# VulnCheck

# Canary Intelligence
## Capture live exploitation. Confirm real risk.

## Outpace Your Adversaries

| | |
|---|---|
| Outpace adversaries with rich intelligence up to 14 days faster than other solutions. | Improve vulnerability prioritization with contextual intelligence. |
| Accelerate remediation of high-risk vulnerabilities based on evidence of exploitation. | Align vulnerability patching efforts to clear and present threats, not just severity scores. |
| Reduce mean time to detect and respond in real-time. | Drive the smartest and fastest cybersecurity decision possible. |
| Action on data extrapolated from 400+ cyber threat intelligence and internet sources. | Utilize over 4,000,000 CVE records to proactively protect your organization. |

## What is Canary Intelligence?

VulnCheck Canary Intelligence provides exploitation data from globally deployed vulnerable hosts revealing the first signs of vulnerability exploitation and tracking which CVEs are being targeted in the wild, and by whom. VulnCheck Canaries data provides deep insight into vulnerability exploitation attempts, including the detection signatures used, the attackers involved, their locations, the targets location, and the specific methods and payloads used to exploit the vulnerable host. This way, organizations can correlate real attacker activity with threat actor behavior, ransomware families and in-the-wild exploits to enrich VulnCheck's other intelligence solutions and inform cyber response teams with a unique dataset that arms security analysts with rich, targeted intelligence on actively weaponized vulnerabilities so they can prioritize faster, patch smarter, and stay ahead of breaches.

```
{
  "src_ip": "193.26.115.195",
  "src_port": 47922,
  "src_country": "US",
  "dst_country": "BR",
  "cve": "CVE-2025-24893",
  "signature_id": 12700499,
  "signature": "VULNCHECK XWiki CVE-2025-24893 Exploit At
  "category": "Web Application Attack",
  "severity": 1,
  "payload": "R0VUIC94d2lraS9iaW4vZ2V0L01haW4vU29sclNlYXJj
  "http": {
    "url": "/xwiki/bin/get/Main/SolrSearch?media=rss&text
    "http_user_agent": "Mozilla/5.0 (bang2013@atomicmail.
    "protocol": "HTTP/1.1"
  },
  "timestamp": "2025-11-07T07:58:51.064Z"
},
{
  "src_ip": "172.206.196.45",
```

## Your Problems Solved

- See real exploitation first. Get early, verified visibility into emerging threats, days before public sources like CISA KEV.
- Back your decisions with proof. Communicate the risk clearly to customers or executives using factual evidence of active exploitation, and not speculative opinions.
- Track attacker evolution. Observe how exploit chains develop, payload hosting IPs, and infrastructure evolution in real-time.

# VulnCheck

# Canary Intelligence Features

| Verified Exploitation | Actor Infrastructure Insight | Actionable Attack Context |
|---|---|---|
| • Confirms exploitation of vulnerabilities through direct observation of live attacks against real systems.<br><br>• Automatically updates VulnCheck Exploit & Vulnerability Intelligence, Initial Access Intelligence, and IP Intelligence with confirmed exploitation signals.<br><br>• Serves as the only real-time / real-activity early warning system on emerging threats.<br><br>• Maps to MITRE ATT&CK to provide context around exploitation techniques. | • Links attacker IPs, payload hosts, and infrastructure to targeted CVEs.<br><br>• ASN and geolocation data appears when Canary observations are delivered through VulnCheck IP Intelligence.<br><br>• Enables early recognition of coordinated activity and supports threat trend analysis.<br><br>• Correlates across the broader VulnCheck ecosystem to flag vulnerabilities exploited by known threat actors and inform defense strategies with adversary behavior. | • Provides full HTTP requests, methods, user agents, and encoded payloads for enrichment.<br><br>• Offers machine-readable evidence suitable for automation, detection tuning, and incident response.<br><br>• Surfaces exploit and threat intelligence that correlates directly to live attacker behavior for teams to build detections.<br><br>• Extract encoded commands in payloads to view new delivery mechanisms for malicious behavior.<br><br>• Pivot from URLs, file hashes, or domain names within payloads to infrastructure datasets. |

# VulnCheck Canary Intelligence Embeds Into Your Workflows and Cyber Products

Just like all VulnCheck intelligence products, VulnCheck Canary Intelligence is delivered in machine-readable feeds, and can be ingested into existing vulnerability management technologies, workflows, SIEMs, and ticketing systems. This ensures that critical threat data is available where and when it matters - and in real-time, as attacker activity is tracked, validated and correlated with exploit and vulnerability intelligence. VulnCheck intelligence is designed to enrich scoring, alerting, and response actioning to power automation platforms, workflows and playbooks to significantly speed up response times to emerging threats with context and correlation to live exploitation.

# Integrations to Drive Action

Threat Intelligence
Platforms

SBOM Solutions

Firewalls

SIEMs

Business Intelligence
Platforms

Vulnerability
Management Solutions

Ticketing Systems

Applications Security Platforms

Asset Management
Solutions

Remediation & Patch
Management Solutions

servicenow.

ThreatConnect.

THREATQUOTIENT

Filigran

Vertex

CYWARE™

tines

splunk>
a CISCO company