REDSEAL

LARGE SOUTHERN U.S. HEALTHCARE PROVIDER

SITUATION

The security team for this large Southern US healthcare system needed help to pass a PCI audit. They didn't know how their network was segmented or what subnets had PCI card holder data. They also wanted one "source of truth" for all their inventory, their ServiceNow CMDB. They expected the network device data to come from SolarWinds NCM but weren't confident that all the information was there. They looked to Tenable SC for their endpoint/host information, but again they weren't confident that everything was being scanned. Additionally, their vulnerability management team wanted to improve patching prioritization by understanding potential access within the network. They knew the vulnerability severity and the value of the asset, but they wanted to know if the asset could be directly accessed from an untrusted network—and what an attacker could reach if the asset was compromised.

- Needed to pass a PCI audit, but didn't know their segmentation or subnets with PCI data.
- Wanted one inventory "source of truth" but weren't confident that their NCM and vulnerability scanner were providing complete information.
- Wanted to improve vulnerability prioritization by understanding network access.

REDSEAL SOLUTION

RedSeal professional services used the RedSeal platform to discover what was on the network and identify missing devices and missing subnets. Then, RedSeal was able to update the SolarWinds NCM and to identify what hosts Tenable SC was missing. Next, the team used RedSeal to analyze network access and uncovered lots of unintended (and high-risk) access from the internet. RedSeal imported vulnerability scan results and added knowledge of network access to better prioritize patching efforts based on the actual risk to this network.

- RedSeal provides a topology map separating devices and hosts into regions, sites and services including clouds.
- RedSeal discovered what was on the network and updated NCM and vulnerability scanner.
- RedSeal ran network access analyses, uncovering lots of unintended access.
- RedSeal risk scoring used to better prioritize patching efforts.

LARGE SOUTHERN U.S. HEALTHCARE PROVIDER

RESULTS

RedSeal continues to identify missing subnets and devices and update SolarWinds and Tenable SC, so the security team has a reliable source of truth. RedSeal's continually updated network understanding helps the security team be confident that scanners are reviewing a true list of devices and hosts.

To improve that understanding, the RedSeal network topology map separates devices and hosts into geographical regions, remote sites and data centers, then by service type. Since RedSeal includes public cloud, private cloud and physical environments in its calculations, the topology map includes Oracle and Azure clouds.

Most immediately, the security and network teams are evaluating and mitigating lot of unintended access. RedSeal found that the port WannaCry uses was open. And that the DMZ had access to the entire internal network. With RedSeal's knowledge of network access, the security team is confident that they are patching the most critical things first.

NEXT STEP

The security team will work with RedSeal professional services to establish change control policies using RedSeal to evaluate change requests.

- **RedSeal identified missing subnets and devices and continues to update and NCM and vulnerability scanner.**
- **The security and network teams discovered unwanted open access and continue to evaluate and mitigate a lot of unintended access.**
- **The security team is confident that they are patching the most critical things first.**
- **The security team is confident that scanners are reviewing a true list of devices and hosts.**

REDSEAL

1600 Technology Drive, San Jose, CA 95110

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

MARCH 2020