VulnCheck

Product Datasheet

Initial Access Intelligence

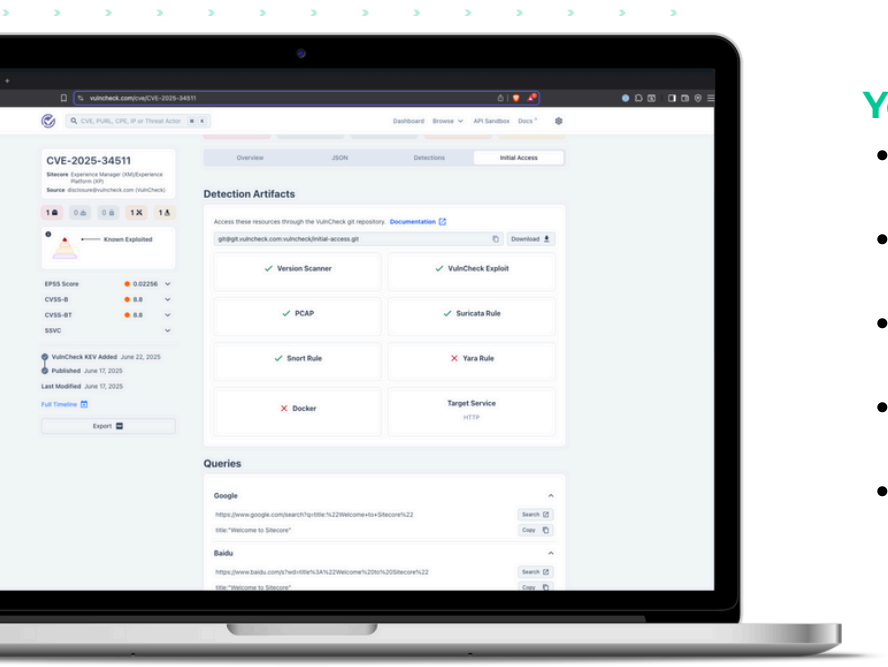
Beat attackers to the punch. Outpace them with VulnCheck.

Actionable, Preemptive Cyber Intelligence

VulnCheck's Initial Access Intelligence (IAI) delivers an early warning system for exploited vulnerabilities AND likely-to-be-exploited in security incidents, focusing strongly on actionable detection, emerging threat response, and active cyber defense. Built for cyber product management, threat hunting, pentesters, red teams, and blue teams, IAI delivers homegrown detection artifacts like exploit PoCs, PCAPs, Snort/Suricata rules, and internet scanning tools, often weeks ahead of NIST NVD or CISA KEV details. VulnCheck empowers proactive defense against remote code execution (RCE) threats and helps stop breaches before they begin.

Initial Access Intelligence for Exploit Visibility and Impact

Identify threat actor targeted and high-risk vulnerabilities before they are exploited in the wild.	Deploy ready-to-use IPS/IDS detections to know if you are being targeted before remediation is available from the vendor.
Enable Blue Teams with in-house built queries for Censys, Shodan, FoFa, and ZoomEye.	Enable pentesters and red teams to validate exploitability with VulnCheck-authored exploits.



Your Problems Solved

- Lack of early warning about vulnerabilities on the brink of exploitation.
- Slow vendor response for detection rules and countermeasures.
- Blindness to how much of your infrastructure is exposed to emerging threats.
- Difficulty creating reliable detection and hunting artifacts during zero-day windows.
- No way to preemptively defend from high-risk and potentially exploitable vulnerabilities.

VulnCheck IAI Features

Detection Artifacts	Identify High-Value Targets	In-house Developed Exploits
Turn intelligence into preemptive defense.	**Understand your risk exposure instantly.**	**Drive active cyber defense.**
• Snort, Suricata and YARA-based detection rules for emerging threat CVEs • Network Packet Captures showing attack signatures of attacks in action on the network • Predictive analysis of vulnerability exploitation for preemptive defense	• Pre-built Censys, Shodan, FoFa, and Zoom Eye queries for emerging threats on potentially vulnerable IP hosts • Accurate CPE mappings and remote version scanning capabilities	• Execute VulnCheck-authored exploits with bypass rules with go-exploit framework to validate that potentially vulnerable hosts are exploitable • Test against vulnerable containerized targets provided by VulnCheck • Identification of 0-Day vulnerabilities to trigger incident response playbooks

VulnCheck IAI Embeds Into Your Workflows and Your Cyber Tooling

Initial Access Intelligence integrates seamlessly integrates into the security tools you already use, delivering real-world exploit artifacts built by industry-leading researchers. Initial Access artifacts are designed for speed. Snort and Suricata rules drop into IDS/IPS systems, PCAPs allow for quick behavior validation, and exploit code makes it easy to replicate behavior in-house for threat hunting. It points to what matters, the real exploit techniques beyond the CVE IDs.

Integrations to Drive Action