deepwatch

Vulnerablity Management **Case Study**

The Customer

Industry: Healthcare

Security Team Size: 12

Revenue: $1 Billion

Endpoints: 6,000

The Challenges

- Patch Management
- Patch Prioritization
- Vulnerability Management
- CVE & CVSS Tracking
- High Vulnerability and Patch Related Technology Debt

The Goal

The customer had been entrenched with a Managed Security Services Provider (MSSP) for a number of years. The MSSP was using outdated vulnerability scanning technology and wasn't able to provide the level of coverage and service that the business required. As part of an IT and security modernization initiative the customer deployed Tenable.IO solution to augment the MSSP's efforts and fill any gaps. The Chief Information Officer and his team conducted a vulnerability risk audit and it became clear that they needed to hire a new MSSP that could manage a more robust and comprehensive vulnerability management program. They wanted a new partner to:

- Outsource the vulnerability management program to a trusted partner
- Refocus time and resources spent by the security operations and incident response (IR) teams on vulnerability management tasks to more mission critical cybersecurity responsibilities
- Reduce the attack surface and overall cyber risk exposure
- Collaborate with the MSSP to enhance its vulnerability and patch management capabilities over time
- Manage, update, and enhance existing Application Programming Interface (API) integrations
- Integrate applications and processes for comprehensive vulnerability management coverage

The Criteria

The CISO and his team built a strong list of criteria needed for a planned switch to a new MSSP. The new MSSP capabilities needed to include:

- Deep technical expertise with vulnerability and patch management processes and procedures that enable comprehensive management
- Metrics to evaluate cyber risk posture and security maturity
- Previous experience with Tenable.IO along with an understanding of the technologies strengths and how to maximize them
- Internal engineering talent that could enhance API integrations
- Ability to quickly assess and prioritize vulnerabilities by mission criticality, exploitability, and risk
- Proactive vulnerability hunting processes to uncoveritems that vulnerability tools won't necessarily capture
- Reporting capabilities that provide trends, context, and risk exposure

Outcomes

The CISO and his team selected deepwatch to manage their vulnerability management program. The deepwatch Vulnerability Management Services team followed a risk-based onboarding methodology that exposed gaps in their vulnerability and patch management processes. Via collaboration and onboarding practices, deepwatch learned the company's criteria, risk profile, and mission critical applications and systems. deepwatch developed tailored patch management and vulnerability prioritization processes for the customer. Initial vulnerability scans exposed over 100,000 high priority vulnerabilities that had gone unpatched. After three months of close collaboration with deepwatch, the customer fixed over a million vulnerabilities.

Two years later the customer has managed to significantly narrow their attack surface and protect critical assets. As a result of the program's success, the customer renewed its partnership with deepwatch for three additional years.

ABOUT DEEPWATCH

deepwatch delivers data-driven managed security services while extending customers' cybersecurity teams and proactively advancing their SecOps maturity. Powered by our innovative cloud-native platform, deepwatch is trusted by leading global organizations to provide 24/7/365 managed security services.

CONTACT US

sales@deepwatch.com
7800 E Union Ave, Suite 900 Denver, CO 80237
855.303.3033

deepwatch.com