SKYBOX SECURITY

Attack surface visibility for critical infrastructure

Visualize your complete attack surface across converged IT/OT estates. Reduce cyber risk and eliminate security blind spots through a unified view of assets and vulnerabilities across the IT/OT attack continuum.

Challenges

Our nation's critical infrastructure including food, water, and energy supplies is increasingly under attack by malicious threat actors. These attacks have disrupted civic life and, in extreme cases, even threatened our survival. Yet, the risk is vastly underestimated. In a recent study, **83% of organizations surveyed acknowledged that they had at least one OT security breach within the past 36 months, though 73% of CISOs and CIOs believed their security postures to be strong.**[1]

You cannot protect what you cannot see. Asset visibility is foundational for managing a modern enterprise's attack surface that spans IT, cloud-native, hybrid cloud, and OT environments. It is the starting point for many cybersecurity exercises, from proactive activities such as cyber risk quantification, penetration testing (red, blue, and purple team drills), and breach-readiness tabletop exercises – to reactive but business-critical projects around incident response and zero-day vulnerability management.

Use cases

- **Unified view of IT and OT assets and vulnerabilities**
- **Network model combines infrastructure context and threat intelligence**
- **Scanless detection that augments active scanning in sensitive OT environments**
- **Nuanced, multi-factor asset and vulnerability risk scoring and prioritization**

[1] Cybersecurity risk significantly underestimated by OT organizations, Skybox Security, November 2021

Visibility into an organization's vulnerabilities is equally important. Software vulnerabilities are the root causes of breaches and attacks. For example, the CVE-2017-0144 SMB v2 vulnerability was weaponized in the EternalBlue exploit, was then utilized in the NotPetya ransomware attack that resulted in more than $200m in financial damages for Maersk2. Vulnerability management is a proactive exercise and, if executed effectively, it can reduce an organization's spend on reactive technologies such as threat hunting or breach detection and response.

Asset and vulnerability visibility, though, is a problem that is particularly acute for organizations that manage OT environments and critical infrastructure. While IT/OT convergence has produced an attack continuum, security practitioners are grappling with visibility tool sets that offer limited interoperability and integration. A comprehensive single-pane-of-glass view of assets that can increase attack surface visibility is missing.

Solution

The Skybox Security Posture Management Platform unlocks unprecedented visibility of assets, vulnerabilities, and exposures spanning the entire Purdue Enterprise Reference Architecture (PERA). Atomic visibility of assets and vulnerabilities in field, control, and process levels of PERA is facilitated by a portfolio of integrations with specialized OT scanning vendors.

Infrastructure modeling

The platform creates an abstraction of the corporate infrastructure by ingesting and normalizing configurations and routing information from networking and security devices, public and private clouds, configurations, assets, patch management repositories, and much more. These data sets are correlated with vulnerability definitions and threat intelligence from multiple sources. The model uniquely combines infrastructure context with threat intelligence and helps administrators visualize the entire network topology, including zones and locations, network path connectivity, and access rules that govern the converged infrastructure. Specialized devices custom-built for supporting industrial applications and hazardous environments, such as the Siemens Rugged.com 1400 and 1500 family of intelligent edge routers are supported in the model.

Configuration hygiene checks

The Skybox platform exposes cyber hygiene blind spots by comparing network and security configuration settings with out-of-the-box or easily customizable configuration policies. This leads to easy identification and speedy remediation of misconfigurations or control gaps such as the use of default passwords on routers, switches, and firewalls or the use of Telnet instead of SSH for device administration. The platform also ensures overall compliance with STIG, MITRE ATT&CK framework, CIS benchmarks, IEC 62443, or industry best practices.

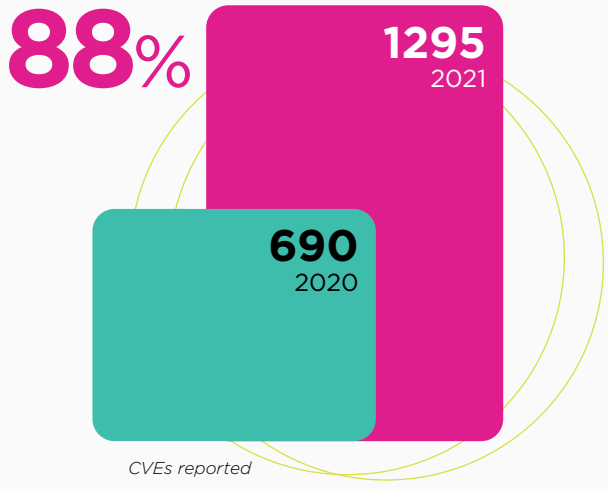
Asset and vulnerability information collection

The Skybox platform employs multiple techniques for ingesting asset and vulnerability information3 from active scan-based vulnerability asset tools, endpoint detection and response solutions, OT passive scanning solutions, and various asset data repositories. The result is a single-pane-of-glass view of assets and vulnerabilities across IT and OT environments. Through this process, the platform enables the identification of cyber hygiene gaps such as insecure operations, older operating systems, assets lacking up-to-date patches.

Scanless vulnerability discovery

Scanless detection expands coverage by correlating asset information from generic configuration management database (CMDB) parsers and patch management repositories with updated vulnerability data from Skybox threat intelligence. The result is continuous non-intrusive discovery on routers, switches, firewalls, and non-scannable assets. Gaps between active scan events on scannable assets are also filled. This critical capability reduces dependence on intrusive processes such as active scanning, that can increase downtime risks in sensitive OT environments.

New OT vulnerabilities increased[2]



[2] Vulnerability and threat trends report 2022, Skybox Security

Multi-factor risk scoring and prioritization

Prioritization of vulnerabilities using the static CVE-based ranking system can leave large organizations struggling under crushing operational workloads as they pore over millions of vulnerability occurrences that are captured in manual spreadsheets. The Skybox platform uses a flexible and customizable algorithm to compute risk scores for assets and vulnerability occurrences based on the following factors:

+ **Asset importance** is based on an asset's value to the enterprise and allows prioritization of mission-critical OT devices.
+ **Attack path analysis** identifies the reachability of a target from potential threat origins.
+ **Exploitability** is based on Skybox threat intelligence which flags vulnerabilities that are exploited in the wild or that have available exploits.
+ **A CVSS score** that is assigned by the US National Vulnerability Database (NVD) and affiliated bodies.

Capabilities that differentiate the Skybox platform include:

+ The ability to support modern quantitative approaches to cyber risk management by expressing the Maximum Impact (the highest possible economic impact of an asset's loss, usually based on its replacement cost) and the Risk Exposure (the likely Value-at-Risk or VaR, usually derived by combining Maximum Impact with the Asset Risk Score as calculated above) in monetary units.
+ A deeper understanding of a vulnerability's exploitability that is based on its association with malware names and malware types. The result – the platform becomes a single source of truth for both vulnerability management and threat hunting teams in understanding how vulnerability remediation can retire threat debt.
+ Granular details from attack path analysis beyond the binary verdicts of accessibility or inaccessibility (*see Figure: 1 below*).
+ Formula flexibility, so that each organization can control the risk factors to be included in the algorithm, as well as the weight for each factor, resulting in a tailored risk posture that is defined by an organization's business logic.

Outputs from attack path analysis

Direct exposure	One or more attackers have a direct network path to the vulnerable asset.
Presumed direct exposure	One or more attackers have a direct network path to the vulnerable asset but it cannot be verified if the service port on the asset is listening for incoming connections.
Indirect exposure	The assets can be exploited through lateral movement from other exploited assets.
Potential exposure	The vulnerability can be accessed but requires additional authentication on the asset to be exploited.
Protected	The vulnerability is protected by an IPS signature.
Inaccessible	The vulnerability is not accessible over the network.

Figure: 1

Dashboards and reports

The Skybox platform enables extensive reporting through customizable out-of-the-box dashboards and reports. Prebuilt templates allow administrators to query underlying Elasticsearch clusters quickly and intuitively for numerous attributes. Assets and vulnerabilities can be grouped by business units, so business owners can focus their efforts on remediation within the SLA. Some useful reports for continuous trend analysis and program benchmarking include:

+ Remediation within the SLA of vulnerabilities with high-risk scores
+ Decrease in scan frequency
+ Assets with overdue scan status
+ Increase in high-risk vulnerability occurrences or exposed vulnerabilities

Benefits

- **Full visibility of IT and OT assets and vulnerabilities across PERA**
- **Common vernacular for expressing risk across converged enterprise**
- **A single source of truth for vulnerability management and threat hunting teams**
- **Reduce downtime risks in sensitive OT environments with scanless detection**
- **Support of quantitative models for cyber risk modeling**
- **Robust attack path analysis capabilities – beyond binary verdicts**
- **Avoid unplanned downtime resulting from cyber attacks**

Contact an expert

Schedule a 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.