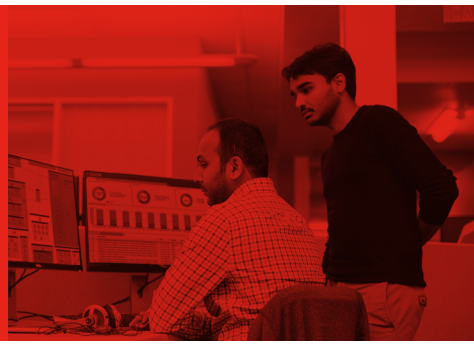
REDSEAL

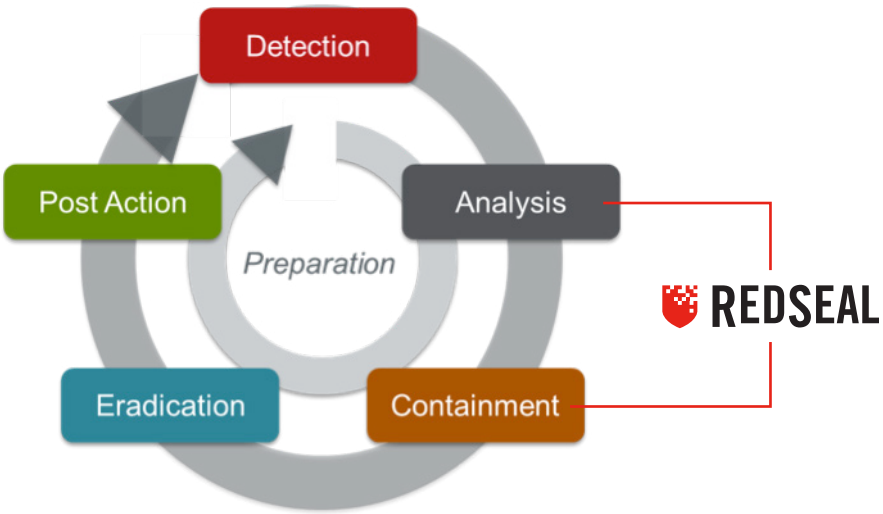
ACCELERATE INCIDENT INVESTIGATION
WITH NETWORK CONTEXT



THE CHALLENGE

Although detecting threats is critical to security, the key to minimizing a security incident's impact is a swift incident investigation phase—uncovering the device's location, what it is, what type of access it has, and whether it can reach other critical assets on the network.

Finding all possible paths to all critical assets can be tedious and time-consuming. If you must decide how to contain the incident without full network context, you run a high risk that the attacker will be able to maintain a presence in your network. And, while you are analyzing and planning how to contain the threat, threat actors have more time to cause damage by spreading out and establishing deep footholds in your network.



IBM QRadar

BENEFITS

- Launch incident investigation queries from IBM QRadar
- Quickly locate and investigate a breach
- Determine if a command and control server can be reached
- Prioritize risk based on asset value and potential for attack
- Block pathways an adversary can use to exploit vulnerable assets
- Accelerate the incident investigation
- Provide key insights to inform containment decisions
- Empower incident responders with key information inside this familiar platform

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085
+1 408 641 2200 | 888 845 8169 | redseal.net

REDSEAL AND IBM QRADAR

SOLUTION

As part of your incident investigation workflow, RedSeal provides quick answers to key questions about a potentially compromised device:

- The device's OS, applications (services), MAC address, subnet (e.g., finance, sales, engineering) and policy group.
- The switch and port number the device is connected to.
- A list of downstream assets that the device can access—prioritized based on the downstream target's asset value and the severity of known vulnerabilities that can be exploited.
- Detailed host information for each reachable asset, along with detailed pathways to these downstream assets, including the firewall rule (or ACL) allowing access.
- Whether the device 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.
- The information you need for a thorough containment plan

WHAT YOU NEED

- IBM QRadar Security Intelligence v7.2.8 or later
- RedSeal 8.4.2 or later

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

+1 408 641 2200 | 888 845 8169 | redseal.net

OCTOBER 2018