Network Security Audit

Case Study

A Manufacturing Giant's Story

The Fast Track to Passing Network Security Audits

CHALLENGE

A large manufacturing company with a complex network of approximately 1000 routers and switches. The company underwent an external security audit and was flagged with several critical vulnerabilities in their network device configurations. The auditor requested detailed network information, including:

A complete list of all network devices (routers, switches, firewalls, AP etc.) with their make, model, serial number and OS version. Identification of any devices nearing the end of their support lifecycle from the manufacturer. Up-to-date Layer 2 (L2) and Layer 3 (L3) diagrams illustrating the network layout and connectivity between devices. Fixing multiple security weaknesses discovered during the audit posing high risk.

Time Constraints: The company was pressed for time to respond to the auditor's findings to address the security gaps. Manually collecting and compiling the requested information from approximately 1000 devices would have been a monumental task, potentially delaying their response and jeopardizing their security posture.

SOLUTION

UTORA came to the rescue. UTORA is a network automation platform designed to streamline network discovery, data collection, and configuration management.

Rapid Network Inventory: UTORA automatically discovered and documented all 1000 network devices, providing a comprehensive inventory within hours.

EOL Device Identification: UTORA compared device models with manufacturer databases, pinpointing devices reaching their EOL and flagging them for potential security risks and upgrade needs.

Automated Topology Mapping: UTORA leveraged network communication protocols to automatically generate up-to-date L2 and L3 network topology diagrams, saving the company significant time and effort.

Security Gap Remediation: UTORA's built-in compliance libraries were used to identify configurations that deviated from security best practices. The platform then guided the network team through the process of fixing these security gaps on the same day.

BENEFITS

Reduced Risk: By promptly addressing security vulnerabilities, the company minimized their exposure to potential cyberattacks.

Improved Efficiency: UTORA's automation capabilities saved the company countless hours compared to manual data collection and configuration changes.

Enhanced Compliance: The rapid response to the audit findings ensured the company remained compliant with security regulations.

Informed Decision Making: Having a complete network inventory and visibility into EOL devices allowed for informed decisions about network upgrades and maintenance.

Audit-Readiness: Its not just about passing a single audit, It's a continuous state of preparedness that ensures your network can withstand external scrutiny at any time.

CONCLUSION

UTORA's network automation capabilities proved invaluable in this case study. By providing a quick and efficient way to gather network information to address security gaps, UTORA helped the manufacturing company achieve compliance, improve security posture, and save valuable time and resources. This case study highlights the critical role automation can play in maintaining a secure and efficient network infrastructure, especially for large and complex networks.

> “Automated the full network discovery, assessment & compliance cycle thereby fostering a culture of **continuous Audit-Readiness.**”