Secureworks®
a SOPHOS company

WHITE PAPER

The Imperative Integration of Threat Detection and Response with Vulnerability Management

The threat landscape is constantly evolving and growing in complexity, with threat actors seizing each new opportunity.

Organizations face the daunting challenge of protecting themselves against the myriad of new vulnerabilities that can be exploited by attackers.

These cybercriminals make wide use of scan-and-exploit attacks where they scan networks, systems, and applications to identify vulnerabilities to exploit and then commence their attacks. In fact, vulnerabilities and stolen credentials are the largest initial access vectors used by threat actors, accounting for 72 percent of ransomware attacks.[1]

Regular and timely vulnerability patching remains as important as ever in preventing bad actors from compromising networks. But vulnerability management presents an array of challenges for organizations. As cyber threats grow in sophistication, organizations must fortify their defenses with a comprehensive security program that integrates vulnerability management with threat detection and response.

What is Vulnerability Management?

Since the first computer shipped, vulnerabilities have been an inherent problem. Vulnerabilities are flaws within technology that allow threat actors to gain unauthorized access to an organization's data and devices, or to perform unauthorized actions. Vulnerability management as a formalized IT discipline emerged in the late 1990s and early 2000s, coinciding with the rapid expansion of the internet and the increasing complexity of IT systems. As organizations began to connect their networks to the internet, the exposure to external threats grew, leading to a greater awareness of the need to identify and mitigate security vulnerabilities.

Today, vulnerability management is vital to cybersecurity strategies, with ongoing efforts to develop more proactive and predictive approaches to dealing with vulnerabilities before they can be exploited by malicious actors.

The role of the vulnerability management team is to identify, assess, and prioritize vulnerabilities within an organization's IT infrastructure. By keeping an inventory of assets and continuously scanning for weaknesses, this team acts as the first line of defense, aiming to proactively patch any security holes before they can be exploited. But with the proliferation of vulnerabilities, IT and security teams have struggled to manage, prioritize, and mitigate them.

40,000 vulnerabilities published by the National Vulnerability Database in 2024 alone[2]

The Challenges of Managing Vulnerabilities

The increasing adoption of cloud services and remote work has expanded the attack surface, further complicating the task of securing enterprise environments. The National Vulnerability Database published 40,000 new vulnerabilities in 2024 alone.[2] Given the sheer volume of vulnerabilities, it's nearly impossible for security teams to patch them all. Plus, effective prioritization has long been a challenge. Mean Time to Remediate (MTTR) critical severity vulnerabilities is 65 days, and industry reports estimate that adversaries are now able to exploit a vulnerability within 15 days (on average) of discovery.[3] This discrepancy between the time to remediate and the time to exploit highlights a critical gap in cybersecurity defenses. It's clear that organizations need to reduce the window of opportunity for threat actors. ***But how?***

Mean Time to Remediate (MTTR) critical severity vulnerabilities is **65 days**

The Traditional Approach to Vulnerability Management

Security teams have historically tried to combat vulnerabilities by investing in point solutions. Typically, these solutions focus on known vulnerabilities that can be discovered through automated scanning tools and databases like the Common Vulnerabilities and Exposures (CVE) system, which allows organizations to systematically identify, classify, prioritize, and remediate vulnerabilities. However, these systems tend to have a one-size fits all approach to vulnerability prioritization, overlooking the unique context of an organization's environment. This problem is compounded by the fact that many organizations struggle to hire, train, and retain security staff, and the combination of gaps in visibility and missing context only increases the burden on limited security resources.

adversaries are now able to exploit a vulnerability within **15 days** (on average) of discovery[3]

Many organizations utilize CVSS (Common Vulnerability Scoring System), a framework for rating the severity of security vulnerabilities. This helps security teams identify and patch the most critical vulnerabilities first and prevents the

overwhelming scenario where teams are inundated with a high volume of vulnerabilities without a clear understanding of which ones pose the greatest risk to their operations. Given that security teams cannot feasibly remediate every single detected vulnerability, it is essential to have automated systems in place that can accurately prioritize vulnerabilities based on risk using context from the environment. This approach uses hypothetical risk scores and threat intelligence about what's being exploited in the wild, but it's missing a key piece of information: the vulnerabilities that are actively exploited in the environment and creating alerts for security analysts to manage.

Unifying Vulnerability Management and Threat Detection

On the more reactive side of a security program, the Security Operations Center (SOC) is responsible for monitoring, detecting, and responding to security incidents. SOC analysts have immediate insights into the nature of attacks, the tactics used by adversaries, and, potentially, the vulnerabilities being exploited. This real-time information is invaluable for understanding the threat landscape and responding to incidents as they occur. The problem is that the SOC and the vulnerability management team often don't have insight into what the other is seeing. These functions tend to operate in silos, creating a disjointed and inefficient response to threats. Without real-time threat context from the environment, the efforts of the vulnerability management team can be akin to shooting in the dark.

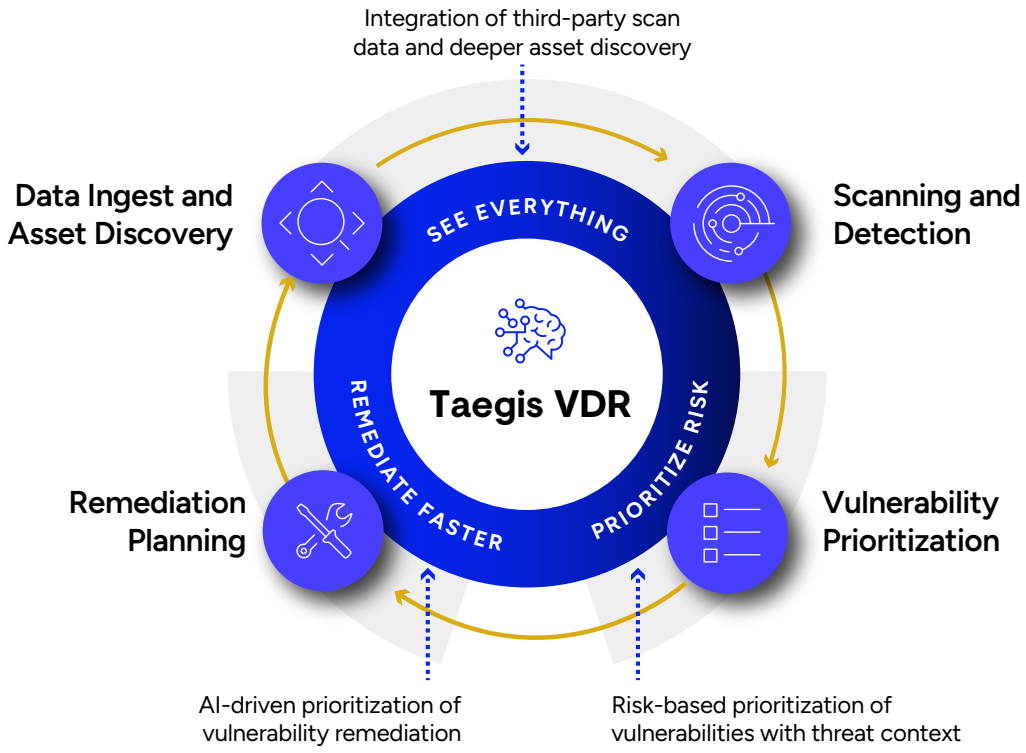
But, when these functions do work in tandem, the strengths of each side are amplified. When both sides have insight into what the other is seeing, they gain a comprehensive view of the threat and vulnerability landscape, leading to better defensive strategies, more effective countermeasures, and expedited response.

> **When the next Log4j inevitably occurs, security operations and vulnerability management teams need to be in lockstep"**
>
> Forrester Research,
> How to Improve Collaboration Between VRM and the SOC, May 2023

This collaboration enables a response that is swift and coordinated when a vulnerability is exploited, minimizing the potential damage. It also allows the vulnerability management team to prioritize vulnerabilities based on real exploitability and impact to the environment, rather than relying solely on hypothetical risk assessments. Vulnerability data also provides insights into the potential entry points and methods used by attackers, aiding in root cause analysis. Plus, security teams can ensure they are allocating resources to the most important actions in the context of their overall risk posture. Typically, when these teams do work together, it often requires manual effort: manually sharing documentation and findings, manually stitching data to identify root cause, etc. Fortunately, Secureworks provides a more innovative approach that automates these workflows.

Secureworks Innovative Approach

Secureworks improves the speed and consistency of vulnerability management with automation, enhanced prioritization, and accelerated remediation. Secureworks customers can combine threat detection and response with vulnerability management to further improve security posture, prevent attackers from exploiting known vulnerabilities, and expedite response times.



Secureworks Taegis™ VDR is a risk-based vulnerability management platform that prioritizes the most critical vulnerabilities informed by context from the environment and continuously updated threat intelligence from the Secureworks Counter Threat Unit™. Customers can achieve a 352% return on their investment with Taegis VDR
via cost savings, risk reduction and productivity gains.[4] Taegis VDR leverages automation and intelligent machine learning algorithms to prioritize vulnerabilities using over 40 internal and external risk factors. The solution provides a prioritized list of assets to patch and remediate that includes the reasoning behind the ratings with remediation planning and tracking.

Additionally, vulnerability data from Taegis VDR is automatically added to threat detection and response workflows in the Secureworks extended detection and response platform, Taegis XDR. By combining these solutions, organizations can uncover vulnerabilities associated with security investigations to pinpoint the systems that are being targeted and prioritize them for remediation. Taegis XDR shows vulnerabilities on alerted-on endpoints, providing context during investigations to help organizations take proactive measures to defend against attacks. When an alert corresponds to a specific vulnerability or is related to a potential attack exploiting a known vulnerability, it is flagged at the top of the list. Taegis XDR also highlights new vulnerabilities by severity, identifies vulnerabilities that are associated with a tenant's most alerted-on endpoints, and shows the vulnerability status of each endpoint. This approach offers insights into attackers' entry points and methods, helps with root cause analysis, and enhances security teams' responses.

Customers can integrate their current third-party vulnerability scanner to improve visibility and enhance the richness of available vulnerability context or leverage the Taegis Vulnerability Scanner with Taegis VDR. The Taegis scanner is a lightweight, network-based scanner that automatically discovers assets throughout the environment. Whether you use the Taegis Vulnerability Scanner or a third-party scanner, your vulnerability data can be prioritized in Taegis VDR and integrated into threat detection and response workflows in Taegis XDR.

352%
return on investment with Taegis VDR

$250k
value of breaches avoided

$70k
reduction in people costs

$519k
total savings over three years

<6 months
payback period

Stronger Defenses Against Threats Now and in the Future

It's safe to assume attack surfaces will continue to grow, vulnerabilities will increase, and threat actors will work to shrink their time to exploit. Ensuring your SOC and vulnerability management teams can work together efficiently will become a critical part of raising your cybersecurity posture to defend against threats now and in the future. By combining the power of Taegis VDR and XDR, you can take a proactive stance to thwarting attackers and building a cohesive security team that is stronger than the sum of its parts.

NEXT STEPS

Want to see how Taegis VDR and Taegis XDR work together?

Request a demo to see how Taegis VDR delivers impact throughout the threat detection and response process.

Sources:

1. 2024 State of the Threat Report: A Year in Review, October 2024
2. National Vulnerability Database (NVD)
3. Edgescan: 2023 Vulnerability Statistics Report, October 2023
4. Forrester Total Economic Impact™ of Secureworks Taegis VDR, April 2023

Secureworks®
a SOPHOS company

Secureworks is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of thousands of organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.