

Exceptional service in the national interest

Cybersecurity Risk Management Pilot Abstract

The Production Operations Area at Sandia National Laboratories has conducted a cybersecurity risk management pilot with goal of improving its security posture. The objectives for this pilot were multi-purpose:

- Establish a quantifiable cyber security baseline for the Production Operations Area.
- Establish the ability to track and compare scans, over time, to quantify cyber security improvement.
- Ensure the benefits of aggregating, correlating and prioritizing the cyber security information for the Production Operations Area are easily understood.
- Establish an action plan to help improve the overall cyber security posture.

The pilot included the proof of a secure process to deploy a tool, including recurring upgrades, training, and maintenance, along with the full exercising of the analytical capabilities necessary to improve management of cyber security risks. The pilot results were beneficial and helped the technical staff, as well as management, understand the overall security posture.

The tool, RiskSense, aggregates data for network assets and applications, using information from leading commercial network and application scanners. It then correlates the data to provide comprehensive insight into an organization's current security posture. Once the security posture is known and understood, a prioritized strategy for remediation can be established.

This presentation will provide information about RiskSense, discuss the process, and demonstrate how the product was able to satisfy the production operations area's need to aggregate, correlate, and prioritize cyber security information.