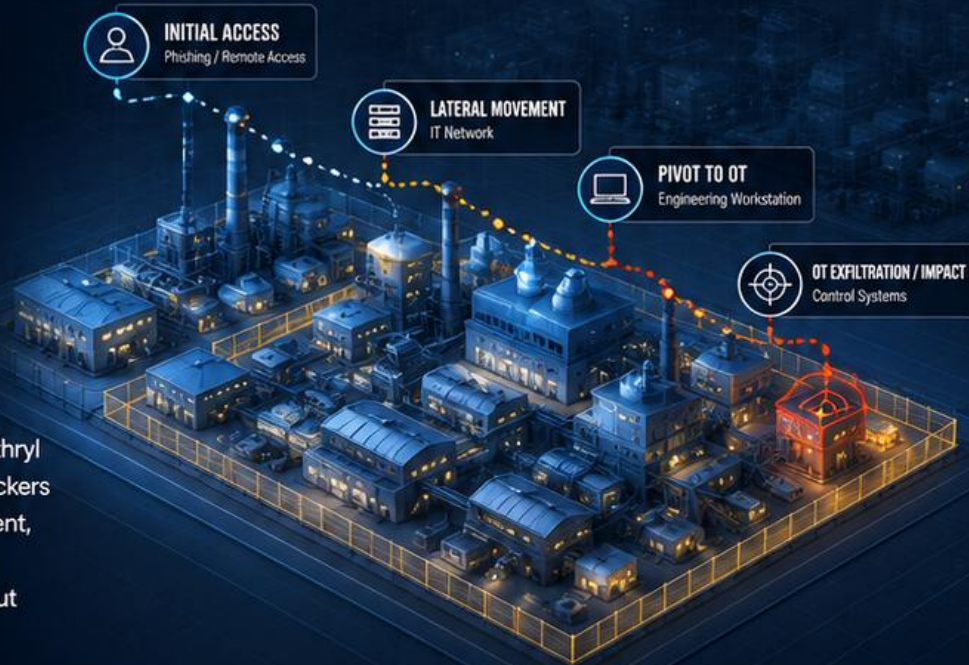




OT RED TEAM ASSESSMENT

Validate Operational Resilience Before an Attacker Does

Traditional penetration tests identify vulnerabilities. Mithryl Systems OT Red Team Assessments validate how attackers could actually move through your industrial environment, identify exploitable attack paths, and measure your organization's ability to detect and respond, all without disrupting operations.



ADVERSARIAL VALIDATION

Safely emulate real attacker behavior across IT and OT environments.



OPERATIONAL SAFETY

Assess cyber resilience without disrupting production.



ACTIONABLE FINDINGS

Deliver prioritized recommendations that reduce operational risk.

THE CHALLENGE

Compliance proves controls. It doesn't prove resilience.

Many organizations know which assets they own.

Far fewer know whether an attacker could move from IT into OT without being detected.

An OT Red Team Assessment validates real world attack paths, detection capability, and operational readiness.

FROM ATTACK PATHS TO OPERATIONAL RESILIENCE



ATTACK SURFACE

Identify assets, exposures, and potential entry points.



ATTACK SIMULATION

Safely emulate real attacker behavior across IT and OT environments.



DETECTION VALIDATION

Measure detection coverage and response effectiveness.



PRIORITIZED FINDINGS

Deliver clear, evidence-based insights and recommendations.



OPERATIONAL RESILIENCE

Strengthen defenses, reduce risk, and protect critical operations.



Operational Resilience. Validated.

Mithryl Systems OT Red Team Assessments give you the confidence that your industrial environment is resilient against real-world attackers.



See Your Environment Through an Attacker's Eyes

SCHEDULE AN OT RED TEAM ASSESSMENT

www.mithrylsystems.com





THE MITHRYL RED TEAM METHODOLOGY

End-to-end adversarial validation for industrial environments.



BUSINESS BENEFITS

- Realistic Attack Simulation Without Downtime**
Uncovers hidden risks without interrupting critical operations.
- Cross-Domain Visibility**
Bridges IT, OT, and human telemetry for a complete security picture.
- Data-Driven Risk Prioritization**
Provides clear, evidence-based insights for budget and resource allocation.
- Protocol-Level Resilience**
Reveals systemic weaknesses in legacy protocols still used across critical infrastructure.
- Compliance & Audit Alignment**
Supports NIST 800-82, ISA/IEC 62443, and CISA OT security guidelines with actionable evidence.
- Continuous Improvement Enablement**
Establishes a baseline for repeat testing, continuous monitoring, and cyber fusion integration.

HOW OT RED TEAMING WORKS



DELIVERING MEASURABLE BUSINESS VALUE

- VALIDATE ATTACK PATHS**
Identify how attackers could move from IT into critical OT assets before they do.
- IMPROVE DETECTION READINESS**
Measure whether existing detections identify real-world attacker behavior.
- REDUCE OPERATIONAL RISK**
Prioritize remediation based on operational impact rather than technical severity.
- STRENGTHEN CYBER RESILIENCE**
Improve readiness through realistic adversarial validation and continuous testing.
- SUPPORT REGULATORY READINESS**
Generate evidence that supports NIST SP 800-82, ISA/IEC 62443, and CISA OT guidance.



Operational Resilience. Proven.

See your environment through an attacker's eyes and strengthen what keeps your operations running.



See Your Environment Through an Attacker's Eyes

SCHEDULE AN OT RED TEAM ASSESSMENT
www.mithrylsystems.com