CUSTOMER TESTIMONIAL

Improving Detection, Response, and Regulatory Readiness for a United States Major Utility Provider



OBJECTIVES

A leading utility provider set out to strengthen cybersecurity validation across distributed IT and OT environments while improving detection consistency and the effectiveness of its controls, processes, and security workforce amid increasingly complex and distributed attack scenarios.

SOLUTION

The utility deployed a tailored SCYTHE Adversarial Exposure Validation (AEV) program designed specifically for distributed utility environments.

Key capabilities included:

- Deployed the SCYTHE platform in the central lab and selected substations
- Enabled realistic adversary emulation across IT and OT environments
- Conducted expert-led purple team exercises across IT, OT, and IR teams
- Added hybrid tabletop and live emulation exercises
- Expanded from the central lab to high-risk operational sites

THE RESULTS

Threat Coverage & Validation Improvement

Validated 20+ priority attack techniques across IT and OT, uncovering previously untested IT–OT attack paths.

Detection & Response Readiness

Detection coverage improved by 47%, time to detect intrusions fell by 50%, and multiple high-risk substation gaps were identified and remediated.

Operational Consistency

Standardized purple team exercises across sites, with a repeatable annual program and improved IT, OT, and IR coordination.

Regulatory & Audit Impact

Improved executive reporting increased leadership confidence in incident preparedness.

AT A GLANCE

Challenges

- Distributed attack surface
- IT-OT/ICS convergence
- Infrequent, high-cost exercises
- Regulatory & audit pressure

Benefits

- 47% detection coverage gain
- 20+ priority TTPs validated
- 50% reduction in MTTD
- Results reported by this customer



"We moved from infrequent, manual exercises to a continuous validation program across IT and OT.

That shift improved detection coverage, accelerated response readiness, and gave our leadership a much clearer view of our true security posture."

Director of Security Engineering, US Utilities Provider