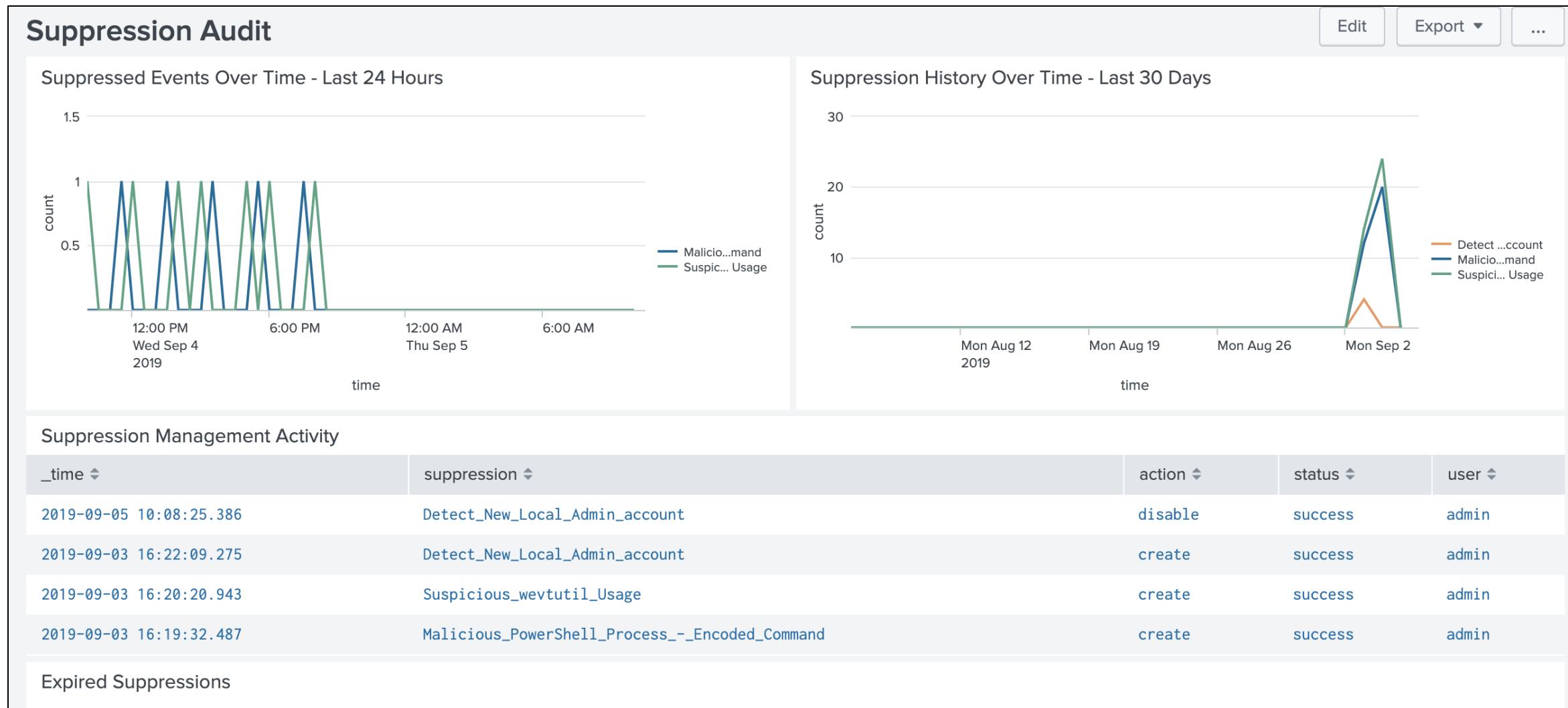
count

critical
high
informational
low
medium

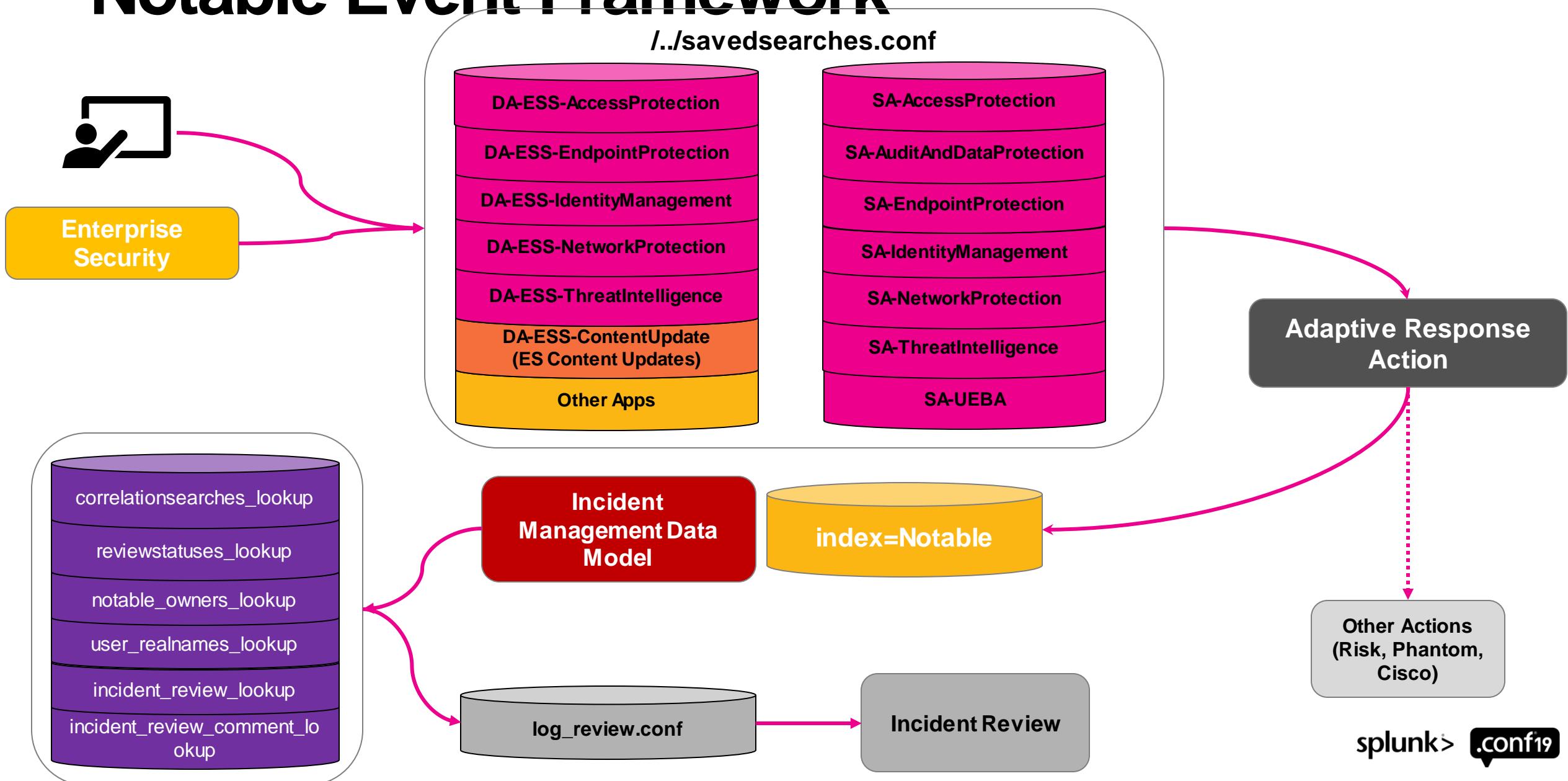
Mean Time To Triage - Last 14 days

Mean Time To Closure - Last 60 days

Suppression Audit



Notable Event Framework



Helpful Links

Splunk Security Essentials – More Ideas for Correlation Searches

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

ES Content Update

- <https://splunkbase.splunk.com/app/3449/>

Tutorial – Create a Correlation Search

- <https://docs.splunk.com/Documentation/ES/5.3.1/Tutorials/CorrelationSearch>

Incident Management/Notable Event Framework

- <http://dev.splunk.com/view/enterprise-security/SP-CAAAFA9>

Enhancing Incident Review

- <http://www.georgestarcher.com/splunk-enterprise-security-enhancing-incident-review/>

Upgrades after 4.5 – Saved Search v Correlation Search

- <https://docs.splunk.com/Documentation/ES/5.3.1/Admin/Upgradecorrelationsearches>

Modifying the Incident Review Page

- <https://www.splunk.com/blog/2019/02/15/modifying-the-incident-review-page.html>

Closing Thoughts

1. Incident Management Framework drives Notable Events
2. Good Deal of Flexibility to Handle How You Deal with Different Notables and What The Analyst Sees
3. Ensure your notables are high fidelity before leveraging event sequencing
4. Suppression provides a trackable method to handle noisy notables but action is required!

.conf19

splunk>

Thank
You!

Go to the .conf19 mobile app to

RATE THIS SESSION





Appendix

Correlation Search Mapping to .conf file

Search Name *	Detect New Local Admin account
App *	ES Content Updates ▾
UI Dispatch Context *	Enterprise Security ▾ <p>Set an app to use for links such as the drill-down search in a notable event or links in an email adaptive response action. If None, uses the Application Context.</p>
Description	This search looks for newly created accounts that have been elevated to local administrators. Describes what kind of issues this search is intended to detect.
Mode	Guided Manual
Search *	sourcetype=wineventlog:security EventCode=4720 OR (EventCode=4732 Group_Name= Administrators) transaction Security_ID maxspan=180m search EventCode=4720 EventCode=4732 table _time user dest EventCode Security_ID Group_Name src_user Message

action.correlationsearch.label

request.ui_dispatch_app

description

search

ESCU - Detect New Local Admin account

Configure in ES

Description
This search looks for newly created accounts that have been elevated to local administrators.

Explain It Like I'm 5
This search looks for Windows Event Code 4720 (account creation) and 4732 (account added to a security-enabled local group), where the group name is "Administrators", and determines whether they are generated for the same user's Security ID within three hours of each other. It will return the user account that was added, the Security ID, the group name to which the user was added, the account name of the user who initiated the action, and the subsequent message returned.

Search

```
sourcetype=wineventlog:security EventCode=4720 OR (EventCode=4732 Group_Name="Administrators") | transaction Security_ID maxspan=180m | search EventCode=4720 EventCode=4732 | table _time user dest EventCode Security_ID Group_Name src_user Message
```

All time

How to Implement
You must be ingesting Windows Security logs. You must also enable the account change auditing (here). Additionally, this search requires you to enable your Group Management Audit Logs in your Local Windows Security Policy and to be ingesting those logs. More information on how to enable them can be found here. Finally, please make sure that the local administrator group name is "Administrators" to be able to look for the right group membership changes.

Known False Positives
The activity may be legitimate. For this reason, it's best to verify the account with an administrator and ask whether there was a valid service request for the account creation. If your local administrator group name is not "Administrators", this search may generate an excessive number of false positives.

ATT&CK
Valid Accounts Defense Evasion
Persistence
Kill Chain Phases
Actions on Objectives
Command and Control
CIS Controls
CIS 16
Data Models
Technologies Microsoft Windows
Asset at Risk Windows
Confidence medium
Creation Date 2018-03-26
Modification Date 2018-03-26

action.escu = 0
 action.escu.enabled = 1
 action.escu.creation_date = 2018-03-26
 action.escu.modification_date = 2018-03-26
 action.escu.asset_at_risk = Windows
 action.escu.channel = ESCU
 action.escu.confidence = medium
 action.escu.el5 = This search looks for Windows Event Code 4720 (account creation) and 4732 (account added to a security-enabled <snip>
 action.escu.how_to_implement = You must be ingesting Windows Security logs. You must also enable the account change auditing <snip>
 action.escu.full_search_name = ESCU - Detect New Local Admin account
 action.escu.mappings = {"mitre_attack": ["Valid Accounts", "Defense Evasion", "Persistence"], "kill_chain_phases": ["Actions on Objectives", "Command and Control"], "cis20": ["CIS 16"], "nist": ["PR.AC", "DE.CM"]}
 action.escu.known_false_positives = The activity may be legitimate. <snip>
 action.escu.search_type = detection
 action.escu.providing_technologies = ["Microsoft Windows"]
 action.escu.analytic_story = ["DHS Report TA18-074A"]

Time Range

© 2019 SPLUNK INC.

Earliest Time

-1440m@m

Set a time range of events to search. Type an earliest time using relative time modifiers.

Latest Time

-5m@m

Type a latest time using relative time modifiers.

Cron Schedule *

0 9 * * *

Enter a cron-style schedule. For example `*/5 * * * *` (every 5 minutes) or `'0 21 * * *'` (every day at 9 PM). Real-time searches use a default schedule of `*/5 * * * *.`

Scheduling

Real-time

Continuous

Controls the way the scheduler computes the next execution time of a scheduled search. This controls the `realtime_schedule` setting. [Learn more](#)

Schedule Window

auto

Let report run at any time within a window that opens at its scheduled run time, to improve efficiency when there are many concurrently scheduled reports. The "auto" setting automatically determines the best window width for the report.

Schedule Priority

Higher ▾

Raise the scheduling priority of a report. Set to "Higher" to prioritize it above other searches of the same scheduling mode, or "Highest" to prioritize it above other searches regardless of mode. Use with discretion.

`dispatch.earliest_time = -1440m@m`

`dispatch.latest_time = -5m@m`

`cron_schedule = 0 9 * * *`

`schedule_window = auto`

`schedule_priority = higher`

Trigger Conditions

© 2019 SPLUNK INC.

Trigger alert when

Number of Results ▾

is greater than ▾ 0

counttype = number of events
relation = greater than
quantity = 0

Throttling

Window duration

1

day(s) ▾

How much time to ignore other events that match the field values specified in Fields to group by.

Fields to group by

user 

Type a field and press enter

Type the fields to consider for matching events for throttling. [Learn more](#) 

alert.suppress = 1
alert.suppress.period = 86400s

alert.suppress.fields = user

action.notable = 1
action.makestreams.param.verbose = 0
action.nbtstat.param.verbose = 0
action.notable.param.verbose = 0
action.nslookup.param.verbose = 0
action.ping.param.verbose = 0
action.send2uba.param.verbose = 0
action.threat_add.param.verbose = 0

Adaptive Response Actions

+ Add New Response Action ▾

- >  Risk Analysis 
- >  Notable 

Adaptive Response Actions

+ Add New Response Action ▾

▼  Risk Analysis

Risk Score*	40
Risk Object Field*	user
Risk Object Type*	system

Learn more [🔗](#) about risk modifiers.

```
action.risk = 1  
action.risk.param._risk_score = 40  
action.risk.param._risk_object = user  
action.risk.param._risk_object_type = system  
action.risk.param.verbose = 0
```

▼  Notable

Title
Notable events created by this search will have this title. Supports variable substitution.

Description
Notable events created by this search will have this description. Supports variable substitution.

Security Domain

Severity
Used to calculate urgency for notable events.
[Learn more](#) 

Default Owner

Default Status

`action.notable.param.rule_title = New local admin account
$user$ created by src_user.`

`action.notable.param.rule_description = The new user account
$user$ was created on $dest$ by src_user.`

`action.notable.param.security_domain = access`

`action.notable.param.severity = medium`

`action.notable.param.default_owner = abluebird`

`action.notable.param.default_status = 2`

Drill-down Name

View All Local Admin Accounts

Supports variable substitution with fields from the matching event.

Drill-down Search

sourcetype=wineventlog:security (Event)

Supports variable substitution with fields from the matching event.

Drill-down Earliest Offset

1d

Set the amount of time before the triggering event to search for related events. For example, 2h. Use `$info_min_time$` to set the drill-down time to match the earliest time of the search

Drill-down Latest Offset

6h

Set the amount of time after the triggering event to search for related events. For example, 1m. Use `$info_max_time$` to set the drill-down time to match the latest time of the search

Investigation Profiles

Admin Issues X

Asset Extraction

src X dest X dvc X orig_host X

Identity Extraction

src_user X user X

action.notable.param.drilldown_name = View All Local Admin Accounts

action.notable.param.drilldown_search = sourcetype=wineventlog:security (EventCode=4732 Group_Name= Administrators) | table _time user dest EventCode Security_ID Group_Name src_user Message

**action.notable.param.drilldown_earliest_offset = 86400
action.notable.param.drilldown_latest_offset = 21600**

action.notable.param.investigation_profiles = {"profile://Admin Issues":{}}

action.notable.param.extract_assets = ["src","dest","dvc","orig_host"]

action.notable.param.extract_identities = ["src_user","user"]

Next Steps

Insert Adaptive Response Action ▾

Recommended following steps:

1. [[action|escu_contextualize]]: Based on ESCU context gathering recommendations:
 - ESCU - Get Authentication Logs For Endpoint
 - ESCU - Get Notable History
 - ESCU - Get Notable Info

Describe next steps and response actions that an analyst could take to address this threat. Add a link to an action with the syntax:
[[action|nameOfAction]]

```
action.notable.param.next_steps =
{"version":1,"data":"Recommended following
steps:\n\n1. [[action|escu_contextualize]]: Based on
ESCU context gathering recommendationsect:\n  -
ESCU - Get Authentication Logs For
Endpoint\n <snip>"}
```

Recommended Actions

All

Recommended

Filter
→ →
Send email
Run a script
AWS SNS Alert
Stream Capture
Nbtstat
Nslookup

Filter
← ←
ESCU-Contextualize
ESCU-Investigate
Run Playbook in Phantom

```
action.notable.param.recommended_actions =
escu_contextualize,escu_investigate,runphantompla
ybook
```

```
action.notable.param.next_steps =  
{"version":1,"data":"Recommended  
following steps:\n\n1.  
[[action|escu_contextualize]]: Based on  
ESCU context gathering  
recommendationsect:\n<snip> - ESCU - Get  
Risk Modifiers For User\n - ESCU - Get  
User Information from Identity Table\n\n2.  
[[action|escu_investigate]]: Based on ESCU  
investigate recommendations:\n - ESCU -  
Get Parent Process Info\n - ESCU - Get  
Process Info\n"}
```

Next Steps:

Recommended following steps:

1. [ESCU-Contextualize](#): Based on ESCU context gathering recommendations:
 - ESCU - Get Authentication Logs For Endpoint
 - ESCU - Get Notable History
 - ESCU - Get Notable Info
 - ESCU - Get Risk Modifiers For Endpoint
 - ESCU - Get Risk Modifiers For User
 - ESCU - Get User Information from Identity Table

2. [ESCU-Investigate](#): Based on ESCU investigate recommendations:
 - ESCU - Get Parent Process Info
 - ESCU - Get Process Info