SPOTLIGHT

RISKSENSE Acquired by Ivanti | CSW Cyber SecurityWorks | CYWARE™

Ransomware

Through the Lens of Threat and Vulnerability Management

Index Update Q3 2021

2021

Introduction

The Ransomware Index Update Q3 2021 continues to show a steady increase in all key ransomware markers. Our ransomware research has identified ransomware groups expanding their attack arsenal with 12 new vulnerability associations in Q3, twice that of the previous quarter.

The Q3 Ransomware Index update highlights the results of our in-depth research related to ransomware groups and the vulnerabilities and weaknesses they go after. The Report also focuses on some of the key trends we have observed and aims to provide organizations the knowledge they need to stay safe from falling victims to such attacks.

The Top Five Findings:

1. The number of vulnerabilities associated with ransomware has increased from 266 to 278 in Q3 2021.
2. There has been a 4.5% increase in trending vulnerabilities that are being actively exploited to mount attacks, taking the total count to 140.
3. With 5 new ransomware families identified in Q3, we now have a total of 151 ransomware families.
4. Ransomware groups continue to find and leverage zero-day vulnerabilities even before the CVEs are added to the National Vulnerability Database (NVD) and patches are released.
5. The total count of older* vulnerabilities associated with ransomware is now 258, which is a whopping 92.4% of all vulnerabilities tied to ransomware.

*Vulnerabilities identified before 2021 are considered older

Executive Summary

Our analysis of ransomware groups and their weaponry in Q3 2021 shows that they are continuously upping their game. Newer, more sophisticated techniques, such as trojan-as-a-service and dropper-as-a-service, are being adopted in attacks. There have also been increased instances of the ransomware code being leaked online, providing the perfect impetus for less sophisticated groups to amp up their exploits.

In the Q2 2021 report, we highlighted a prominent trend of ransomware groups leveraging zero-day vulnerabilities, sometimes even before the vendor could identify the existence of the flaw. Continuing the trend in Q3, the REvil group went after a vulnerability in Kaseya VSA servers that the company was preparing to patch.

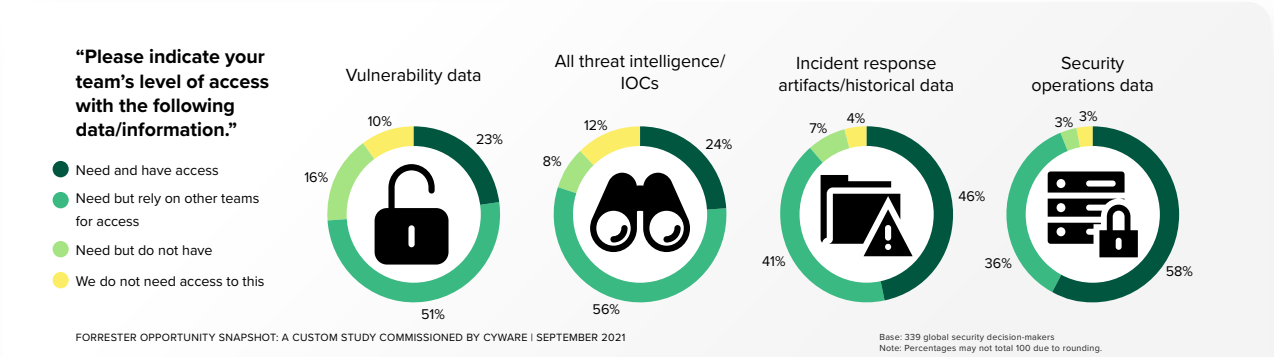
Ransomware groups have also targeted some of the most dangerous vulnerabilities in this quarter (PrintNightmare, PetitPotam, and ProxyShell), weeks after they were first identified as trending in the wild. We also observed the Cring ransomware group going after two-decade-old vulnerabilities, CVE-2009-3960 and CVE-2010-2861. Incidentally, the vulnerabilities existed in Adobe ColdFusion versions that had reached their end of life and thus were no longer supported by their vendors.

Dropper-as-a-service: *This is a service that allows newbie threat attackers to distribute their malware through droppers. Droppers are programs that — when run — can execute a malicious payload onto a victim's computer.*

Trojan-as-a-service: *Popularly called malware-as-a-service, anyone with an internet connection can obtain customized malware services for rent, allowing them to acquire, implement, and cash in on the service, all on the cloud with zero installation.*

On Nov 3, 2021, Cybersecurity Infrastructure Security Agency (CISA) issued a Binding Operational Directive (BOD) listing 287 vulnerabilities that are actively exploited by adversaries. The directive has not only laid out clear requirements for federal civilian agencies to reduce their security debt but also provided them with a due date before which these vulnerabilities need to be addressed.

Our analysis of this list has revealed that 52 vulnerabilities have been called out in the Ransomware Reports (25 CVEs in Spotlight Report '21, 18 in Q1'21, 2 in Q2'21, 7 in Q3'21). These are cumulatively associated with 91 ransomware families and CVE-2018-4878 alone is linked to 41 of them. Of these, Microsoft is the most vulnerable vendor with 27 CVEs across its products. 35 of these vulnerabilities are also associated with Advanced Persistent Threat (APT) groups, making them all the more dangerous. The CISA mandate directs federal agencies to remediate 20 of them by the end of 2021, and the remaining by May 2022.



Recently, a commissioned study conducted by Forrester Consulting on behalf of Cyware discusses the major hurdles organizations face while dealing with ransomware and other such threats. The Opportunity Snapshot report states that "Improved threat detection and incident response is the top-ranked organizational cybersecurity objective over the next 12 months." However, the report also goes on to outline the following: "Seventy-one percent of security leaders report their teams need access to threat intelligence/indicators of compromise (IOC), security operations data, incident response artifacts/historical data, and vulnerability data, but direct access is a struggle."

It is this very problem that our continued research tries to address. We aim to help organizations realize the realities of risk from vulnerabilities across their attack surface through the Ransomware Report with actionable intelligence for faster remediation. This quarter, Cyber Security Works and RiskSense (acquired by Ivanti) have partnered with Cyware to collaborate and broaden awareness.

FOCUS	PREVIOUSLY REPORTED	NEW TOTALS	CHANGE FROM Q2' 21 TO Q3'21
CVEs Associated with Ransomware	266	278	4.5% increase
Low-Scoring* CVEs Tied to Ransomware * CVSS v2 score less than 8	159	168	5.6% increase
Actively Exploited* and Trending Vulnerabilities *Used with Ransomware	134	140	4.5% increase
Number of Ransomware Families	146	151	3.4% increase
Exploit Kits in Use by Ransomware	31	31	-
Number of APT Groups Associated with Ransomware	40	40	-
Old Vulnerabilities Associated with Ransomware	255* *2020 and earlier	258* *2020 and earlier	1.2% increase
CWEs	52	52	6 new CWEs* *Some CVE-CWE associations have been updated
Vulnerable Vendors	96	98	2.1% increase
Vulnerable Products	722	760	3.3% increase

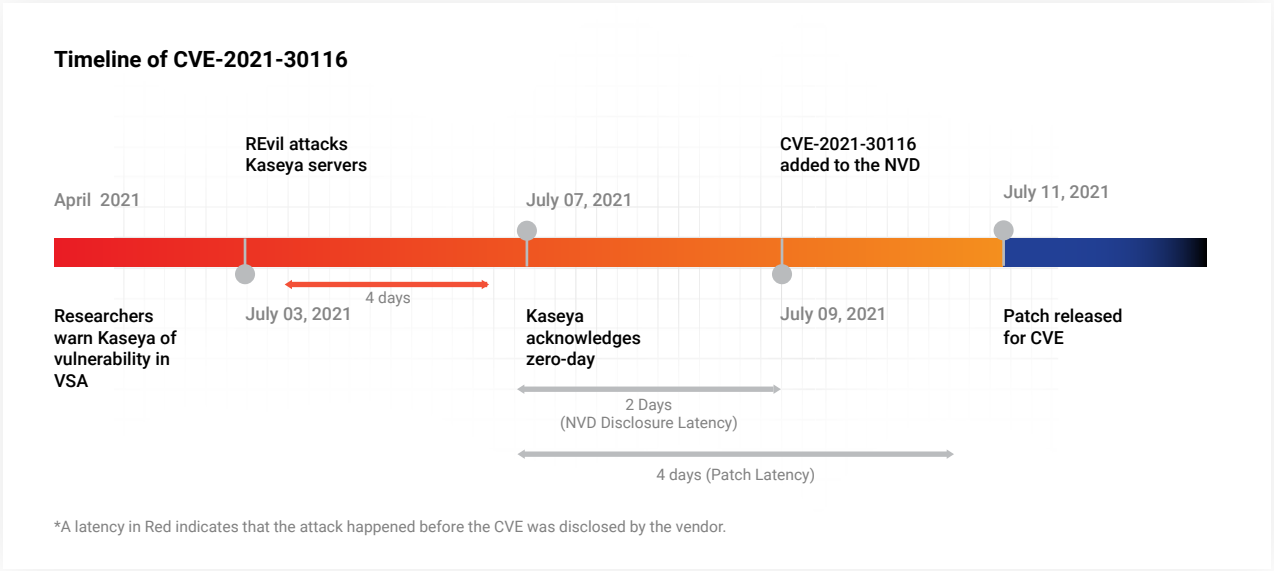
Q3 Ransomware Index Findings

4.5% Increase in Vulnerabilities Tied to Ransomware

In Q3 2021, we noticed that 12 vulnerabilities were newly associated with 7 ransomware strains. With this update, we now have 278 vulnerabilities with ransomware associations.

Newly-Associated Vulnerabilities	CVSS Score	CVSS Severity	Presence of Exploit	Ransomware Groups
CVE-2021-34473	9.8	CRITICAL	RCE	Conti and LockFile
CVE-2021-34523	9.8	CRITICAL	RCE	Conti and LockFile
CVE-2021-30116	9.8	CRITICAL	N/A	REvil/Sodinokibi
CVE-2021-34527	8.8	HIGH	RCE	Conti, Magniber, and Vice Society
CVE-2021-1675	8.8	HIGH	RCE	Conti and Vice Society
CVE-2010-2861	7.5	HIGH	DoS/WebApp	Cring
CVE-2019-7481	7.5	HIGH	WebApp	HelloKitty
CVE-2021-30120	7.5	HIGH	N/A	REvil/Sodinokibi
CVE-2021-31207	7.2	HIGH	RCE	Conti and LockFile
CVE-2021-30119	5.4	MEDIUM	WebApp	REvil/Sodinokibi
CVE-2021-36942	5.3	MEDIUM	N/A	LockFile
CVE-2009-3960	4.3	MEDIUM	DoS/WebApp	Cring

One of the new vulnerabilities identified in this quarter follows Q2's zero-day exploit trend that we noticed. CVE-2021-30116, a zero-day vulnerability in Kaseya Unitrends Service, was exploited in the massive supply chain attack on July 03, 2021 by the REvil group, which affected several third-party companies using the attacked server. Following the attack, the vulnerability was acknowledged by Kaseya on July 07, 2021 and was added to the NVD on July 09, 2021. Successively, a patch for the same was released on July 11, 2021. Interestingly, the vulnerability was exploited by REvil ransomware even as the security team at Kaseya was preparing to release a patch for their systems (after reporting the vulnerability back in April 2021).



The Kaseya attack by REvil brings up two important facts:

- The continuing trend of ransomware groups exploiting zero-day vulnerabilities even before the NVD publishes them
- A need for an agile-patching cadence that addresses vulnerabilities as soon as they are identified, rather than waiting for a regular sprint cycle

Vulnerability Analysis

- Of the 12 vulnerabilities newly associated with ransomware, five belong to the most dangerous exploit category—remote code execution (RCE). Four others are capable of exploiting web applications, of which two can be manipulated to launch denial-of-service (DoS) attacks.
- Three CVEs belong to CWE-269, a weakness that leads to improper management of privileges and is often capitalized by ransomware groups.
- The newly added vulnerabilities include three critical severity vulnerabilities (each with a CVSS score of 9.8) acquired by the Sodinokibi, Conti, and LockFile families.
- Interestingly, only four of these vulnerabilities (CVE-2021-1675, CVE-2021-34473, CVE-2021-34523, and CVE-2021-34527) have been found trending with active exploits in the wild during Q3.

4.5% Increase in Actively Exploited Vulnerabilities

The number of active and trending vulnerabilities continues to grow. Six more vulnerabilities with publicly available exploits have been identified as trending in Q3. In total, there are 140 of them today, marking a 4.5% increase from Q2.

3.4% Increase in the Number of Ransomware Families

Our analysis of ransomware families in Q3 brought up five new ones, which have cumulatively added 10 vulnerabilities to their corpus. The total ransomware family count now stands at 151, a 3.4% increase from last quarter's 146.

New Ransomware Families	No. of CVEs Leveraged by the Family
Babuk	2
HelloKitty	1
LockBit	1
LockFile	4
Vice Society	2

All new ransomware groups have regularly been trending in the dark web and hacker channels in Q3. The groups have also gone after powerful vulnerabilities, quickly capitalizing on PetitPotam (CVE-2021-36942), ProxyShell (CVE-2021-31207, CVE-2021-34473, and CVE-2021-34523), and PrintNightmare (CVE-2021-1675) that have been exploited in the wild by malicious attackers. We also noticed these vulnerabilities being chained together, as in the case of Lockfile, to gain access and penetrate deeper into networks. Competing with the new groups, we observed that Cerber (+1), Conti (+12), Cring (+2), eCh0raix (+1), Nefilim (+1), and the Sodinokibi (+3) families are also expanding their vulnerability arsenal.

> The Conti Ransomware group is notable for expanding its arsenal by 12 CVEs this quarter, the single most significant increase we have seen so far in a span of three months.

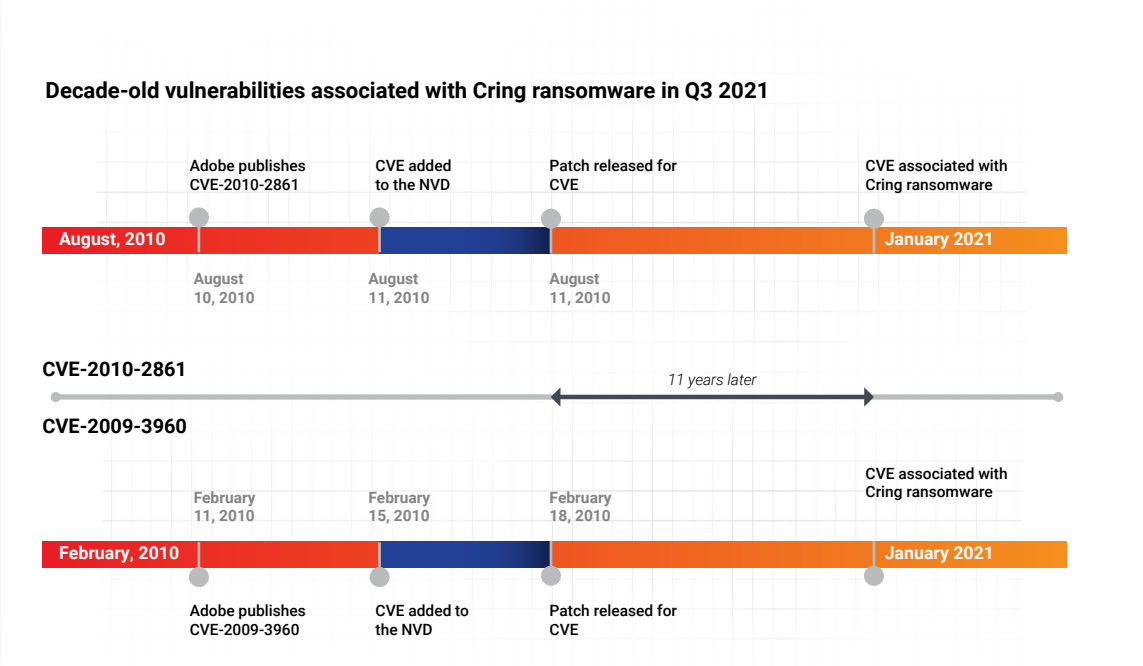
5.6% Increase in Low-Scoring Vulnerabilities Tied to Ransomware

We have demarcated vulnerabilities with CVSS v2 scores less than 8 as low scoring for our ransomware research. We noticed that 9 of the 12 new vulnerabilities belong to this category, recording a 5.6% increase in low-scoring vulnerabilities tied to ransomware. The revised count now stands at 168.

1.2% Increase in Older Vulnerabilities Tied to Ransomware

Three vulnerabilities from 2020 or earlier have become associated with ransomware in Q3 2021. This increases the total count of older vulnerabilities associated with ransomware to 258, a whopping 92.38% of all vulnerabilities tied to ransomware.

HelloKitty ransomware uses CVE-2019-7481, a CVE with a CVSS score of 7.5. The Cring ransomware family has added two vulnerabilities (CVE-2009-3960 and CVE-2010-2861), both of which have been around with available patches for over a decade now. Notably, these vulnerabilities exist in Adobe ColdFusion version 9 that reached its end of life in 2016. Ironically, the incident involving the exploitation of these vulnerabilities had the ColdFusion server running an outdated version of Microsoft Windows.



Note: In our report and this quarterly update, we have considered vulnerabilities from 2010 to 2021. However, CVE-2009-3960 has been included in this edition as it was recently linked to the Cring ransomware, making it a vulnerability that organizations need to promptly review and upgrade, or use an alternative remediation tactic for this active exposure risk.

Six New Weakness Categories Associated with Ransomware

Our analysis of the ransomware vulnerabilities in Q3 2021 added six new categories to the list of unique software weaknesses that power ransomware vulnerabilities.

NEW RANSOMWARE CWES IN Q3 2021	WEAKNESS CATEGORY	IMPACT	CWE LISTED IN OWASP / MITRE TOP CWES?
290	Authentication Bypass by Spoofing	Authentication can be bypassed, resulting in sensitive information disclosure, denial of service, and loss of reputation.	OWASP Top 10
330	Use of Insufficiently Random Values	Attackers can predict values that will be generated and use these values to impersonate another user or access sensitive information.	OWASP Top 10
522	Insufficiently Protected Credentials	Attackers can hack into networks or storage to steal credentials and access/manipulate sensitive data.	MITRE Top 25, OWASP Top 10
798	Use of Hard-Coded Credentials	Sensitive information can be used to log in to or compromise applications.	MITRE Top 25, OWASP Top 10
829	Inclusion of Functionality from Untrusted Control Sphere	An attacker can use this weakness to compromise a secure application that communicates with a vulnerable component, whose functionality can be exploited to launch attacks.	OWASP Top 10
862	Missing Authorization	Missing authorization can lead to sensitive information disclosure, bypass of protection mechanisms, and unauthorized access to data.	MITRE Top 25, OWASP Top 10

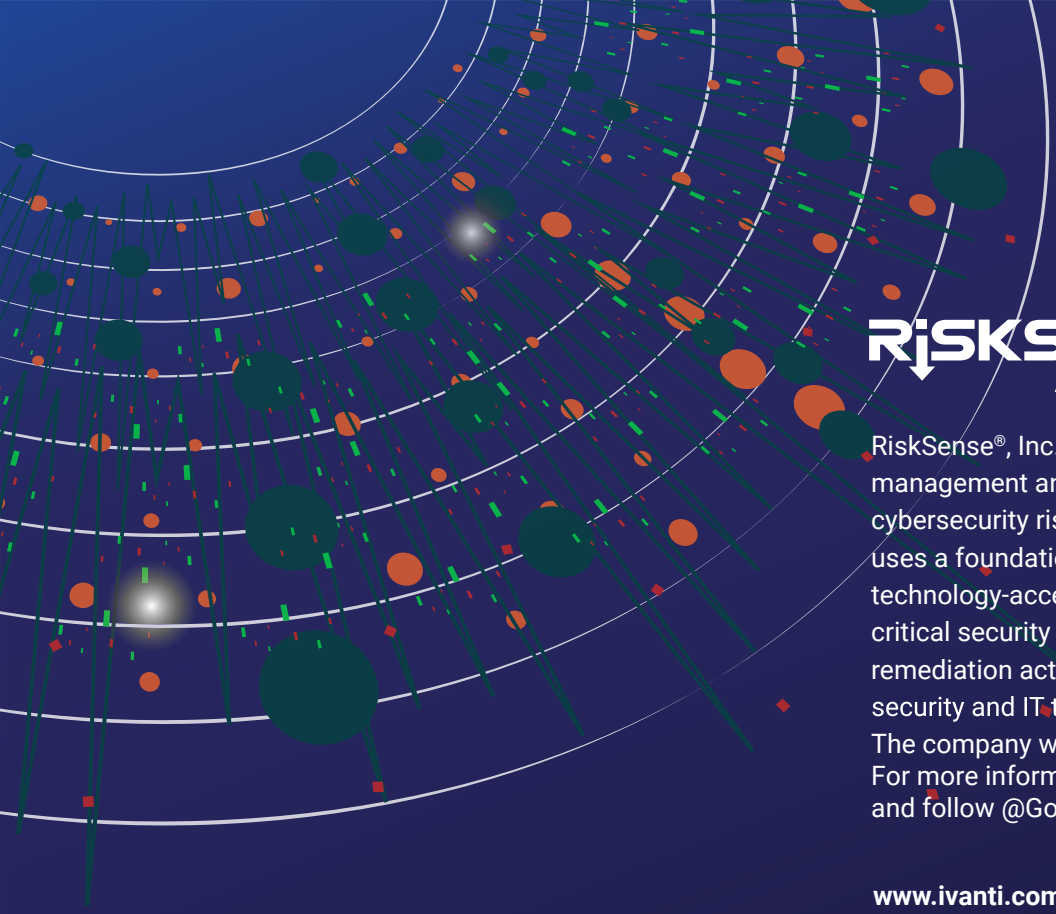
A Pentester's Perspective

- **CWE-290** is a weakness that manifests as an authentication bypass vulnerability that can be subjected to spoofing attacks if authentication processes are not properly implemented. In many cases, this can be escalated to file inclusion and code execution vulnerabilities.
- **CWE-330** is a weakness that results in software generating insufficient random numbers or values in a security context that relies on unpredictability. This allows malicious attackers to predict the sequence of patterns, allowing them to guess access keys or resource identifiers, as the case may be.
- **CWE-522** arises when applications do not provide sufficient protection to stored credentials. With unencrypted access data exposed in the file or browser storage, attackers can steal sensitive information, leading to data breaches.
- **CWE-798** is a result of hard-coded sensitive data during application development. Present in the web page or application builds, this can impact organizations in multiple ways, from unauthorized logins to data breaches.
- **CWE-829** surfaces when applications use any functionality from vulnerable endpoints. A vulnerability in the external endpoint, be it end users or assets, can be exploited by attackers to gain access to organizational networks and even execute arbitrary code or DoS attacks.
- **CWE-862** is a weakness in applications that do not check for authorization. The lack of access control checks can help malicious attackers gain access to sensitive information, leading to data thefts or even loss of reputation.

2.6% Increase in Vendor Products with Ransomware Vulnerabilities

Our research identified ransomware vulnerabilities present across 760 products from 98 different vendors. This includes two new vendors that have been added to the list in Q3. Kaseya has three new vulnerabilities (CVE-2021-30116, CVE-2021-30119, and CVE-2021-30120) in 2021 present across its virtual system administrator and associated agent and server. The second addition is Tenable, with CVE-2019-11043 present in its Security Center deployments.

Note: Our Ransomware Report is updated periodically with relevant changes and highlights based on our continued research and dynamic analysis of ransomware trends and markers.



RISKSENSE™
Acquired by Ivanti

RiskSense®, Inc. provides risk-based vulnerability management and prioritization to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated penetration testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness. The company was acquired by Ivanti in August 2021. For more information, visit www.ivanti.com and follow @GoIvanti.

www.ivanti.com

CSW Cyber SecurityWorks

CSW is a cybersecurity services company focused on attack surface management and penetration testing as a service. Our innovation in vulnerability and exploit research led us to discover 45+ zero days in popular products such as Oracle, D-Link, WSO2, Thembay, Zoho, etc., among others. We became a CVE Numbering Authority to enable thousands of bug bounty hunters and play a critical role in the global effort of vulnerability management. As an acknowledged leader in vulnerability research and analysis, CSW is ahead of the game, helping organizations worldwide to secure their business from ever-evolving threats. For more information, visit www.cybsercurityworks.com or follow us on LinkedIn and Twitter at @CswWorks

www.cybersecurityworks.com

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.

https://cyware.com/