

CUSTOMER TESTIMONIAL

Validating OT Defenses Through Real-World Adversary Testing at Electric Substations



OBJECTIVES

A leading US electric utility set out to validate whether its cybersecurity architecture, visibility strategy, segmentation model, and defensive capabilities perform as intended inside real substation production environments, not just in isolated labs, simulations, or digital twins.

SOLUTION

The utility deployed purpose-built SCYTHE agents in production OT to safely emulate adversaries along high-value attack paths.

Key capabilities included:

- Mapped attack paths from architecture and threat intel
- Agents modeled substation systems and trust relationships
- Emulated attacks in live substations and control centers
- Measured detection, monitoring, segmentation, and response in place

THE RESULTS

Architectural Effectiveness

Assessed whether an adversary can reach meaningful operational objectives, and whether defenses raise the cost, complexity, and likelihood of detection.

Validated Defensive Investments

Evaluated whether each control materially changes attacker opportunity, not simply whether it is deployed.

Visibility & Detection Priorities

Identified blind spots, implicit trust relationships, and monitoring gaps, and prioritized detection engineering.

Continuous Capability Assessment

Moved from compliance-oriented validation to an ongoing program that informs future OT design decisions.

AT A GLANCE

Challenges

- Controls unproven in live OT
- Unverified segmentation
- Visibility gaps near crown jewels
- Point-in-time compliance tests

Benefits

- Testing in live substations
- Attack-path driven emulation
- Measured, not assumed, defense



"Rather than asking whether a control is deployed, we can now evaluate whether it materially changes attacker opportunity, improves observability, or constrains movement toward critical operational assets."

"That is a more meaningful measure of cyber resilience than traditional control validation alone."

**OT Cybersecurity Architect,
US Electric Utility**