Secureworks®
a SOPHOS company

DATA SHEET

Secureworks Taegis VDR FAQ

Frequently Asked Questions

How Does Secureworks Leverage Real Threat Data from My Environment to Inform Vulnerability Management?

Secureworks® integrates our extended detection and response (XDR) and vulnerability management platforms to help organizations gain a comprehensive view of their threat and vulnerability landscape, leading to better defensive strategies, more effective countermeasures, and expedited response. In Taegis™ XDR, security analysts can view vulnerabilities associated with alerted-on endpoints, providing context during investigations to help analysts 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.

Visibility between Secureworks Taegis XDR and Taegis VDR platforms enables a response that is swift and coordinated when a vulnerability is exploited, minimizing the potential damage. This collaboration also enables the vulnerability management team to prioritize vulnerabilities based on real exploitability and potential impact to their 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.

“The integration of vulnerability management and security operations is not just a matter of convenience; it is a strategic imperative. Secureworks’ latest innovation bridges the gap between these functions, bringing vulnerability context and threat detection and response together to reduce risk." – Dave Gruber, Principal Analyst with Enterprise Strategy Group

What is Secureworks Process for Prioritizing Vulnerabilities?

Secureworks Taegis VDR provides a risk-based approach to vulnerability management, prioritizing the most critical vulnerabilities informed by context from the environment and continuously updated threat intelligence. Taegis VDR creates a prioritized list of assets to patch and remediate, including the reasoning behind the ratings. Our Contextual Prioritization Engine uses automation and intelligent machine learning algorithms to prioritize critical vulnerabilities informed by over 40 internal and external risk factors. Those factors fall into five categories:

1. The characteristics of the vulnerability itself
2. The asset on which the vulnerability resides
3. The network environment where the asset is located
4. How the asset relates to the organization and its priorities (asset criticality)
5. The ever-evolving external threat environment

"We know we are materially improving the risk profile of small to medium-sized businesses by leveraging Secureworks Taegis VDR." – Jeff Kramer, Executive Vice President, Digital Transformation and Cybersecurity Advisory Services, Aprio

©2024 Secureworks, Inc. All rights reserved. Availability varies by region.

Secureworks leverages common vulnerability scoring system (CVSS) scores and these factors to automatically prioritize vulnerabilities based on the risk profile of the unique organization. Once the vulnerabilities are prioritized in Taegis VDR, they can be automatically added to threat detection and response workflows in Taegis XDR.

Does Taegis VDR Include Scanning Capabilities?

The Taegis Vulnerability Scanner is an optional add-on to Taegis VDR. The Taegis Vulnerability Scanner is a lightweight, network-based scanner that automatically discovers all your assets daily within specified IP ranges. During the network scanning process, Taegis runs a variety of detection types on network assets to discover and determine risk. These fall into four categories:

- Outdated or EOL software with known vulnerabilities
- Default credentials or passwords
- Web application vulnerabilities
- Misconfigurations (cryptographic, server, or network-layer protocol)

Once assets are identified, organizations can automatically schedule reoccurring scans over specific cadences for any discovered assets within the network. The scanner is designed to be easy to set up and configure.

Can Taegis VDR Integrate with Third-Party Vulnerability Scanners?

Yes, Taegis VDR integrates with third-party vulnerability scanners to maximize flexibility and existing investments. Ingesting data from additional third-party vulnerability scanners further improves visibility and enhances the richness of available vulnerability context. Today, organizations can integrate Qualys, Tenable, or Microsoft Defender for Endpoint, with more integrations planned. Vulnerability data from third-party scanners is prioritized in Taegis VDR and then can be automatically sent to Taegis XDR and embedded into detection and response workflows.

What is the Relationship Between Secureworks Prioritization Engine and the CVSS Score?

The CVSS score is limited by a lack of available up-to-date context specific to a unique organization. The CVSS base score is constant for a given vulnerability, without considering the network the vulnerability is on, or more importantly, the specific location on the network, the asset, and other important context. While there are allowances in CVSS v3.x for additional metrics, these factors must be known, maintained, and applied to the system and vulnerability combination. Without this information, for example, a locally exploitable vulnerability with a CVSS score of 3 or 4 on the same machine as three web applications is likely a higher risk. The hyper-fluid nature of enterprise networks and the external threat environment makes a static score unreliable.

©2024 Secureworks, Inc. All rights reserved. Availability varies by region.

Secureworks Contextual Prioritization begins with the CVSS base score, and then applies an additional 40+ factors (as discussed above) to determine the risk of each vulnerability. Secureworks does this every five minutes, recognizing that the risk changes as the environment does.

How Does Taegis VDR Leverage AI/ML?

Taegis VDR uses machine learning (ML), artificial intelligence (AI), and automation to continuously enhance the effectiveness of the solution and up-level security resources. Taegis VDR automates tasks that security personnel would typically perform manually, freeing up those resources to focus on other, more important work. Given that security teams cannot feasibly remediate every single detected vulnerability, AI and automation can accurately prioritize vulnerabilities based on risk using context from the organization's environment. The platform automatically gathers context, which helps to not only find the security issue, but also understand the causes and implications of the issue. The solution also integrates threat intelligence for better context and prioritization. Prioritization is key to establishing a robust and secure vulnerability management process. By integrating AI, ML, and automation into Taegis, Secureworks helps drive greater efficiency and accuracy for our customers.

Secureworks commissioned Forrester Consulting to conduct a Total Economic Impact (TEI) study and examine the potential return on investment (ROI) of Taegis VDR. The study found a potential ROI of 352% over three years for Taegis VDR customers.

How Does Taegis VDR Help Customers Build Effective Remediation Plans?

Secureworks prioritizes remediation recommendations by first automatically grouping CVEs in a remediation-centric display of information. Secureworks provides a numbered list of remediation activities that will optimize risk reduction based on our 40+ factor prioritization engine. Depending on the type of vulnerability, specific remediation recommendations are presented for discovered vulnerabilities. These can be recommended patches or software upgrades, configuration changes, or other types of compensating controls unique to the type of vulnerability.

Taegis VDR also includes a remediation scenario function that allows users to build remediation plans, and then understand how each plan would improve the organization's vulnerability health if implemented. Secureworks customers can therefore build multiple remediation plans and assess how effective each plan is before committing resources. Detailed remediation information is included with the prioritized recommendations so that the risks and remediation actions can be easily understood and implemented by the teams responsible for remediation.

"Secureworks provides justification for taking remediation actions, including showing what the possible impact would be if we don't fix an issue. It saves us time on getting the information that you need to decide what to do." – Security Analyst, Manufacturing and Retail

How is the Secureworks Solution Delivered and Priced?

Secureworks Taegis VDR is a SaaS solution that can be purchased standalone or combined with Taegis XDR to further reduce organizational risk. Customers have the option to purchase the Taegis Vulnerability Scanner or integrate their existing third-party solution to scan their environment, including Qualys, Tenable, and Microsoft Defender for Endpoint. Taegis VDR is priced by number of assets. Secureworks also offers Professional Services for customers who need additional assistance. For more information on pricing, contact Secureworks to talk with an expert.

©2024 Secureworks, Inc. All rights reserved. Availability varies by region.

How Does Secureworks Account for the Discovery of New Vulnerabilities?

Secureworks provides continuous updates to our vulnerability database, releasing new signatures up to multiple times per day when new vulnerabilities are published. The Taegis Vulnerability Scanner runs on an ongoing basis, meaning that all assets are scanned for new vulnerabilities. When a new vulnerability is discovered, relevant scans are automatically triggered, all without the need for manual intervention.

What Customization Options are Available Within the Solution?

Taegis VDR offers advanced search capabilities that enable users to use our search syntax to perform complex and specific queries of their vulnerabilities and assets. In addition, these searches can be saved, and users can schedule the application and export of these searches within the UI or delivered via email. Taegis VDR also integrates with PowerBI to give users a variety of reporting options.

"The reduction in labor necessary to deploy and run the product is significant…Taegis VDR consistently found services and vulnerabilities other products did not, simply because it never stops looking." – Security Weekly Labs

Next Steps

Want to see how VDR works?

Request a demo to see how VDR delivers impact throughout the vulnerability management process.

LEARN MORE ABOUT VDR

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.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com

©2024 Secureworks, Inc. All rights reserved. Availability varies by region.