splunk> .conf2017

Need for Speed:

Unleashing the Power of SecOps with Adaptive Response

Malhar Shah | CEO, Crest Data Systems

Meera Shankar | Alliance Manager, Splunk

September 27, 2017 | Washington, DC

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

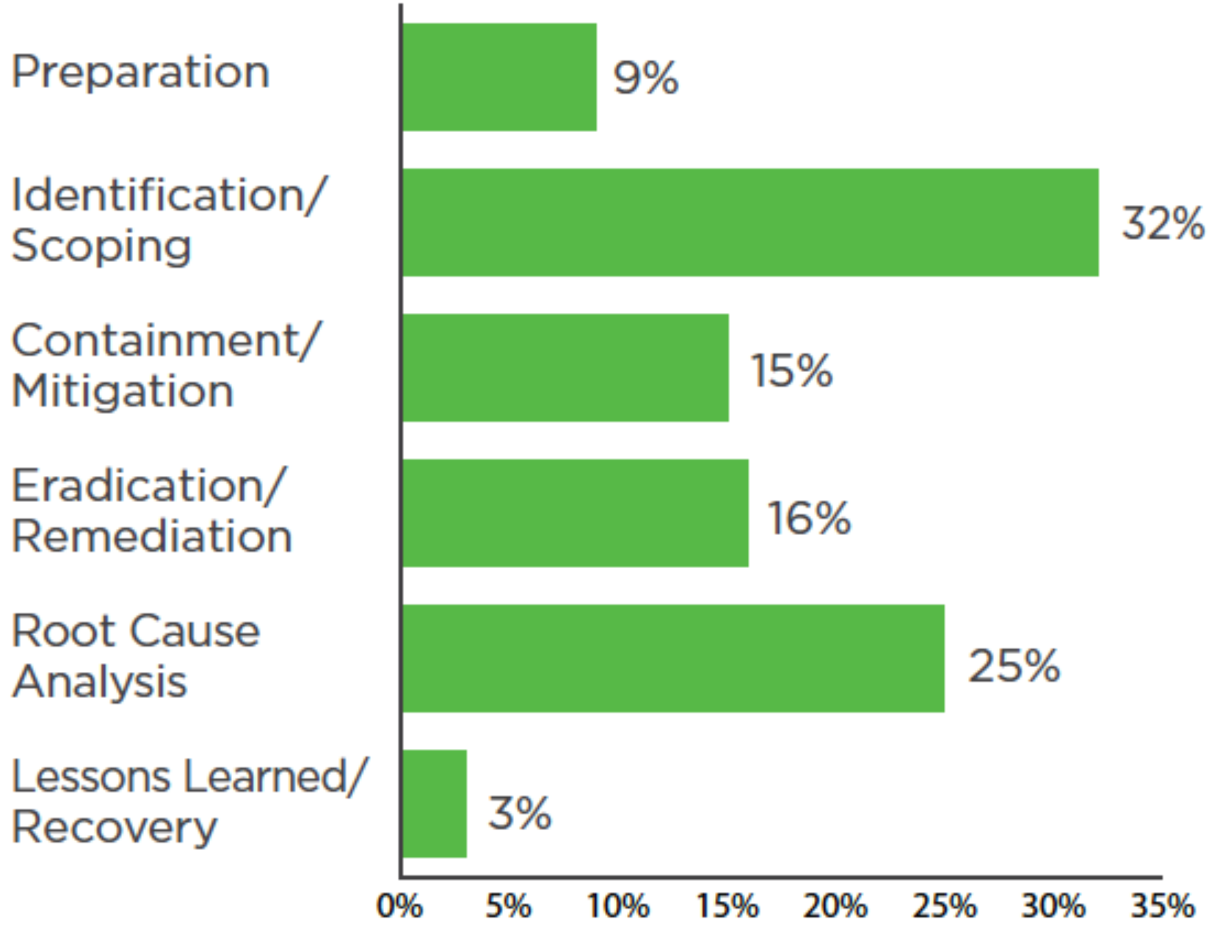
Challenges Facing SecOps

- **Complex correlations**
  - Detect targeted attacks across **multiple vectors**
  - Provide context across **multiple** (security) **domains**

- **Operationalize security**
  - Get **all** the right people involved in security investigations
  - Respond at **scale** without automation also helping the “bad guys”

Where Does Your Time Go?

When working an incident which phase generally takes the longest to complete in your organization?



Day in the life of a security professional survey
© 2016 Enterprise Management Associates, Inc.

N=100

Time = Risk => The Need for Speed!

paloalto NETWORKS

illumio

ATLASSIAN

SWIMLANE

DomainTools

okta

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

cisco Cisco Umbrella

QUALYS

DEMISTO

Corvil

Symantec.

FORTINET

SailPoint

REDSEAL

RESOLVE SYSTEMS

resilient an IBM Company

CYLANCE

THREATCONNECT

ANOMALI

CROWDSTRIKE

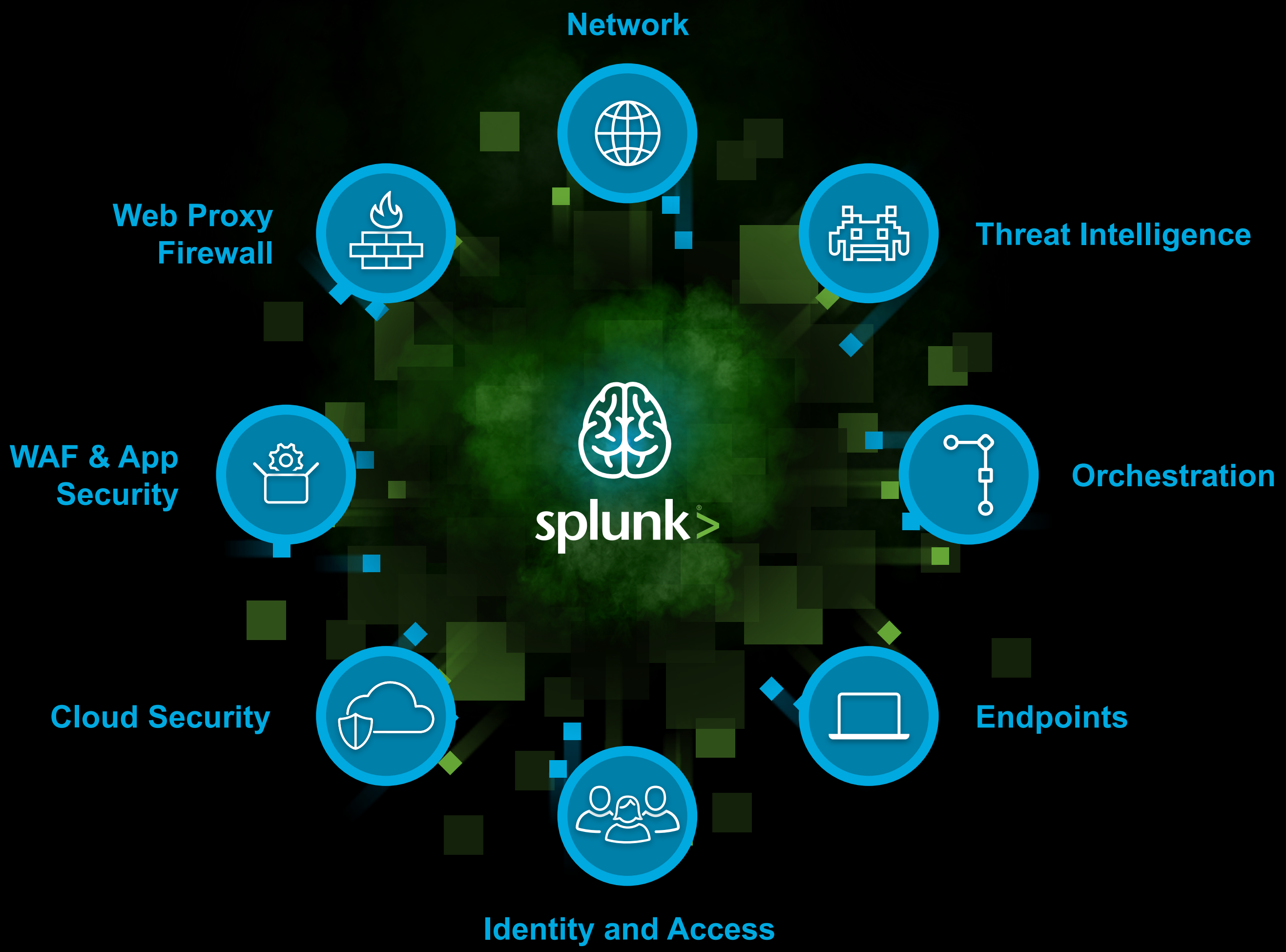
cisco

Phantom

ACALVIO

Gigamon

proofpoint



Network

Threat Intelligence

Orchestration

Endpoints

Identity and Access

Cloud Security

WAF & App Security

Web Proxy Firewall

splunk>

amazon web services

ForeScout

ziften

TANIUM

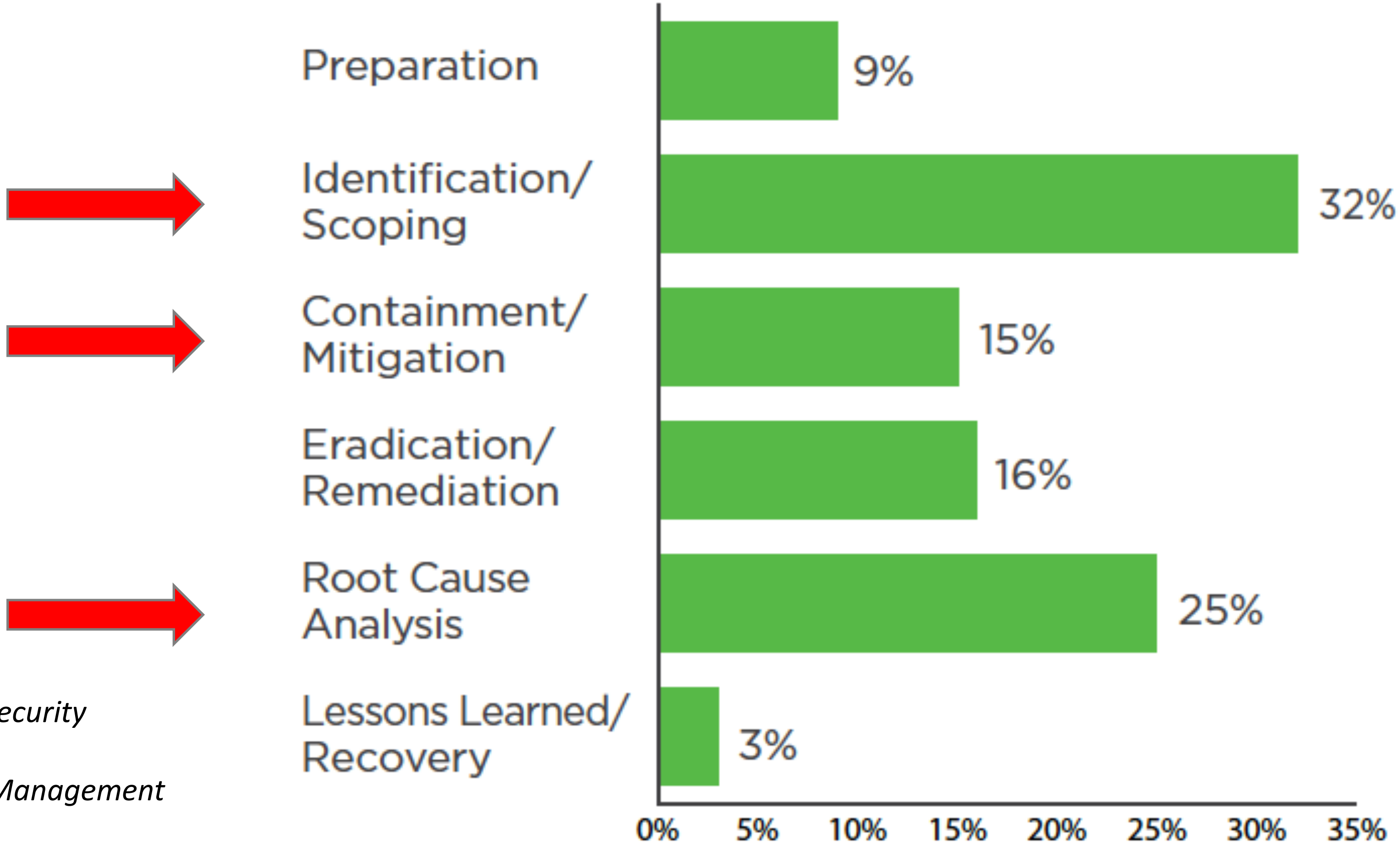
Recorded Future CREATING AN INSIGHTFUL WORLD

CARBON BLACK

CYBERARK

Adaptive Response addresses 72% of your time budget

When working an incident which phase generally takes the longest to complete in your organization?



Day in the life of a security professional survey
© 2016 Enterprise Management Associates, Inc.

N=100

splunk> .conf2017

Adaptive Response in Real Life: Symantec

Symantec ATP helps detect and remediate complex attacks across endpoint, email, network, and web from a single console

Sample of Symantec AR Actions*:

- Isolate Endpoint
- Rejoin Endpoint
- Query File for Disposition

> *Splunk Adaptive Response has the power to help reduce workload on customer SOC teams by speeding up decision making and associated actions through automation.*
> - Peter Doggart, Vice President of Business Development, Symantec

*Actions built by Crest Data Systems

Adaptive Response in Real Life: ForeScout

ForeScout CounterACT enables its customers to monitor real-time NAC events and respond to security threats at endpoints

Sample of ForeScout AR Actions*:

- Redirect endpoint to specific web browser
- Send email messages to users
- Kill peer-to-peer application

> *Leveraging the ForeScout Extended Module for Splunk via Adaptive Response will enable us to minimize the time and resources needed to respond to emerging threats.*
>
> \- Clayton Colwell, Associate security engineer, **Brown-Forman Corporation**

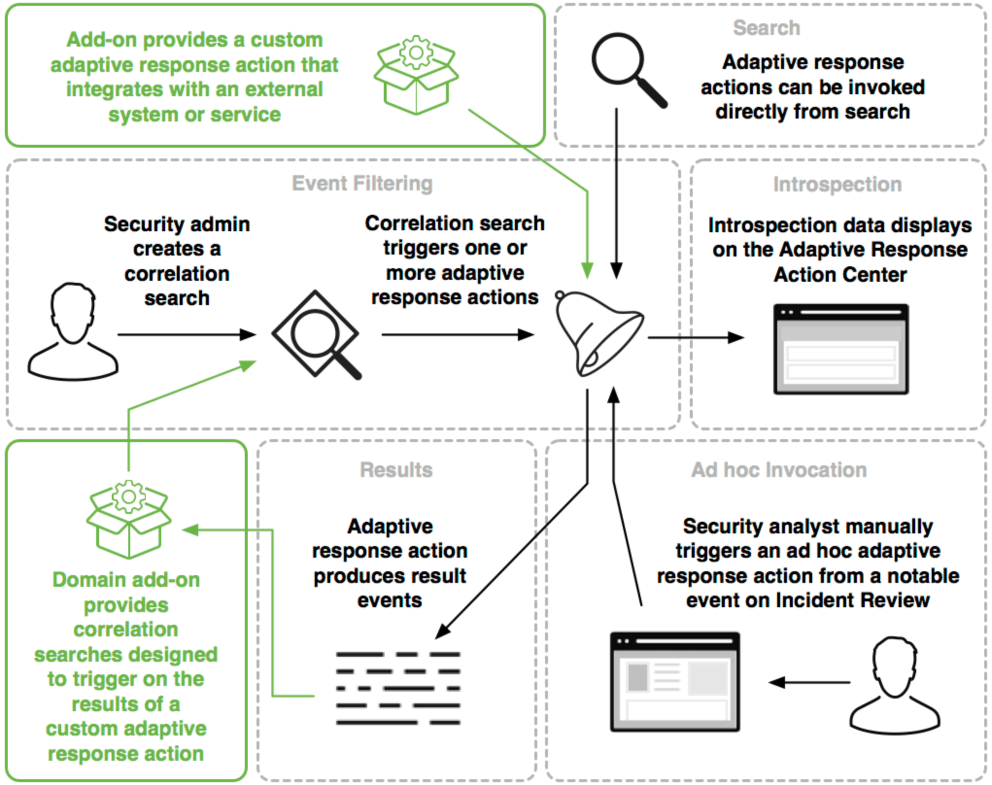
*Actions built by Crest Data Systems

Build AR Actions in 5 Easy Steps

AR Development Guidelines

Some of the most common questions we get asked

- AR Actions are built as part of an independent add-on or can be combined with data collection add-on
- Build Domain Add-on for Custom Correlation Searches
- HTML forms are built to take user inputs while taking actions
- AR Actions can be attached with Enterprise Security (ES) incident manually or can be auto-triggered
- Results from Correlation searches are passed to AR actions as inputs


Add-on provides a custom adaptive response action that integrates with an external system or service
Search
Adaptive response actions can be invoked directly from search
Event Filtering
Security admin creates a correlation search
Correlation search triggers one or more adaptive response actions
Introspection
Introspection data displays on the Adaptive Response Action Center
Results
Adaptive response action produces result events
Domain add-on provides correlation searches designed to trigger on the results of a custom adaptive response action
Ad hoc Invocation
Security analyst manually triggers an ad hoc adaptive response action from a notable event on Incident Review

http://dev.splunk.com/view/enterprise-security/SP-CAAAFBE

AR App Development in 5 Easy Steps

[TA-add-on-name]	1 Create a File structure
Appserver	
static / [app_icon].png	
alert_actions.conf.spec savedsearches.conf.spec	2 .spec files declares alert action parameters for alert_actions.conf and savedsearches.conf
default / alert_actions.conf	Register the Custom Alert Action
bin / [custom_alert_action_script].py	3 Python script to take Alert Action on 3rd party device
data / ui / alerts / [custom_alert_action].html default / restmap.conf	4 Validate the Action Parameters through HTML file Define user interface for Alert Configuration
default / tags.conf default / eventtypes.conf	5 Tags created event type with tag “modaction_result” Defines results produced by Action as an Event Type
README	

Step #1 Setup File Structure for AR

1 Create a File structure

[TA-add-on-name]

- Appserver
  - static / [app_icon].png
  - alert_actions.conf.spec
  - savedsearches.conf.spec
  - default / alert_actions.conf
  - bin / [custom_alert_action_script].py
  - data / ui / alerts / [custom_alert_action].html
  - default / restmap.conf
  - default / tags.conf
  - default / eventtypes.conf
  - README

Step #2 Define Parameters for your Actions

[TA-add-on-name]

Appserver

static / [app_icon].png

alert_actions.conf.spec

savedsearches.conf.spec

default / alert_actions.conf

bin / [custom_alert_action_script].py

data / ui / alerts / [custom_alert_action].html

default / restmap.conf

default / tags.conf

default / eventtypes.conf

README

2 Register the custom alert action

```
[<actionname>]
is_custom = 1
label = <label for the action>
description = <action description>
icon_path = <icon file name>
payload_format = json
ttl = <time to live for search artifacts in seconds>
param._cam = {
"drilldown_uri": "<drilldown URL>",
 "supports_adhoc": true|false,
"category": ["<category>"],
"task": ["<task>"],
 "subject": ["<subject>"],
 "technology": [{"vendor": "<vendor>", "product":
"<product>", "version": "<version>"}]
}
```

Declares alert action parameters for alert_actions.conf and savedsearches.conf

alert_actions.conf.spec

```
[<actionname>]
param.<param_1> = <type and description>
param.<param_2> = <type and description>
```

savedsearches.conf.spec

```
[<stanza name>]
action.<actionname>.<param>.<param_1>  = <type and description>
action.<actionname>.<param>.<param_2>  = <type and description>
```

Step #3 Write Python Scripts for your Actions

[TA-add-on-name]

Appserver

static / [app_icon].png

alert_actions.conf.spec

savedsearches.conf.spec

default / alert_actions.conf

bin / [custom_alert_action_script].py

data / ui / alerts / [custom_alert_action].html

default / restmap.conf

default / tags.conf

default / eventtypes.conf

README

3 Python script to take Alert Action on 3rd party device

Create python script that contains:

- Logic of AR actions
- Progress logging of action
- Write out the result events
- Parameter validation coming from HTML form so as to validate them when the AR action is invoked as an ad hoc action

Step #4 Define User Interface and Validation

[TA-add-on-name]

- Appserver
  - static / [app_icon].png
  - alert_actions.conf.spec
  - savedsearches.conf.spec
  - default / alert_actions.conf
  - bin / [custom_alert_action_script].py
  - data / ui / alerts / [custom_alert_action].html
  - default / restmap.conf
  - default / tags.conf
  - default / eventtypes.conf
  - README

4 Define User Interface for Alert Configuration
Validate the Action Parameters through HTML file

<actionname>.html

<AR action code that renders form to take input parameters from users>

restmap.conf

```
[validation:savedsearch]

action.<actionname>.param.<param_1>  = validate(match('action.<actionname>.param.<param_1>', "<any_regular_expr>"), "<message to display in case of failure>"
```

Step #5 Create Event Types and Tags

[TA-add-on-name]

Appserver

static / [app_icon].png

alert_actions.conf.spec

savedsearches.conf.spec

default / alert_actions.conf

bin / [custom_alert_action_script].py

data / ui / alerts / [custom_alert_action].html

default / restmap.conf

default / tags.conf

default / eventtypes.conf

README

5

Tags created event type with tag “modaction_result”

tags.conf

```
[eventtype=<actionname>]
modaction_result = enabled
```

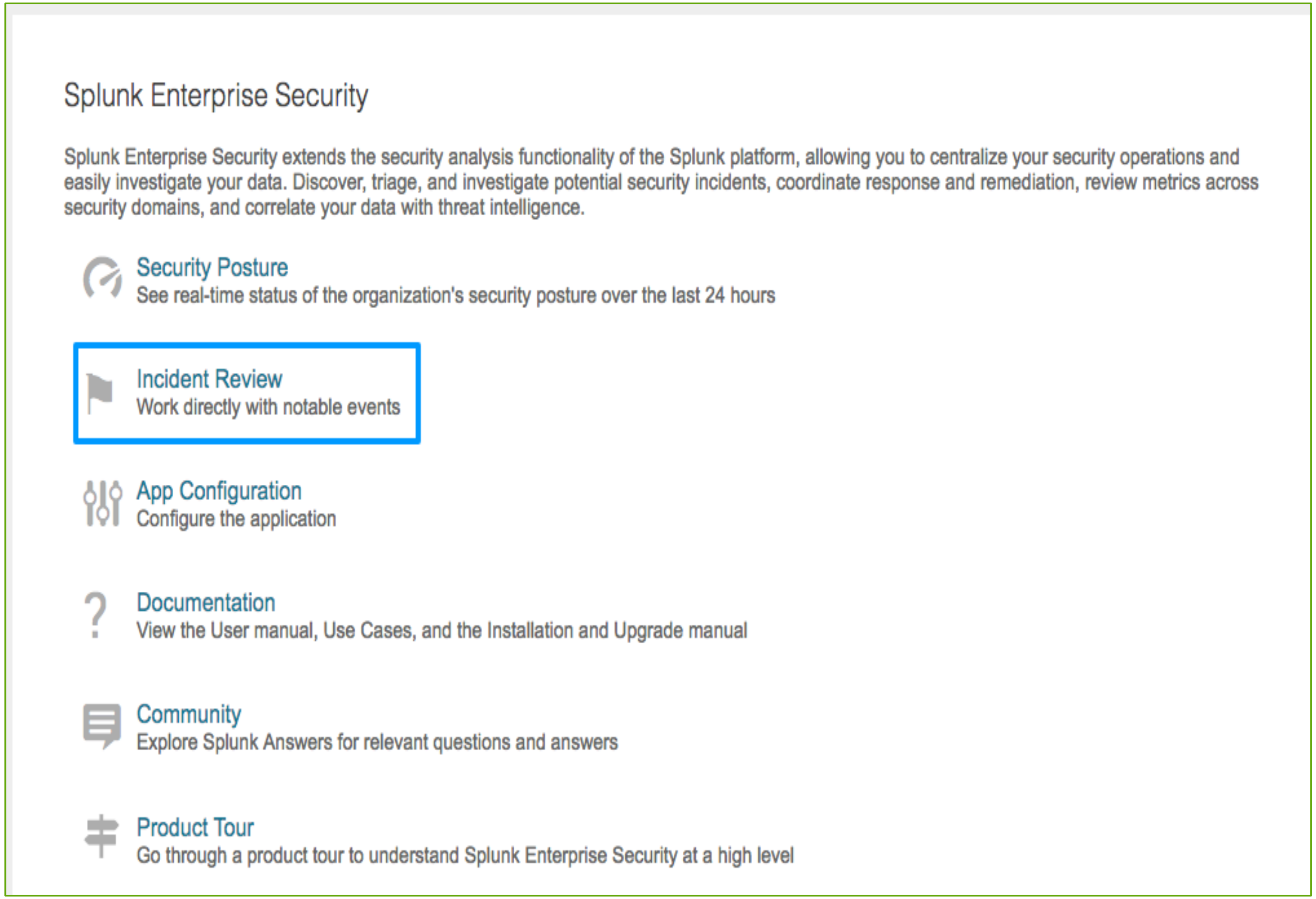
Defines results produced by Action as an Event Type

eventtypes.conf

```
[<actionname>]
search = index=<myaction_results>
sourcetype=<myaction:results>
```

Invoke AR Actions

1. Go to Incident Review



Splunk Enterprise Security

Splunk Enterprise Security extends the security analysis functionality of the Splunk platform, allowing you to centralize your security operations and easily investigate your data. Discover, triage, and investigate potential security incidents, coordinate response and remediation, review metrics across security domains, and correlate your data with threat intelligence.

Security Posture
See real-time status of the organization's security posture over the last 24 hours

Incident Review
Work directly with notable events

App Configuration
Configure the application

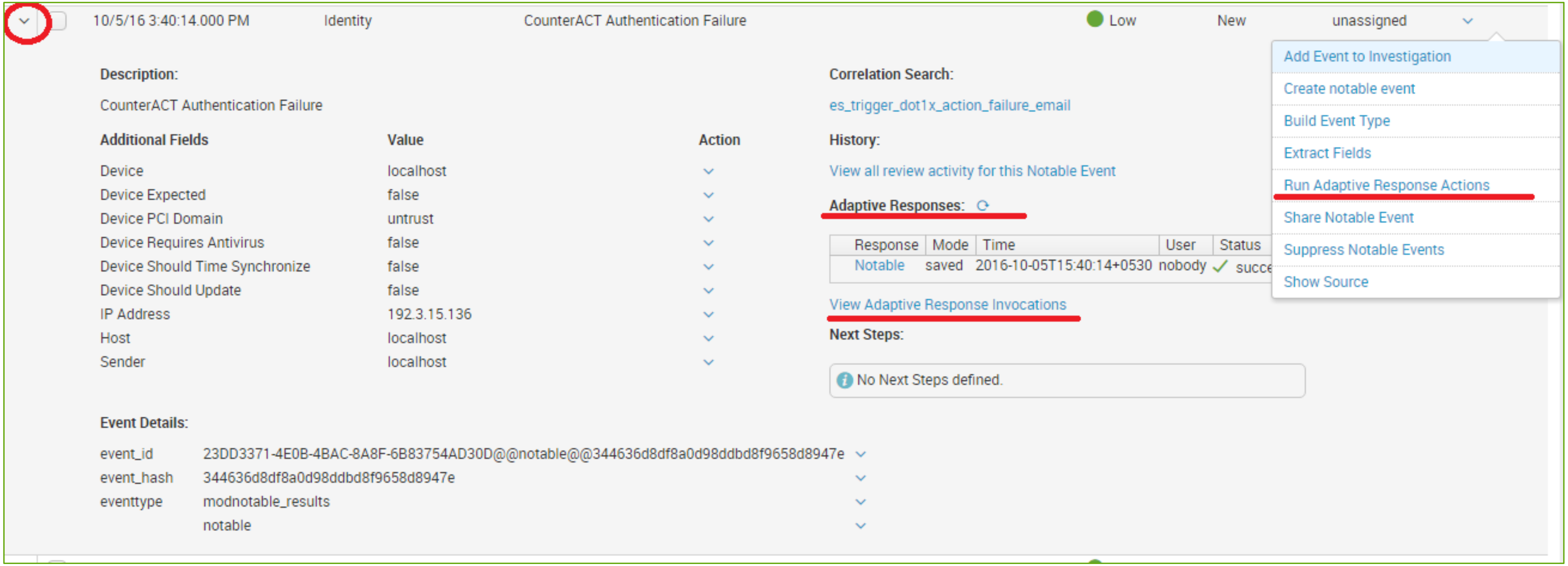
Documentation
View the User manual, Use Cases, and the Installation and Upgrade manual

Community
Explore Splunk Answers for relevant questions and answers

Product Tour
Go through a product tour to understand Splunk Enterprise Security at a high level

Invoke AR Actions

2. Click on Specific Events on which Adaptive Response Actions needs to be invoked



10/5/16 3:40:14.000 PM	Identity	CounterACT Authentication Failure	● Low	New	unassigned

Description:

CounterACT Authentication Failure

Additional Fields	Value
Device	localhost
Device Expected	false
Device PCI Domain	untrust
Device Requires Antivirus	false
Device Should Time Synchronize	false
Device Should Update	false
IP Address	192.3.15.136
Host	localhost
Sender	localhost

Correlation Search:

es_trigger_dot1x_action_failure_email

History:

View all review activity for this Notable Event

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2016-10-05T15:40:14+0530	nobody	✓ succe

View Adaptive Response Invocations

Next Steps:

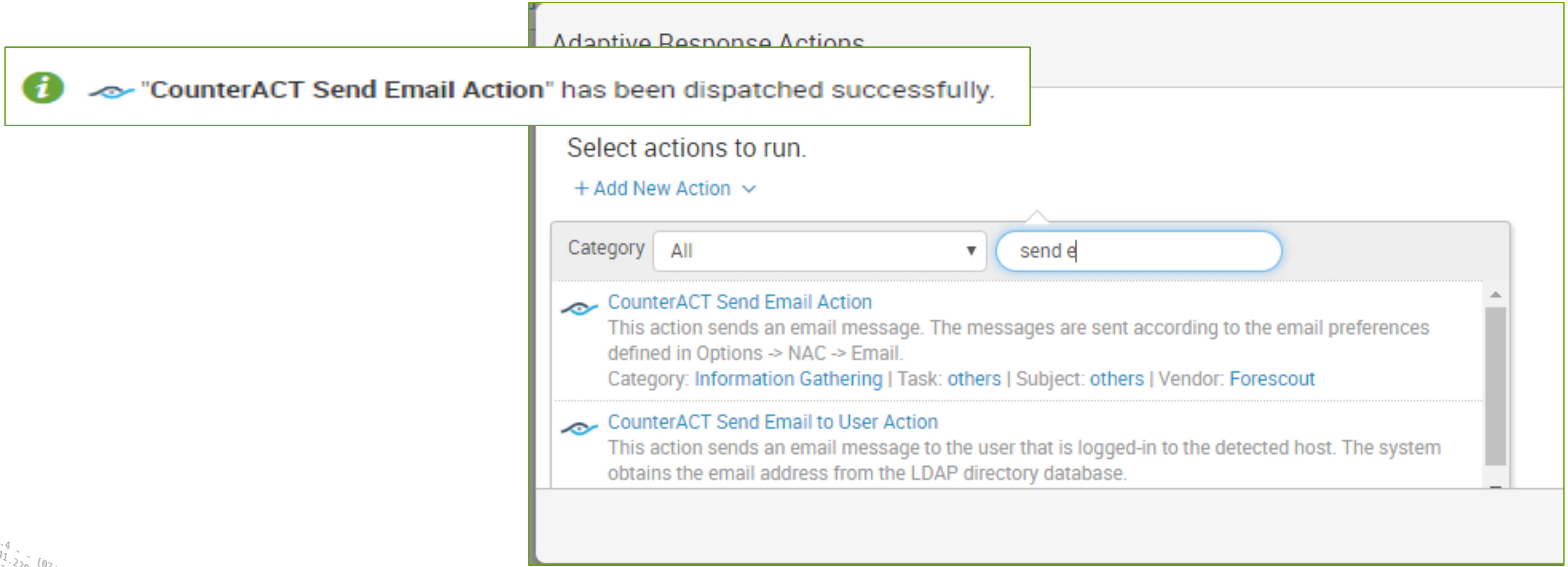
No Next Steps defined.

Event Details:

event_id	23DD3371-4E0B-4BAC-8A8F-6B83754AD30D@@notable@@344636d8df8a0d98ddbd8f9658d8947e
event_hash	344636d8df8a0d98ddbd8f9658d8947e
eventtype	modnotable_results notable

Invoke AR Actions

3. Select Specific Action which needs to be executed
4. Review the status based on the response from security product on the action taken



"CounterACT Send Email Action" has been dispatched successfully.

Adaptive Response Actions

Select actions to run.

Category: All

send e

CounterACT Send Email Action
This action sends an email message. The messages are sent according to the email preferences defined in Options -> NAC -> Email.
Category: Information Gathering | Task: others | Subject: others | Vendor: Forescout

CounterACT Send Email to User Action
This action sends an email message to the user that is logged-in to the detected host. The system obtains the email address from the LDAP directory database.

Key Takeaways

Need for Speed for SecOps

1. Adaptive Response delivers **multi-vendor security workflow automation**
2. SecOps teams can **find and remediate breaches** within the same environment
3. Adaptive Response delivers on the much desired **need for speed**!

Thank You

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

splunk> .conf2017