Skybox Security Intelligence

VULNERABILITY AND THREAT INTELLIGENCE FEED FOR ACCURATE PRIORITIZATION AND FAST MITIGATION

To deploy resources in the right place, in the right way, vulnerability management teams need to know the intersection of vulnerabilities, network context and the threat landscape.

The Skybox™ Security Suite brings this understanding to your fingertips thanks to real-time vulnerability and threat intelligence provided by Skybox™ Security. Skybox’s security intelligence is derived from the findings of the Skybox™ Research Lab, our team of security analysts who examine daily more than 30 security data feeds and investigate more than 700,000 sites in the dark web. The team analyzes information on ransomware, malware, exploit kits and targeted attacks, yielding the most accurate intelligence on attacker activity relevant to you.

Skybox uses this intelligence to correlate vulnerabilities in an organization’s environment with those being actively exploited in the wild. Skybox also integrates this intelligence with network security operations — the intelligence feed plays a major role in modeling how network changes could impact your security or compliance status.

How it Works

Skybox Security brings comprehensive and up-to-date vulnerability and threat intelligence to the Skybox Security Suite from data sources such as:

- NVD (National Vulnerability Database)
- Published vulnerability repositories
- Vulnerability scanners
- Threat intelligence feeds and platforms
- Research of more than 700,000 sites in the dark web
- Vendor IPS signature feeds, including Fortinet FortiGuard, McAfee IPS, Palo Alto Networks, Trend Micro TippingPoint and Cisco SourceFire

The Skybox Research Lab then creates a detailed model of all newly published vulnerabilities and matches each vulnerability to its reported IPS signature and other severity information.

Researchers provide information regarding exploitability levels, adding exploitation preconditions and effects, and configuring attack patterns to be used in Skybox’s patented attack simulations.

USES FOR SKYBOX SECURITY INTELLIGENCE

1. **Consolidate** — Get vulnerability and threat intelligence from 30 public and private sources and investigations of 700,000+ sites in the dark web

2. **Model** — Match details of newly published vulnerabilities to IPS signatures and other information on severity, exploits and attack patterns

3. **Enhance** — Augment vulnerability data in your environment with real-time threat intelligence to improve prioritization accuracy

4. **Standardize** — Normalize vulnerabilities to coincide with industry scoring methods and the Skybox™ Vulnerability Index

5. **Inform** — Find references to scanners and plug-in IDs, as well as links to helpful information
Skybox intelligence helps significantly reduce false positives and increases accuracy in attack simulation by adding information such as: details of IPS exploits, vulnerability-based signatures, exploit commonality, severity, platform versions, research sources, malware catalogs and more.

Each vulnerability in the intelligence feed is presented in a standard, normalized format that correlates to industry scoring methods:

- CVE ID (Common Vulnerabilities and Exposures)
- CVSS (Common Vulnerability Scoring System) scores, following V3 standard
- Skybox Vulnerability ID (SBV ID)

The vulnerability descriptions also include references to scanners and plug-in IDs, links to relevant sources that describe the vulnerabilities, affected platforms and versions, external product catalogs, and vendor-suggested solutions.

Roles in the Skybox Security Suite

The entire portfolio of Skybox products relies on the Skybox intelligence feed for vulnerability and threat management, firewall and change management and attack surface visualization.

**VULNERABILITY CONTROL**

*Skybox™ Vulnerability Control* harnesses the intelligence feed for the most accurate vulnerability assessment, prioritization and remediation planning. Its scanless vulnerability assessment feature uses the feed to extract vulnerabilities from data repositories in the network, providing on-demand information on your vulnerabilities.

Vulnerabilities are then examined in the context of asset exposure and criticality, as well as intelligence on exploit availability and use in the wild. Exposed vulnerabilities and those being actively exploited are targeted for immediate remediation, dramatically reducing the risk of attack. Other vulnerabilities are slated for gradual risk reduction; Skybox monitors these vulnerabilities to ensure their threat level doesn’t escalate as the threat landscape changes.

Skybox intelligence informs vulnerability management teams about remediation options such as available patches or IPS signatures. This up-to-date information is key to focusing resources where they’re needed most so actions are efficient and effective.

**THREAT MANAGER**

*Skybox™ Threat Manager* uses the feed to consolidate a wide range of threat intelligence sources and vendor security advisories, analyzing and prioritizing threat intelligence in the context of the attack surface.

Detailed threat impact analysis and remediation guidance enables rapid response to critical threats in minutes. With Skybox security intelligence, Threat Manager optimizes threat remediation tasks with built-in workflows and automated status tracking tools to increase efficiency and ensure threats are neutralized.

**HORIZON**

The attack surface visualization solution, *Skybox™ Horizon*, utilizes security intelligence data to show where an organization is most vulnerable to attack. Horizon pinpoints vulnerabilities with publicly available exploits and those actively exploited in the wild, based on the real-time threat intelligence provided by the feed.
Horizon visually displays these vulnerabilities in an interactive model of the attack surface. Security leaders can quickly see where vulnerabilities exist in the network, what are the surrounding security controls (or lack thereof) and what risk level they pose. Combined attack surface visibility and vulnerability and threat intelligence gives organizations the power to take proactive action against the biggest threats in their network.

**NETWORK ASSURANCE**

In Skybox™ Network Assurance, security intelligence data is used to find and view vulnerabilities at the host level during network path analyses. By identifying vulnerabilities associated with a specific host while troubleshooting access, network security managers have immediate knowledge of any possible exposure if a new network path is opened. The proactive risk assessment of the proposed connectivity request or network change helps to reduce exposures to attacks even as your network evolves.

**FIREWALL ASSURANCE**

The Skybox intelligence feed enables Skybox™ Firewall Assurance to analyze IPS signatures, providing visibility into the security controls and their effectiveness within the network.

Firewall Assurance analyzes and reports on the IPS signature functionality integrated within next-generation firewalls, helping quickly determine several items, such as: Is the IPS signature in prevention or detection mode? Which IPS signatures cover current vulnerabilities in the organization? And, which signatures cover recent threats? Firewall Assurance also provides recommendations to tune each IPS signature for increased performance and greater coverage, maximizing the IPS feature’s ability to mitigate risk.

Additionally, the security intelligence data is required for performing scanless vulnerability detection on Skybox–supported firewalls, including Juniper ScreenOS, Juniper JunOS, Cisco ASA/FWSM and Check Point.

**CHANGE MANAGER**

Skybox™ Change Manager correlates security intelligence with vulnerability assessment data from third-party scanners and Vulnerability Control’s scanless assessments. Armed with this data, Change Manager spots potential security or compliance impacts of vulnerabilities that would be exposed by a proposed change.

By integrating security intelligence with Change Manager’s automated workflows, IT security teams can be sure they have the needed context to quickly determine the risk of a proposed change. The result is fast, secure and compliant changes, greatly reducing the chance of error and the need for rework.

**About Skybox Security**

Skybox arms security leaders with the broadest set of solutions for security operations, analytics and reporting. The Skybox Security Suite integrates with 100+ technologies and uses network modeling, attack vector analytics and multi-factor vulnerability assessment to give unprecedented visibility of the attack surface and key indicators of exposure (IOEs). This gives security leaders the insight needed for effective, threat-centric vulnerability management and automated firewall and security policy management across physical, virtual and cloud networks.