REDSEAL

US GOVERNMENT AGENCY USES REDSEAL

TO AVOID HUMAN ERROR, SPEED NETWORK VISUALIZATION AND ACHIEVE SURPRISE-FREE COMPLIANCE AUDITS

In 2014, information assurance engineer John America was hired to support the deployment of RedSeal at a US government agency. As part of a team of 200 cybersecurity professionals, John was asked to solve a major problem: figure out what was actually happening on the network.

Previously, the only option was to ask the network team to manually search the network for devices that could be routed to and from. The network engineers would sift through thousands of lines in the configuration files of routers and firewalls to try to figure out how these complex combinations of settings were affecting access between points in the network. This approach was both inaccurate, due to human error, and unstainable from a resource standpoint. It would take a few days to complete the map of the network, distract engineers from other critical tasks, and resulted in weaknesses in security going undetected and continued risk of security breaches.

Today, with RedSeal deployed, the entire process of visualizing network access is fast and accurate. How? RedSeal examines all those configuration files and automatically calculates all access paths, so the potential for human error has been significantly reduced. More complex analysis is now possible, such as using RedSeal to examine all configuration files on a network and automatically calculate all access paths.

For example, the agency's cybersecurity leadership asked John's team to evaluate command and control protocols across the entire enterprise. They wanted to know where all their systems were and if they were accessible via Secure Shell (SSH) or Remote Desktop Protocol (RDP.) With RedSeal, they were able to determine which devices could be accessed from the Internet or from an unauthorized internal network device. The entire project, nearly impossible before, took two people just two days.

RedSeal also transformed the agency's cyber auditing and compliance process. In the past, they used a combination of single, discrete audits and continuous monitoring. Often, this meant a duplication of efforts. For example, the agency has many audits that check on STIG compliance. "Engineering loves RedSeal's ability to instantly report STIG compliance status as it saves them an enormous amount of time not repeating the same checks," John explained.

Recently, even though his team was surprised by a CCRI (Cyber Command Readiness Inspection), "The network had zero surprises," John said. "Everything else in the audit was a disaster, but the network was clean — in no small part due to RedSeal."

Going forward, John's team is looking at using RedSeal's Digital Resilience Score. They currently track a lot of activity based on a home grown heat map for risk management. He wants to use RedSeal to get a more strategic understanding of the network and to track progress over time.

Another area where John sees more uses for RedSeal is importing DISA's Ports, Protocols, and Services Management (PPSM) data to manage policy compliance. John's information assurance team currently gets many questions about access between devices. Having a clear, visual understanding of how access flows from any point to any another in his agency's complex network will allow them to make better risk based decisions.

A final area where John expects to use RedSeal is the deployment of Amazon Web Services (AWS) at his agency. AWS is currently a mystery to many of the network and cybersecurity team members. They struggle to understand how it works and how it integrates with legacy networks. They need to ensure that improper access doesn't exist from AWS to the agency or between virtual private clouds. RedSeal will map all the possible connections and present a unified version of his network. He'll see the data in a simple, normalized, and understandable way.

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

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

Mar 2017