

.conf2015

Sierra-Cedar's Best Practices for Building a Security Operations Center

Robert Miller

Manager Corporate Security,
Sierra-Cedar, Inc.



Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

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

About Me

- Sierra-Cedar, Inc.
 - One of the largest independent North American IT services companies
 - Provider of full scale PeopleSoft hosting services with over 50 hosted clients
 - Currently support over 600 PeopleSoft environments and over 17,000 concurrent PeopleSoft users
- My Role
 - Support security and compliance activities for both US and overseas operations
 - Manage five person team located in US, Canada, and India
 - Splunk Certified Architect, Computer Forensics Analyst, Computer Programmer, Incident Response Manager, etc.

Agenda

- What problem are we trying to solve?
- Using Splunk App for Enterprise Security (ES) to detect malicious activity
- Using Splunk App for Stream for targeted analysis of external threats
- Detecting malicious activity using the integration of Splunk Apps for Stream and Enterprise Security
- Takeaways



.conf2015

What Problem Are We
Trying to Solve?

splunk>

Scenario

The Splunk App for Enterprise Security triggers an alert that traffic on your network is communicating with an IP address from one of your threat intelligence feeds.

- What is this traffic?
- Did our firewalls block this traffic?
- Do we have any tools capturing the traffic to give us more information?
- How many of these alerts are we getting and can our team keep up?

Before Splunk App for Stream

- We have enabled several free threat intelligence feeds in the Splunk App for Enterprise Security
- We have created several notable events that trigger when a threat IP is identified
- The security team researches these events to identify what traffic is being received/sent
 - Currently a manual process that involves several searches, dashboards, etc.
 - Could lead to conducting computer forensics
- Security team may coordinate with the network team to setup packet captures in hopes of capturing session details

After Splunk App for Stream

- Security team has additional insight into network traffic that was not previously able to be captured
- Selective data capture uses our Splunk license more efficiently
- Correlation with other security relevant data helps with quick incident resolution
 - Fast incident resolution ➡ less damage during a breach ➡ less financial impact to the business



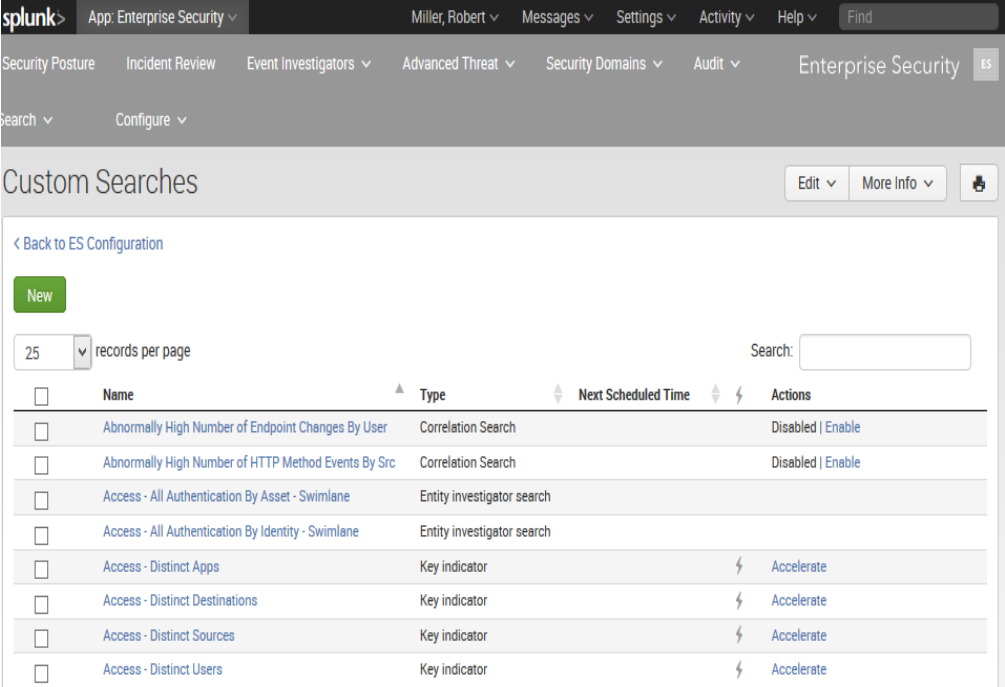
.conf2015

Using ES to Detect Malicious Activity

splunk>

Correlation Searches- Critical to Detect Threats

- There are almost 200 pre-built notable events
- Not all pre-built notable events will be relevant for your environment
 - Turn on searches one at a time and determine relevance



The screenshot displays the Splunk Enterprise Security (ES) interface. The top navigation bar includes the Splunk logo, application name 'App: Enterprise Security', user 'Miller, Robert', and various menu items like 'Messages', 'Settings', 'Activity', and 'Help'. Below this, a secondary navigation bar shows 'Security Posture', 'Incident Review', 'Event Investigators', 'Advanced Threat', 'Security Domains', 'Audit', and 'Enterprise Security'. The main content area is titled 'Custom Searches' and features a 'New' button, a 'records per page' dropdown set to 25, and a search input field. A table lists several pre-built correlation searches, each with a checkbox, name, type, next scheduled time, and actions.

<input type="checkbox"/>	Name	Type	Next Scheduled Time	Actions
<input type="checkbox"/>	Abnormally High Number of Endpoint Changes By User	Correlation Search		Disabled Enable
<input type="checkbox"/>	Abnormally High Number of HTTP Method Events By Src	Correlation Search		Disabled Enable
<input type="checkbox"/>	Access - All Authentication By Asset - Swimlane	Entity investigator search		
<input type="checkbox"/>	Access - All Authentication By Identity - Swimlane	Entity investigator search		
<input type="checkbox"/>	Access - Distinct Apps	Key indicator		Accelerate
<input type="checkbox"/>	Access - Distinct Destinations	Key indicator		Accelerate
<input type="checkbox"/>	Access - Distinct Sources	Key indicator		Accelerate
<input type="checkbox"/>	Access - Distinct Users	Key indicator		Accelerate

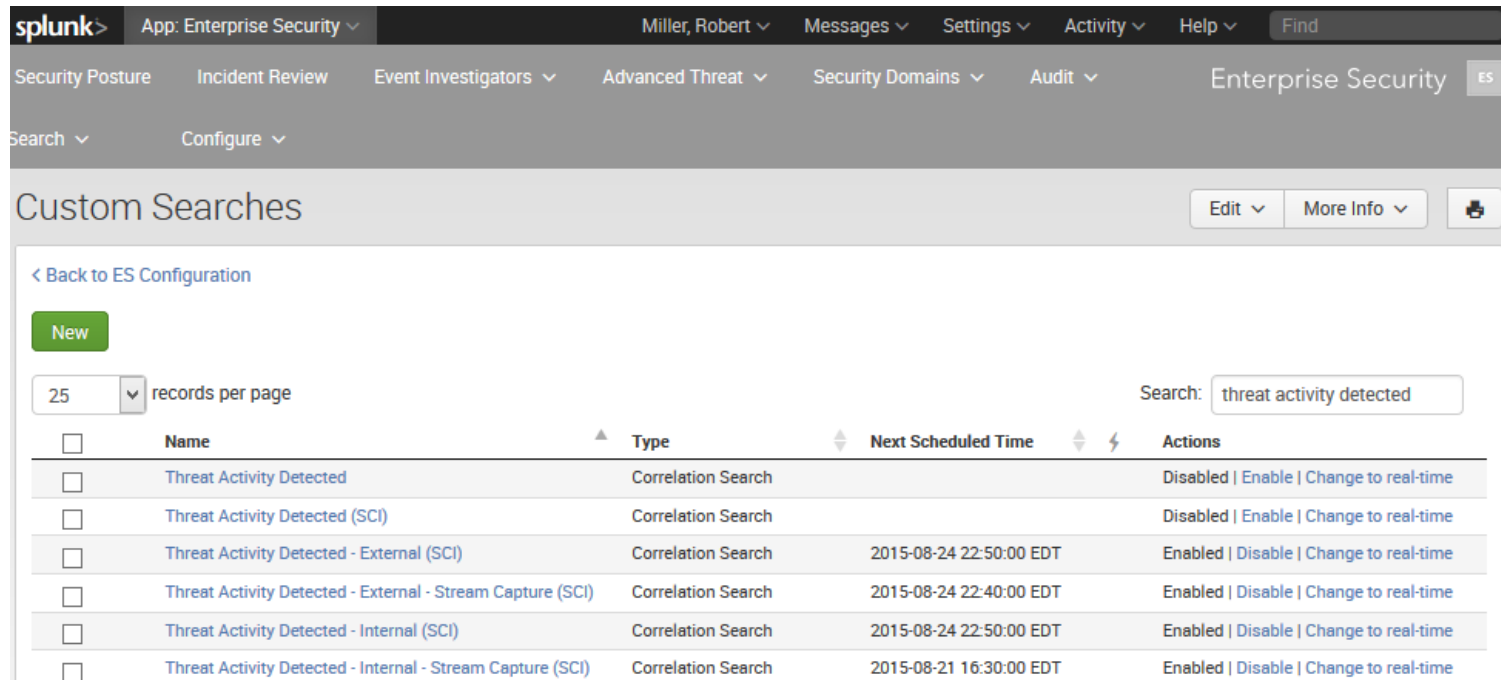
To Detect External Threats

Account access, account activity, login attempts and activity searches were used

- Access – Local Account Created
- Access – Local Admin Account Created
- Activity from Expired User Identity
- Anomalous Audit Trail Activity Detected
- Brute Force Access Behavior Detected
- Cleartext Password At Rest Detected
- Default Account Activity Detected
- Default Account At Rest Detected
- Excessive Failed Logins
- Geographically Improbable Access Detected
- Inactive Account Activity Detected
- New User Account Created on Multiple Hosts
- Short Lived Account Detected
- Threat Activity Detected – External – Stream Capture
- Threat Activity Detected – Internal – Stream Capture

Threat Activity- Correlation Searches

We created an inbound, outbound “Threat Activity Detected” search

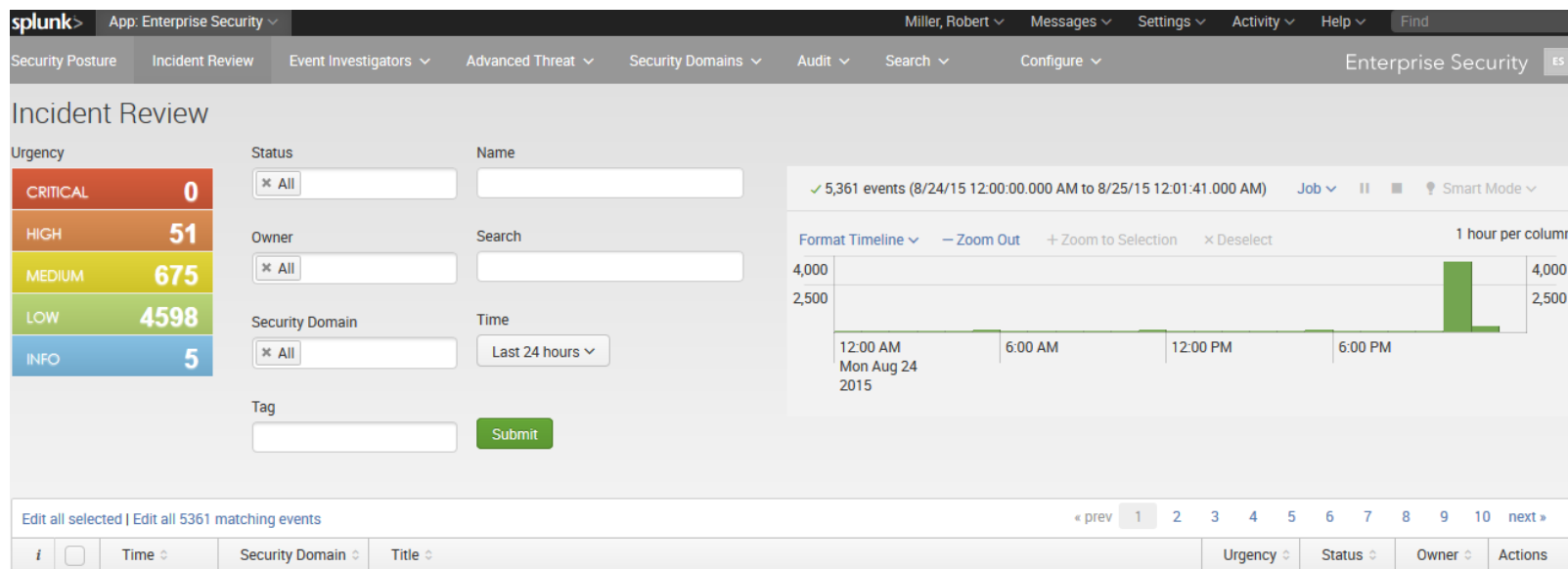


The screenshot shows the Splunk Enterprise Security interface. The top navigation bar includes 'splunk>', 'App: Enterprise Security', 'Miller, Robert', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar. Below this, there are tabs for 'Security Posture', 'Incident Review', 'Event Investigators', 'Advanced Threat', 'Security Domains', and 'Audit'. The main content area is titled 'Custom Searches' and features a 'New' button, a '25 records per page' dropdown, and a search input field containing 'threat activity detected'. A table lists several correlation searches, including 'Threat Activity Detected' and various 'Threat Activity Detected - External (SCI)' and 'Internal (SCI)' variants, some with stream capture options. Each row includes a checkbox, the search name, type, next scheduled time, and actions like 'Enabled', 'Disable', and 'Change to real-time'.

<input type="checkbox"/>	Name	Type	Next Scheduled Time	Actions
<input type="checkbox"/>	Threat Activity Detected	Correlation Search		Disabled Enable Change to real-time
<input type="checkbox"/>	Threat Activity Detected (SCI)	Correlation Search		Disabled Enable Change to real-time
<input type="checkbox"/>	Threat Activity Detected - External (SCI)	Correlation Search	2015-08-24 22:50:00 EDT	Enabled Disable Change to real-time
<input type="checkbox"/>	Threat Activity Detected - External - Stream Capture (SCI)	Correlation Search	2015-08-24 22:40:00 EDT	Enabled Disable Change to real-time
<input type="checkbox"/>	Threat Activity Detected - Internal (SCI)	Correlation Search	2015-08-24 22:50:00 EDT	Enabled Disable Change to real-time
<input type="checkbox"/>	Threat Activity Detected - Internal - Stream Capture (SCI)	Correlation Search	2015-08-21 16:30:00 EDT	Enabled Disable Change to real-time

Incident Review

- We used the incident review dashboard to track all notable events that are triggered



Incident Review– Case Assignments

Edit Events [X]

Status: New [X] ▾

Urgency: [X] ▾

Owner: esanalyst [X] ▾

Comment: Open a ticket and investigate.

Cancel Save changes

- Example : Ability to assign an analyst to a notable event

Threat Intelligence Downloads

- We used the out of the box, free threat intelligence feeds
- In addition, you have the ability to add additional ones


Threat Intelligence Downloads

Data inputs » Threat Intelligence Downloads



New

Showing 1-48 of 48 items

Results per page 100 

Name ↕	Type ↕	Description ↕	URL ↕	Weight ↕	App ↕	Status ↕	Actions
AlienVault BOT	Bot	Bot network	http://reputation.alienvault.com/reputation.data	1	SplunkEnterpriseSecuritySuite	Enabled Disable	Clone Delete
AlienVault Phishing	Phishing	Phishing websites	http://reputation.alienvault.com/reputation.data	1	SplunkEnterpriseSecuritySuite	Enabled Disable	Clone Delete
AlienVault Spam	Spam	Spam websites	http://reputation.alienvault.com/reputation.data	1	SplunkEnterpriseSecuritySuite	Enabled Disable	Clone Delete



.conf2015

Using Splunk App for Stream for Targeted Analysis of External Threats

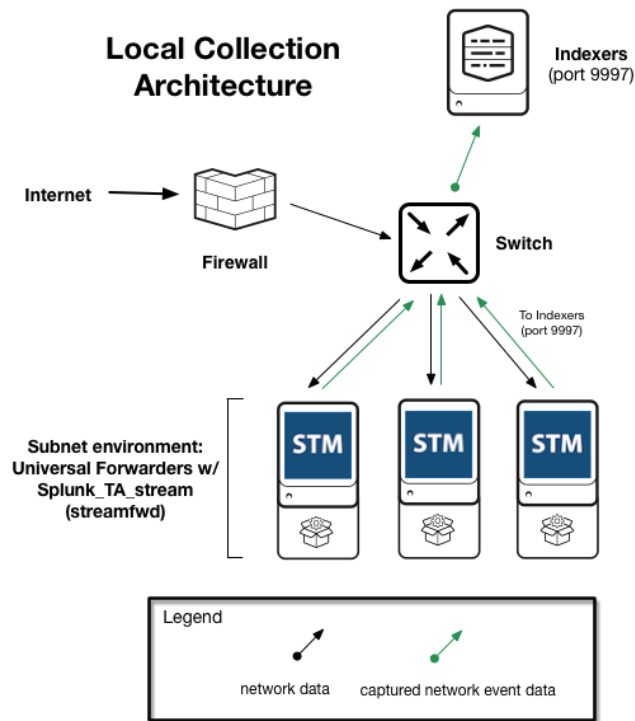
splunk >

Our Benefits

- Ability to capture database traffic without making changes to the database
- All details of traffic are in JSON format and makes it easy to search
- Deployment is not complicated
- No longer have to engage another team to get packet captures
- Security and IT Operations use cases

Our Architecture

- We are using the local network collection architecture
- Deployed Splunk_TA_Stream to all universal forwarders using Deployment Server
- All universal forwarders need to access server running Splunk Apps for Stream and Enterprise Security





.conf2015

Detecting Malicious Activity Using the Integration of Splunk Apps for Stream and Enterprise Security

splunk >

Configuration Checklist

- The Splunk App for Stream needs to be installed on same server as the Splunk App for Enterprise Security
 - Confirm hardware specs
- All universal forwarders need access to server running app
 - Possible firewall rule changes
- Identify notable events or create your own to use for stream capture

Configuration Step 1: Edit Correlation Search

Use case: threat activity detected

- Confirm the following fields are defined:
 - src
 - src_ip
 - dest
 - dest_ip

Edit Correlation Search

[Back to Custom Searches](#)

Correlation Search

Search Name *

Application Context

Description

Describes what kind of issues this search is intended to detect

Search *

```
| datamodel Threat_Intelligence Threat_Activity search | drop_dm_object_name("Threat_Activity") | dedup threat_match_field,threat_match_value | get_event_id | table raw_event_id,source,src,dest,threat* | per_panel_filter(ppf_threat_activity,"threat_match_field,threat_match_value") | makesy(src) | makesy(dest) | get_threat_attribution(threat_key) | rename source as orig_source,source_* as threat_source_*,description as threat_description | map_notable_fields | fields - *time | eval risk_object_type=case(threat_match_field=query OR threat_match_field=src OR threat_match_field=dest, system, threat_match_field=src_user OR threat_match_field=user, user, 1=1, other) | eval risk_object=threat_match_value | eval src_ip=src | eval dest_ip=dest
```

Configuration Step 2: Edit Correlation Search

Use case: threat activity detected

- Confirm checkmark is next to “Create notable event”
- Scroll to “Actions” section
 - Place checkmark in “Start Stream capture”
 - Choose protocols to capture
 - Choose amount of time for capture

Notable Event

Create notable event

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)

Actions

Include in RSS feed

Send email

Run a script

Start Stream capture

on

for

Define duration and protocols to capture

Initiates a Stream capture for all IP addresses (src_ip, dest_ip) in the corresponding events

Configuration Step 3: Confirm Captures Are Working

- On Incident Review dashboard, once new event shows up navigate to the Splunk App for Stream
- Click on the Ephemeral link
 - All current streams will show up on this page
 - Option to kill any streams that are listed

Streams Config Clone Stream

Stream Type: Permanent Ephemeral

Group By: Applicat

all >

Stream >

SA-Utils >

Stream Buckets

Ephemeral Streams give users of integrated Splunk apps the ability to schedule stream data capture for a user-defined period of time. Users configure and schedule ephemeral stream capture from inside the UI of the integrated app. Ephemeral streams are always clones of default streams. [Learn more.](#)

Bulk Edit

i	<input type="checkbox"/>	Name	# of Streams	Application	Start Time	End Time	Time Remaining	Status	Actions
>	<input type="checkbox"/>	generic	9	SA-Utils	August 24, 2015 8:28 PM	August 24, 2015 8:54 PM		All Enabled	>

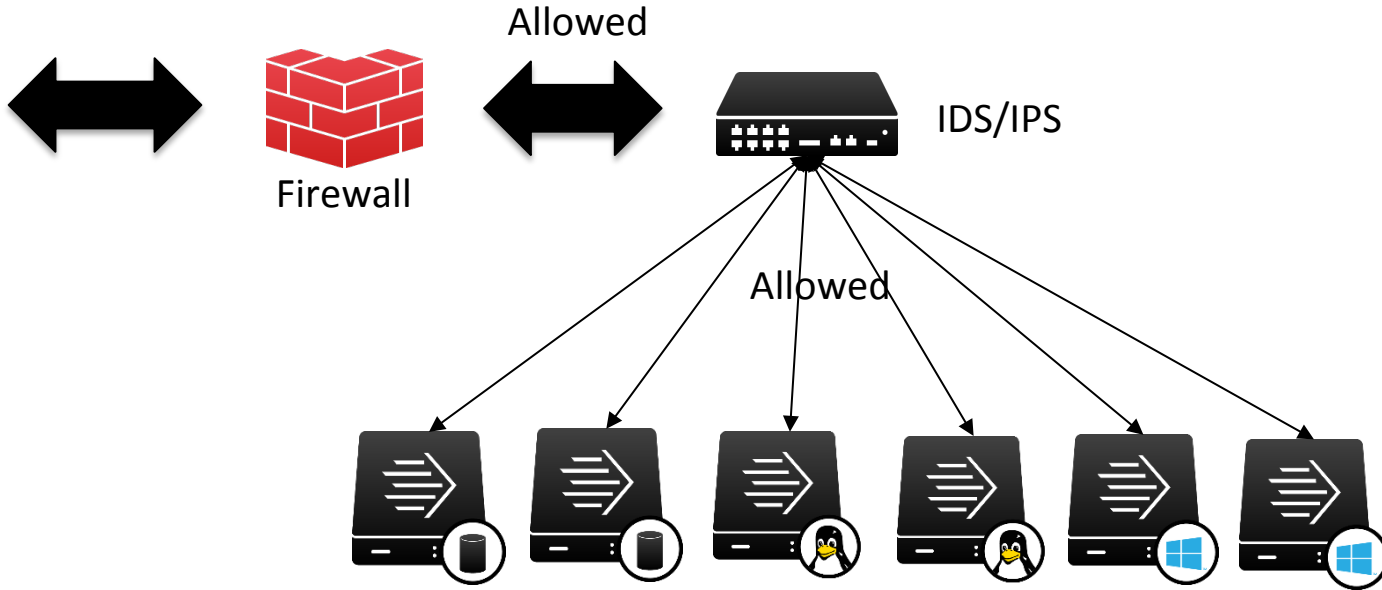


.conf2015

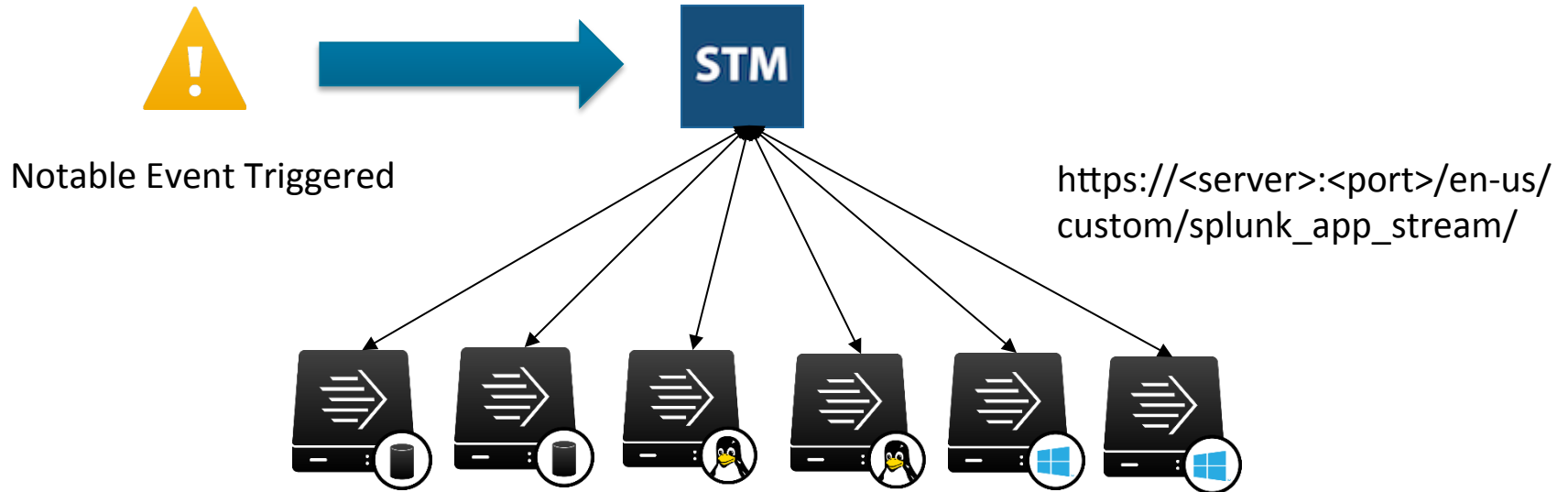
How Does It Work?

splunk>

Attacker Accessing Network



ES Notable Event Triggers Stream Capture





.conf2015

Takeaways

Why We Love It?

- Additional visibility into network traffic
- Selective data capture limits license usage
- Targeted analysis of external threats with selective data capture
- Doesn't require a change control process to a server/
network appliance
- No longer need to use 3rd party tools to read packet captures
- Additional logs in a centralized location to help with
intrusion detection

Recap of Takeaways

- Make sure all your logs are CIM compliant
- Depending on your environment, choose the correct collection architecture
- When first starting off, disable all streams in the “defaultgroup”
- All universal forwarders need to access server running Splunk App for Enterprise Security and Splunk App for Stream

What's Next for Us?

- Add Splunk App for Stream collection to additional correlation searches
- Look at possibly having Splunk App for Stream running 24/7 for certain protocols and/or groups of servers
- Extend the capture time from 15 minutes to a longer interval

Questions?



.conf2015

THANK YOU

splunk>