

IP Intelligence

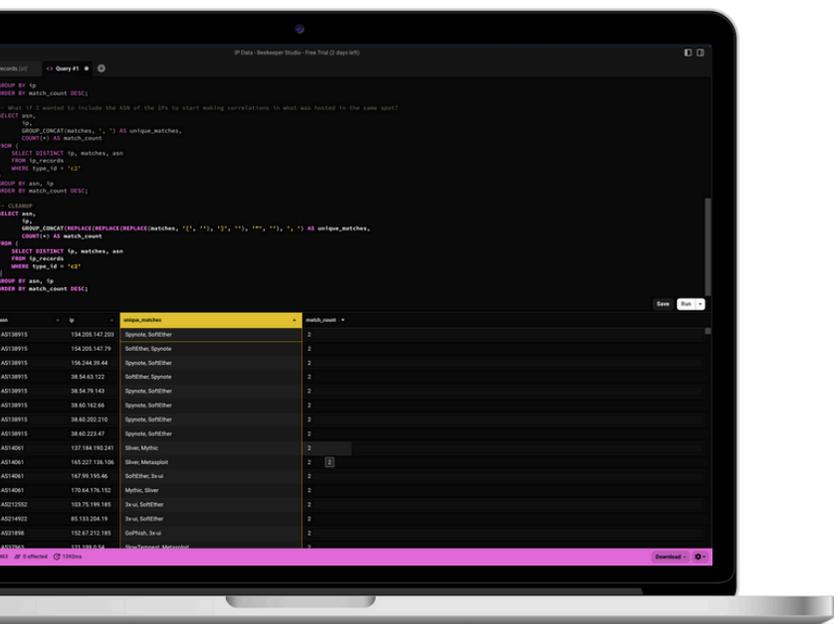
Continuously defend vulnerable assets. Identify attacker infrastructure.

IP Intelligence

VulnCheck's IP Intelligence (IPI) provides cyber defenders and red teams with early warning and deep visibility into active vulnerabilities, hostile infrastructure, and attack exposure. Supporting use cases across early threat detection and scanless vulnerability management (VM), IPI continuously monitors IP addresses and their metadata, maps CVEs to IP hosts, identifies C2 infrastructure, and tracks honeypot deployments. This empowers teams with flexible query and enrichment capabilities. IPI delivers comprehensive threat insights that help security teams stay ahead of adversaries and proactively defend critical assets.

Turn attacker infrastructure into intelligence

Identify and prioritize internet-facing assets vulnerable to exploitation.	Track real-world exploitation risk mapped to active IP addresses.
Detect and block threat actor Command and Control (C2) infrastructure.	Strengthen Proactive DNS (PDNS), ASM, and threat detection initiatives.
Accelerate prioritization, investigation, threat hunting, red teaming, and incident response.	Early warning system for emerging threats and preemptive defense.



Your Problems Solved

- The window between exploit code release and widespread exploitation is shrinking and it increases the risk of exposures exponentially.
- Exposed infrastructure revealed by internet scanners before it's secured.
- Botnets weaponize CVEs through Command and Control nodes that evade detection, driving likelihood of exploitation.
- Alignment of defenses with real-world attacker interests and intent.
- Insufficient proof of active, emerging threats delays vulnerability response.

VulnCheck IPI Features

Vulnerability and Asset Intelligence	Adversary Infrastructure Tracking	Flexible Enrichment and Integration
Continuous CVE mapping to exposed IPs.	Command and Control (C2) detection at scale.	Drive faster detection, investigation, and response.
<ul style="list-style-type: none"> • Maps live internet IPs to hundreds of known vulnerabilities (CVEs) • Prioritizes risks across external assets for attack surface management • Provides 3, 10, 30, and 90-day historical data indices for trending analysis 	<ul style="list-style-type: none"> • Tracks 100+ C2 frameworks and malware infrastructure globally • Updates C2 IPs and hostnames daily for Protective DNS and security platforms • Provides flexible APIs for blocklisting and automated threat protection 	<ul style="list-style-type: none"> • Searchable by IP, CIDR range, hostname, CVE, port, and ASN • Unlimited API access and bulk backup downloads for local analysis • Easy enrichment of PDNS, SIEMs, ASM, and red team operations with detailed metadata

VulnCheck IPI Embeds Into Your Workflows and Cyber Tooling

VulnCheck’s machine-readable and ingestible IP Intelligence fits seamlessly into attack surface management, threat hunting, Protective DNS enforcement, and red team engagements.

Whether enriching SIEM events, enhancing PDNS blocking lists, discovering vulnerable assets, or mapping active C2 infrastructure, VulnChecks IP Intelligence acts as a real-time force multiplier for proactive security teams.

Integrations to Drive Action

