SafeBreach

QUICK READ

Increasing Resilience in Integrated IT/OT Environments with Breach & Attack Simulation

Key considerations for validating security controls in converged OT/IT environments

SAFEBREACH.COM

The Changing Landscape of IT/OT

For years, industrial asset owners didn't consider their operational technology (OT) environment to be a significant security risk. But, due to extensive digital transformation initiatives, enterprises in verticals like power and energy; oil and gas; healthcare; and manufacturing now have deeply integrated IT/OT environments whose centralized security ownership falls under the CISO due to increased cyber risk factors.

As a result, security teams must address not only the vulnerabilities within the OT environment itself, but the ways in which adversaries compromise and traverse the IT network to gather information and gain access to OT control and safety systems. This brief, informational guide aims to address the challenges, best practices, and key considerations for validating security controls in converged OT/IT environments.

Industrial organizations have seen an 87% year-over-year increase in ransomware attacks.

Key Challenges Driving Increased Cyber Risk for Industrial Asset Owners

Increased Attack Surface

As operational environments became more highly networked to optimize efficiencies and facilitate data sharing across the enterprise and with third parties, the attack surface expanded. The OT network, which had traditionally been "air-gapped," was now connected to the enterprise business networks and the outside world. This convergence increased OT's vulnerability to "spill-over" from attacks originating in the enterprise's IT environment.

Less Stringent Security Measures in OT Environments

Historically, operations teams have managed OT assets due to concerns that software updates and configuration changes could put uptime at risk. Engineering workstations and HMIs running commercial OSs like Windows and Linux contained known vulnerabilities, but were not patched and updated diligently for fear that they would either jeopardize production schedules or create ongoing disruption.

Shifting Ownership & Lack of Visibility

As digital transformation has broken down IT-OT barriers, industrial enterprises now have deeply integrated IT/OT environments and security teams are often responsible for managing cyber risk across this extended network. However, because operations teams generally managed all OT assets, IT and security teams had poor visibility into that environment and could not implement—and consistently update—appropriate security controls.

CLICK HERE TO READ OUR BLOG POST:
How to Bring IT & OT Security Together

Understanding Vulnerabilities across a Combined IT/OT Environment

Attacking an OT network is a complex undertaking. A sophisticated adversary who is motivated to disrupt or modify an industrial process will need to maintain access to their targeted environment for enough time to collect intelligence, navigate to the OT control systems, and execute the final objective. Because of this, most OT attacks begin by compromising the IT network. Attackers will often launch a spear phishing campaign targeting employees (or vendors in the target's supply-chain) who are likely to have login credentials or information related to the operational environment.

Once a spear phishing target is tricked into clicking on a malicious link or attachment and the adversary establishes remote access to their workstation, the reconnaissance stage begins. The adversary will attempt to learn about the target's control processes and network mapping to formulate the attack, figure out how to pivot to the OT systems and bypass security controls. Once enough intelligence is gathered to formulate the attack plan, the attacker moves forward to their final objective.

It is critical in any OT security strategy to think of the IT and OT networks as two pieces of the same puzzle. Security teams must address the vulnerabilities within the OT environment itself, in addition to the ways adversaries could compromise and traverse the IT network to gather information and gain lateral access to deeper OT control and safety systems.

Several high-profile OT cyber attacks—like Triton, BlackEnergy, and Industroyer—began with incursion through the IT network.

CLICK HERE TO WATCH THE WEBINAR:

Validating Security Controls in an Integrated IT/OT Environment

Leveraging BAS to Validate Security Controls & Improve Visibility in a Combined IT/OT Architecture

Security teams are increasingly using breach and attack simulation (BAS) technologies to gain visibility into what the attack surface of their combined IT/OT environment looks like—across the IT network, through the OT demilitarized zone (DMZ) and the critical OT operations control layer. A BAS platform enables security red teams to continuously run simulated attacks based on the tactics, techniques, and procedures (TTPs) used by malicious actors to help validate security controls, identify vulnerable attack paths, and prioritize and expedite remediation.

These simulations—which are run on clones of production systems so as not to put the OT network at risk of disruption—can be executed on an automated and continuous basis to measure risk in real-time and identify drift over time. This is particularly relevant for OT asset owners, as a recent KPMG survey indicated 80% of industrial organizations only run an industrial control system (ICS) security assessment once per year or less.

How BAS Supports TSA Requirements for Enhancing Cyber Resilience

The requirements in the TSA's SD-02DA are another great example of where a comprehensive BAS platform can be helpful in establishing and maintaining compliance, not only by validating TSA-mandated security controls, but also in reducing the time and effort required to comply with the audit and reporting requirements. Many of the SD-02D requirements where BAS can be most beneficial are listed in Section G of the security directive.

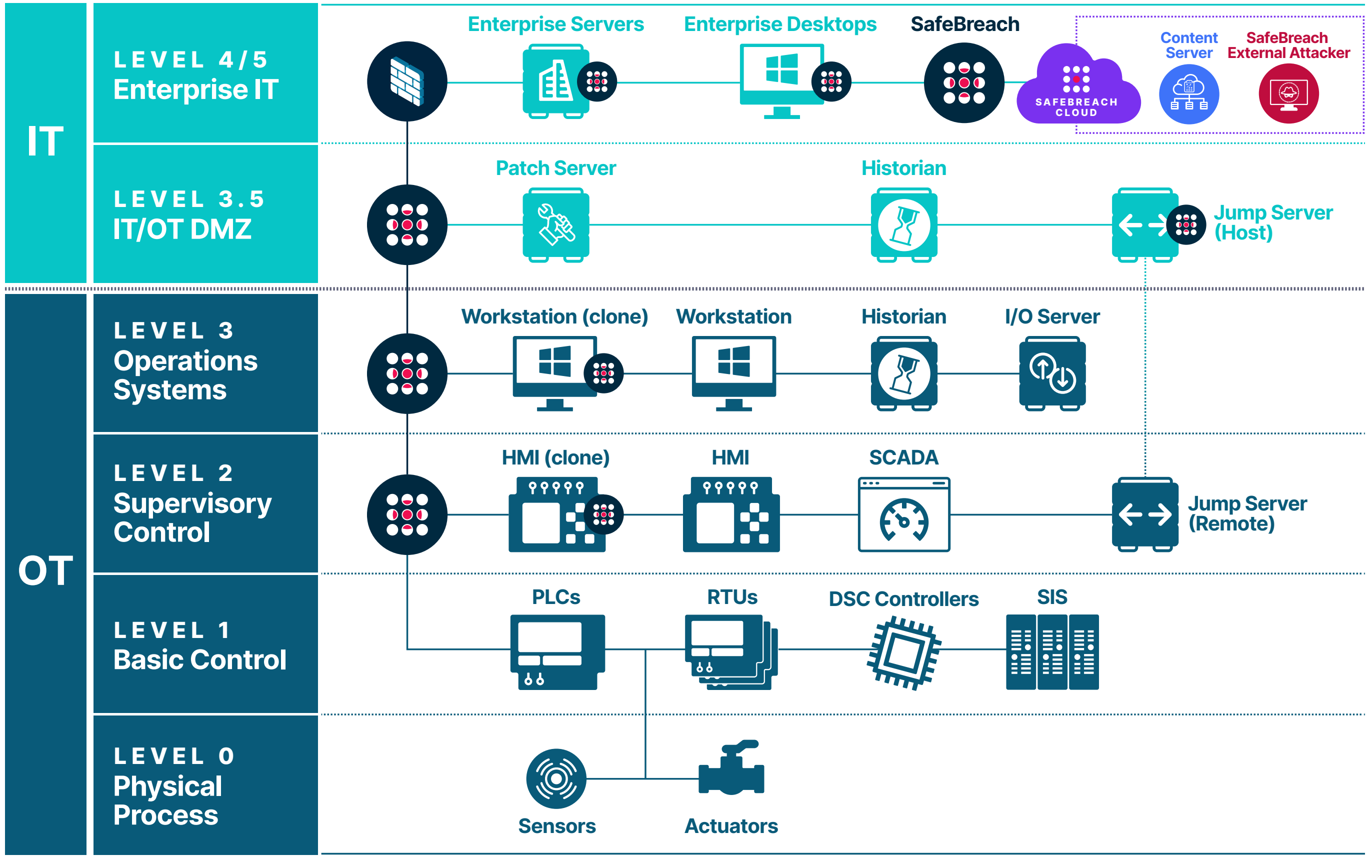
Read the full blog to learn more.

CLICK HERE TO READ OUR SOLUTION BRIEF:
Increase Your IT/OT Resilience with the SafeBreach BAS Platform

Utilizing BAS with the Purdue Model in a Combined IT/OT Architecture

The Purdue model is generally accepted as the standard for building an ICS network architecture in a way that supports OT security, separating the layers of the network to maintain a hierarchical flow of data between them. It consists of six network levels, defined by the technologies and systems that reside in each. IT systems occupy the upper two levels, while OT systems occupy the lower three, and a converged “demilitarized zone” resides between them.

As an example, we’ve identified how a BAS platform like SafeBreach could be deployed across a typical Purdue Model architecture.



IT

LEVEL 4/5
Enterprise IT

Enterprise Servers
Enterprise Desktops
SafeBreach
SAFEBREACH CLOUD
Content Server
SafeBreach External Attacker

LEVEL 3.5
IT/OT DMZ

Patch Server
Historian
Jump Server (Host)

OT

LEVEL 3
Operations Systems

Workstation (clone)
Workstation
Historian
I/O Server

LEVEL 2
Supervisory Control

HMI (clone)
HMI
SCADA
Jump Server (Remote)

LEVEL 1
Basic Control

PLCs
RTUs
DSC Controllers
SIS

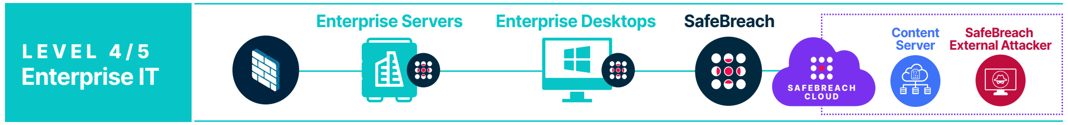
LEVEL 0
Physical Process

Sensors
Actuators

How it Works

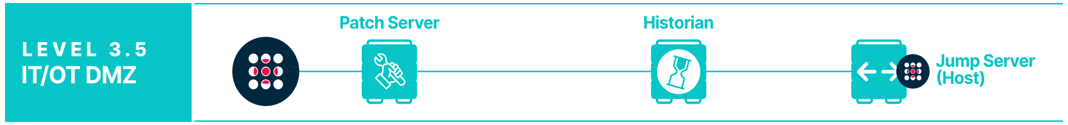
AT LEVELS 4/5

Attack simulators are deployed to typical enterprise desktops, laptops and servers, while the content server and external attacker are deployed in the SOC. At this level SafeBreach's simulated attacks validate endpoint security controls, firewall detection rules, access-control list (ACL) rules, and verify events are being logged by the security information and event management (SIEM) solution.



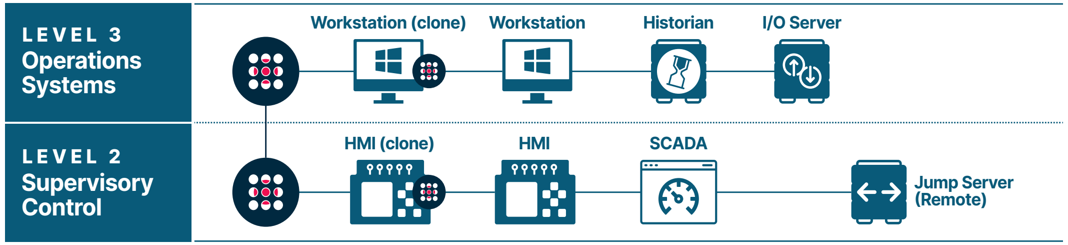
AT THE IT/OT DMZ (LEVEL 3.5)

Simulators are testing the firewall that regulates access to this level, as well as validating the controls of the jump host (probably Linux-based) to ensure remote access to the lower OT levels is secure.



AT LEVELS 2&3

When thinking about OT network endpoints, many people think of the specialized assets such as PLC and RTU units that are directly controlling production processes. But even in the OT environment, the assets often at greatest risk of compromise are the engineering workstations and HMIs which are likely running either a Windows or Linux environment. It is critical to include these assets in the attack simulation, as OT endpoints often have different security controls and configurations than endpoints on the IT network.



CLICK HERE TO READ OUR BLOG POST:
How BAS Fits into a Combined IT/OT Architecture Using the Purdue Model

Unifying IT & OT Security with BAS

Breach and attack simulation is one of the most effective tools to assess and validate the security controls across a combined IT and OT environment. Enterprise industrial organizations leveraging BAS technology are able to gain greater visibility into what their entire attack surface looks like, so they can:

Confidently Support OT Digital Transformation

Ensure your operations IT and security teams are working together — from the same information — to meet the demands for both productivity and protection as your operational environment transforms.

Enable Remediation & Reporting Across IT & OT

Create a consolidated view of your IT and OT security environment to quickly identify and remediate weaknesses and vulnerable points of "spill-over" from one network to the other during an attack.

Increase Confidence with Stakeholders

Share automated reporting with key stakeholders to clearly communicate risk within the organization and ensure security investments are prioritized.

Manage Supply-Chain Security Risk

Before working with third-party suppliers, precisely assess their cybersecurity posture to understand the potential risks they may bring to your environment.

Ready to learn more about how SafeBreach's BAS platform can help provide better visibility and protection in your integrated IT/OT environment?

SCHEDULE A DEMO:

Connect with a SafeBreach Expert Today

About SafeBreach

Combining the mindset of a CISO and the toolset of a hacker, SafeBreach is the pioneer in breach and attack simulation (BAS) and is the most widely used continuous security control validation platform. SafeBreach continuously executes attacks, correlates results to help visualize security gaps, and leverages contextual insights to highlight remediation efforts. With its Hacker's Playbook™, the industry's most extensive collection of attack data enabled by state-of-the-art threat intelligence research, SafeBreach empowers organizations to get proactive about security with a simple approach that replaces hope with data.

Learn more at **SafeBreach.com.**

SafeBreach