SKYBOX SECURITY

De-risk IT/OT convergence with Skybox Security®

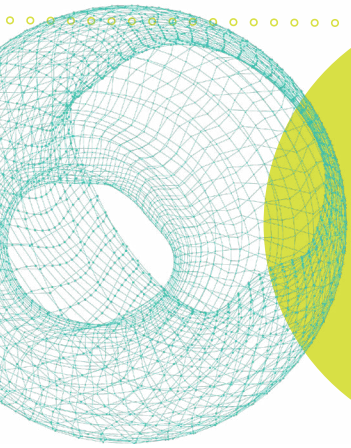
Achieve a unified view of IT and OT infrastructure, prioritize vulnerability remediation based on risk, and comply with evolving CIP regulations

Challenges

Historically, operational technology (OT) infrastructures were comprised of highly specialized proprietary devices with long lifespans that meet real-time or near real-time performance requirements and were often deployed in remote locations. Equipment malfunctions can result in tragedy; consequently, the benefits of adopting innovation must be judiciously balanced against Health, Safety, and Environment (HSE) concerns. For this reason, industrial automation equipment and critical infrastructure were traditionally "air-gapped" or not connected to the public internet.

Risk factors

- **Specialized devices with long lifespans**
- **Previously isolated "air-gapped" systems now connected and accessible**
- **Software obsolescence and difficulty in patching devices**
- **Cybersecurity talent gap**
- **Overarching Health, Safety, & Environment (HSE) concerns**
- **Fragmented visibility of IT and OT assets and vulnerabilities**
- **Compliance with increasingly stringent CIP regulatory standards**



The exploitation of IT and OT vulnerabilities represented

40%

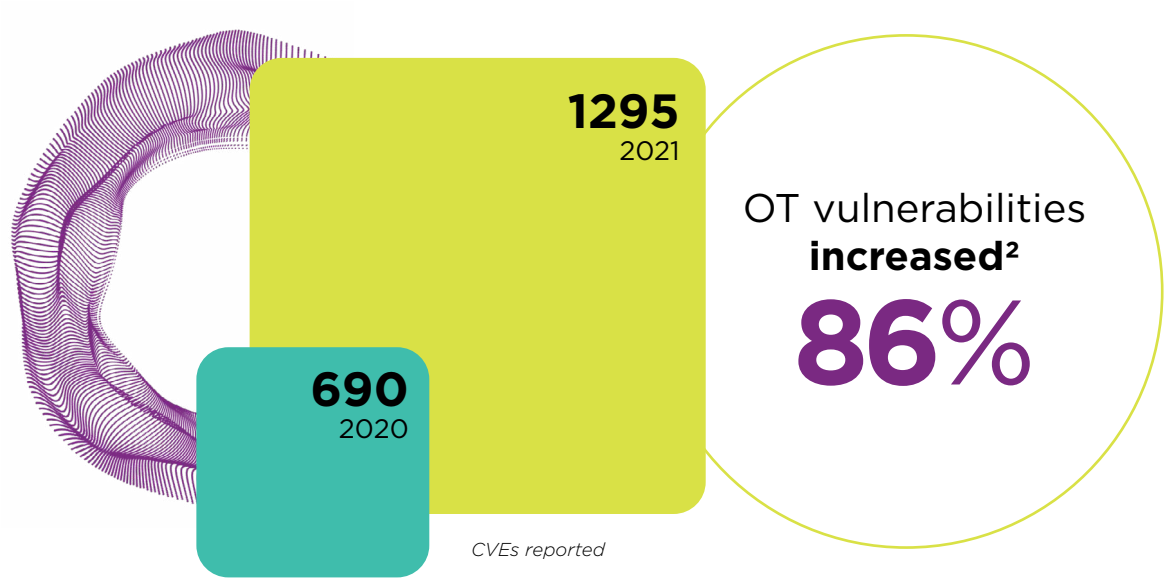
of initial infection vectors for attacks on organizations connected to OT networks[1]

[1] Attacks on operational technology from IBM X-Force and Dragos Data, 2020

Challenges

However, over recent years, tangible benefits of IT/OT convergence have catalyzed a new hyperconnected Industrial Internet of Things (IIoT) realm. Increasingly OT sensing devices are connected to the network and thus exposed to a broad array of cyber-attacks, proving the existence of an IT/OT attack continuum. Further, device longevity and deployment in remote locations increase the likelihood of software obsolescence and unpatched vulnerabilities. A simple patching procedure may require complex change management processes due to the risk of equipment downtime or unforeseen hazards. The cybersecurity talent gap, particularly a lack of specialized IT/OT architecture expertise, compounds the challenges.

Explosive growth in OT system vulnerabilities is helping cybercriminals compromise industrial control systems and critical infrastructure. In parallel, IT environments can also enable pathways for threat actors to reach OT assets. Studies of attacks with OT targets demonstrate a common pattern with IT vulnerability exploitation often acting as initial infection or propagation vectors. Practitioners struggle to view the complete attack surface or effectively address the riskiest vulnerabilities threatening the converged infrastructure.



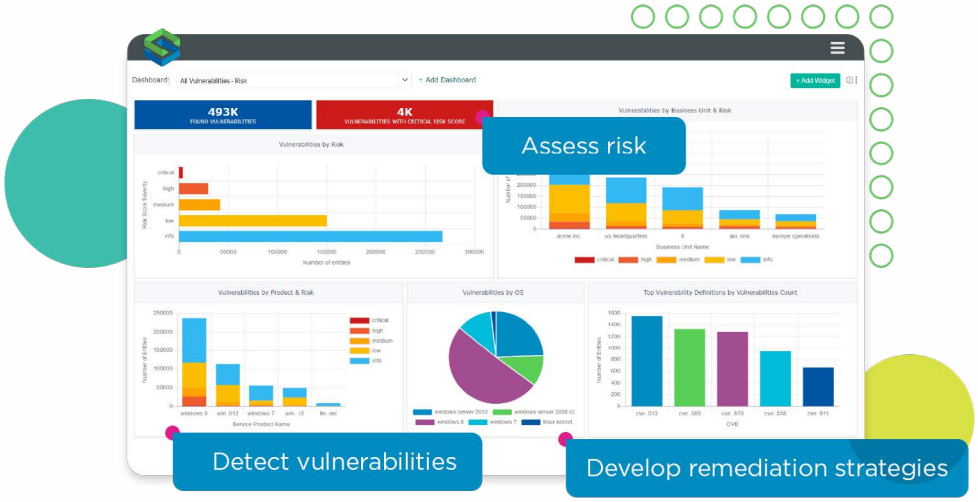
Additionally, organizations must demonstrate compliance with evolving regulatory standards and guidelines for Critical Infrastructure Protection such as NERC CIP, ISA/IEC 62443, the Australian Critical Infrastructure Bill of 2021, or the Biden administration's Industrial Control Systems Security Initiative. Due to acute cybersecurity talent shortage, small teams have to manage the daunting tasks of compliance and audit readiness in large complex converged environments, severely taxing their resources.

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

Solution

We cannot address threats we cannot see.[3] The cornerstone of an effective cyber security strategy is a comprehensive inventory of assets and vulnerabilities spanning IT and OT estates, across levels 0-5 of the Purdue Enterprise Reference Architecture. This view must aggregate asset and vulnerability information from active scanning solutions such as traditional VA scanners, specialized passive scanning-based OT security platforms, and unique scanless detection techniques, powered by Skybox technology.

A vulnerability lifecycle-based approach encompasses automated workflows for discovery, prioritization, remediation, and reporting. The sheer volume of vulnerabilities marked critical or high severity based on CVSS scores can increase alert fatigue for overworked vulnerability management analysts, leading to breaches from missed alerts. Asset importance, vulnerability exploitability (based on threat intelligence) and asset exposure (based on context-driven network analytics) are more accurate indicators of risk than CVSS scores. Multi-factor risk prioritization algorithms separate the signal from the noise, ensuring that the riskiest vulnerabilities are remediated quickly. As patching is often not feasible due to downtime and process interruption, a defense-in-depth approach requires network-based remediation solutions that reduce dependency on patching. Granular dashboards and flexible reports track program efficacy over time, including remediation performance against SLAs.



Threat intelligence, combined with context from the converged IT/OT infrastructure can automate operational workflows for network segmentation, access and configuration compliance and vulnerability assessment. This approach enables regulated entities to demonstrate continuous compliance with evolving CIP regulatory standards. Network segmentation and access analysis capabilities help organize the network into zones and conduits as mandated by ISA/IEC 62443. The Configuration Change Management and Vulnerability Assessment Standard of NERC CIP 010 recommends an annual risk assessment covering network path analysis, business justification for enabled ports and services, and configuration checks.

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

Why Skybox?

Infrastructure context from the network model

The Skybox network model is an abstraction of the converged infrastructure that provides crucial context and visibility, allowing relatively small teams to manage complex heterogeneous environments. Teams use automated workflows to flag and fix rule, access, or configuration violations against policies mapped to CIP regulatory standards, accomplishing in minutes or hours what previously took days.

Exposure analysis based on attack simulation

Attack simulation against the Skybox network model classifies assets and vulnerabilities by their level of exposure to potential threat origins. Besides exposure, the Skybox risk scoring algorithm also factors in CVSS value, exploitability (based on Skybox threat intelligence), and asset importance. Weights assigned to each factor can be customized, resulting in a risk posture uniquely tailored to a customer's business needs.

Non-intrusive methods for discovery and remediation

Strict uptime requirements render OT systems sensitive to intrusive processes such as active scanning and patching. Unique scanless detection technology from Skybox correlates asset information from CMDB parsers and patch management repositories with vulnerability information from Skybox threat intelligence for continuous, low-risk vulnerability discovery between active scan events. Network based remediation solutions such as IPS signatures, firewall rule modification, or network segmentation reduce the dependence on patches and software updates.

Outcomes

+ Easier to comply with relevant CIP standards
+ Unified view of IT and OT assets and vulnerabilities
+ Vulnerability prioritization based on exposure analysis and threat intelligence
+ Network-based vulnerability remediation solutions for reduced patching dependence
+ Cyber resiliency through context-driven network and path analysis

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.