Secureworks®

WHITE PAPER

Vulnerability Management: 4 Key Challenges to Creating an Effective Program

Vulnerability management (VM) is one of the most challenging components in cybersecurity to develop and mature to meet addressable risk. Many organizations struggle to secure a comprehensive and mature vulnerability management program. And while it's foundational to cybersecurity and integral to security strategy, if you don't handle vulnerability management basics correctly, then the overall strategy is set to fail.

Technology can only be part of the equation — people, policy, and process will ultimately decide success — and it's important to know some of the challenges and obstacles to developing a program that will help companies identify areas of improvement. Some technologies, however, can help you focus on the process and outcomes, as opposed to management and configuration.

In this paper, we discuss four customer challenges commonly faced when creating an effective VM program.

Vulnerability management is one of the most important components of an enterprise security program, and yet it's consistently contentious and difficult to implement. It requires an organization to understand the inherent risk of security breaches to its business, as this understanding will help shape the program. It's key to ensure the VM program appropriately addresses risk to provide a solution that balances requirements, business risk, and cost.

1. Asset Identification

Asset identification is foundational to all programs and frameworks. Without a comprehensive view of all assets — including hardware, operating systems, virtual systems, and web applications — there will be no base from which to start, making it hard to accurately define scope and risk within the environment.

You should identify asset owners in order to define the criticality of the asset to the business. This often requires insight and cooperation with multiple internal business units and stakeholders to understand function and context. From here, you can identify criticality, scanning cadence, and whether you can — or should — apply exceptions to exposures. Understanding where those assets live within the environment is also important. Some of the biggest gripes are slow scans or impacts on network performance, and if you are somehow scanning assets on the wrong side of a firewall, it's no surprise this is happening. Much of the effort for this phase of the program is consultative, often lengthy and continuous throughout the program lifecycle.

Discovery scans are an important element to make sure the view of the environment is accurate and up to date, as well as to identify assets that pose a risk. Unknown and unmanaged assets can create gaping holes through which adversaries can gain access. Authenticated scans will help the business understand vulnerabilities on a device, as well as gain visibility into applications across the environment.

There are opportunities to reduce burden and accelerate the time-to-value through next-generation platforms. These technologies use machine learning and automation to overcome common obstacles when creating and administering a VM program.

2. Remediation and Prioritization

This is probably one of the hardest elements to master in any VM program. In the two years spanning 2019 and 2020, nearly 40,000 vulnerabilities were identified[1]. It's common for organizations to have thousands of internal and external vulnerabilities

[1] National Institute of Standards and Technology (NIST), National Vulnerability Database

which have existed for a long time. The average time to resolve critical application vulnerabilities is often between two and three months. Some vulnerabilities have taken much longer to resolve — if they've been resolved at all. This exposure creates significant risk.

There are an overwhelming number of vulnerabilities for companies to validate and resolve. Just as SOC analysts are often overwhelmed with alerts, vulnerability management administrators frequently get overwhelmed by their workload too. This fatigue can result in missed critical vulnerabilities, exposing organizations to the risk of a breach.

The application of threat intelligence is critical to understanding the real-world risk that vulnerabilities pose to an organization. Prioritization of threats allows administrators to focus on risks which are actively exploited in the wild by threat actors. This approach vastly reduces the burden on administrators and focuses attention on what can provide an intrinsic reduction of risk to the business. A key element to the application of threat intelligence is the laborious tasks completed earlier in your program development: asset identification and classification.

Each environment is unique, and standard feeds and classifications of vulnerabilities are unlikely to completely apply to individual architectures. A complete picture of assets, locations, their classifications, criticalities, and characteristics will help prioritization efforts. Identifying those key assets in an environment can direct remediation efforts to address the most critical vulnerabilities first.

A point of emphasis: Platforms and technology can help assist prioritization. But you should assess vulnerabilities in the context of where the asset resides in your environment, its criticality, and in accordance with external intelligence. Otherwise properly assessing the true risk a vulnerability poses will require much more work.

3. Executive Sponsorship

There is another important element to a successful vulnerability management program: Support from the top. Without executive sponsorship and buy-in from key stakeholders, an organization's program will struggle.

Key stakeholders within business units need to be identified. They often come from leaders in endpoint, network, server infrastructure, and software development. Communication and buy-in from these leaders will underpin the program to ensure timely and effective remediation of vulnerabilities, as well as helping provide support and tackle reporting issues.

Remediation planning is a critical element. The planning of remediation efforts should be closely linked with the prioritization of vulnerabilities and the management platform, which provides a closed loop process for tracking and reporting purposes.

Vulnerability management can't be an isolated effort. Engagement from all business units is necessary, and communication and participation from across the organization is critical. Those key parties will include not just various IT business units, but other departments such as legal, HR, and executive leadership. If there is a breach, those groups will need to understand the root cause and whether it could have been prevented – a concern of particular importance for organizations with cyber insurance.

4. Program Evolution and Maturity

Resources are critical. Understanding resource constraints will help define the maturity level an organization can achieve. Security budgets are often tight, and this can limit the ability to build a gold-standard vulnerability management program.

Overreach will strain the program and impact results. Set realistic expectations so the program can pursue achievable goals. A top-down approach can help bring available resources into the VM team, and allow all stakeholders to share the program's responsibility and success. Whether it's a shared requirement or the VM team's responsibility, resources need to orchestrate and validate the program and outcomes. That validation step will ensure — from a technical perspective — that risks are addressed (mitigated, transferred, or accepted) and, from a governance perspective, results are measured, reported, and effectively communicated across the business.

Understanding how to measure success helps you assess whether your strategy has reduced security risk for the business, and helps you communicate this to leadership and stakeholders. Vulnerability management is not measured by numbers.

Effective communication is essential. Ensure all relevant information is passed to key stakeholders and included in executive-level reporting. Most executives don't want to see a list of vulnerabilities and their associated patches – those will be for your technical stakeholders. High-level charts demonstrating a reduction over time are more likely to resonate with leadership.

Reducing

40,000

vulnerabilities to

20,000

won't necessarily reduce risk if high-risk vulnerabilities aren't addressed.

Keys to Success: In Conclusion

Without a clear strategy and buy-in from leadership, your vulnerability management program is likely to struggle. The initial planning, design, and build phases of your program are often the most critical, as they provide a solid base for investment across the business. This will help the team discover and assess all assets. Without this, you'll never know true risk, and the desired outcome of measurable risk reduction will be compromised.

Applied threat intelligence is also essential to understanding risk and prioritizing remediation efforts. Threat intelligence allows focus on vulnerabilities that are most impactful to the business and pose the greatest risk. Initial visibility into the risk to an organization will ultimately inform reporting and governance, empowering a team to reduce risk rather than the numbers of vulnerabilities, and provide measurable value to the business, underpinning initiatives throughout.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp