

Initial Access Intelligence for **Detection & Response**

The threat landscape has changed.

IBM reported the global average **cost of a data breach reached \$4.45M in 2023** - an all-time high for the report and a 15% increase over the last 3 years.

According to Mandiant, the leading cause of data breaches in 2022 was the **Exploitation of Known Vulnerabilities**, outpacing phishing for the first time.

Though VulnCheck finds only **2.25% of vulnerabilities are exploited in the wild or have weaponized exploits**, exploit weaponization has accelerated dramatically.

In 2018, vulnerabilities took almost a year to go from public disclosure to attacks in the wild. **In 2022, vulnerabilities were exploited, on average, in just 8 days.**

What's the Plan?

When the next Internet-level mass exploitation event begins unfolding, how will you know? What will you do? Which partners will you rely on to provide you the information you need quickly?

Key challenges:

Knowing which vulnerabilities are likely to be exploited before breaches begin and before they show up in the CISA KEV list.

Obtaining detection artifacts such as exploit proof of concept code, PCAPs, YARA, Suricata & Snort rules, to respond faster.

Measuring the attack surface with Censys & Shodan queries, accurate CPEs, and remote version scanners, to know the exposure.

Initial Access Intelligence

Leverage Initial Access Intelligence detection artifacts to detect & respond to remote code execution (RCE) vulnerabilities.

Exploit Code

VulnCheck authors proprietary exploit PoC code to test systems and countermeasures against the latest emerging threats.

PCAPs

Network Packet Captures (PCAPs) are provided to defenders to see what the exploited vulnerabilities look like on the wire.





Suricata & Snort Rules

VulnCheck authors proprietary Suricata & Snort rules to detect vulnerabilities accurately, before other vendors have responded yet.

Measure Attack Surface

Using Censys & Shodan queries authored by VulnCheck, quickly see the Internet exposure of the latest emerging threats.

VulnCheck Platform: Benefits at a Glance

-  **Most Exploits**
Industry's largest collection of exploit proof of concept code and evidence of exploitation in the wild.
-  **Exploitation Timeline**
Complete exploitation timeline covering when the vulnerability was first disclosed, when evidence of exploitation was first discovered, when the vulnerability was remediated.
-  **14 Days Faster than NVD**
Respond faster by having information on average 14 days ahead of the NIST NVD.
-  **Vulnerability Prioritization**
Prioritize remediation efforts on the most critical vulnerabilities, those vulnerabilities that are being actively exploited in the wild.