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?

- Preparation: 9%
- Identification/Scoping: 32%
- Containment/Mitigation: 15%
- Eradication/Remediation: 16%
- Root Cause Analysis: 25%
- Lessons Learned/Recovery: 3%

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

N=100
Time = Risk => The Need for Speed!
When working an incident which phase generally takes the longest to complete in your organization?

- Preparation: 9%
- Identification/Scoping: 32%
- Containment/Mitigation: 15%
- Eradication/Remediation: 16%
- Root Cause Analysis: 25%
- Lessons Learned/Recovery: 3%

Day in the life of a security professional survey
© 2016 Enterprise Management Associates, Inc.
N=100
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

http://dev.splunk.com/view/enterprise-security/SP-CAAABFBE
# AR App Development in 5 Easy Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a File structure</td>
</tr>
<tr>
<td>2</td>
<td>.spec files declares alert action parameters for alert_actions.conf and savedsearches.conf</td>
</tr>
<tr>
<td>3</td>
<td>Python script to take Alert Action on 3rd party device</td>
</tr>
<tr>
<td>4</td>
<td>Validate the Action Parameters through HTML file</td>
</tr>
<tr>
<td>5</td>
<td>Tags created event type with tag “modaction_result”</td>
</tr>
</tbody>
</table>

**[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
  - tags.conf
  - eventtypes.conf

- **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

Register the custom alert action

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

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

<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>")

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

Tags created event type with tag “modaction_result”

Tags created event type with tag “modaction_result”

 Defines results produced by Action as an Event Type

tags.conf
[eventtype=<actionname>]
modaction_result = enabled

eventtypes.conf
[actionname] search = index=<myaction_results> sourcetype=<myaction:results>
Invoke AR Actions

1. Go to Incident Review

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
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
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