Security Weekly | LABS
A CyberRisk Alliance Resource

Security Weekly Labs | Taegis

VDR Review

Produced by Security Weekly Labs, a Security Weekly Resource

CyberRisk ALLIANCE

Security Weekly | LABS A CyberRisk Alliance Resource

SC MEDIA

About

Contents

This review is part of the September 2021 assessment of network vulnerability scanners. If you haven't read the category overview, you might want to check it out — it explains the category's basics, use cases and the general value proposition. Our testing methodology explains both how we interact with vendors and how we tested these products.

Vulnerability scanners are the sensors of the vulnerability management process — they reach out and touch systems to determine if they are vulnerable to exploits and other threats. While there are vulnerability scanners for containers, infrastructure-as-code tooling, cloud management consoles, and web applications, this group review will focus on network vulnerability scanners.

Company background

Montreal-based Delve Labs (aka Delve Laboratories, aka Delve Security) was founded in 2014 by a group of ambitious engineers with the goal of making vulnerability management less labor intensive. Leveraging AI, the company was able to automate operational steps, manual scan configuration, and vulnerability validation steps. The result was the first new commercial vulnerability scanner the industry had seen in over a decade, designed with the benefit of hindsight.

The company was acquired by Secureworks in the fall of 2020. Secureworks plans to integrate it with its own internally developed Red Cloak XDR platform. Red Cloak was rebranded as *Taegis XDR*, and the Delve Labs Warden product was rebranded as *Taegis VDR*.

Security Weekly Labs |Taegis VDR Review

Review summary

What folks expect to find in a vulnerability scanner is going to color their impressions of Secureworks' Taegis VDR product. People used to running checks against CIS Benchmarks, generating reports for management, or depend on agents may find this product too austere for their needs. Others, fed up with hundreds of configuration options, cluttered UIs, feature bloat, and a general lack of focus on the core of what really matters in vulnerability management (like us, to be honest) will find this product refreshing.

Ultimately, we think it will create a hard line between those who can use it and those who can't. There might be people in the former category who love what Secureworks is doing here, but just can't live without some of the traditional features that have been standard with the "Big 3" of this space. Regardless, there is innovation here in the true, undiluted, sense of the word. We hope Taegis VDR represents where labor-intensive cybersecurity products in general are headed. This product is proof that there's a lot more room for automation and workflow improvement in cybersecurity.

Target market: Taegis VDR's sweet spot seems to be organizations who may not have the resources or the expertise to identify vulnerabilities on their own. This tends to be mid-sized enterprises who do not have large security operation centers.

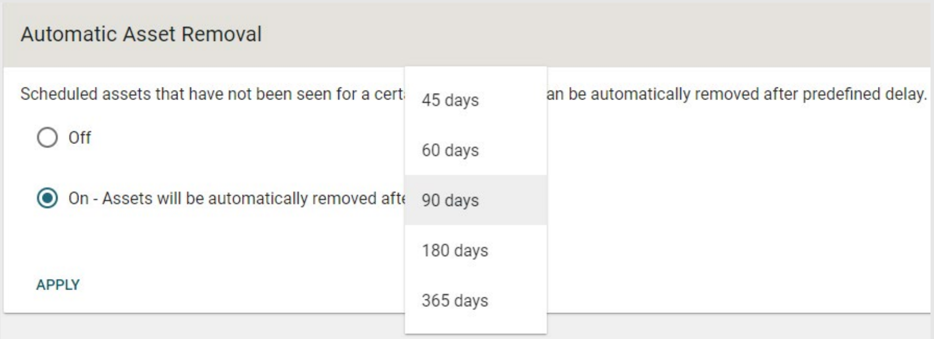
Time-to-value: We're defining value in the vulnerability scanner segment as the moment a scan successfully completes and returns with results on the requested hosts or network ranges.

Time to value will depend heavily on how many scanning sensors need to be deployed and where they need to be deployed (this is discussed in more detail in the Overview document under Scanner Architecture). For this review, our hypothetical small enterprise has 1000 employees, 2000 assets, and a few segmented networks. We should be able to get away with three scanning appliances. Three VMs at a conservative 4GB RAM, 4 vCPUs, 50GB disk each (based on hardware recommendations) might cost $750 a year to run, per instance, for a total of $2,250.

Including time for planning meetings (e.g., a one-hour meeting with four people in it is four hours of labor), we're estimating the effort at around 20 hours of combined effort to get Secureworks Taegis VDR deployed in this size environment. Note that there's a tradeoff here, as competing products offer agents as an alternative to running credentialed scans, which will take additional labor to deploy. Time is saved with Taegis VDR, though without the ability to collect vulnerability data from fully remote systems that can't be reached with network scans or credentialed network scans.

Getting Taegis VDR deployed in an environment of this size in a week seems reasonable (barring delays in getting access to vSphere/ESXi resources to deploy the scanners; we know how that goes).

Maintaining value: While other scanners require some additional elbow grease to ensure scans are scheduled correctly and that monitoring and alerts are set up if scans aren't running, Taegis VDR is happy to figure out the scheduling work. All we needed to do was to feed it a list of IPs and ranges — it handled the rest of the maintenance. There is even an option to automatically remove assets that haven't been seen for a set number of days.



Automatic Asset Removal

Scheduled assets that have not been seen for a cert an be automatically removed after predefined delay.

○ Off

● On - Assets will be automatically removed afte

This isn't to say there won't be any maintenance to do. Perhaps metrics need to be collected for regular reports to management. Or someone changed the credentials used by the scanner, so they have to be updated. Also, there's the regular vulnerability analysis and validation work do be done, though the additional prioritization work done by Taegis VDR should reduce this workload. The ability to mark vulnerabilities as false positives, "snooze" them, verify them in the interface will help with workflow, especially if multiple analysts are working in the same console.

Total cost: Three general categories are considered when calculating total cost: labor cost, product cost, and infrastructure costs. There are a lot of assumptions in here, even within the parameters we've set, so feel free to play with the numbers to make these reflect your environment.

- Product cost: Secureworks didn't provide pricing directly, but pricing we found online is $15.99 per asset per year for our hypothetical small enterprise with around 2,000 assets. That makes the total product cost $31,980 per year.
- Deployment cost (labor): Junior-level folks should be able to deploy these virtual appliances, get them up and running, and add hosts for auto discovery. As mentioned in the time-to-value section, we're estimating 20 hours of labor to get things up and running, which comes out to $673 for junior folks (check out the methodology document for more details on our salary estimates).
- Deployment cost (infrastructure): we've estimated $2,250 for resources to run three virtual appliances, though we know in many cases, the security team will be able to benefit from sunk costs on existing virtual infrastructure.
- Maintaining value (labor): this breaks down into a few categories
  - Maintenance of the scan engine (e.g., tweaking scan configurations) and the underlying OS: none — the virtual appliance maintains itself — we save some labor here. $0.00.
  - The work of building and distributing reports and metrics will vary widely depending on the organization, but we'll say a middle-of-the-road estimate would come to two hours per week, for a total of $3,499.60 per year. Noteworthy here is that Taegis VDR doesn't really have any reporting functionality to speak of (at least, not in terms of custom report building and exporting executive summaries to PDFs, that kind of traditional reporting), so reporting work may be a bit more manual for some folks.
  - As mentioned elsewhere in this report, Taegis VDR does considerably more work than most when it comes to prioritizing vulnerabilities, validating them, and correlating with threat intelligence. These efforts should save analysts considerable time over competitors' products, to the tune of 40% time savings, by our estimates. For our hypothetical organization, we're estimating 48 hours of work in the first month, split 50/50 between senior and junior security staff. After the first month, we estimate 12 hours per month, with the senior/junior workload split going to 25/75, respectively. The total labor spend comes to $7,975.62 per year.
  - Finally, tracking down unknown assets and their owners can also eat a lot of time and has

a similar workload curve that's heavy on the front, but tapers off to a constant value over time. Assuming a split between senior and junior staff that mirrors the previous estimate, we can easily see 40 hours spent on this in the first month and 10 hours per month following. The total comes to $6,646.36.

All told, we estimate running Secureworks Taegis VDR in our hypothetical 2,000-asset enterprise would run around $53,024.57 per year.

Strengths: The reduction in labor necessary to deploy and run the product is significant. While we didn't do a direct performance comparison, Taegis VDR consistently found services and vulnerabilities other products did not, simply because it never stops looking. Much deeper website scanning than competing products offer, for the same price. Vulnerability prioritization models on par with what we see from specialized vendors, not the mainstream scanning vendors.

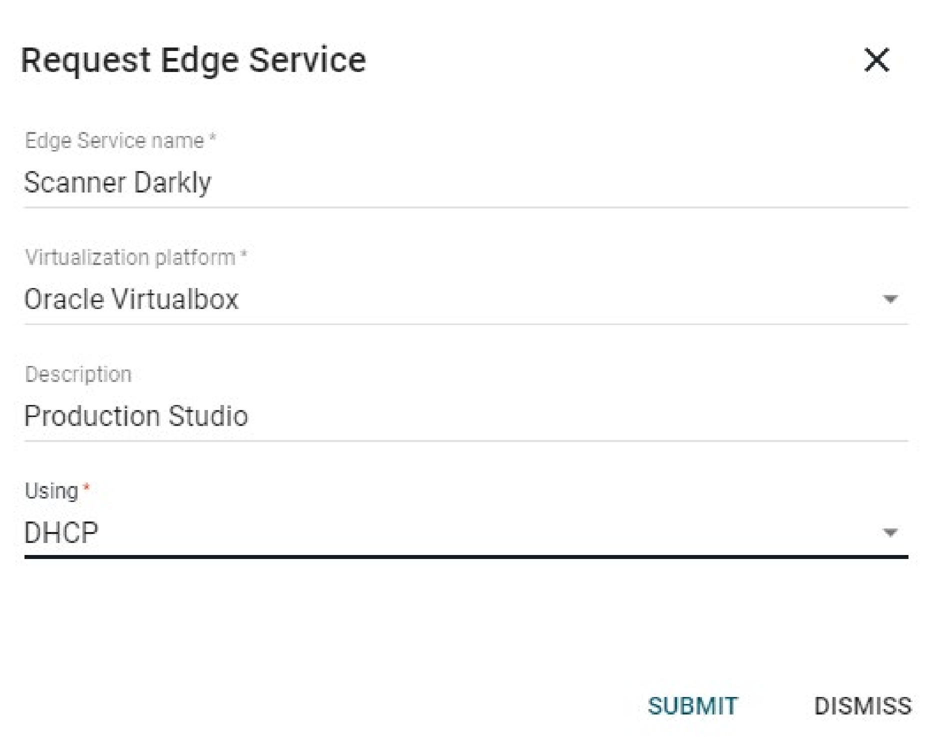
Weaknesses: Assets and remediation plans can't be assigned to individuals, and dynamic asset groups don't exist, though the teams functionality makes it possible to divide up assets and remediation at a group (team) level. Small number of integrations when compared to the competition.

Conclusion: A novel and unique approach to removing much of the manual, mindless work associated with vulnerability management. The bold approach pays off and leaves us wondering, "why doesn't everyone do it this way?"

Deployment and configuration

In Secureworks VDR's architecture is like most modern vulnerability scanners: a SaaS console with a virtual appliance that can be deployed internally. A short trip to the settings page and we find the ability to download a generic virtual appliance (that we will later have to configure) or request a fully preconfigured appliance (but could take up to three hours to generate). If you're not in a rush, choose a preconfigured option and an email will let you know when it is ready.

There are a variety of formats to choose from for the pre-configured option: Linux KVM/QEMU, RAW image, Hyper-V, Azure/Legacy VHD, Virtualbox, or ESXi. When we chose the preconfigured option, we were given the option of choosing DHCP or Static network configurations, further saving manual setup work for us. Network addressing can also be changed from the settings page in the future if the appliance ever needs to be moved.



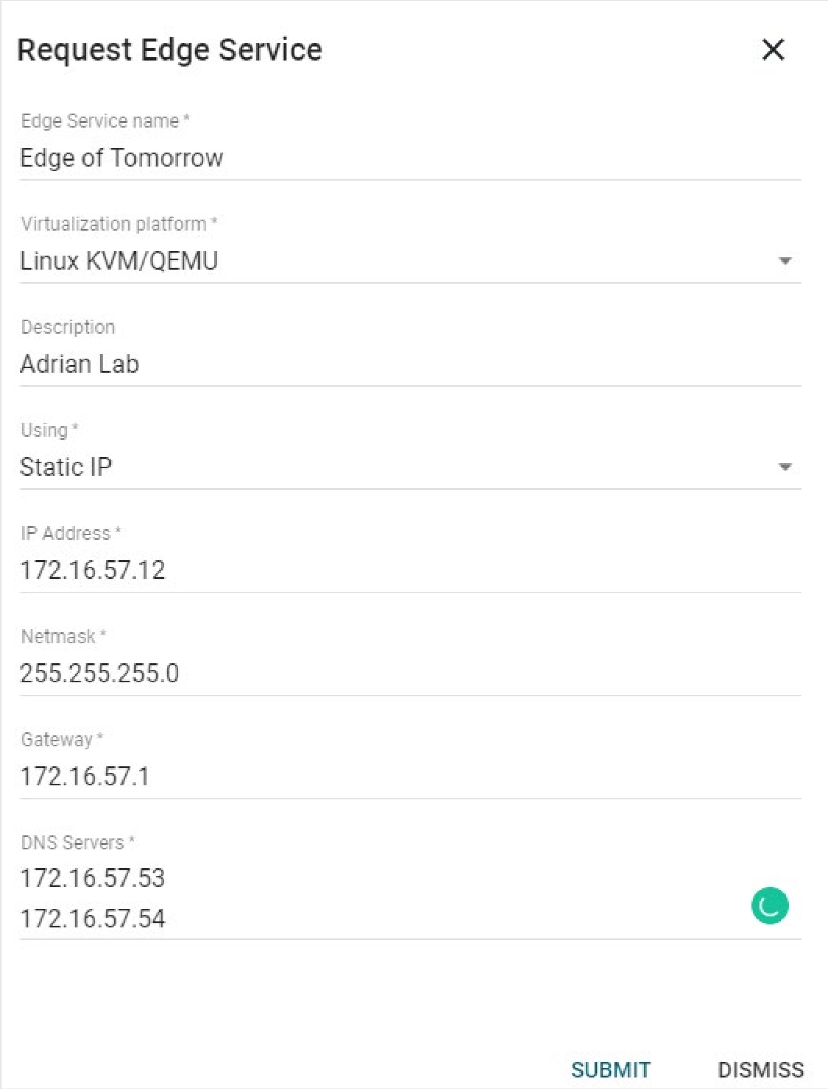
Request Edge Service

Edge Service name *
Scanner Darkly

Virtualization platform *
Oracle Virtualbox

Description
Production Studio

Using *
DHCP



Request Edge Service

Edge Service name *
Edge of Tomorrow

Virtualization platform *
Linux KVM/QEMU

Description
Adrian Lab

Using *
Static IP

IP Address *
172.16.57.12

Netmask *
255.255.255.0

Gateway *
172.16.57.1

DNS Servers *
172.16.57.53
172.16.57.54

Other items that can be created and managed from the settings screen: user accounts, teams, tags, connectors (integrations), automatic asset removal (for inactivity), and credentials (for credentialed scanning). Taegis VDR was designed to be API-first, so all functionality in the web console is available via the API as well (documented here). API access can also be managed on the settings page.

One of Taegis VDR's flagship features is the lack of configuration necessary. On the auto discovery tab, we can simply add IP ranges and choose an edge service (either an internally deployed one, or an external edge service hosted by Secureworks). Taegis VDR then performs some initial scans.

Based on what is found, these scans will probe deeper. If websites are found, web scanning (DAST) techniques are used to crawl web pages and scan for application vulnerabilities. If WordPress is found, Taegis VDR will check for WordPress-specific vulnerabilities.

Eventually, the scanner will check all 65535 TCP and UDP ports on all auto-discovered hosts and crawl all web pages. While this approach would never make sense for a consultant with two days to complete a security assessment, it makes complete sense for a product permanently focused on the same assets, rooted in place, day after day. Why wouldn't we want a scanner to be as thorough as possible? Leave no stone unturned?

With traditional scanners, turning all the options to full, all ports, results in scans less likely to ever finish, more likely to stall, fail, or abort. Once the solution is presented, it seems obvious — don't scan every asset as if you're scanning it for the first time, every time. Instead, spread the scan out over time, building knowledge of the asset piecemeal.

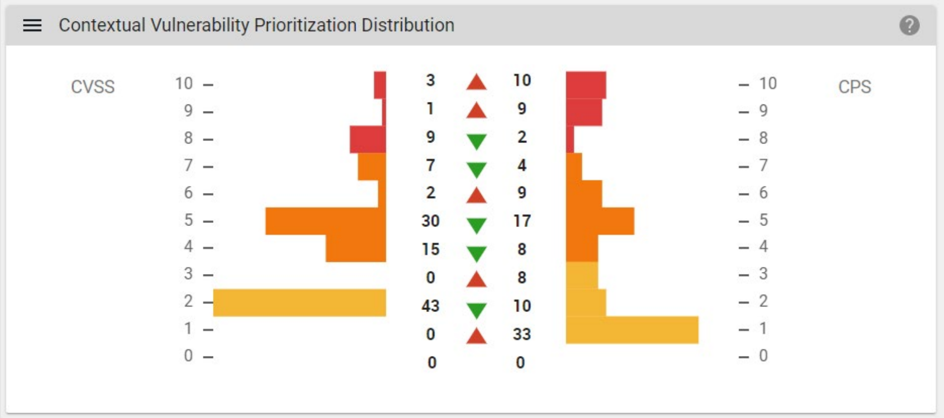
Taegis VDR has a few more tricks designed to save time. The scanner will determine how often to scan an asset, based on the complexity of the asset or how often it changes. Also, Taegis VDR learns when customers mark vulnerabilities as false positives. If a vulnerability has been unanimously voted down as a false positive by customers, the vulnerability is deprioritized. Secureworks continuously monitors findings marked as false-positives and improves or removes detections as necessary.

We once carried the misguided belief that more control and more configuration options made a product more powerful, more valuable. The reality was that we never had time to learn all the options, and the chance that we'd miss an important feature or misconfigure something critical increased with the number of options available. Taegis VDR does have quite a few configuration options, but we never needed to tweak them in our testing. The lack of configuration complexity combined with the knowledge that the product is constantly exploring a bit more, going a bit deeper, gave us a feeling of calm and comfort we didn't find with other vulnerability scanners.

Usage

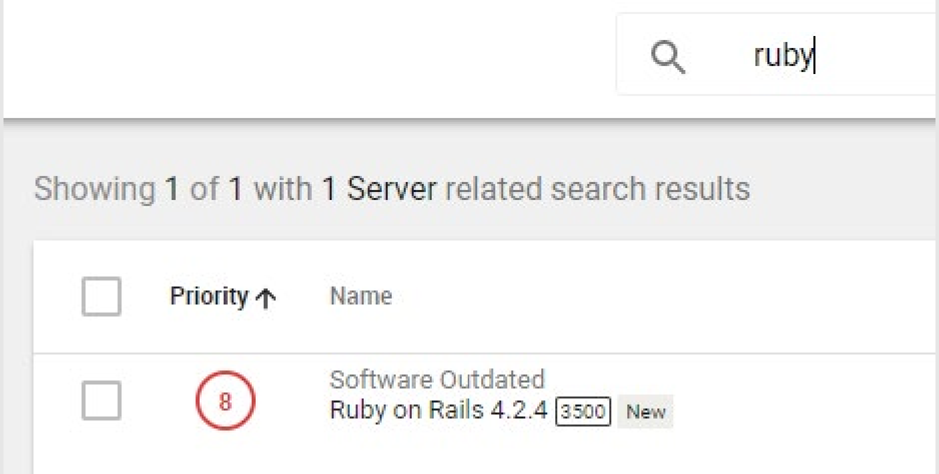
The SaaS console is simply laid out and easy to navigate. Taegis VDR gathers an enormous amount of data but doesn't try to present it all at once. The interface shows the most important data in default views, making it easy to filter and sort through assets and vulnerabilities at a high level. There's a lot more data just under the surface, easily accessible with just a few clicks.

The main dashboard is fine and contains some trending data. An interesting dashboard widget is *Contextual Vulnerability Prioritization Distribution*, which shows how vulnerabilities have been rescored based on context and vulnerability intelligence.



The real action is in the next tab — the Vulnerabilities tab. Occupying most of the screen is a prioritized list of vulnerabilities, in the order Taegis VDR recommends addressing them. Then is the filter on the left-hand side, offering nine different categories of filtering options. We're thrilled to see that exploitability is broken down into different types of exploits — for example, remote code execution (RCE), and denial of service (DOS). This makes a huge difference when analyzing vulnerabilities and not all tools make this distinction. Crashing a service and getting a foothold into an internal corporate network are very different outcomes that need to be distinguished.

Finally, the last major feature of the Vulnerabilities tab is the search bar. There's no complex query language to learn, it's just a freeform text search. Want to check out an asset, but only remember the hostname? That works. Want a list of all the systems running Ruby on Rails and want to see the version number for each? Just type "Ruby on Rails." Searches for custom tags, IP addresses and any other text field associated with assets or vulnerabilities work as expected. A quick, text-based search function is simply the quickest and most familiar way to get answers to questions. It could be argued that more complex query languages are more powerful, but if no one has the time or patience to learn how to use them, it doesn't matter how powerful they could be.



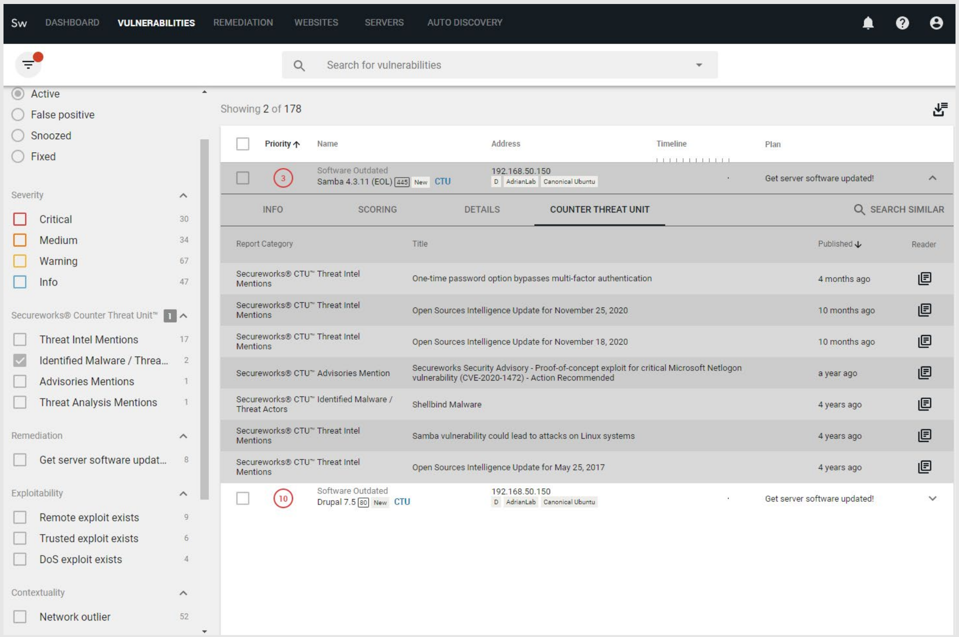
ruby

Showing 1 of 1 with 1 Server related search results

□	Priority ↑	Name
□	8	Software Outdated Ruby on Rails 4.2.4 3500 New

It should also be noted that filters and searches layer. For example, if we searched on Ruby and the results were still too cluttered, we could filter that view to just findings that are critical or tagged as "in production." For anyone that has ever shopped on Amazon or eBay, the interface and controls will be immediately familiar.

Our labs team has used this product extensively in the past, before the Secureworks acquisition. One of the benefits of this acquisition is immediately visible when analyzing individual vulnerabilities: the inclusion of Secureworks Counter Threat Unit (CTU) intelligence. This intelligence even has its own filters (see screenshot). The Identified Malware category especially makes it easy to not only focus on vulnerabilities that are actively being targeted by malware but saves time on researching details on the threats related to these vulnerabilities, since a full CTU report is linked within the console.



Sw DASHBOARD **VULNERABILITIES** REMEDIATION WEBSITES SERVERS AUTO DISCOVERY

Search for vulnerabilities

● Active
○ False positive
○ Snoozed
○ Fixed

Severity

□ Critical	30
□ Medium	34
□ Warning	67
□ Info	47

Secureworks® Counter Threat Unit™ 1

□ Threat Intel Mentions	17
☑ Identified Malware / Threa...	2
□ Advisories Mentions	1
□ Threat Analysis Mentions	1

Remediation

□ Get server software updat...	8

Exploitability

□ Remote exploit exists	9
□ Trusted exploit exists	6
□ DoS exploit exists	4

Contextuality

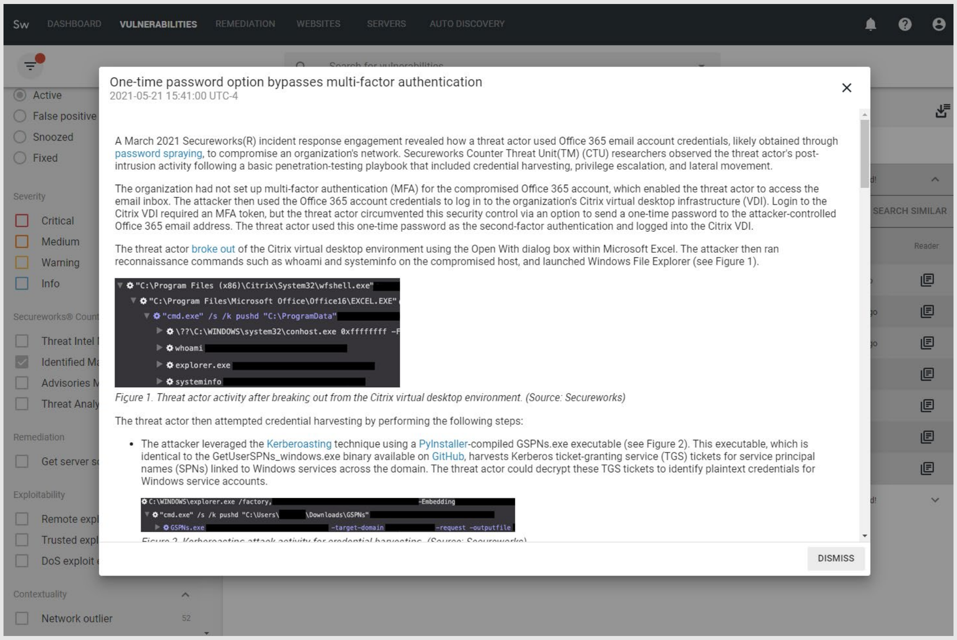
□ Network outlier	52

Showing 2 of 178

Priority ↑	Name	Address	Timeline	Plan
3	Software Outdated Samba 4.3.11 (EOL) 445 New CTU	192.168.50.150 D AdrianLab Canonical Ubuntu		Get server software updated!
10	Software Outdated Drupal 7.5 80 New CTU	192.168.50.150 D AdrianLab Canonical Ubuntu		Get server software updated!

INFO SCORING DETAILS **COUNTER THREAT UNIT** SEARCH SIMILAR

Report Category	Title	Published ↓	Reader
Secureworks® CTU™ Threat Intel Mentions	One-time password option bypasses multi-factor authentication	4 months ago	
Secureworks® CTU™ Threat Intel Mentions	Open Sources Intelligence Update for November 25, 2020	10 months ago	
Secureworks® CTU™ Threat Intel Mentions	Open Sources Intelligence Update for November 18, 2020	10 months ago	
Secureworks® CTU™ Advisories Mention	Secureworks Security Advisory - Proof-of-concept exploit for critical Microsoft Netlogon vulnerability (CVE-2020-1472) - Action Recommended	a year ago	
Secureworks® CTU™ Identified Malware / Threat Actors	Shellbind Malware	4 years ago	
Secureworks® CTU™ Threat Intel Mentions	Samba vulnerability could lead to attacks on Linux systems	4 years ago	
Secureworks® CTU™ Threat Intel Mentions	Open Sources Intelligence Update for May 25, 2017	4 years ago	



Sw DASHBOARD **VULNERABILITIES** REMEDIATION WEBSITES SERVERS AUTO DISCOVERY

One-time password option bypasses multi-factor authentication
2021-05-21 15:41:00 UTC-4

A March 2021 Secureworks(R) incident response engagement revealed how a threat actor used Office 365 email account credentials, likely obtained through password spraying, to compromise an organization's network. Secureworks Counter Threat Unit(TM) (CTU) researchers observed the threat actor's post-intrusion activity following a basic penetration-testing playbook that included credential harvesting, privilege escalation, and lateral movement.

The organization had not set up multi-factor authentication (MFA) for the compromised Office 365 account, which enabled the threat actor to access the email inbox. The attacker then used the Office 365 account credentials to log in to the organization's Citrix virtual desktop infrastructure (VDI). Login to the Citrix VDI required an MFA token, but the threat actor circumvented this security control via an option to send a one-time password to the attacker-controlled Office 365 email address. The threat actor used this one-time password as the second-factor authentication and logged into the Citrix VDI.

The threat actor broke out of the Citrix virtual desktop environment using the Open With dialog box within Microsoft Excel. The attacker then ran reconnaissance commands such as whoami and systeminfo on the compromised host, and launched Windows File Explorer (see Figure 1).

```
▼ ⚙ "C:\Program Files (x86)\Citrix\System32\wfshell.exe" [redacted]
  ▼ ⚙ "C:\Program Files\Microsoft Office\Office16\EXCEL.EXE"
    ▼ ⚙ "cmd.exe" /s /k pushd "C:\ProgramData" [redacted]
      ▶ ⚙ \??\C:\WINDOWS\system32\conhost.exe 0xffffffff -F
      ▶ ⚙ whoami [redacted]
      ▶ ⚙ explorer.exe [redacted]
      ▶ ⚙ systeminfo [redacted]
```

Figure 1. Threat actor activity after breaking out from the Citrix virtual desktop environment. (Source: Secureworks)

The threat actor then attempted credential harvesting by performing the following steps:

- The attacker leveraged the Kerberoasting technique using a PyInstaller-compiled GSPNs.exe executable (see Figure 2). This executable, which is identical to the GetUserSPNs_windows.exe binary available on GitHub, harvests Kerberos ticket-granting service (TGS) tickets for service principal names (SPNs) linked to Windows services across the domain. The threat actor could decrypt these TGS tickets to identify plaintext credentials for Windows service accounts.

```
⚙ C:\WINDOWS\explorer.exe /factory, [redacted] -Embedding [redacted]
  ▼ ⚙ "cmd.exe" /s /k pushd "C:\Users\ [redacted] \Downloads\GSPNs" [redacted]
    ▶ ⚙ GSPNs.exe [redacted] -target-domain [redacted] -request -outputfile
```

Figure 2. Kerberoasting attack activity for credential harvesting. (Source: Secureworks)

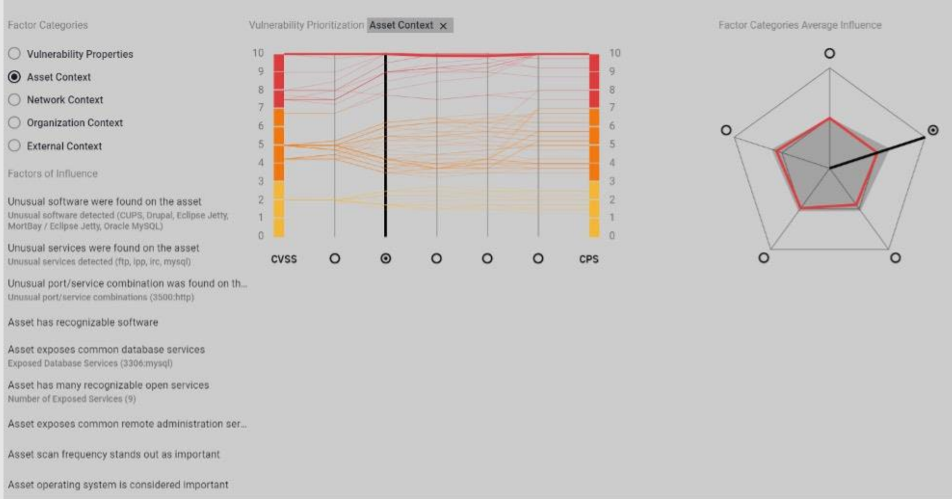
DISMISS

Like many modern vulnerability management offerings, Taegis VDR correlates vulnerabilities with contextual data and threat intelligence. It has been shown by several studies that base CVSS scores alone are not good indicators of risk, so Taegis VDR has its own custom Contextual Prioritization Score (CPS), also based on a 0-10 scale, to better represent the actual risk of each vulnerability.

The CPS is derived from into five categories, with over 40 factors measured across them:

1. **Vulnerability properties:** Many of these factors have to do with the level of confidence in how the vulnerability was detected or could be exploited. Some vulnerability checks must do some guessing, while others are based on easily checkable binary states. Taegis VDR can reprioritize based on these factors.
2. **Asset context:** Much can be learned by paying attention to how an asset is handled. Are manual scans run more often on some hosts than others? Was it manually tagged with a higher importance value? Is it tagged as part of a more critical group (e.g., PCI DMZ)? Do special scheduling windows prevent it from being scanned at certain times? The value of an asset can be inferred from the answers to these questions.
3. **Network context:** Much like how penetration testers and attackers look at assets on networks, looking for patterns that can lead to "low-hanging fruit." Maybe an asset has three times more open services than the average. Maybe it is the only host on the network running a legacy or exotic service or protocol. Maybe it doesn't match the naming convention everything else has. An open-source project that demonstrates this concept can be found here, on GitHub.
4. **Organization context:** Like how Asset Context above infers priority from actions taken relative to certain assets, analyst actions in the Taegis VDR console are also recorded and analyzed. By analyzing how the UI is used, the system can infer which assets seem to be a higher priority to the customer. This category also includes factors like considering how often a detection method used has resulted in a vulnerability being marked as a false positive. Secureworks can also estimate what a normal timeframe to remediate a particular vulnerability should be, across all their customers. If one customer finds themselves outside that window, the CPS can be increased.
5. **External context:** This one is largely self-explanatory. If reliable exploits are available, or folks on threat intel feeds or in certain forums are excitedly talking about a particular vulnerability, the CPS is adjusted accordingly.

The console UI does a great job of detailing the factors within each of these five categories that have contributed to the CPS, for those interested in why the score is what it is. This can be quite practical for analysts looking to spot trends. For example, if contextual details are consistently boosting low CVSS scores to very high CPS, there could be a common reason that this breakdown could make clear.



Factor Categories

○ Vulnerability Properties

● Asset Context

○ Network Context

○ Organization Context

○ External Context

Factors of Influence

Unusual software were found on the asset
Unusual software detected (CUPS, Drupal, Eclipse Jetty, MortBay / Eclipse Jetty, Oracle MySQL)

Unusual services were found on the asset
Unusual services detected (ftp, ipp, irc, mysql)

Unusual port/service combination was found on th...
Unusual port/service combinations (3500:http)

Asset has recognizable software

Asset exposes common database services
Exposed Database Services (3306:mysql)

Asset has many recognizable open services
Number of Exposed Services (9)

Asset exposes common remote administration ser...

Asset scan frequency stands out as important

Asset operating system is considered important

Vulnerability Prioritization
Asset Context ×
10
9
8
7
6
5
4
3
2
1
0
CVSS
CPS
Factor Categories Average Influence

The Websites and Servers tabs are really a different view for the same information on the Vulnerabilities tab but grouped by distinct websites or assets. The final tab, Remediation, allowed us to create and track a project focused on specific vulnerabilities. It shows some basic statistics about the vulnerabilities and gives status on completion. A deadline can also be set. If plans are set, they will also show up in a dedicated column under the Vulnerabilities tab.

Notable integrations

- ServiceNow – synchronizes remediation plans with ServiceNow ITSM
- Qualys – collect inventory and vulnerabilities
- AWS Inspector – collect asset information and vulnerabilities

Support

We were able to find answers to all our questions in the provided documentation (which can be viewed here) and didn't have to contact support for assistance at any point.

Claims

"A solution that keeps getting smarter"

We think this is a fair statement, given that so many of the models that manage prioritization learn from customer actions and actions across all customers (we're trying to avoid saying AI/ML, but yes, that's what's being used here).

"Save Time with Automation"

"Consolidate Vulnerability Management"

These claims are both correct when placed in the correct context. We're happy to report that the correct context is provided everywhere we find these claims. We couldn't find any overstatements or stretched claims on Secureworks' websites, in any of their press releases, or in any marketing or advertisements.

EULA check

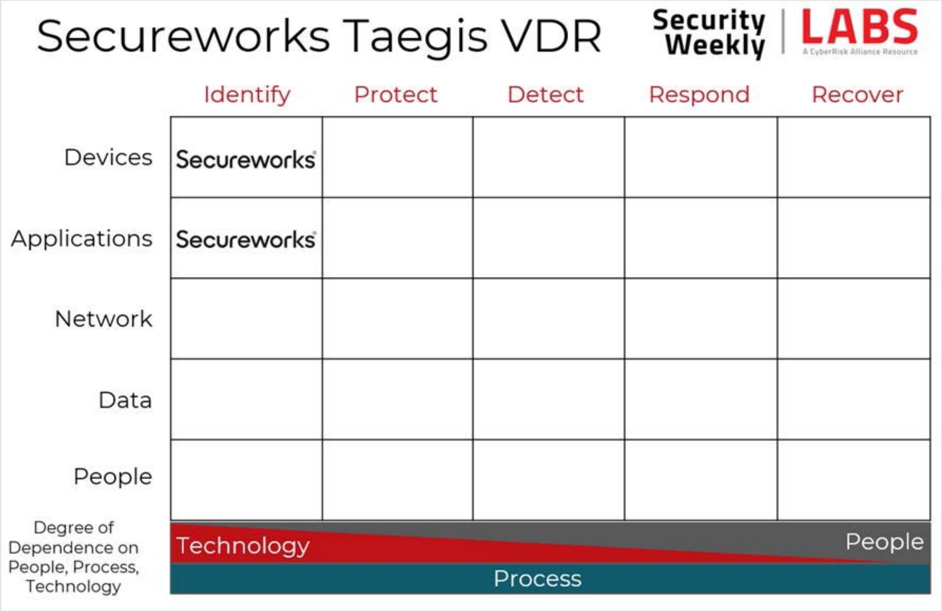
Note: *we're not lawyers and this should not be interpreted as or taken as legal advice.*

We reviewed Secureworks' Customer Relationship Agreement (CRA) and the SaaS Addendum to the CRA. We couldn't find anything preventing us from reviewing their products and sharing the results, though we did find a cause prohibiting using the product to collect competitive intelligence in the SaaS Addendum:

"Customer… will not, for itself, any Customer Affiliate or any third party… access or use the Products for purposes of competitive analysis of the Products, the development, provision, or use of a competing software service or product or any other purpose that is to Secureworks' detriment or commercial disadvantage"

Security program fit

The core of network vulnerability scanners is **identifying** vulnerabilities in **devices**, occupying that upper left-hand corner. All modern vulnerability scanners also have built-in web **application** scanners (DAST) as well, so each of these vendors occupy that second square as well.



Secureworks Taegis VDR

	Identify	Protect	Detect	Respond	Recover
Devices	Secureworks				
Applications	Secureworks				
Network					
Data					
People					

Degree of Dependence on People, Process, Technology
Technology
People
Process

Conclusion

While pricing is competitive with other vulnerability scanners, a direct comparison is difficult. It's true that Taegis VDR lacks some of the workflow and integration depth we see from Rapid7, Tenable, and Qualys. However, in our experience, it surpasses all three incumbent vendors in terms of accuracy and ease of use. Further, this product includes vulnerability prioritization and intelligence typically only found in expensive add on modules, or highly focused products that don't include their own scanners. Once organizations get buried in compliance, audits, reporting, and regulations — they'll likely have to move to one of the more full-featured scanners that have built-in compliance-specific checks and reporting.

In short, if you just need basic vulnerability scanning, analysis, and prioritization, Taegis VDR is an excellent value and is our top choice for small to mid-sized enterprises.

Who We Are

About CyberRisk Alliance

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers and practitioners. CRA's brands include SC Media, Security Weekly, InfoSec World, Cybersecurity Collaboration Forum, our research unit CRA Business Intelligence, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. More information is available at CyberRiskAlliance.com.

About the author

Adrian Sanabria joined CyberRisk Alliance — the parent company of SC Media and Security Weekly — in 2020. He oversees Security Weekly Labs, the company's cybersecurity product review and database initiative. Adrian also provides industry commentary for both SC Media and Security Weekly. He brings two decades of industry experience, working as a practitioner, penetration tester, and industry analyst. He spent the last few years as an entrepreneur, challenging norms in sales and marketing for a variety of vendors. Adrian loves to cook, eat, hike, play music and regale his teenagers with stories of what the early days of the Internet were like.