

Vulnerability Lifecycle Mgmt Automation

DayBlink Consulting supported the Vulnerability Management team of a Large Media company in automating of a variety of lifecycle steps, notably: assignment, rescanning for verification, automated ticket closure and burndown reporting.



Introduction

The Vulnerability Management team of a large U.S.-based Media company engaged DayBlink Consulting to optimize and automate a variety of lifecycle steps, including: assignment (who is responsible for remediation), rescanning for verification (after remediation occurs), automated ticket closure (for project tracking) and burndown reporting (for leadership oversight). We were responsible for redesigning the team's operating model to improve effectiveness through automating as much as was feasible. The mandate also included evaluating the tool stack and processes to support the new operating model.

The client team members had specific goals of future-proofing their capabilities and increasing the burndown volume and velocity of high severity vulnerabilities. They predominantly used CVSS scores to evaluate severity. The team had grown and shrunk in size as the organization had acquired and merged with other companies and then been acquired itself before being divested. This much M&A activity over a few year time period left an unclear mandates and span of control for the team.

Problem

Thousands of vulnerabilities were outside the internal SLAs for remediation and the existing team did not have enough cycles to resolve them

The client team had recently been dramatically reduced in personnel due to a divestiture but had an increased scope and mandate for vuln reduction. Numerous previous organizational, scope and leadership changes had diminished the effectiveness of the VM team which was not highly regarded within the company. Asset management and patch management were both owned outside of the security organization, relegating the previous VM team to scanner operators with limited visibility into what they were being asked to scan or what was done with the results afterwards. The VM team was a successful, but reactive security organization whose leader sought to develop proactive efforts to improve the company's security posture. The existing vulnerability scanning reports were managed in an ad-hoc manner without clear ownership of and reporting of the remediation efforts.

Thousands of known vulnerabilities had been identified, logged and then left unresolved due to a lack of coordination and resourcing. Risk was being accepted by many teams by default, due to an inability to address it rather than a thoughtful understanding and recognition of the potential exposure. As the backlog grew of ignored vulnerabilities, the incentive to resolve the next identified vulns shrunk, further compounding the problem. Eventually, the VM team was left with bad data, an incomplete risk register and no clear path to burning down the backlog. And as a result, Senior leadership had limited visibility into the risks they were accepting.

Vulnerability Lifecycle Automation Requirements



Scanning

Ensure maximum network coverage, including containers. There are a variety of scanning tools available and while there has been some consolidation in the industry, there is not yet a single application that provides all necessary system information. Teams still need to manage a suite of tools.



Triage

Evaluating severity and breadth of impact requires reasonable asset and configuration management (which every organization has been struggling with for years). Enabling resolution within SLAs requires effective patch management (which often gets added to a long backlog of items for development teams).



Reporting

Clear, actionable reporting to management can often provide incentive to continue supporting and funding the necessary programs. Dashboards often form a necessary foundation for reporting, but are rarely sufficient.

Solution

We built a new operating model and collaboration approach between the VM team and the engineering organizations which allowed us to enable automated remediation (and tracking) for a large amount of 'standard' vulnerabilities.

Automation was seen as a path to improved scalability of a recently reduced team. DayBlink drove a variety of individual projects that would automate remediation of large swaths of vulnerabilities. We prioritized and then managed the relevant initiatives, across: vuln scanning, triage and reporting. (Almost all vulnerabilities that affected standard-build systems and could be solved with thoroughly tested patches were eligible for automated remediation efforts.) Each element had opportunities for automation to improve throughput and effectiveness.

We started by expanding Tenable's external network scanning and ensuring additional container vulnerability scanning. Our goal was to ensure maximum network coverage. The client team was managing a variety of scanning tools - each focused on a specific type of asset. We then enabled auto-remediation of standard builds and configurations by more clearly defining assignment,

rescanning rules and automating ticket closure and burndown reporting.

Lack of complete asset and configuration management often pose challenges, but typically the automation opportunities all fall with the known/standard networks. Next we developed processes to decouple compliance and vuln scanning which improved PCI scanning compliance reporting. By operationalizing standard rules and approaches across the organization, we enabled better usage of the Security organization's CVE-producing tools. This improved the auto-remediation capabilities because there were far fewer false positives. Finally, we implemented BU-Level SLA tracking & reporting with defined trackable metrics.

The management team decided to continue supporting and funding the organization rather than further devolving the requirements to the engineers as a result of the reports.



Outcome

By providing education and additional standardization to the engineering teams which allowed process adjustments, automated remediation efforts fixed many out of SLA vulns and automated rescanning efforts properly updated those that had been patch from the backlog

DayBlink enabled the client's VM team to effectively manage a job previously performed by 4 times the people. Despite the smaller organization, we helped dramatically increase the effectiveness and satisfaction of the engineering teams. Over the following 6 months, the team effort improved vulnerability burndown times due to increased visibility and automation of subset of deployed patches which then enabled the VM team to provide value beyond operating scanners through consultative remediation advisory for non-automatable efforts.

By the end of the project, the team's effort dramatically increased the burndown of high-severity vulnerabilities within their SLAs through an increased use of automation. And the tracking efforts produced data which helped numerous stakeholders, from engineers through senior leadership with better understanding the current security risk.

95%

Reduction in aged vulnerabilities showing up on weekly scanning reports

2,000+

Aged vulns resolved and removed from backlog

100%

On time remediation of assessed risked against severity determined remediation dates

Making the Case for Automation

We believe that automation 'done right' can unlock incredible ROI and streamline operations for long-term success. Your teams can experience the transformative power of streamlined vulnerability identification and remediation to ensure that the team has the opportunity to focus on the most important requirements.

WASHINGTON D.C.
(Headquarters)
*8609 Westwood Center Dr., Suite 110,
Tysons Corner, VA 22182*

CONTACT US

Michael Morgenstern, Partner
michael.morgenstern@dayblinkconsulting.com



www.dayblinkconsulting.com