Solution Brief on Cyware VulnCheck Integration

Enabling Exploit Intelligence at Scale with Machine Speed

Cyware Intel Exchange + VulnCheck Integration

Benefits

- Gain massive-scale efficiencies with architectural flexibility and seamless workflow capabilities to optimize around intelligence.
- Adapt to attack surface changes at machine speed with a scalable solution that enables 'any-to-any' intelligence orchestration.
- Automatically trigger response workflows, orchestrate incident resolution

The single biggest cybersecurity challenge today is remediating unpatched vulnerabilities before they're weaponized and exploited by threat actors.

The average time to weaponize vulnerabilities today is eight days or less. Five years ago, it took one year on average - meaning it has become much easier and more lucrative for attackers to cherry-pick run-of-the-mill vulnerabilities to exploit. While zero-days are still a major threat, a random CVE exploit can create havoc for response teams.

With security teams already lagging, being inundated with alerts and data from other tools impacts how efficiently organizations can respond to weaponized vulnerabilities.

VulnCheck's real-time exploit intelligence and vulnerability intelligence solutions feed into Cyware's real-time threat intelligence management platform, giving teams a prioritized view of VulnCheck and Cyware help security teams focus on preventing exploits by defending against adversaries before they can weaponize.

VulnCheck takes vulnerability management to the next level by incorporating exploit intelligence, helping teams prioritize vulnerabilities and then take action on the exploits in real-time with real-world context in Cyware Intel Exchange.

Challenge

MITRE's CVE program is on pace to add 25K vulnerabilities every year right now. Verizon's 2024 DBIR recently found a 180% YoY increase in attacks exploiting vulnerabilities. As a result, organizations are often faced with identifying the vulnerabilities that would have the greatest impact on their specific organization.

Further compounding the issue is most enterprise teams have far too many tools producing too much data and too many alerts without optimized, efficient workflows that prioritize and action intelligence the right way. With alerts and data flowing into security teams in rapid succession, being able to manage those vulnerabilities posing the most significant risk in a threat intelligence platform and then enriching with exploit intelligence for real-time remediation is paramount.

Solution

Cyware and VulnCheck make it possible for organizations to rapidly identify and prioritize vulnerabilities that matter, which reduces response times, gains threat context and visibility, and minimizes risk exposure. The integrated solution offers teams an unprecedented level of intelligence-powered defense that's automated at every level.

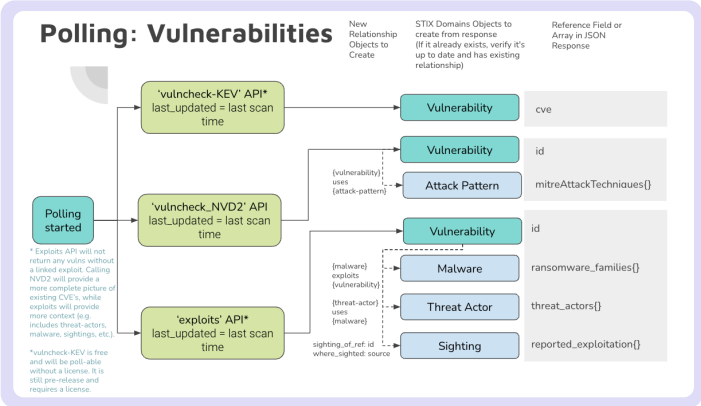
VulnCheck's solutions are 100% autonomous, meaning the data can be automatically consumed by Cyware's threat intelligence platform since it is machine-readable and machine-consumable. Vulnerability management in turn becomes a real-time function versus waiting for vendors to disclose and release patches. Once the workflow hits Cyware, teams can easily correlate against threat feeds, enabling enterprise security teams to prevent and respond to the exploits that matter most with zero human interference.

Use Cases

VulnCheck KEV + Cyware Intel Exchange

- Build enrichment and polling integrations with free VulnCheck KEV in Cyware Intel Exchange.

- VulnCheck KEV is continuously maintained and refreshed with 80% more vulnerabilities vs. CISA KEV, so the exploited vulnerabilities data set is always delivered in real-time, with accurate analysis performed by VulnCheck with attribution, threat context and remediation information.

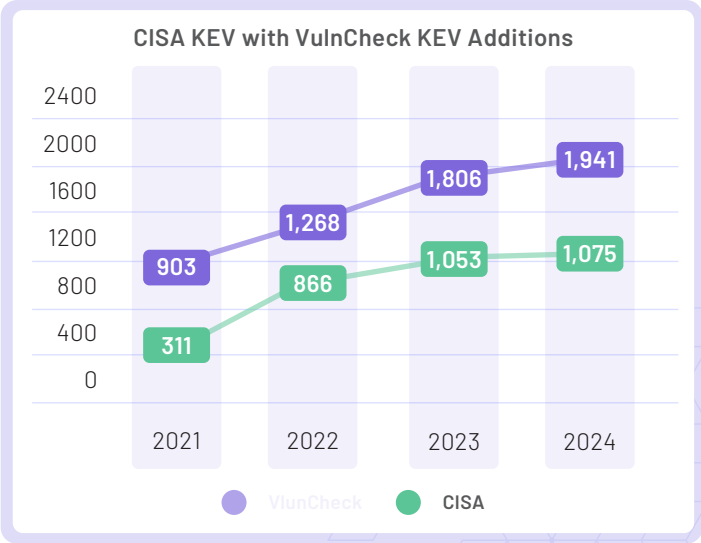


Screenshot of actual dashboard showing the incorporation of KEV vs. KEV.

Exploit & Vulnerability Intelligence (EVI) + Cyware Intel Exchange

- Build enrichment and polling integrations with paid (BYOL) VulnCheck EVI and NVD2 data in Cyware Intel Exchange.

- VulnCheck provides industry-leading collection of exploit data across with a data aggregation covering the entire internet with evidence of exploitation data that is machine-consumable and 100% autonomous.



VulnCheck has grown its tracked CVE's in its KEV and continues to outpace other catalogs like CISA KEV.

About Cyware

Cyware Intel Exchange is a threat intelligence management platform with collaborative threat intelligence capabilities that seamlessly integrate with internal technologies to empower security teams. With comprehensive threat feed ingestion and bi-directional intelligence sharing, Intel Exchange enables collaboration across organizations and industry sectors, fostering collective action against threat actors. This solution enhances decision-making, threat visibility and proactive mitigation.

About VulnCheck

VulnCheck KEV is a community resource that enables security teams to manage vulnerabilities and risk with additional context and evidence-based validation.

Learn more at **www.cyware.com**

Learn more at **www.vulncheck.com**

Cyware
111 Town Square Place Suite 1203, #4
Jersey City, NJ 07310
855-MY-CYWARE

sales@cyware.com | cyware.com

VulnCheck
6 Longfellow Road
Lexington, MA

marketing@vulncheck.com