REDSEAL

REDSEAL ACCELERATES INCIDENT INVESTIGATION

THERE IS AN INDICATOR OF COMPROMISE ON YOUR NETWORK

RedSeal will tell you:

- What is being attacked
- Where it is—physically and logically
- Where the attacker can reach from there
- How the attacker would get there
- Valuable information for containing threats

IMMEDIATE INVESTIGATION QUESTIONS: HOW REDSEAL HELPS

WHICH SPECIFIC ASSET WAS COMPROMISED AND WHERE IS IT?

RedSeal helps you quickly identify the compromised asset and find its precise logical and physical location.

WHAT CRITICAL ASSETS CAN BE ACCESSED FROM AN IOC?

In an instant, RedSeal can display all other assets reachable from the IoC.

WHAT IS THE PATH FROM THE IOC TO THESE ASSETS?

RedSeal shows you the exact detailed paths that lead to any reachable assets. You can immediately focus security efforts to protect your most critical assets.

WHAT ADDITIONAL INTELLIGENCE DO WE NEED TO ACT?

RedSeal identifies the exact configuration enabling unwanted access, quickly guiding you to remediation options. RedSeal's network map also includes L2 and L3 devices, so you can determine where to place intrusion detection systems or honeypots.

NIST INCIDENT RESPONSE LIFECYCLE: REDSEAL BUILDS RESILIENCE

Preparation

RedSeal clearly identifies what access, known or unknown, is permitted to all parts of network. You can ensure that your devices are configured securely and that there is no unintended access to anywhere in the network.

Analysis

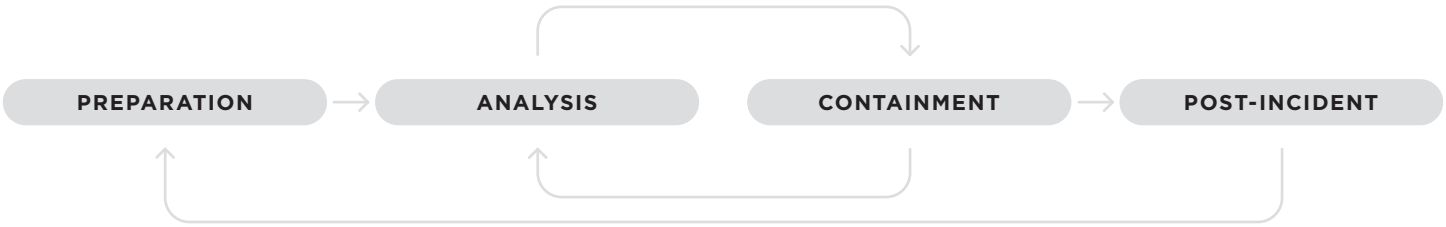
RedSeal quickly locates any IoCs and helps prioritize them by identifying reachable (and valuable) assets.

Containment

RedSeal shows the detailed path from an IoC to reachable assets. You'll get specific port and switch information so that you can act quickly.

Post-Incident

With RedSeal, you can immediately re-scan your network to ensure your network's security post-remediation. It can also export data to help you easily document this process.



REDSEAL WORKS WITH YOUR EXISTING SIEM

RedSeal integrates with all industry leading SIEMs such as Splunk Enterprise Security, IBM QRadar, or MicroFocus ArcSight ESM, accelerating your investigations by providing immediate and meaningful network context.

RedSeal is also certified on Splunk's Adaptive Response Framework.

> **"What RedSeal does, is act as a force multiplier for every other security device within a network"**
>
> *CSO Review*

splunk> IBM QRadar MICRO FOCUS

REDSEAL

1600 Technology Drive, San Jose, CA 95110

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