

Enterprise Security Biology III:

Incident Review Framework

John Stoner | Principal Security Strategist

October 2019

.conf19

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.

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

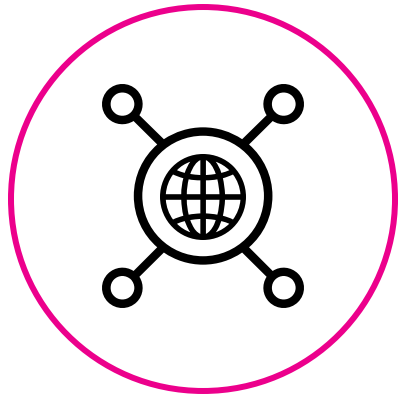
Correlation Searches

Notables

Incident Review

Event Sequencing & Audit

Enterprise Security Frameworks



Threat Intelligence



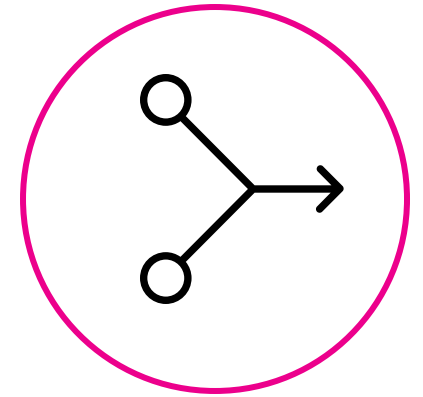
Incident Management



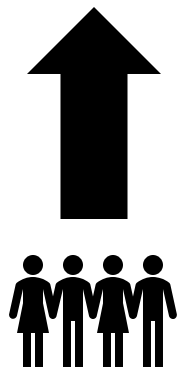
Asset & Identity



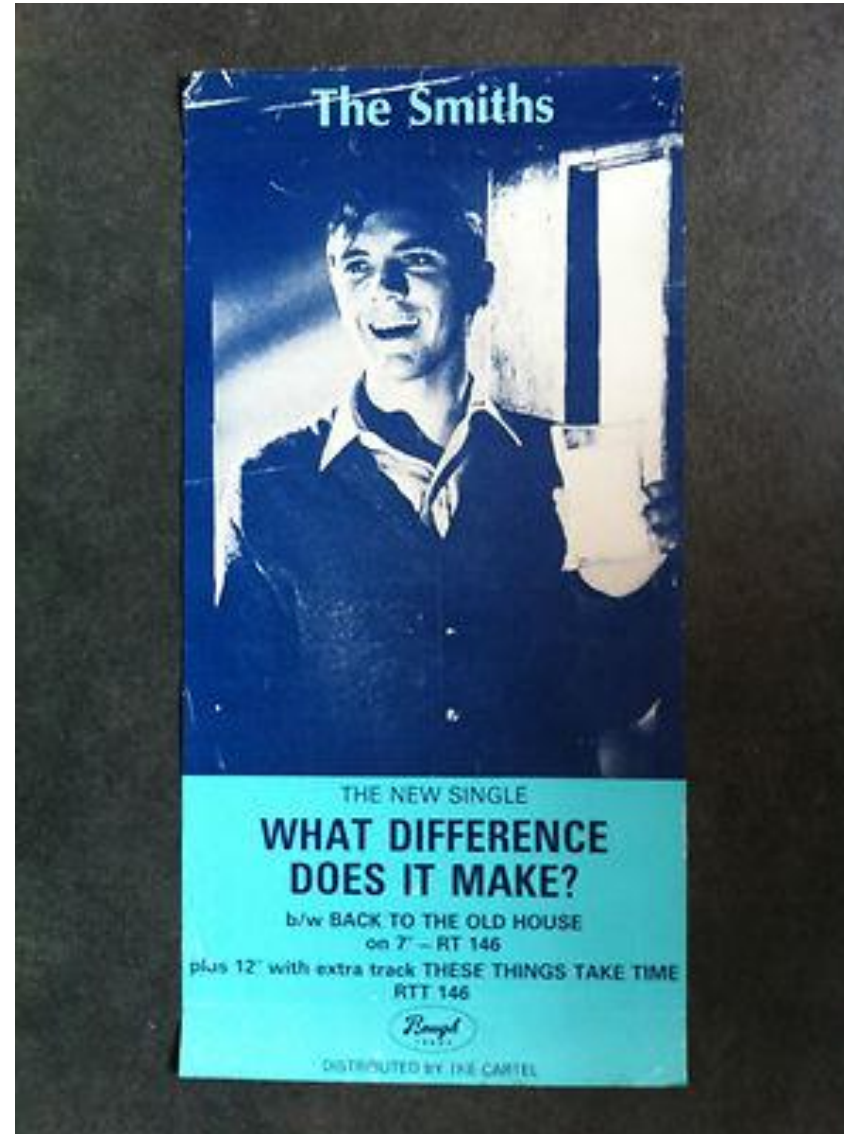
Risk



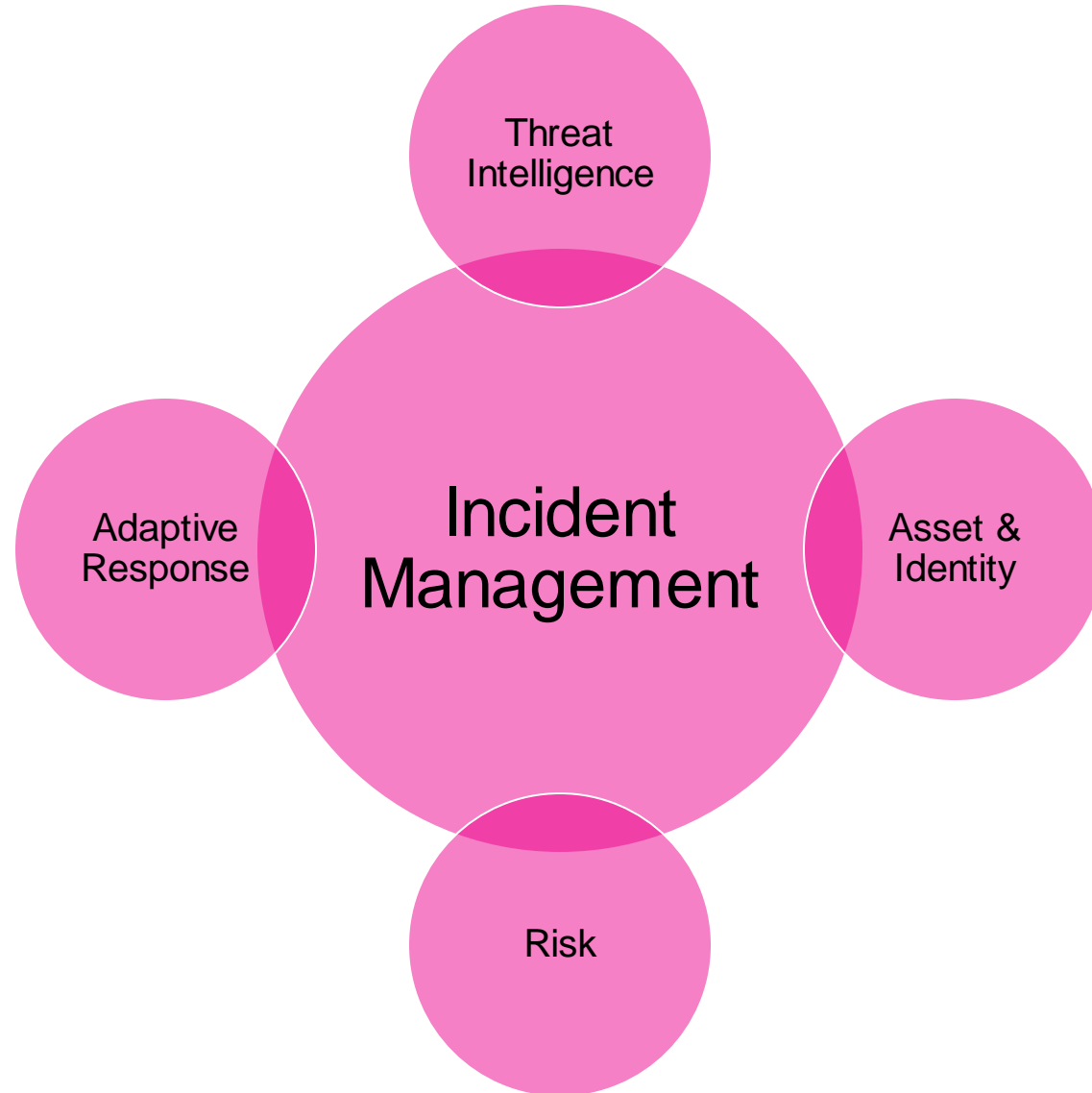
Adaptive Response



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

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

Additional Fields

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

Related Investigations:
Investigation (No Permission)

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"
```

[View original event](#)

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

[View Adaptive Response Invocations](#)

Next Steps:

No Next Steps defined.

Our Goal Today?

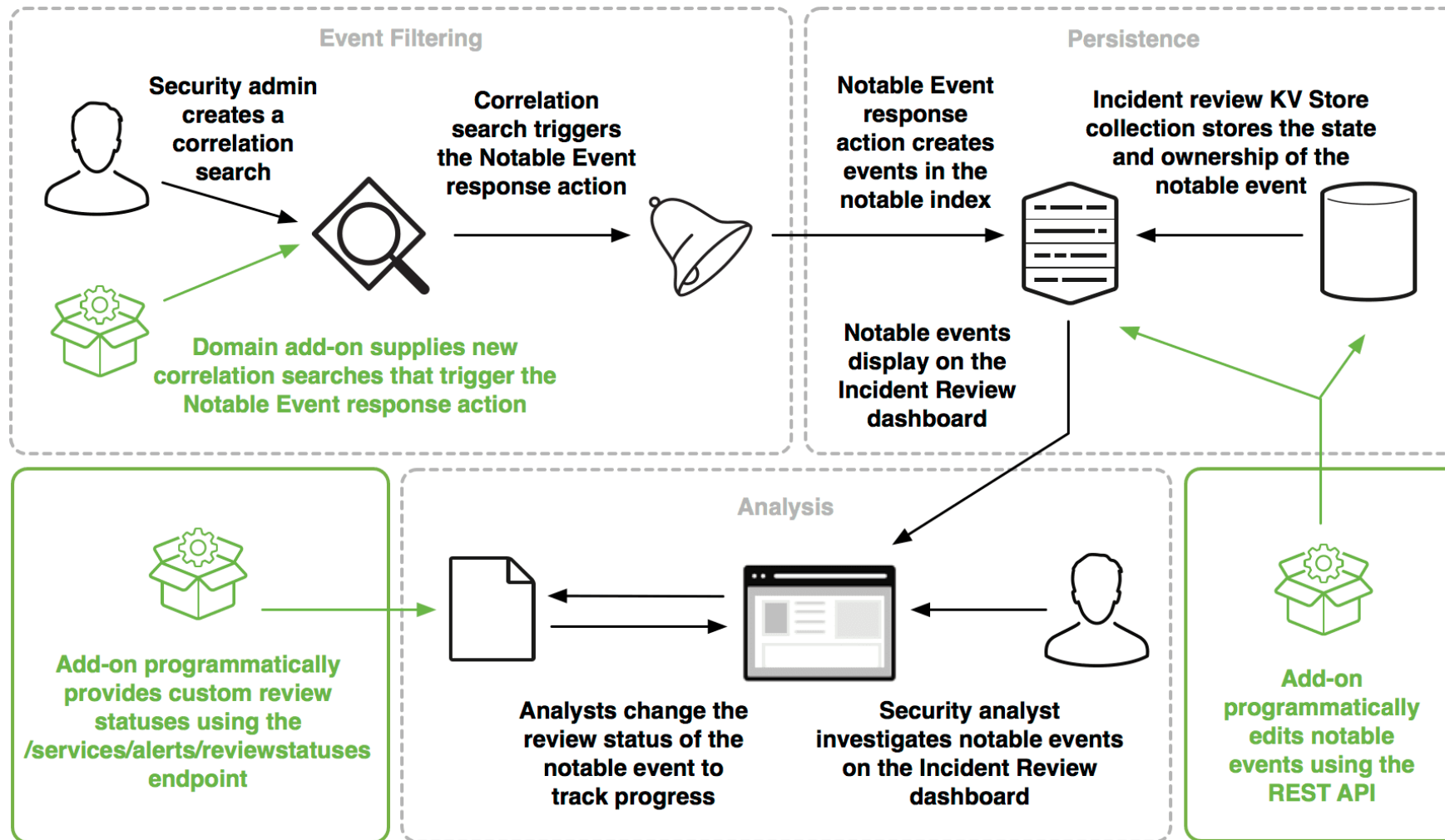
Better understand how
Splunk processes
notable events in
Enterprise Security

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



Notable Event Framework

<http://dev.splunk.com/view/enterprise-security/SP-CAAFA9>

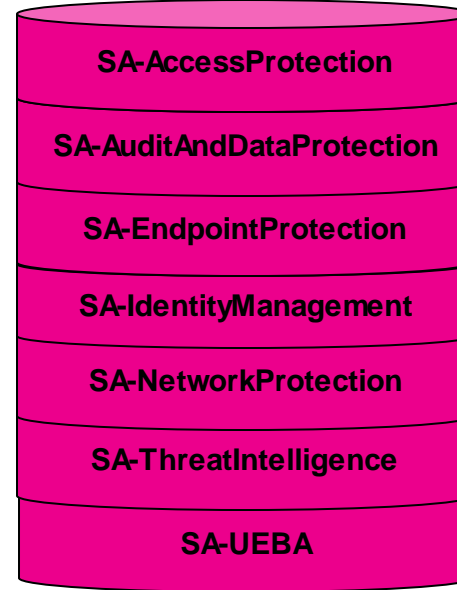
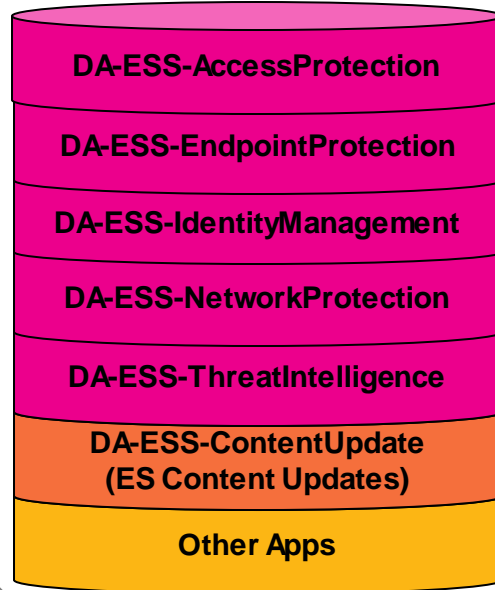


Notable Event Framework

`./savedsearches.conf`



Enterprise Security



Adaptive Response Action

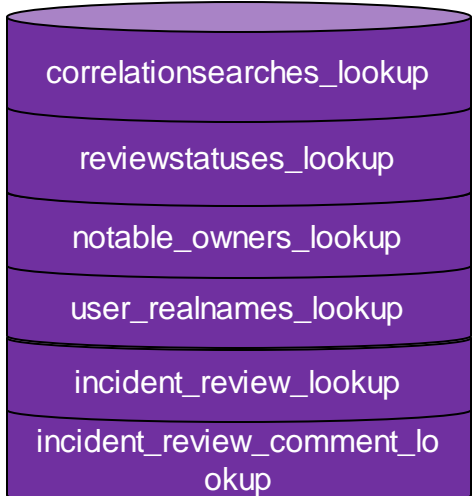
Incident Management Data Model

`index=Notable`

`log_review.conf`

Incident Review

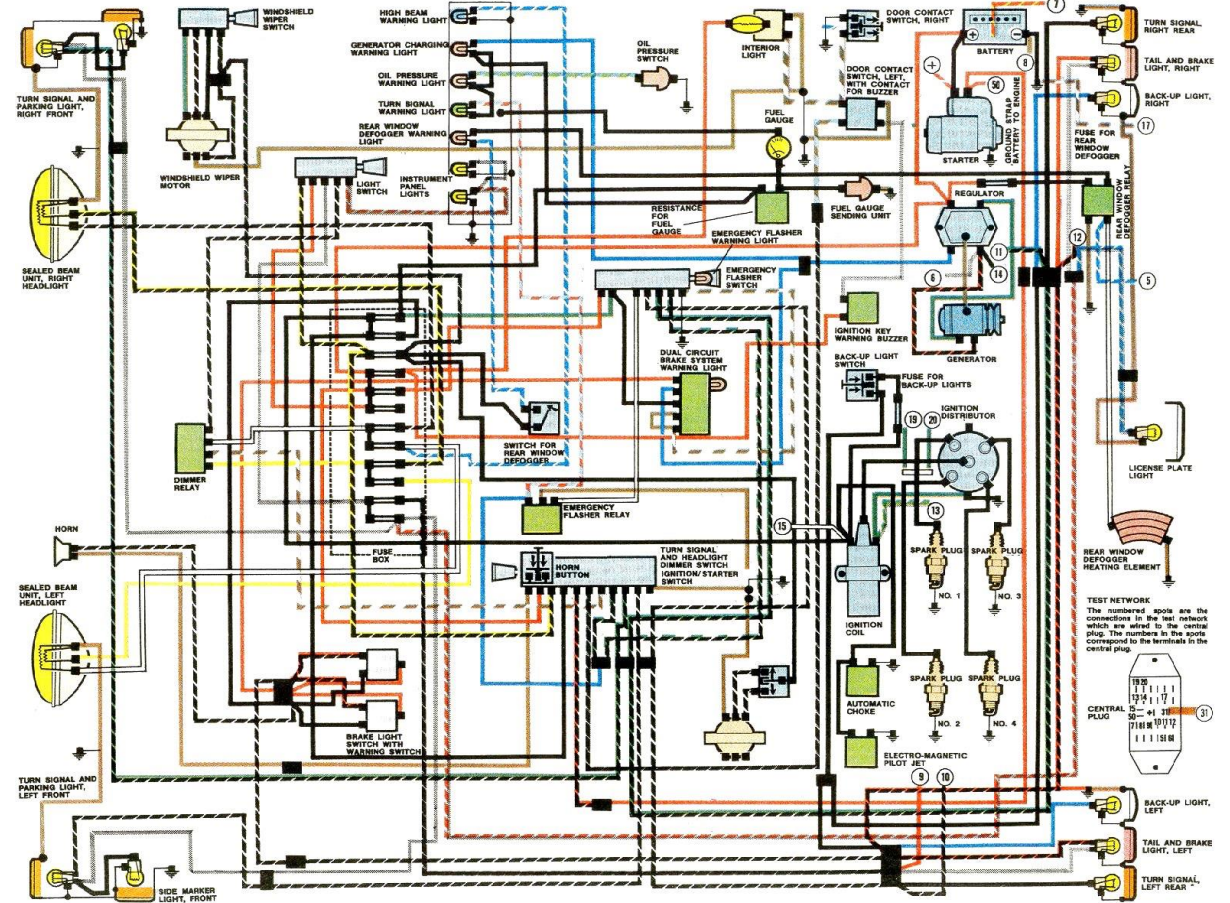
Other Actions (Risk, Phantom, Cisco)



Why This Presentation...



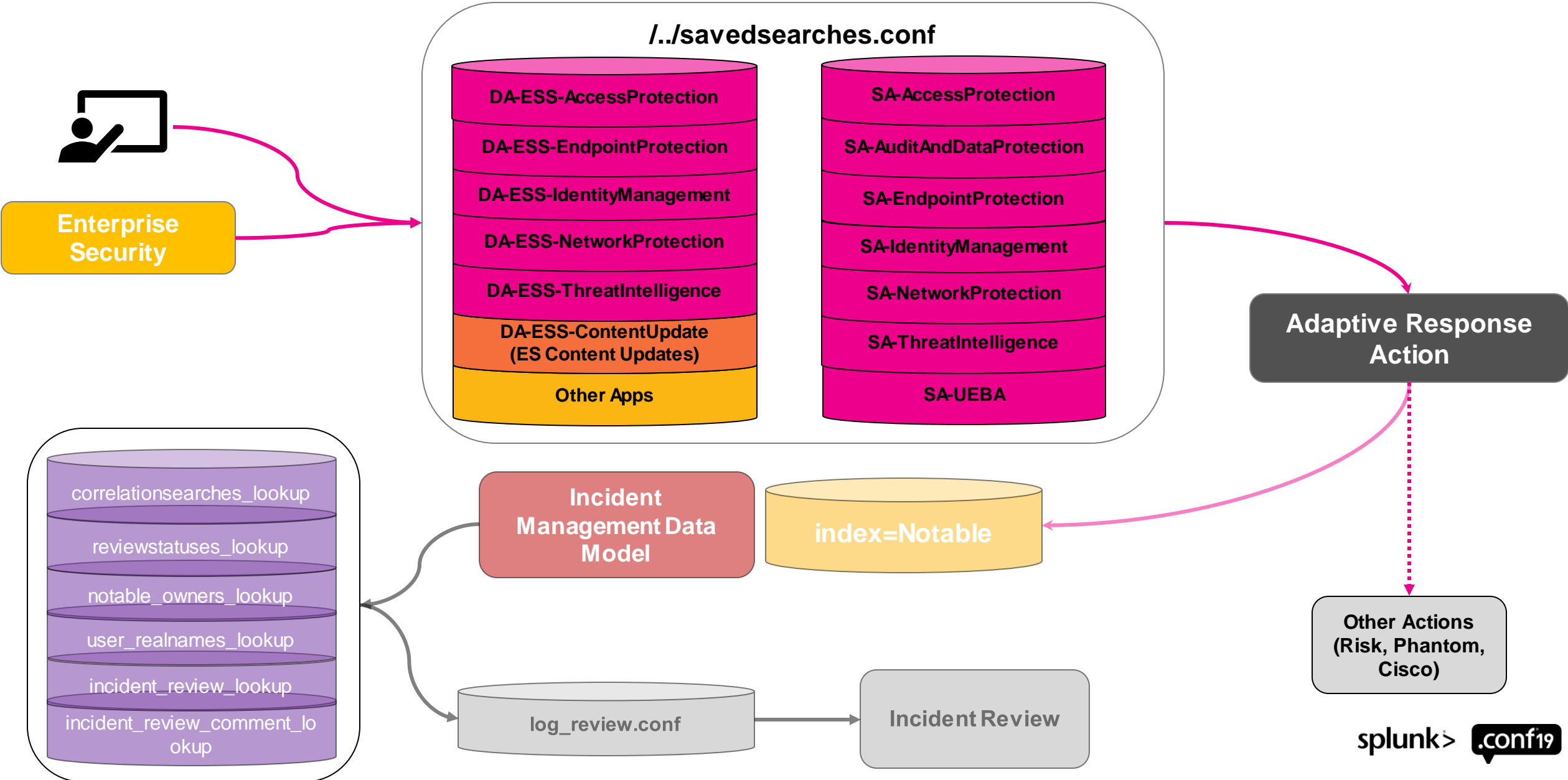
1972 BEETLE AND SUPER BEETLE





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](#)

8 Objects **Type: Correlation Search ▾** App: ES Content Updates ▾ Status: All ▾ ad 25 per page ▾

<input type="checkbox"/>	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

Progress: Data (active) | Filter | Aggregate | Analyze | Done

Data source: Data Model Lookup File

Data Model:

Dataset:

Summaries only?: Yes No

Time Range:

Preview

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

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

+ 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

- 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.

[Back to ES Configuration](#) Create New Content

9 Objects Edit selection Type: Correlation Search App: All Status: Enabled Clear filters 25 per page

<input type="checkbox"/>	i	Name	Type	App	Next Scheduled Time	⚡	Actions
<input type="checkbox"/>	▼	Detect New Local Admin account This search looks for newly created accounts that have been elevated to local administrators. Statistics 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	Correlation Search	ES Content Updates	Sep 9, 2019 6:32 AM PDT		Enabled Disable
<input type="checkbox"/>	>	Detection of DNS Tunnels	Correlation Search	ES Content Updates	Sep 9, 2019 6:34 AM PDT		Enabled Disable

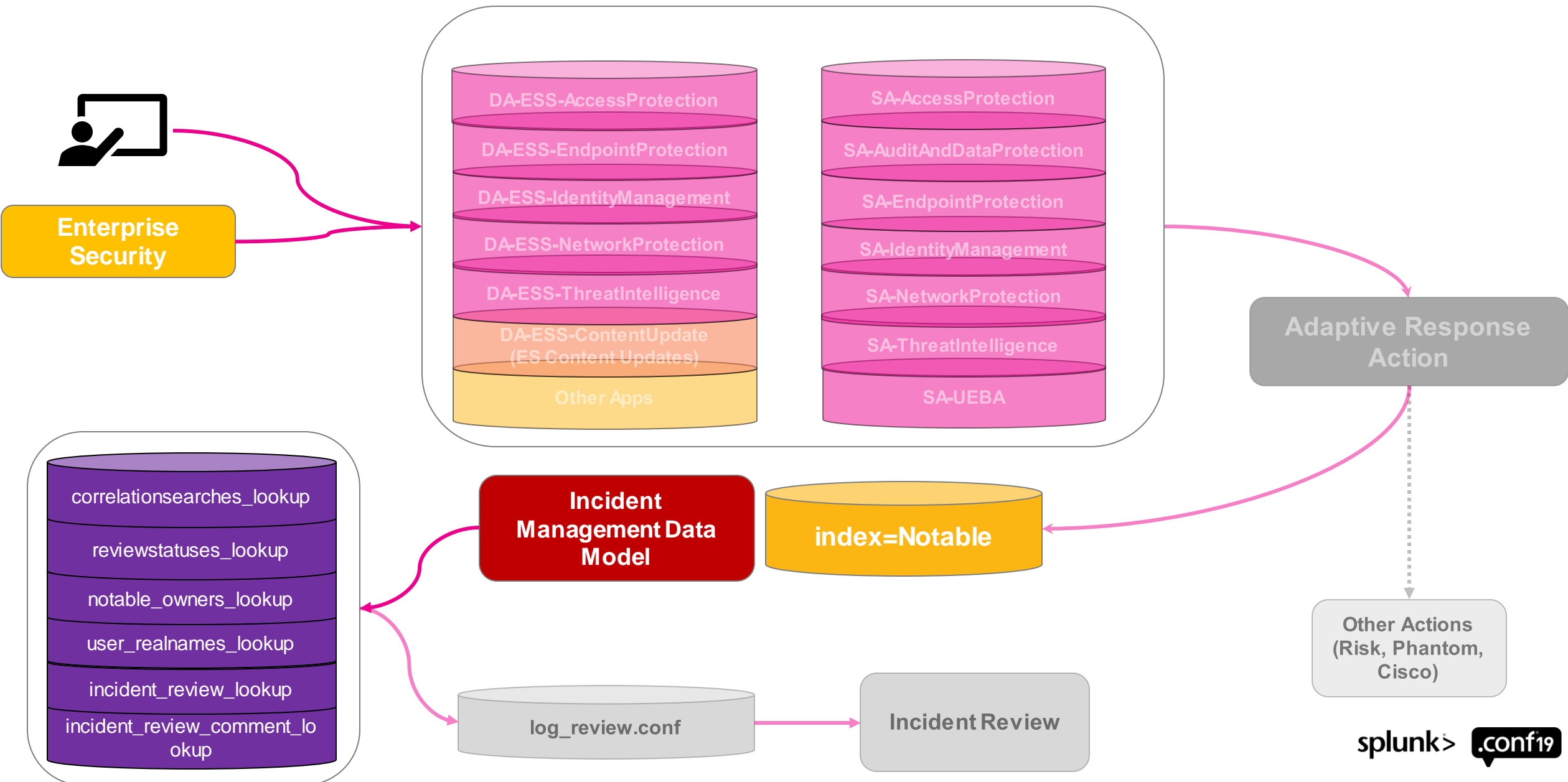
The index has no events from the past 24 hours.

Lookups
✔ [mitre_attack](#)



Responses – Notables

Notable Event Framework



Incident Management Data Model

Events

- Notable Events (Metadata Only)

Searches

- Notable Events
- Suppressed Notable Events
- Incident Review
 - 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

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](#)

Notable Events

Notable_Events

BASE SEARCH

`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	Eval Expression
src	String	Eval Expression

index=notable

| from datamodel:"Incident_Management.Notable_Events"

`notable`

```
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...	ablu bird	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...	ablu bird	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
✓	<input type="checkbox"/>	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

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...

[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_source_type="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"
```

``notable``

``incident_review``

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", d
escription="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.fr
othly.local", identifier="T1078", info_max_time="1568031720.000000000", info_min_time="1483257600.000000000", info_search_time="156803
2322.654381000", src_user="service3", tactic="Initial Access, Persistence, Privilege Escalation, Defense Evasion", technique="Valid Ac
counts", user="svcvnc"
```

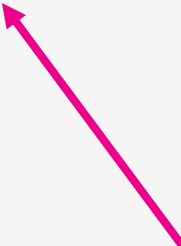
Description:

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

Additional Fields

Additional Fields	Value	Action
Event Code	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: - 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 -	▼

`notable`



Related Investigations:

Currently not investigated.

Correlation Search:

ESCU - Detect New Local Admin account - Rule

History:

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

`incident_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

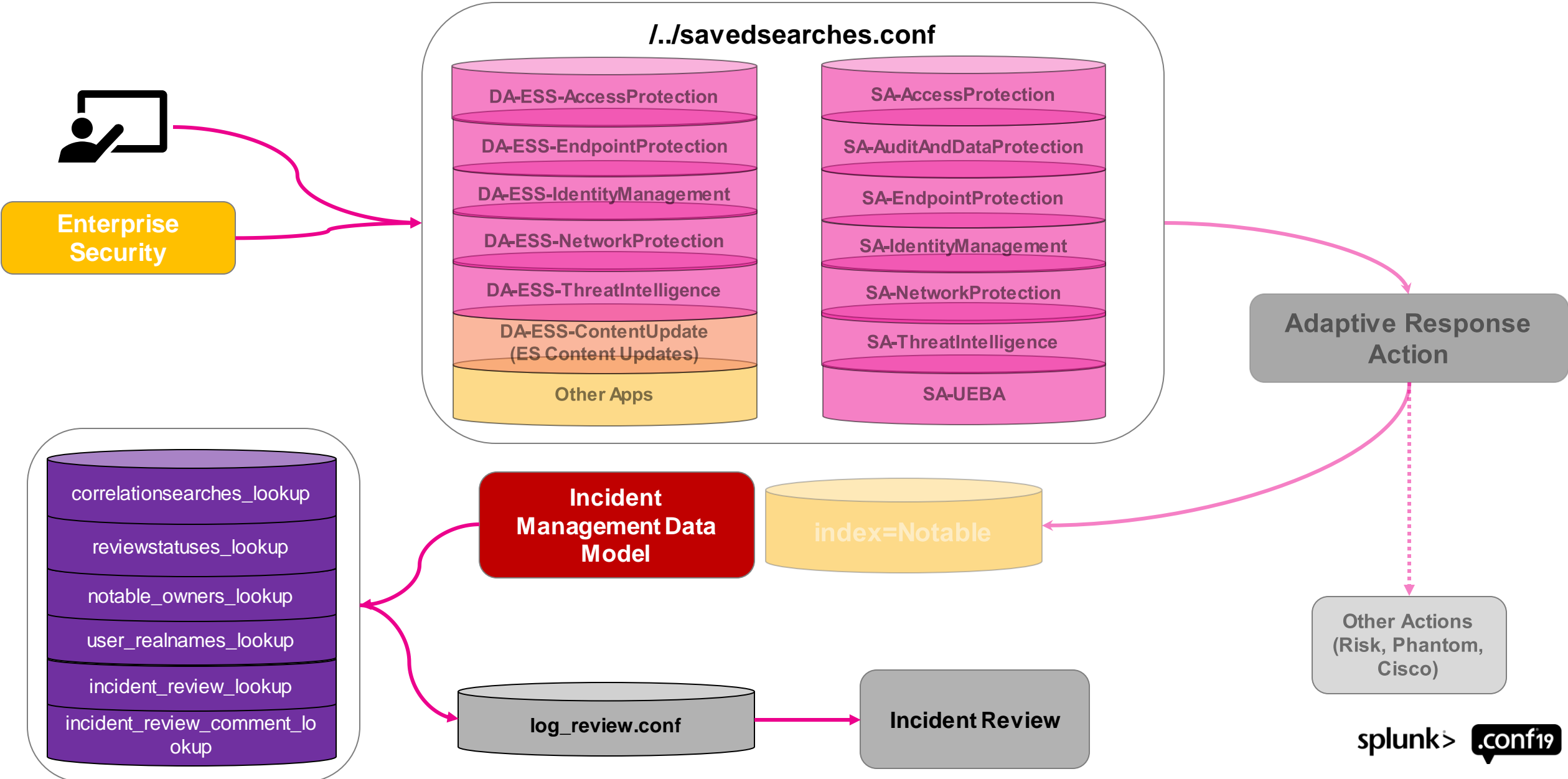
Next Steps:

- 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

Notable Event Framework



Urgency Calculation

Notable

Title: PowerShell process with an encoded cc
Notable events created by this search will have this title. Supports variable substitution.

Description: The system \$dest\$ executed a powersh
Notable events created by this search will have this description. Supports variable substitution.



Security Domain: Endpoint

Severity: Medium

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

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

priority	urgency
medium	low
high	medium
critical	medium
unknown	low
low	low
medium	medium
high	high
critical	high
unknown	medium
unknown	medium
low	high
high	high
critical	critical
unknown	high
low	high

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

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 Minimum length of a comment if required.

Incident Review - Default Time Range

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

Latest Time 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

Additional Fields	Value	Action
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	▼
	windows	▼
Destination City	San Francisco	▼
Destination Country	US	▼
Destination DNS	wrk-klagerf.frothly.local	▼
Destination IP Address	10.0.2.109	▼
Destination MAC Address	00:0c:29:f5:5e:8e	▼
Destination NT Hostname	wrk-klagerf	▼
Destination Owner	Kevin Lagerfield	▼
First Time of Activity	08/23/2017 20:55:13	▼
ATT&CK Identifier	T1047	▼
Last Time of Activity	08/23/2017 20:55:13	▼
Process	C:\Windows\System32\WindowsPowerShell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBIAFQAVABZAHAAZQAoACcAUwB5AHMAAdABIAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQBOAGkAbABzACcAKQB8AD8AewAkAF8AfQB8ACUAEwAkAF8ALgBHAEUAdABGAekARQB8AGQAKAAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQB8AGUAZAAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAAdABhAHQAaQBIAcCAKQAuAFMARQBOAFYAYQBMAHUA	▼

Related Investigations:

Currently not investigated.

Correlation Search:

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

History:

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

Adaptive Responses:

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

The screenshot displays the 'Notable Event Suppressions' configuration page in Splunk. At the top right is a green 'Create New Suppression' button. Below the header, there is a 'Show 25 entries' dropdown and a search box. A table lists suppression entries with columns for Label, Description, Start Time, and Expiration Time. The entry 'Malicious_PowerShell_Process_-_Encoded_Command' is highlighted with a pink box. A context menu is open over this entry, with 'Suppress Notable Events' selected and highlighted in pink. To the right, the 'Suppress Notable Events' dialog box is open, showing the suppression name, description, start and end times, selected fields (dest, user, process_name), and a search preview. The dialog has 'Cancel' and 'Save' buttons at the bottom.

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 frequency of throttling this.		
Suspicious_wevtutil_Usage	Need to revise and review the frequency of throttling this.		

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-btun.frothy.local" _time>=1567569600`

Buttons: Cancel Save

Notable Event Suppression

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

✓ 14 events (9/2/19 9:00:00.000 PM to 9/4/19 9:00:01.000 PM) No Event Sampling
Job || ■ → 🖨 ↓ Smart Mode

Events Patterns **Statistics (14)** Visualization

10 Per Page Format Preview < Prev 1 2 Next >

<code>_time</code>	<code>eventtype</code>	<code>tag</code>
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
2019-09-04 01:42:14	modnotable_results notable notable_suppression-Malicious_PowerShell_Process_-_Encoded_Command	modaction_result watchlist



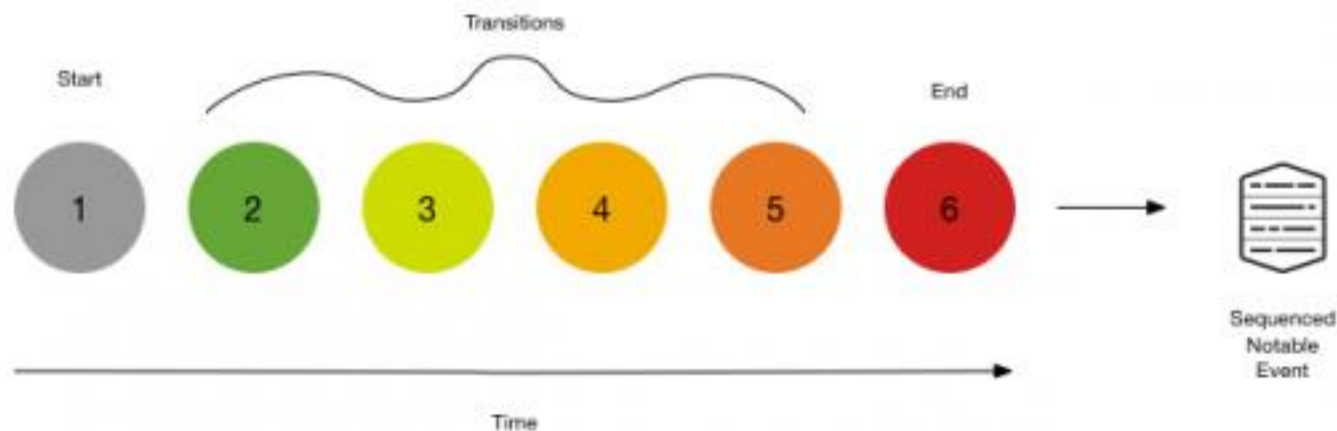
Event Sequencing and Audit

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"/>	i	Name ^	Type ⇅	App ⇅	Next Scheduled Time
<input type="checkbox"/>		Taedonggang APT	Sequence Template	ES Content Updates	
<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	×

+ 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

Correlation Search ?

Expression ?

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

Correlation Search ?

Expression ?

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 ?

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

Time Limit ?

Actions

Sequenced Event

Event Title
Supports state token substitution.

Event Description
Supports state token substitution.

Urgency

Security Domain

Output Fields

<input type="text" value="user"/>	<input type="text" value="\$user\$"/>	<input type="text" value="X"/>
<input type="text" value="dest"/>	<input type="text" value="\$dest\$"/>	<input type="text" value="X"/>
<input type="text" value="process"/>	<input type="text" value="\$process\$"/>	<input type="text" value="X"/>

[+ Add Field](#)

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

Glass Tables **Security Intelligence** Security Domains

- Risk Analysis
- Protocol Intelligence >
- Threat Intelligence >
- User Intelligence >
- Web Intelligence >
- Sequence Analysis

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

Field	Value
Destination	wrk-klagerf.frothly.local 40
Destination Category	workstation windows
Destination City	San Francisco
Destination Country	US
Destination DNS	wrk-klagerf.frothly.local
Destination IP Address	10.0.2.109
Destination MAC Address	00:0c:29:f5:5e:8e
Destination NT Hostname	wrk-klagerf
Destination Owner	Kevin Lagerfield
End Time	Sep 4, 2019 2:33 PM
Process	C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARqBdAC4AQQBTAHMARQBNAGIATABZAC4ARwBIAFQAVABZAHAAZQAoACcAUwB5AHMAAdABIAG0ALqBNA
Start Time	Sep 4, 2019 12:33 PM
User	FROTHLY\service3

History:
 No History

Adaptive Responses:
 No Adaptive Responses found

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

Additional Fields	Value
Destination	wrk-klagerf.frothly.local 40

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

Testing Your Event Templates

```
`execute_sequence_template(template_name, false)`
```

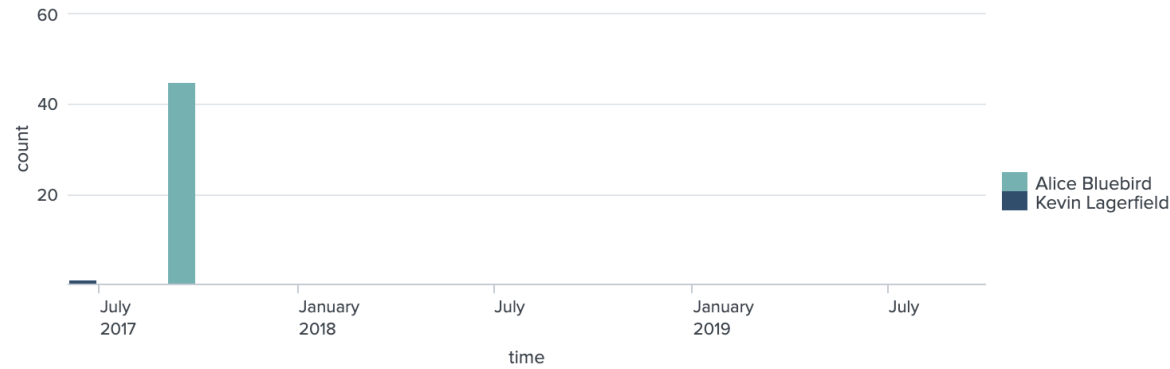
```
{ [-]
  dest: wrk-klagerf.frothly.local
  end_time: 1567690399
  events_spl: earliest=1567683199.0 latest=1567685164.0 `event_seq_events` | search event_id="C8A9AB2D-487E-49CB-99D8-A570A
  orig_rid: 0f7b2bab-4c82-4798-966c-4453a824f4df
  orig_sid: 1567690579.3925
  process: C:\Windows\System32\WindowsPowershell\v1.0\powershell -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":
  urgency: critical
  user: FROTHLY\service3
}
```

Incident Review Audit

Incident Review Audit

Edit Export ...

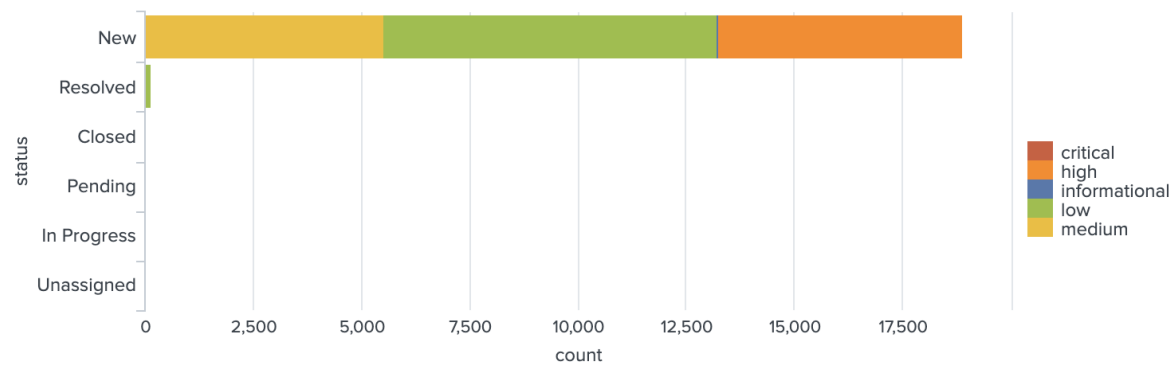
Review Activity By Reviewer



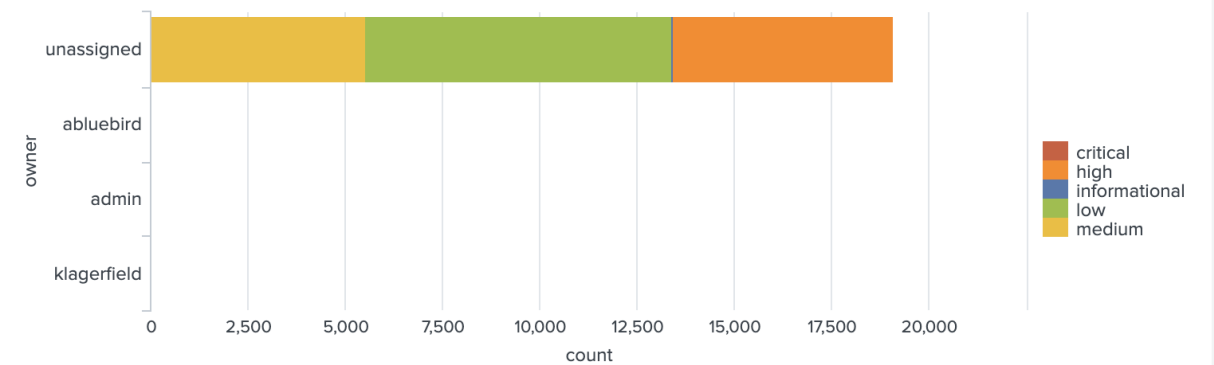
Top Reviewers

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



Notable Events By Owner - Last 48 Hours



Mean Time To Triage - Last 14 days

Mean Time To Closure - Last 60 days

Suppression Audit

Edit
Export ▾
...

Suppressed Events Over Time - Last 24 Hours

Suppression History Over Time - Last 30 Days

Suppression Management Activity

_time ▾	suppression ▾	action ▾	status ▾	user ▾
2019-09-05 10:08:25.386	Detect_New_Local_Admin_account	disable	success	admin
2019-09-03 16:22:09.275	Detect_New_Local_Admin_account	create	success	admin
2019-09-03 16:20:20.943	Suspicious_wevtutil_Usage	create	success	admin
2019-09-03 16:19:32.487	Malicious_PowerShell_Process_-_Encoded_Command	create	success	admin

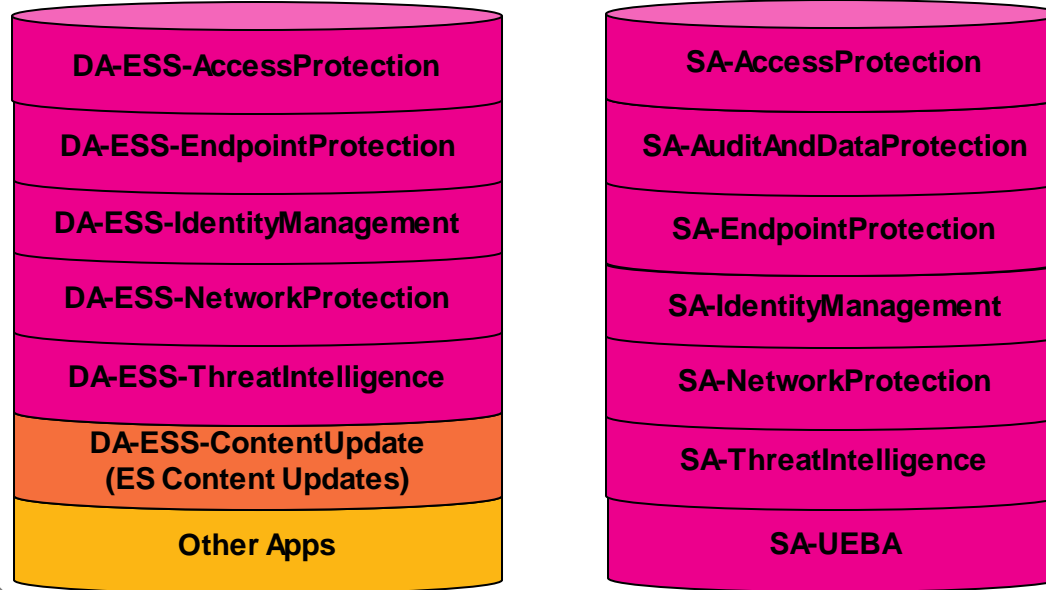
Expired Suppressions

Notable Event Framework



Enterprise Security

../savedsearches.conf



Adaptive Response Action

Incident Management Data Model

index=Notable

- correlationsearches_lookup
- reviewstatuses_lookup
- notable_owners_lookup
- user_realnames_lookup
- incident_review_lookup
- incident_review_comment_lo
okup

log_review.conf

Incident Review

Other Actions (Risk, Phantom, Cisco)

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-CAAFA9>

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!



splunk>

Thank

You!

Go to the .conf19 mobile app to

RATE THIS SESSION





Appendix

Correlation Search Mapping to .conf file

Correlation Search

Search Name *

Detect New Local Admin account

App *

ES Content Updates ▼

UI Dispatch Context *

Enterprise Security ▼

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.

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


```
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.eli5 = 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 Object ives", "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"]
```

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

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

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

Time Range

Earliest Time

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

Latest Time

Type a latest time using relative time modifiers.

Cron Schedule *

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

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

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

Trigger alert when

Number of Results ▼

is greater than ▼ 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 x

Type a field and press enter

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

Adaptive Response Actions

+ Add New Response Action ▼

>  Risk Analysis x

>  Notable x

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

```
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

```
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
```


+ Add New Response Action ▾


▾  Risk Analysis

Risk Score*

Risk Object Field*

Risk Object Type* ▾

[Learn more](#)  about risk modifiers.

▼  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 = ablu
```

```
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: `[[actionNameOfAction]]`

Recommended Actions

All

Filter

→ →

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

Recommended

Filter

← ←

ESCU-Contextualize
ESCU-Investigate
Run Playbook in Phantom

```
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>
```

```
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