REDSEAL & SPLUNK

GETTING MORE FROM YOUR SIEM WITH REDSEAL INCIDENT RESPONSE

SOLUTION OVERVIEW

According to the 2016 Verizon Data Breach Investigations Report (DBIR), IT staff continue to struggle with breach detection and response. Indeed, internal breach discovery detected fewer incidents than did fraud detection, third parties and law enforcement. Part of the problem is that most organizations are protected by perimeter defenses. But, increasingly, phishing attacks are putting the attacker inside the network. And, according to the Verizon DBIR, 30 percent of phishing messages were opened by the targeted recipient within the first two minutes of receipt.

To detect attacks that originate inside organizations, many companies are purchasing Security Information and Event Management (SIEM) systems. The intent is to feed all non-security and security data into a single repository to baseline normal user and traffic activity. Using this baseline, analytics can detect the anomalies and outliers that may be advanced threats. Statistics can help with this detection by looking for events that are standard deviations from the norm. Correlations can also help by detecting combinations of events that are rarely seen and are suspicious. But, to analyze and contain these breaches, you need to really understand your network.

REDSEAL INCIDENT RESPONSE

Once an Indicator of Compromise (IOC) is detected, the incident response team begins a thorough investigation into the extent of the breach. They'll ask five questions:

1. What is the compromised device?
2. Where is it physically and logically located?
3. Can it access other assets?
4. Can it reach an untrusted network?
5. What are the pathways to these assets?

RedSeal provides all the tools you need to quickly answer these questions. For example, it provides the OS, applications (services), MAC address, the device's subnet (e.g., Finance, Sales, Engineering) and the policy group it is part of. It also gives you the switch and port number the device is connected to.

Importantly, RedSeal also provides a list of downstream assets that the compromised device can access. This list is prioritized based on the downstream target's asset value and the severity of known vulnerabilities that can be exploited. RedSeal also shows you detailed host information for each reachable asset. In addition, you'll be able to see detailed pathways to these downstream assets, including the firewall rule (or ACL) that is allowing access to these devices.

You'll also want to know if the compromised host can be accessed from an untrusted network. If it can, it might be connecting to a command and control server, which could be exfiltrating confidential information. In this case, containment is a high priority and you can use RedSeal's detailed path information to locate a firewall or ACL that can block access.

BENEFITS

- Quickly locate and contain a breach within L2 information
- Determine if a command and control server can be reached
- Mitigate risk based on asset value and potential for attack
- Block pathways an adversary can use to exploit vulnerable assets

WHAT YOU NEED

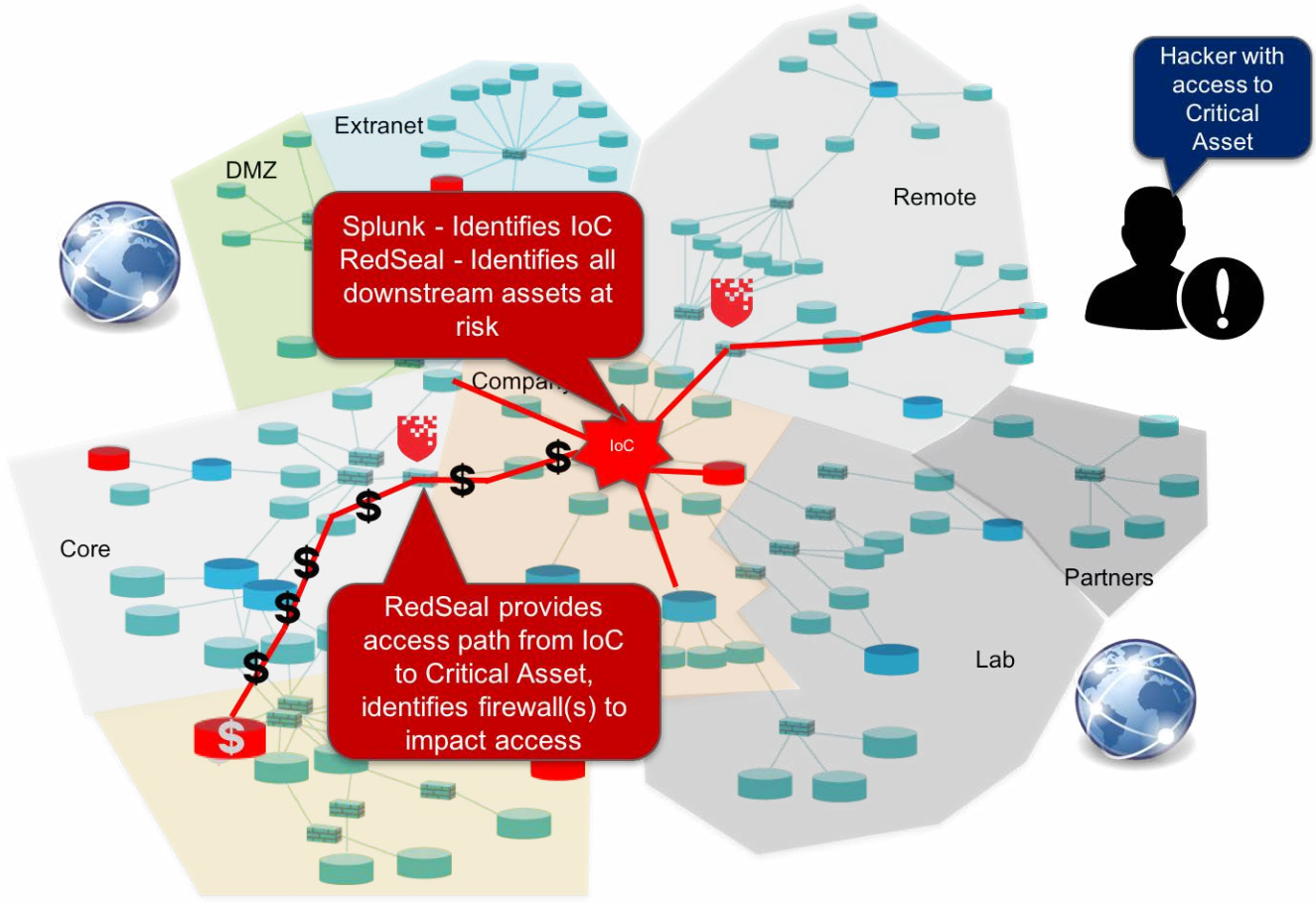
- Splunk Enterprise X.X
- RedSeal 8.3

REDSEAL & SPLUNK

GETTING MORE FROM YOUR SIEM WITH REDSEAL INCIDENT RESPONSE

SITUATIONAL AWARENESS

Breaches may be inevitable but the outcome doesn't have to be. RedSeal security analytics allows you to identify, process and comprehend the critical elements of your network so that you can contain the breach. You will quickly know if a compromised host has access to an untrusted network and potentially to a Command and Control server. You'll get a list of downstream assets that can be reached by a compromised host prioritized by asset value and the risk of attack. You'll be able to see the detailed paths available to an adversary in a graphical display that includes the firewall rule or ACL that is allowing access. And the physical and logical locations of these devices will give you the actionable intelligence you need to mitigate the breach.



REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

+1 408 641 2200 | 888 845 8169 | redseal.net/integration-apps