

Cyber Fusion for Vulnerability Management

Proactively identify, prioritize, and remediate
the high-risk vulnerabilities at scale

The State of Vulnerability Management

Maintaining effective vulnerability management is a bit like eating broccoli. We all know it's good for us and yet, nobody wants to do it.

The reasons why differ, of course. Where broccoli is tough and bitter, vulnerability management is arduous, overwhelming, and frustratingly difficult to do well. In fact, with so many vulnerabilities to process, it's easy to wonder if Elton John and Tim Rice were moonlighting as vulnerability analysts when they wrote the opening song to *The Lion King*:

**“There's more to see than can ever be seen,
More to do than can ever be done.
There's far too much to take in here,
More to find than can ever be found.”**

And **because** vulnerability management is so overwhelming, it's easy to be distracted by more exciting areas of security—fancy tools that protect against APTs and zero day threats, for example.

But that would be a mistake. Vulnerability management is a crucial element of cyber hygiene that underpins every other area of cybersecurity. You can have all the fancy tools and blinking lights you like, but it could all be for nothing if you don't get the basics right.

In [*Practical Vulnerability Management*](#) (2020), Andrew Magnusson gives a simple example of the importance of effective vulnerability management. He describes a situation where a mid-sized organization has a comprehensive set of security controls in place, including:

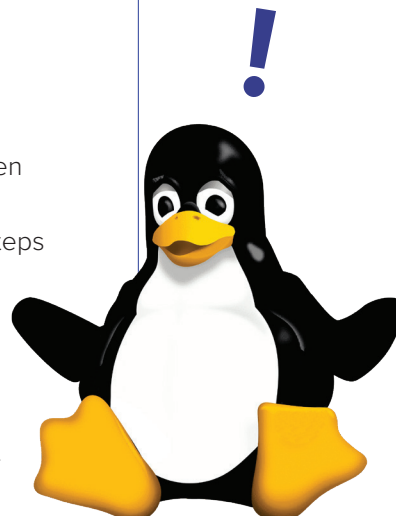
- Firewalls to block unwanted incoming traffic
- Egress filtering to block unauthorized exit traffic
- Antivirus on all endpoints
- Hardened servers

...but there's a problem. An old Linux webserver—a relic of a forgotten business initiative—is running an outdated version of Tomcat that's vulnerable to a five-year-old Java exploit. Using it, an attacker sidesteps all the organization's fancy controls and gains a foothold inside the network.

This is why fundamental cyber hygiene factors like vulnerability management are so important. A network is only as strong as its weakest link—and often, that weakest link is an unpatched vulnerability.

Contents

The State of Vulnerability Management	2
What's the Risk of an Unpatched Vulnerability?	3
Vulnerability Management Challenges	3
What's Needed for Better Vulnerability Management?	5
Enhancing Vulnerability Management with Cyber Fusion	6
How Does Cyber Fusion Support Vulnerability Management via Next-gen Threat Intelligence and SOAR	7
Cyber Fusion Benefits	8
7 Cyber Fusion Use Cases for Vulnerability Management	9
Reign in Vulnerability Risk with Cyber Fusion	13



What's the Risk of an Unpatched Vulnerability?

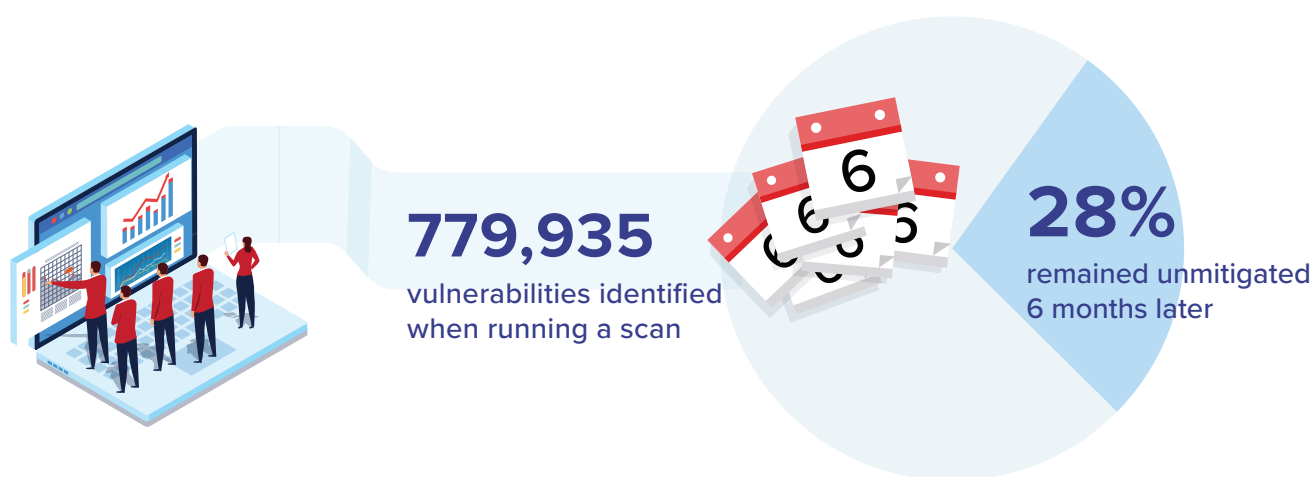
There is disagreement over what proportion of breaches are caused or exacerbated by known, unpatched vulnerabilities. [One study](#) claims the answer is 42%, while [another](#) proposes 34%. Meanwhile, [some security experts](#) have raised their eyebrows at such self-reported studies, suggesting the true figure could be much higher.

While there's no agreement on the topic, it's safe to say the answer is "a lot" and "this is a big deal."

Note that often, breaches aren't caused by a single factor. What ultimately presents as ransomware or mass data theft often starts as something less dramatic—a phishing

email, basic web application attack, credential stuffing... or exploiting an unpatched vulnerability.

Once an attacker obtains a foothold within a network, they often 'dwell' there, slowly expanding privileges and moving laterally through the network to avoid raising suspicion until they can achieve their objective. This is what makes vulnerable systems dangerous. Something as basic as a forgotten, unpatched server can provide the 'toehold' an attacker needs to launch a major attack.



Vulnerability Management Challenges

1. INCOMPLETE ASSET INVENTORY

Every IT professional understands the importance of an accurate, current register of digital assets. Perhaps the most common form—the Configuration Management Database, or CMDB—has been a feature of the globally-used ITIL framework since the 1980s. Unfortunately, keeping an up-to-date CMDB was tough back then, and today it's a tremendous challenge.

You can only scan and patch what you can see. With complex environments and shadow IT, many organizations don't fully grasp the extent of their attack surface. This poses a huge risk. If some assets are unknown, they may also be unpatched and potentially vulnerable—which, as we've seen, can create an easy entry point for an attacker.

2. OVERWHELM

[According to IBM](#), the average organization with 1,000+ employees identifies 779,935 vulnerabilities when running a scan. Over any six months, roughly 28% of these remain unmitigated—and as a result, these organizations have an average backlog of 57,555 identified vulnerabilities.

These numbers are insane. Today's vulnerability management teams face an impossible challenge, as there is simply no way to patch this many vulnerabilities with the resources available.

Vulnerability Management Challenges (Continued)

3. PRIORITIZING VULNERABILITIES

If you can't do everything, the solution is to prioritize.

The [Common Vulnerability Scoring System \(CVSS\)](#) is the most widely used scoring system for vulnerability risk. It assesses vulnerabilities on a five-tiered scale from 'None' to 'Critical.' However, CVSS scores are generic and don't explain the risk a vulnerability poses to a specific organization—what's Critical for one organization could be negligible for another.

This creates a challenge for prioritization. In practice, even the list of Critical vulnerabilities identified by a scan is often too long to fully address. Meanwhile, vulnerabilities could be overlooked due to low CVSS scores that actually pose a significant risk to their organization.

This is the 'false positive' problem. 60% of respondents to the [IBM study](#) mentioned above say wasting time on false positives and minor vulnerabilities is a huge risk to their organization.

4. MANUAL PROCESSES AND LACK OF AUTOMATED RESPONSE

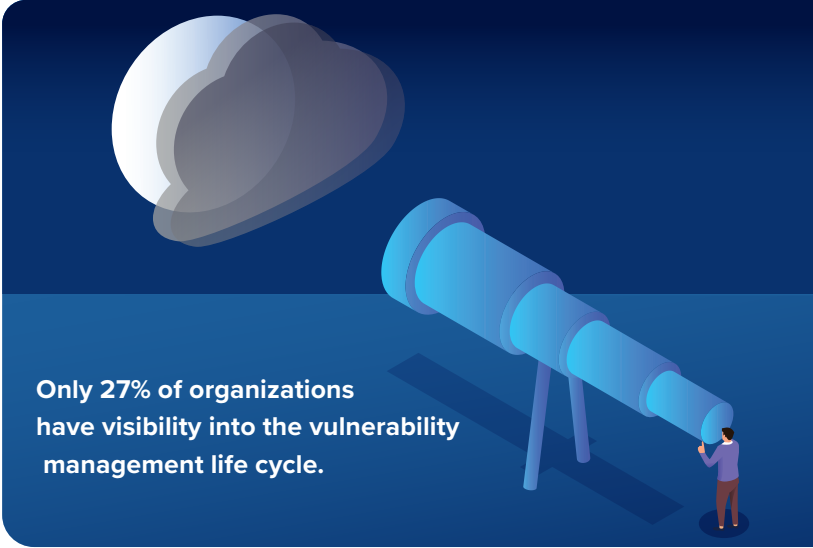
Many of the processes surrounding vulnerability prioritization and remediation are manual, making them difficult to scale and prone to human error. Patching, in particular, is slow and arduous and often requires time-consuming back-and-forth communication between the VM team, asset owners, and other stakeholders before the patching process can even begin.

When patching does begin, it's typically a manual process where VM teams are forced to start from scratch for each new vulnerability. With limited integration between security and IT tools—and often no automation at all—the process is inefficient and labor-intensive. In fact, according to a recent [research study](#), Forrester determined that 61% of security practitioners find it extremely challenging to automate incident responses playbooks.

5. MONITORING AND REPORTING

Keeping a record of vulnerability management processes and KPIs is essential, but it's tough to do reliably and thoroughly when everything is manual. Organizations can (and do) define processes to record activities and outcomes, but there will always be gaps in manual recording, and these activities add even more manual work to an already arduous process.

As an example, high impact vulnerabilities such as those with a CVSS score of nine or higher should be reported to security leaders as soon as they are identified. Meanwhile, lower impact vulnerabilities can be safely handled by VM teams without further escalation. However, administering this type of process is time consuming and error prone. Typically, security leaders see either too many vulnerability reports, wasting their time and causing them to lose interest, or they aren't reliably informed about high impact vulnerabilities until it's too late.



Only 27% of organizations have visibility into the vulnerability management life cycle.

[IBM](#) found only 27% of organizations have full visibility into the vulnerability management life cycle. That's not because three-quarters of organizations are negligent—it's because keeping track of vulnerability identification, prioritization, and remediation manually is a huge challenge. As a result, many organizations have limited visibility of their past and present vulnerability remediation activities, making it difficult to truly understand vulnerability risk or investigate possible mistakes.

6. LACK OF HUMAN RESOURCES

The omnipresent cybersecurity skills gap leaves no team unhindered, and vulnerability management is among the hardest hit. With an endless workload and many manual processes, teams are always playing catch-up—and it's only a matter of time until an unpatched vulnerability is exploited.

What's Needed for Better Vulnerability Management?

In its 2021 [Data Breach Investigations Report](#), Verizon claims the mantra for vulnerability management should be *smarter, not harder*. VM teams need help from technology to find and fix the highest risk vulnerabilities while discarding false positives and low-impact results. This will reduce vulnerability risk and relieve some of the factors that can overwhelm vulnerability management teams.

Nobody will invent a tool that allows VM teams to patch hundreds of thousands of extra vulnerabilities each year—at least, not any time soon. However, with greater visibility, accurate prioritization, enhanced monitoring and audit, and more orchestration and automation support, VM teams can dramatically reduce the risk of unpatched vulnerabilities.

Today, vulnerability management teams need four things:

1. An accurate asset inventory that provides **complete visibility** of their environment.
2. Fast, **intelligence-led prioritization** of vulnerabilities that threaten *their* organization.
3. Greater **monitoring** of the vulnerability management process and outcomes.
4. Comprehensive **automation and orchestration** to reduce effort and improve outcomes.

“Anything you can do to avoid patching vulnerabilities that do not improve your security keeps you just as secure but involves much less work (and less chance of burnout from your employees).”

VERIZON



Enhancing Vulnerability Management with Cyber Fusion

A Cyber Fusion strategy and framework unifies all security and IT operations tools into a single solution, allowing different security functions to collaborate and share intelligence seamlessly.

A Cyber Fusion Center (CFC) solution combines the full functionality of a Security Orchestration, Automation, and Response (SOAR) and Threat Intelligence Platform (TIP) while expanding three additional essential capabilities:

- Enhanced any-to-any integration and orchestration
- Threat intelligence sharing and collective response
- Providing situational awareness and threat context

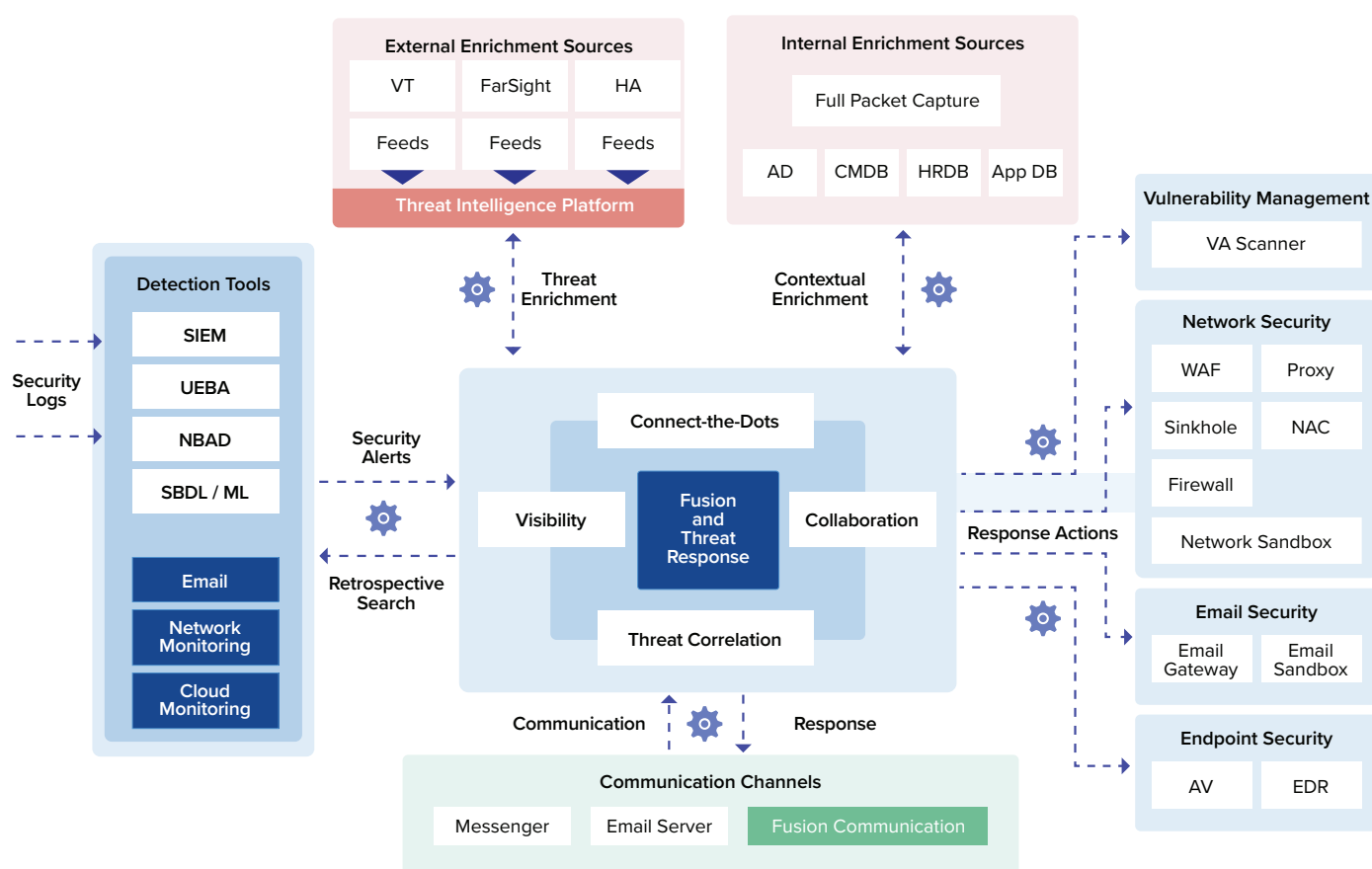
While SOAR and TIP provide a limited version of these capabilities, it's not enough to support effective

collaboration between security functions or fully empower vulnerability management teams to identify, prioritize, and remediate high-risk vulnerabilities.

By combining these capabilities, CFC delivers what vulnerability management teams really need: instant access to all relevant vulnerability intelligence, complete visibility into the vulnerability management process, and seamless orchestration and automation of any process, including audit.

The architecture diagram below demonstrates how a Cyber Fusion Center (CFC) solution unifies security, giving teams a single location to access all data and functionality.

Cyber Fusion Center Architecture



How Does Cyber Fusion Support Vulnerability Management?

A CFC solution provides four essential capabilities that support effective vulnerability management:

1. Connectivity. A CFC solution is the connective tissue between all security and IT operations tools and data. This allows vulnerability management teams to use every tool and data repository available to them to monitor all assets, including which software and versions they are running. This oversight helps to solve one of the key vulnerability management challenges—incomplete asset data—and has a profound impact on vulnerability risk.

2. Centralized vulnerability intelligence. CVSS scores don't help organizations understand the risk a vulnerability poses to them. For that, they need to reference data and intelligence from multiple internal and external sources, which can be a frustratingly manual exercise. A CFC solution addresses this by collecting all intelligence into a single location and making it readily available to vulnerability management teams.

- Asset data from CMDBs, endpoint clients, attack surface scanners, and more.
- Vulnerability data from scanners and threat feeds.
- Exploit data from [Exploit Database](#), [Metasploit](#), and other sources.
- CTI from threat feeds, proprietary exploit data, intelligence sharing groups, etc.

This allows teams to assess vulnerability risk based on a comprehensive picture of the internal and external landscape. Best of all, much of this work can be orchestrated into a proprietary risk assessment playbook that automatically prioritizes the results of vulnerability scans.

3. Any-to-any orchestration. Many SOAR tools claim to offer comprehensive orchestration, but most are limited to integrations with specific tools or vendors. A CFC solution provides true any-to-any, cross-environment integration and orchestration, including between internal and cloud tools.

This allows teams to orchestrate processes that combine functionality from multiple tools, including CMDB, EDR, TIP, and case management. For example, teams can automatically risk assess and prioritize vulnerabilities *and* take remediation steps like patching and stakeholder communications.

“Doesn’t SOAR do that?”

SOAR vendors position their tools as all-encompassing solutions that address many of the challenges discussed in this paper. However, most SOAR tools present several challenges:

- They provide limited integrations, often restricted to tools produced by specific vendors.
- They don't support the seamless collection of intelligence from all available sources.
- Automation capabilities often require coding skills and therefore go unused.
- They aren't designed to support intelligence sharing between teams and organizations.

These limitations force vulnerability management teams to spend time on laborious tasks such as switching between tools, manual data and intelligence collection, and data transfer.

How Does Cyber Fusion Support Vulnerability Management? (Continued)

4. Situational awareness and intelligence sharing.

A deciding factor in vulnerability risk is whether a known vulnerability is actively being exploited at a point in time. A CFC solution facilitates real-time sharing of CTI and other contextual information between security teams, roles, and organizations. Intelligence sharing communities like ISACs use CFC solutions to quickly inform partners and industry colleagues when they observe a vulnerability being exploited, allowing the entire community to proactively reduce risk by remediating it.

5. Automated remediation. A CFC solution provides true orchestration and no-code playbook building, allowing vulnerability management teams to automate time-consuming processes into a single button click. Where appropriate, playbooks can trigger automatically, completely removing the burden from analysts.

Orchestrating multi-stage patching processes is a substantial time saver and enables automated audit tracking, ensuring there is a complete and permanent record of all activities. While fully-automated patching is often considered a risk, many organizations use a CFC solution to automate critical remediation steps such as stakeholder communications and follow-up.

Cyber Fusion Benefits

These capabilities provide a host of benefits for vulnerability management teams, including:

Accurate vulnerability risk assessment

More consistent remediation

Prioritize response to high-risk vulnerabilities

Reduced manual burden on teams

Eliminate false positives and no-risk vulnerabilities

Fewer opportunities for human error

Fully automated audit trail

Significantly reduced vulnerability risk

7 Cyber Fusion Use Cases for Vulnerability Management



Organization-specific Vulnerability Risk Assessment

We've established that CVSS scores don't help organizations understand vulnerability risk. Instead, vulnerability management teams need access to relevant data and intelligence sources to build a true picture of the risk posed by a vulnerability. But that takes time—and with tens of thousands of vulnerabilities outstanding, even the fastest manual process is untenable.

A CFC solution can automate the enrichment of vulnerability scan results with all available internal and external data and intelligence sources, including the current list of assets connected to the network and the software versions they are running. This can inform an automated prioritization playbook that identifies which vulnerabilities pose the highest risk to the organization right now.

The solution can go a stage further by comparing enriched vulnerabilities to open security incidents to see if any relate to an asset that could be affected by the vulnerability. If an incident is identified, the vulnerability management team can take immediate action to remediate the vulnerability.



#2

Automated Remediation

Without effective orchestration and automation tools, vulnerability remediation can be an arduous, manual process. Patch management tools provide some help, but without robust orchestration scaling up is tough.

A CFC solution enables vulnerability management teams to orchestrate and automate the entire patching process. In most cases, patching playbooks will be triggered by a human, but that's all the input required—the entire patch installation and validation process happens at machine speed. Playbooks can be set to run at a specific time, protecting system uptime during business hours.



#3

Automated Audit Trails

Keeping track of activities is critical for audit purposes—without a clear record of what has been done, it's tough to investigate possible issues or mistakes. From a business perspective, metrics matter. Without clear evidence, it's tough to evidence the need for more resources, or even prove the impact of the resources already allocated. In traditional manual vulnerability management practices, audit trails are typically sparse, as they require manual effort to record.

A CFC platform can automatically record all process metrics, helping teams see exactly what has happened. For example, an automated patching playbook will keep track of successful and unsuccessful patch applications, making it easy to identify unpatched assets.



Vulnerability Intelligence Sharing

The highest risk vulnerabilities are those being actively exploited today. Intelligence sharing between organizations and communities like ISACs is a core component of Cyber Fusion, and it holds the key to faster, more accurate identification of the highest-risk vulnerabilities.

Vulnerability intelligence sharing is two-way. If an organization identifies it has been targeted by an exploit—whether the attack is successful or not—it can share that information with its peers, partners, and vendors. This helps to mitigate third party risk, which is a huge source of cyber risk.

An organization can also receive a notification through an intelligence-sharing community that an exploit is in active use in its industry or geographic area. This prompts the vulnerability management team to assess the organization's exposure and act accordingly.

Similarly, vulnerabilities can also be escalated internally and between organizations based on criticality. Vulnerabilities with high CVSS scores are typically most concerning and can be automatically escalated or shared with security leaders, while less critical vulnerabilities can be shared as needed based on individual roles, locations, and industries.



Assessing Vulnerability Exposure

Assessing exposure to specific vulnerabilities is a common need—often to answer executive questions or respond to the discovery of a new vulnerability that is being actively exploited.

Using a CFC solution, an analyst can run a playbook that:

1. Enriches a vulnerability report with all available internal and external data and intelligence
2. Immediately identifies any affected assets
3. Creates a ticket in the case management tool
4. Looks up the owners of affected assets and sends them an email

The ability to assess exposure to any vulnerability in minutes and automatically begin remediation steps is unique to Cyber Fusion and has a profound impact on reducing vulnerability risk.

#6

Discovering Rogue Assets

Unknown assets are a source of risk, but many organizations have no effective way to identify them. A CFC solution can automatically compare the content of a CMDB or other asset inventory to results from vulnerability scans, host enumeration, attack surface scanners, patch managers, and EDR tools to identify assets with unknown MAC addresses.

Depending on the significance of identified unknown assets, a CFC solution can begin appropriate remediation steps—for example, creating a ticket in the case management system to investigate.

A similar automated process can be used to identify assets that are approaching end of life and need to be upgraded, replaced, or retired. A playbook can check assets to uncover software versions that are approaching the end of their support life, and take appropriate action—e.g., creating a ticket or contacting asset owners.



#7

Vulnerability Threat Hunting

For high-risk vulnerabilities, proactive identification and remediation are best. When a brand new vulnerability is discovered, security teams can use a CFC solution to automatically search the entire environment for exposed assets. Once a list of assets is generated, the playbook can automatically contact the owner of each asset and create a ticket enriched with asset details, network segments, vulnerability intelligence, and everything else needed to remediate the vulnerability.

Reign in Vulnerability Risk with Cyber Fusion

Despite the valiant efforts of vulnerability management teams, most organizations fall further behind each year. The average organization has tens of thousands of open vulnerabilities and very little chance of knowing which to prioritize and which to ignore. While vulnerability scanners and patch management tools provide vital functionality, they don't offer the broader capabilities and centralized intelligence needed to meaningfully reduce vulnerability risk.

This paper has made a case for Cyber Fusion as a way to orchestrate a comprehensive vulnerability identification, prioritization, and remediation program based on organization-specific risk—and dramatically reduce the manual burden on vulnerability management teams.

Key learning points include:

- **Vulnerability management is a foundational component of cyber hygiene that underpins many of the more 'exciting' aspects of security.**
- **Teams face a monumental challenge to prioritize and remediate the “sea of red” vulnerabilities they are faced with.**
- **The requirements for risk-based vulnerability management are improved visibility, CTI-led prioritization, automated monitoring, and configurable automation and orchestration.**
- **Cyber Fusion unifies security and IT operations tools into a single solution, allowing teams to more effectively identify, prioritize, and remediate vulnerabilities.**
- **Cyber Fusion solutions support better vulnerability management outcomes by delivering all four of the additional requirements described in this paper.**
- **The top benefits of Cyber Fusion for vulnerability management include accurate prioritization, elimination of false positives, decreased manual burden, and reduced vulnerability risk.**

This paper has laid out seven common use cases for Cyber Fusion in vulnerability management. In practice, there are many more applications to reduce risk and the manual burden on security teams.

To see how Cyware's virtual Cyber Fusion Center solution can help your enterprise security team boost collaboration and improve vulnerability, [arrange a free demo](#) today.

About Cyware

Cyware helps enterprise cybersecurity teams build platform-agnostic virtual cyber fusion centers. Cyware is transforming security operations by delivering the cybersecurity industry's only **virtual** cyber fusion center platform with next-generation SOAR (security orchestration, automation, and response) technology. As a result, organizations can increase speed and accuracy while reducing costs and analyst burnout. Cyware's Virtual Cyber Fusion solutions make secure collaboration, information sharing, and enhanced threat visibility a reality for enterprises, sharing communities (ISAC/ISAO), MSSPs, and government agencies of all sizes and needs.



228 Park Avenue S #77147
New York, NY 10003-1502
855-MY-CYWARE • sales@cyware.com

www.cyware.com

©2022 All rights reserved. Cyware is a trademark of Cyware, Inc. All other product names are trademarks or registered trademarks of their respective companies.