



Threat Intelligence Service

Integrated threat intelligence reveals precisely how vulnerabilities could impact your IT assets.



Solution

The Skybox **Threat Intelligence Service** delivers a comprehensive daily threat intelligence feed. Leverage this aggregated feed to correlate vulnerabilities in your environment with the latest threat intelligence from the Skybox **Research Lab**. The service enriches both security policy management and vulnerability management programs, by providing:

- + **A comprehensive guide to the latest vulnerabilities**
- + **Analysis of the assets in the estate hosting exploitable vulnerabilities**
- + **Evidence of the extent to which each vulnerability is being actively exploited in the wild**
- + **Identification of IPS signature updates that could be used to remediate each vulnerability.**

Benefits

Definitive threat intelligence

Identify vulnerabilities in standard operating systems, browsers, software, databases, firewalls, and network devices using aggregated threat intelligence from over 35 separate sources.

Instantly identify vulnerable assets

Quickly discover which assets in your estate host vulnerabilities currently being exploited and predict the likelihood that a vulnerability will be actively exploited in the future.

Incorporate exploitability in vulnerability prioritization

Current and likely future exploitability analysis from the threat intelligence feed is automatically incorporated into Skybox's multi-factor prioritization, along with an assessment of CVSS severity, the business impact of asset loss, and exposure across the network.

Analyze attack paths

Overlay threat intelligence onto your attack surface map and see how attackers could use network access paths to compromise a vulnerable asset.

Cyber Threat Intelligence Feeds

The service is continuously updated with the latest aggregated information from a wide range of different intelligence feeds, including:

+ Vulnerability Scanners

- Qualys Cloud Platform
- Rapid7 Nexpose
- Tenable Nessus
- Tripwire IP360

+ Vendor Advisories

- Adobe
- Apple
- Check Point
- CloudBees
- Cisco
- F5
- Google Chrome
- Google Android
- IBM
- Microsoft
- Mozilla
- Oracle
- Red Hat
- SAP
- Siemens
- VMware

+ IPS

- Cisco Sourcefire
- HP Tipping-Point
- McAfee IPS
- Palo Alto Networks
- Check Point IPS

+ Databases

- NIST NVD
- Red Hat CVE Database

+ Exploitability Notifications

- Exploit-DB
- AlienVault OTX
- X-Force Exchange

+ Expert Advisories

- CISA Known Exploited Vulnerabilities
- Mitre CVE
- CERT & ICS CERT
- First.org EPSS
- Security researchers via social media
- Vulnerabilities and exploits published in security news sites.



Want to learn more? Get a demo or talk to an expert:

skyboxsecurity.com/request-demo 

ABOUT SKYBOX SECURITY

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. Our Security Posture Management Platform delivers complete visibility, analytics and automation to quickly map, prioritize and remediate vulnerabilities across your organization.