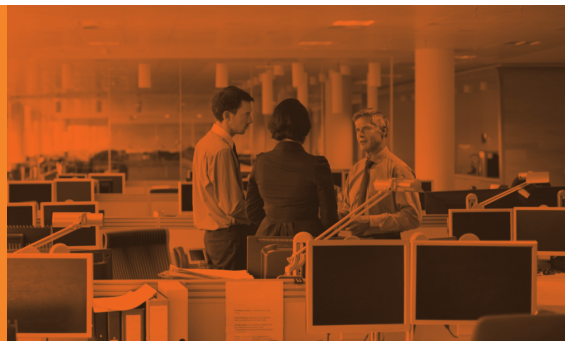
REDSEAL

NERC-CIP AND REDSEAL



A leading US integrated power company is required to meet the government standards set forth by NERC (North American Electric Reliability Corporation). The NERC CIP (Critical Infrastructure Protection) plan is a set of requirements designed to secure the assets required for operating North America's bulk electric system. The plan consists of 9 standards and 129 requirements covering the security of electronic perimeters and the protection of critical cyber assets as well as personnel and training, security management and disaster recovery planning.

The two keys to a successful compliance program are embedding security into operations and automating routine tasks. Embedding security into operations makes security part of a daily mindset. Compliance becomes a byproduct of that security. The other key is automating routine processes. This enables operations and compliance teams to shift to a management by exception mindset rather than reviewing every piece of data that is available. Two of the most labor-intensive tasks for both security and compliance are logical segmentation and firewall rule analysis. Many organizations perform this work manually, some using software to visualize a single firewall at a time. But these approaches don't allow an organization to evaluate their network as a whole. The company needed to see how traffic might flow from one subnet to another and evaluate the risk of vulnerabilities specific to their environment.

The company implemented RedSeal in 2015 as part of a CIP version 5 program implementation. The primary uses for RedSeal were firewall rule evaluation and proving logical segmentation. The uses have expanded as the company gained experience with the platform, and RedSeal has become a key part of their daily security and compliance processes.

"Using RedSeal reduced the time it takes us to evaluate our systems for specific vulnerabilities from one person/month to 15 minutes.

We can spend our time on mitigation, rather than assessment."

Director, NERC CIP Operations, Cybersecurity

NERC-CIP AND REDSEAL

KEY SECURITY AND COMPLIANCE USE CASES

Firewall Rule Business Justification
NERC-CIP requires a business justification for every firewall rule. RedSeal simplifies the evaluation of firewall rules and allows a business justification for each rule to be documented.

Logical Segmentation
Logical segmentation of plant control systems can increase security and reduce the compliance exposure of those systems. Logical segmentation that prevents one cyber system from impacting another can limit the likelihood that a potential cyber-attack could impact the entire facility. By limiting potential impact, the CIP risk rating of the segmented system can be reduced, which reduces the number of applicable CIP compliance requirements. Specifically, reducing CIP risk ratings from Medium to Low reduces the compliance obligation from 129 requirements for a Medium system to only 4 for a Low system.

Firewall Rule Change Monitoring
RedSeal is configured to import all firewall rules on a daily basis. It displays a dashboard displaying the status of any firewall changes. This simplifies the process of ensuring that business justifications for new firewall rules have been completed. The company has created policies based on the approved logical segmentation rules. The policy is automatically run each time firewall rules are imported. The CIP Team is alerted by email to any exception to the logical segmentation policy.

Vulnerability Evaluation
Many security vulnerabilities can't be exploited unless certain ports or communication paths are open. RedSeal's network modeling to evaluates the actual risk level of vulnerabilities—based on the location of assets within the network and the firewall rules in place. The company has been able to reduce the time required to evaluate the impact of vulnerabilities and now has a more methodical approach to mitigation based on true risk rather than responding to every vulnerability as an emergency.

CIP AUDIT READINESS

CIP audits require entities to show the business justification for all firewall rules and configurations. RedSeal's reporting capability significantly reduces the time required to build reports for compliance. Additionally, the automation it provides in monitoring firewall rule changes and logical segmentation policies demonstrates a strong control over those processes. Automation and strong controls factor into the depth and frequency of CIP audits.

NERC-CIP AND REDSEAL

CYBERSECURITY THREAT MODELING AND MITIGATION

NERC Alerts require the company to evaluate its systems for specific vulnerabilities. This evaluation frequently requires reviewing firewall rules at all its plants. The task took the equivalent of one full-time person a month to complete—with possible exposure from the threat the entire time.

When the WannaCry ransomware attack was released in May 2017, the company had to find sites with port 445 open to assess possible vulnerabilities. Using RedSeal, the task took one person 15 minutes—rather than one month. The team can now spend time on mitigation efforts rather than assessment.

PRIORITIZING VULNERABILITIES

Other parts of the company are also starting to use RedSeal now that it's fully implemented and processes have matured. For example, RedSeal integrates with Tenable, a product used for malware protection and network scanning. RedSeal provides a network "heat" map to visually identify vulnerabilities. This allows teams to see where a vulnerability is located within their network, to prioritize risk (i.e. if it's buried deep vs. exposed to the outside), and to mitigate the most critical vulnerabilities based on both severity and access to the outside.

RedSeal has improved the company's threat response capabilities, automated manual processes, and allowed the organization to be ready for a NERC CIP audit at any time. Infodat continues to support the company as RedSeal matures and new features are implemented.

ABOUT INFODAT:

Infodat has been delivering value based IT and security solutions for over 20 years. We have helped mid and enterprise organizations to drive out costs, improve customer experience and to develop ecosystems to support strategic objectives

- **Microsoft Gold Partner** Dynamics CRM, Sharepoint, SQL Server, .NET and mobile apps, Azure, etc.
- **Data and Analytics** Hadoop, Power BI, Datameer, Qlik, data consolidation and cleansing, etc.
- **Security Solutions** Compliance readiness, endpoint protection, threat management, etc.
- **Application Modernization** DevOps, API development, Green screen to modern UI, etc.

ABOUT REDSEAL:

RedSeal's network modeling and risk scoring platform is the foundation for enabling enterprise networks to be resilient to cyber events. RedSeal helps customers understand their network from the inside out—providing actionable intelligence, situational awareness and a Digital Resilience Score to help enterprises measure and improve their resilience. Government agencies and Global 2000 companies around the world rely on RedSeal to help them validate their overall security posture, accelerate incident investigation and increase the productivity of their security and network teams.

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

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