Case Study

IT Organization at Large Enterprise Creates Vulnerability Management Program

The client

This large and growing enterprise supports organizations with critical business platforms. Its technology solutions are powered by innovation and a diverse workforce located around the globe.

The challenge: Deploy timely security patches and ensure compliance with FedRAMP

The IT organization of the corporation had its fair share of security challenges to overcome. The security team, a separate group, had long pressured the IT organization to get current on patching, but didn't provide operational guidance on how to accomplish this without impacting the business.

Of particular concern was the fact that the company needed to maintain compliance with FedRAMP (Federal Risk and Authorization Management Program) guidelines in order to continue servicing government agencies, partners, and supporting organizations. Risk management and enterprise mobility management were key areas that needed attention.

Industry:

Enterprise technology

Insight provided:

- Four-phased vulnerability management project delivery
- Comprehensive assessment of vulnerability management practices
- Triage and mitigation planning
- Remediation and plans for continual improvement

Insight services:

- Security Services

The solution: Remediation, and development of a new vulnerability management program

Insight came in to help the client implement an effective vulnerability management program, with a controlled approach to system patching and vulnerability scanning.

Key objectives included:

- Incorporating best practices related to the analysis, prioritization, and remediation of information security threats
- Developing metrics and dashboards to track vulnerabilities and measure the success of the program
- Improving efficiency through automation and reducing risk across the enterprise

Our work with the client was four-phased and focused on an environment of 3,000 devices, including Windows® and Linux® systems and Azure® tenants. We worked closely with the client's CIO, CSO, and security and engineering teams.

Phase 1 — Identification of vulnerability sources

We reviewed existing processes, resources, assets, scope, tool sets, compliance requirements, monitoring sources, and incident response protocols surrounding vulnerability management.

Phase 2 — Triaging vulnerabilities

First, we coached the client team on appropriate vulnerability triaging and how to assign proper levels of urgency to each asset in question using decision trees. Then, we developed a methodology to follow for vulnerability mitigation in the client's environment.

Phase 3 — Remediation of vulnerabilities

We rebuilt the client's patch management program. This included establishing how devices would be managed when off-network, which was a critical question given the increased size of the client's remote workforce due to COVID-19. We also replaced its legacy vulnerability management solution, as it lacked the tools to support FedRAMP compliance and passive vulnerability management. Lastly, we executed asset classification and Service-Level Agreement remediation.

Phase 4 — Rollout of solution

To validate the new patch management solution, we performed a Proof of Concept (PoC). Once completed, we rolled out the solution to several pilot groups and made iterative improvements up until full production rollout. We executed a three-day migration over to the new patch management solution. Finally, we created supporting documentation for the enhanced solution and took care to transfer ownership to the client's working team and ensure their ongoing success.

The benefits: Modernized and manageable security environment

From day one, there was no doubt in the viability and effectiveness of our solution. Having invested the time and expert resources in analyzing the issues and developing a customized approach, our team could feel confident in implementing the solution and helping the client run with it.

The client is benefitting from a more secure environment with far fewer vulnerabilities and excellent visibility. Modern tool sets and documented policy, processes, and methodology help the client stay on top of patching and vulnerability management, as well as continue to improve its practices.

Benefits:

Timely implementation of security patches within Service Level Agreements (SLAs)

Reduced overall vulnerabilities

Right-fitted vulnerability management program

Modern tool sets for helping mitigate threats

Lower risk and improved threat visibility

Documented methodology to simplify vulnerability management

Insight