Securing the future of energy

Vulnerabilities for utility organizations are proliferating at an unprecedented rate and the convergence of operational technology (OT) and information technology (IT) has produced a far larger attack surface with greater risk.

87%

of utilities suffered OT breaches in prior 36 months[1]

Cybersecurity risk underestimated by operational technology organizations - Skybox Security, November 2021

86%

increase in OT vulnerabilities between 2020 and 2021

Vulnerability and threat trends report 2022, Skybox Security

Without complete network visibility of the OT/IT attack surface, teams cannot see misconfigurations, understand vulnerability exposure, identify access policy violations, tackle weak security controls, and improve change management capabilities.

5 steps to de-risk OT/IT convergence in utility sector

1 Create mature, consistent, and enterprise-wide security posture management

- Deploy a program with visibility and context across both OT/IT environments. This enables utility leaders to reduce exposure to risk by optimizing security planning, deployment and remediation processes.

2 Apply automation to reduce risk of misconfiguration and ensure continuous compliance

- Automating workflows, including change processes and validation, eliminates human errors and streamlines operations, reducing the risk of misconfigurations.

3 Create a common view across security, OT/IT

- Have a visualization of all environments, both in their enterprise-wide context and with specific rules and configurations by applying a network model, so you can run assessments and simulations against all devices, vulnerabilities, and configurations.
- Leverage the network model to assess the effectiveness of security controls. Gauge access compliance with network segmentation requirements, validate configurations and changes, and identify and precisely measure their exposure.

4 Eliminate silos and remove security blind spots

- See everything by collecting and aggregating data from scanners, security, network infrastructure, configuration databases, and non-scannable assets to fill in blind spots and detect vulnerabilities in off-limits network zones and devices.

5 Reduce downtime by optimizing remediation options beyond patching

- Calculate risk scores for assets by factoring together four critical variables: the asset's measured Common Vulnerability Scoring System (CVSS) severity; asset exploitability; asset importance; and asset exposure based on the security controls and configurations in place across the network.
- Use exposure analysis to determine which vulnerabilities would be most costly if compromised.

Success stories

Gas provider gains complete picture of its security posture across OT/IT networks

View here

Energy company detects 3X more cybersecurity vulnerabilities

View here

Gas and electric provider monitors OT network to analyze network access compliance

View here

How Skybox can help

1 Discover what is on your network. You can't defend what you can't see.

2 Validate controls. Work with network teams to identify how systems connect and use Skybox to validate your understanding of segmentation, ascertaining which areas should and should not talk to each other.

3 Prioritize vulnerabilities and work out a plan of action. Decide which vulnerabilities can be addressed now and which should be scheduled for the next maintenance window.

Benefits

1 Materially drive down risk. Shield critical infrastructure and validate segmentation.

2 Demonstrate value of security program. Validate the outcomes to justify security effort and spend.

3 Remediate faster. Don't wait for next maintenance window. Address priority vulnerabilities now.

Complete visibility

At Skybox, we understand the transformative challenges the utilities industry faces. And we're experts when it comes to security visibility, analytics, and automation. To find out how we can help meet your challenges, lets connect.

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

skyboxsecurity.com/request-demo

SKYBOX SECURITY

[1] Cybersecurity risk underestimated by operational technology organizations, Skybox Security, November 2021