Accelerate Incident Investigation With RedSeal and Splunk Adaptive Response Actions

Kurt VanEtten

September 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.

Splunk, Splunk>, Listen to Your Data, 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. © 2017 Splunk Inc. All rights reserved.
RedSeal Creates a Model of Your Network
RedSeal Platform: Improves Existing Jobs Across the Enterprise

- Network Engineers: Access & Policy, M&A
- RedSeal UI
- RedSeal API

- CEO/CFO: Risk/Resilience, Metrics

- CIO/CISO: Policy/Compliance, GRC

- Security Engineers: Prioritization & Speed
- IR
- Vul Mngr

RedSeal Models the Customer Network & Cyber EcoSystem

The right information, in the right place, to the right person, at the right time

RedSeal User Interface, API and In Product Integrations
“What it does [RedSeal] is act as a force multiplier for every other security device within a network, finding vulnerabilities and mapping out the dangers in relation to the specific network being protected”

-CSO Magazine
June 2017
Incident Response Process
Understand the Pain Points - Research Results

Preparation
• Difficult to maintain and tune correlation rules.

Detection
• Far too many Incidents to handle

Analysis
• Inability to locate IoC both logically and physically.
• Extremely tedious and time consuming to find all possible paths to critical assets

Containment
• Inability to execute on containment options because of inability to locate L3 and L2 devices.

Eradication
• Difficult to find all possible malware or access.

Post Action
• Difficult to communicate to non tech teams
Incident Investigation

Analysis
- Inability to locate IoC both logically and physically.
- Extremely tedious and time consuming to find all possible paths to critical assets

Containment
- Inability to execute on containment options because lack need to locate L3 and L2 devices.
Incident Investigations

- What is the asset with the indicator of compromise?
- Where is located logically and physically?
- Where can the attacker traverse to?
- How would they get there?
- What are the options to contain the incident?
Incident Investigations

Possible Command & Control

Reachable Targets
Incident Investigations - Understanding Access Policy

Indicator of Compromise
Incident Investigations - Understanding Access Policy
Incident Investigations - All Possible Access Paths

From IoC to all Possible Target
Incident Investigations - Understanding Access Policy

Path across Cloud, SDN, and on prem

Line Allowing Traffic
Splunk Enterprise Security Adaptive Response
Splunk ES RedSeal Adaptive Response
Splunk ES RedSeal Adaptive Response

IoC IP Address
Splunk ES RedSeal Adaptive Response
Splunk ES RedSeal Adaptive Response

RedSeal Adaptive Response Actions
Splunk ES RedSeal Adaptive Response
Splunk ES RedSeal Adaptive Response
Splunk ES RedSeal Adaptive Response
Splunk ES RedSeal Adaptive Response
Splunk ES RedSeal Adaptive Response

RedSeal Adaptive Response actions executed successfully
Splunk ES RedSeal Adaptive Response Results
Splunk ES RedSeal Adaptive Response

Host Details
Splunk ES RedSeal Adaptive Response

Host Details:
- Attack Depth
- Port, Switch
- Access to Critical Assets
Splunk ES RedSeal Adaptive Response
Splunk ES RedSeal Adaptive Response

Reachable Groups from IoC
Splunk ES RedSeal Adaptive Response

Reachable Groups
SPLUNK
ES RedSeal Adaptive Response

Launch RedSeal
Splunk ES RedSeal Adaptive Response

IP of IoC
Splunk ES RedSeal Adaptive Response

What is it?

Where is it?
Splunk ES RedSeal Adaptive Response

Where can they go?
Splunk ES RedSeal Adaptive Response
Splunk ES RedSeal Adaptive Response
Splunk ES RedSeal Adaptive Response

How would they get there?
Splunk ES RedSeal Adaptive Response
Splunk ES RedSeal Adaptive Response
Splunk ES RedSeal Adaptive Response
Thank you.
Q&A
Thank You

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