Vulnerability lifecycle management for critical infrastructure

Automate the vulnerability management lifecycle based on infrastructure context and threat intelligence to de-risk your OT environment

Challenges

New vulnerabilities in operational technology (OT) products have risen 88% year over year, from 690 in 2020 to 1,295 in 2021[1]. This increase in vulnerabilities can be attributed to vulnerability debt, "the often known, non-critical vulnerabilities that are ignored or rather accepted temporarily so that products are shipped faster"[2] as well as a culture of greater transparency among product manufacturers. In addition to vulnerabilities on OT products, those on IT assets such as servers and workstations can also be weaponized to enable attack paths. In light of this, vulnerability management teams must discover and remediate both IT and OT vulnerabilities to protect critical OT assets. In parallel, the cyber security talent gap has resulted in small teams struggling with complex manual vulnerability management workflows. The resource problem can be rectified by automating operational workflows across the four pillars of vulnerability lifecycle management: discovery, prioritization, remediation, and reporting.

Full-lifecycle protection

- Collection of asset and vulnerability data
- Skybox scanless vulnerability discovery
- Correlation with threat intelligence
- Context-aware exposure and attack path analysis
- Multi-factor risk scoring and prioritization
- Remediation and mitigation workflows
- Dashboards and reports

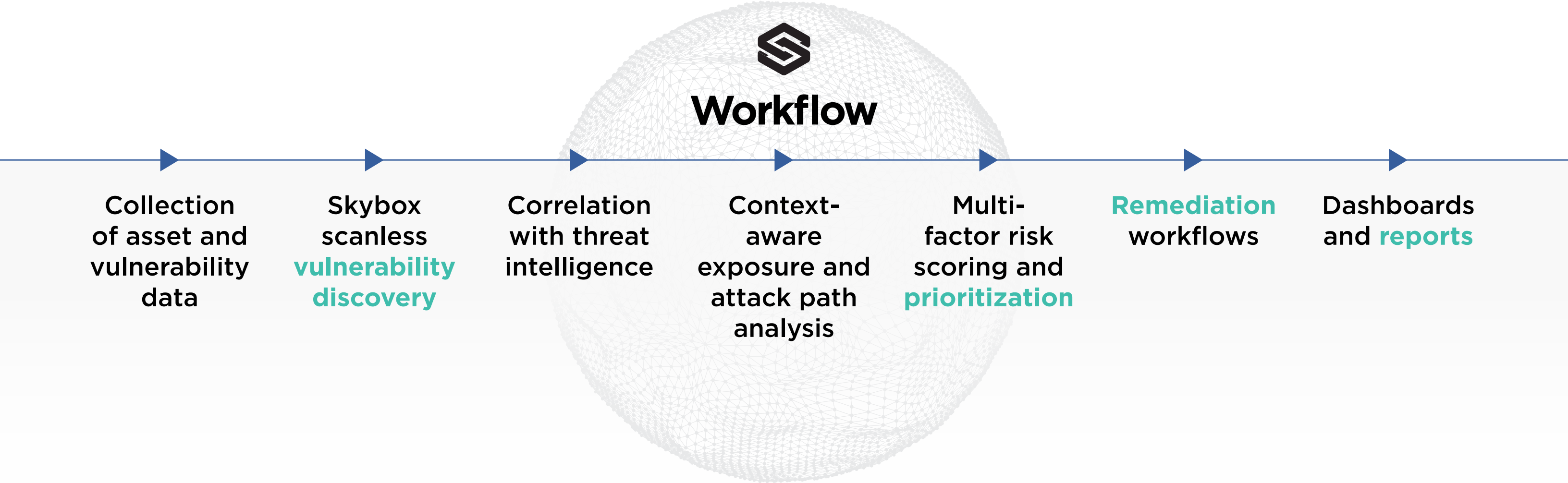
[1] Vulnerability and threat trends report 2022, Skybox Security, April 2022
[2] The vulnerability debt in product security, Forbes, September 2021

Each vulnerability lifecycle pillar poses unique operational challenges:

- **Discovery** - Non-scannable assets, blind spots created by time gaps between active spans, and lack of visibility tools that can encompass both IT and OT environments, result in fragmented visibility of IT and OT estates.
- **Prioritization** – High volumes of critical or high severity CVEs accelerates alert fatigue in already overwhelmed VM teams grappling with spreadsheets and manual analysis, while the most harmful vulnerabilities can remain unaddressed.
- **Remediation** – To avoid unplanned downtime of OT devices, less intrusive approaches to risk mitigation are needed to complement patching and software updates.
- **Reporting** – Lack of consistent, automated dashboards and reports limit confidence in vulnerability management program efficacy, reducing the likelihood of additional investments in the program.

Solution

The Skybox Platform helps customers solve these challenges through a combination of context-driven automation and actionable threat intelligence.


Workflow
Collection of asset and vulnerability data
Skybox scanless vulnerability discovery
Correlation with threat intelligence
Context-aware exposure and attack path analysis
Multi-factor risk scoring and prioritization
Remediation workflows
Dashboards and reports

Vulnerability discovery

The Skybox Security Posture Management Platform ingests and normalizes asset and vulnerability information from multiple sources[3], including active scan-based Vulnerability Assessment tools, Endpoint Detection and Response systems, OT passive scanning solutions, and various asset data repositories.

In addition to vulnerabilities, security risks such as outdated OS versions, or insecure applications and services can be flagged for easy remediation. In parallel, scanless detection expands coverage by correlating asset information from generic CMDB parsers and patch management repositories with

[3] Skybox Device Support Table, skyboxsecurity.com

updated vulnerability data from Skybox threat intelligence. The result is continuous non-intrusive vulnerability discovery on non-scannable assets (routers, switches, and sensitive OT devices) as well as filling in the gaps between active scan events on scannable assets. This comprehensive catalog of IT and OT assets and vulnerability information spans layers 0-5 of the Purdue model and becomes a single source of truth that multiple enterprise security teams can cross-reference.

Prioritization

Skybox uses a flexible and customizable algorithm to compute risk scores for assets and vulnerability occurrences (a specific instance of a vulnerability on an asset). By default, the framework uses four-key criteria or risk factors. The risk scoring algorithm supports formula flexibility such that each organization can control the risk factors to be included in the formula, as well as the weight for each factor. This approach facilitates a tailored risk posture based on an organization's business logic.

CVSS scores: assigned by NVD and affiliated bodies

Exploitability: based on Skybox threat intelligence, flagging vulnerabilities that are exploited in the wild or have exploits available

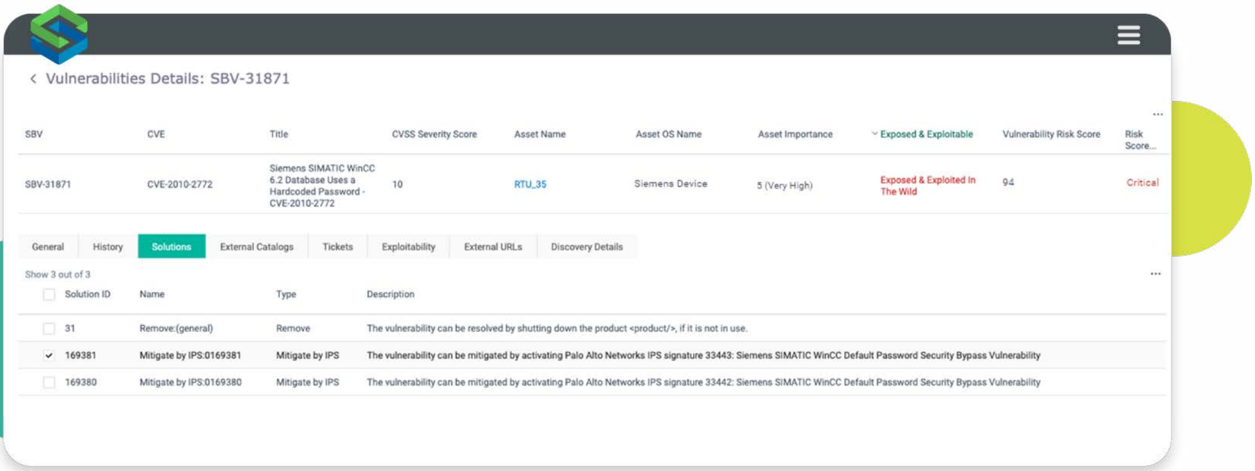
Asset importance: based on the value of an asset to an enterprise and allowing prioritization of mission-critical OT devices

Exposure: based on attack path analysis to identify the reachability of a target from potential threat origins

Remediation

The Skybox Platform, based on contextual analysis of IT, multi-cloud, and OT environments, can recommend diverse remediation solutions including patching, software updates, firewall rule modification, IPS signature, and network segmentation.

Strict system availability requirements for Industrial Control Systems and often remote locations for OT sensing devices mean potentially disruptive processes like patching require careful planning. Network-based remediation solutions can fortify security controls while relieving the urgency around patch application, buying VM teams much-needed time for planning, testing, and deploying patches.



‹ Vulnerabilities Details: SBV-31871

SBV	CVE	Title	CVSS Severity Score	Asset Name	Asset OS Name	Asset Importance	Exposed & Exploitable	Vulnerability Risk Score	Risk Score...
SBV-31871	CVE-2010-2772	Siemens SIMATIC WinCC 6.2 Database Uses a Hardcoded Password - CVE-2010-2772	10	RTU_35	Siemens Device	5 (Very High)	Exposed & Exploited In The Wild	94	Critical

Show 3 out of 3

	Solution ID	Name	Type	Description
□	31	Remove:(general)	Remove	The vulnerability can be resolved by shutting down the product <product/>, if it is not in use.
✓	169381	Mitigate by IPS:0169381	Mitigate by IPS	The vulnerability can be mitigated by activating Palo Alto Networks IPS signature 33443: Siemens SIMATIC WinCC Default Password Security Bypass Vulnerability
□	169380	Mitigate by IPS:0169380	Mitigate by IPS	The vulnerability can be mitigated by activating Palo Alto Networks IPS signature 33442: Siemens SIMATIC WinCC Default Password Security Bypass Vulnerability

Network-based remediation options supplement patching

[3] White House National Security Memorandum on improving cyber security for Critical Infrastructure control systems, 2021

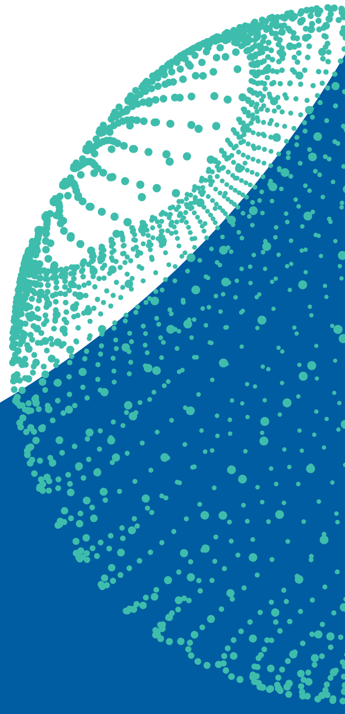
Reporting

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 a wide range of asset and vulnerability attributes. Assets can be grouped by business units for granular visibility by each business owner. Some useful reports for continuous trend analysis and program benchmarking include:

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

Benefits

- **Unified view of IT and OT assets and vulnerabilities**
- **Unique scanless detection technique reducing active scanning blind spots**
- **Identification of cyber hygiene gaps like insecure OS and applications**
- **Customizable, multi-factor risk scoring framework**
- **Reduced dependence on patching for immediate threat mitigation**



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.