REDSEAL

ACCELERATE INCIDENT INVESTIGATION
WITH NETWORK CONTEXT

SOLUTION OVERVIEW

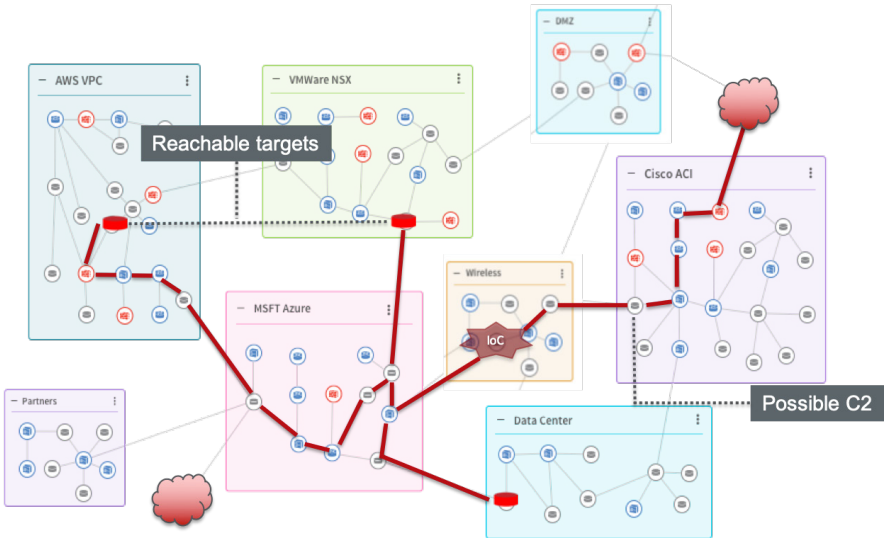
The goal of incident response is to address and manage a security breach in a way that limits damage and reduces recovery time and costs. Your SIEM solution can identify an indicator of compromise (IOC) by analyzing and correlating the massive streams of machine data generated by your IT systems and technology infrastructure.

Through a seamless integration with the Splunk Adaptive Response framework, the combination of RedSeal and Splunk can result in a significant increase in network situational awareness and full visibility of access paths to/from an IOC to critical assets and contain downstream risk, within minutes.

ACCELERATE INCIDENT RESPONSE WITH REDSEAL ADAPTIVE RESPONSE ACTIONS

RedSeal helps in accelerating incident response in two ways—providing insights for correlation to identify IOCs as well as providing immediate answers to the following questions:

1. What is the compromised device?
2. Where is it located both physically and logically?
3. Where can the attacker traverse to? Can it reach my critical assets?
4. What containment options are available to me?



splunk>

BENEFITS

- Quickly locate an IOC—including its physical location and other data
- View all potential paths an intruder can take from an IOC
- List downstream assets prioritized by risk awith access paths for each
- Locate firewall(s) and the rules to help block pathways

WHAT YOU NEED

- Splunk Enterprise 7.2
- RedSeal 9.0

REDSEAL AND SPLUNK ADAPTIVE RESPONSE

RedSeal provides three Adaptive Response actions to quickly answer the above questions:

Display source details

- Get the device's OS, applications, policy group and L2 information

List top reachable groups, launch RedSeal incident response

- Identify all downstream assets that the compromised device can access, prioritized by the business value and the exposure
- Launch RedSeal to get more details in a separate browser window, including the L2 information on each of the reachable targets

View detailed path

- Display access path(s) from the source to the target, listing all the connected devices in-between, with details on the firewall(s) and the configuration rules permitting access

NETWORK SITUATIONAL AWARENESS WITH ACCESS PATHS

RedSeal's model presents an accurate, up-to-date map of your network as it really is—including your cloud and virtual networks, and your physical and wireless infrastructure.

RedSeal's model calculates all access—intended, not intended, active and potential—between any two points on your network. With this network visualization, you can see all the individual devices between one point and another, and pinpoint the exact rules you need to change to affect access on each device.

Please contact your RedSeal account representative to get access to the latest version of the RedSeal Adaptive Response App or download at ***https://splunkbase.splunk.com/app/3473/***

REDSEAL

1600 Technology Drive, San Jose, CA 95110

+1 408 641 2200 | redseal.net