MIDWEST RELIABILITY ORGANIZATION

MRO Security Advisory Council (SAC)

Penetration (Pen) Testing – Lessons from Pen Testing New Software Pre-Go-Live

February 04, 2025

MIDWEST RELIABILITY ORGANIZATION

Shawn Keller

Outreach Coordinator

MRO Upcoming Events

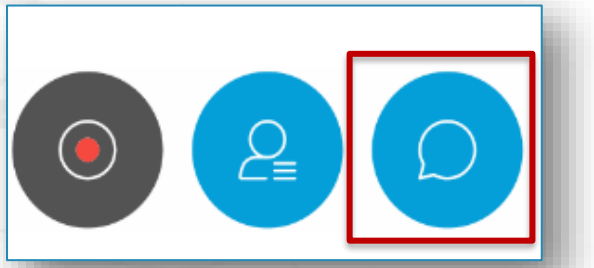
- **Regional Risk Assessment (RRA) Webinar**
  - February 5, 2025, 9:00 a.m. – 11:00 a.m. Central Time
- **ERO Enterprise Women's Leadership Conference**
  - March 4, 2025, 10:00 a.m. – 2:30 p.m. Central Time
- **GridEx VIII Preparation Webinar: An Overview of GridEx VIII**
  - March 20, 2025, 10:00 a.m. – 11:00 a.m. Central Time
- **GridEx VIII Preparation Webinar: Lessons from NPPD's Participation**
  - April 10, 2025, 10:00 a.m. – 11:00 a.m. Central Time
- **Reliability, Security, CMEP Summit**
  - May 20-21, 2025; Omni Hotel, Oklahoma City, OK

Disclaimer Slide

Midwest Reliability Organization (MRO) is committed to providing outreach, training, and non-binding guidance to industry stakeholders on important industry topics. Subject Matter Experts (SMEs) from MRO's organizational groups and the industry may develop materials, including presentations, provided as a part of the event. The views expressed in the materials are those of the SMEs and do not necessarily express the opinions and views of MRO.

Webex Chat Feature

Open the Chat Feature:



The chat feature will appear to the right of the Webex window.

Attendees should chat their questions to: “All Panelists”.

Select All Panelists by using the drop-down arrow in the “To” field.

Please take a moment to complete the survey

https://www.surveymonkey.com/r/MROSACPENtest

MRO Security Outreach & Engagement

MRO Board of Directors

Organizational Group Oversight Committee

Security Advisory Council

Security Threat Forum

Internal MRO Staff Work (Security Dept.)

MRO Security Department

E-ISAC Regional Liaison, Intelligence Agencies and Reports, Cyber, Physical, Operational Security & Threat Expert, Grid-Ex VIII Liaison

https://www.mro.net/program-areas/critical-infrastructure-security/

Annual Security Conference, Quarterly Meetings, Grid Experts
www.mro.net/organizational-groups/security-advisory-council/

Weekly threat call, Open Source Reports, Threat Experts
https://www.mro.net/organizational-groups/security-advisory-council/security-advisory-council-threat-forum/

MRO Security Department

Steen J. Fjalstad, MS, CISSP, CISA, CGEIT, CRISC
Director of Security
steen.fjalstad@mro.net
651-855-1715

Margaret Eastman, MS, CIPP/US
Security Administrator
margaret.eastman@mro.net
651-855-1755

SAC & SACTF MEMBERS - 2025

Security Advisory Council (SAC)

- Clayton Whitacre, Great River Energy
- Daniel Graham, Basin Electric Power Cooperative
- David Johnson, OGE Energy Corp.
- Erich Krueger, Omaha Public Power District
- Ian Anderson, OGE Energy Corp.
- Jay Duncan, Evergy
- Justin Haar, Minnkota Power Cooperative
- Kelly Crist, Engie North America
- Norma Browne, Ameren
- Patrick Glunz, Nebraska Public Power District
- Peter Grandgeorge, MidAmerican Energy Company
- Rocky Tolentino, Southwest Power Pool
- Theresa Greene, Grand River Dam Authority
- Tim Anderson, Dairyland Power Cooperative
- David Webb, MISO

Security Advisory Council Threat Forum (SACTF)

- Brennan Mobarak, Oklahoma Gas and Electric
- Brett Lawler, Xcel Energy
- David Webb, MISO
- Scott Stoner, Nebraska Public Power District
- Shawn Styfco, MISO

Maximizing OT Pentest Value

Tyler Webb
Principal Industrial Penetration Tester
twebb@dragos.com
February 04, 2025

Agenda

Maximizing OT Pentest Value

1. What is OT pentesting?
2. Methodology and alignment with ICS Cyber Kill Chain
3. Value Optimization

What is OT Pentesting?

What is OT pentesting?

Key concepts

- Penetration testing
- Adversary simulation
- Red teaming
- Purple teaming

What is OT pentesting?

Methodologies and practical focuses

- Penetration testing
  - Identify and validate vulnerabilities in a narrowly scoped environment
- Adversary simulation
  - Use known adversary techniques
- Red teaming
  - Expanded scope; extended engagement window; test people, processes and technology; initial access; objective-based
- Purple teaming
  - Red team + blue team; offense + defense; validate detection and response capabilities

What is OT pentesting?

The Dragos flavor

- Hybrid engagement style that blends penetration testing, red teaming, ad-sim, and purple teaming
  - Narrow scope, both in terms of assets and timeframe (Pentesting)
  - Active exploitation (Pentesting/Red teaming)
  - Objective-based (Red teaming)
  - Leverage known adversary TTPs (Ad-sim)
  - Validate detection and response capabilities (Purple teaming)

What is OT pentesting?

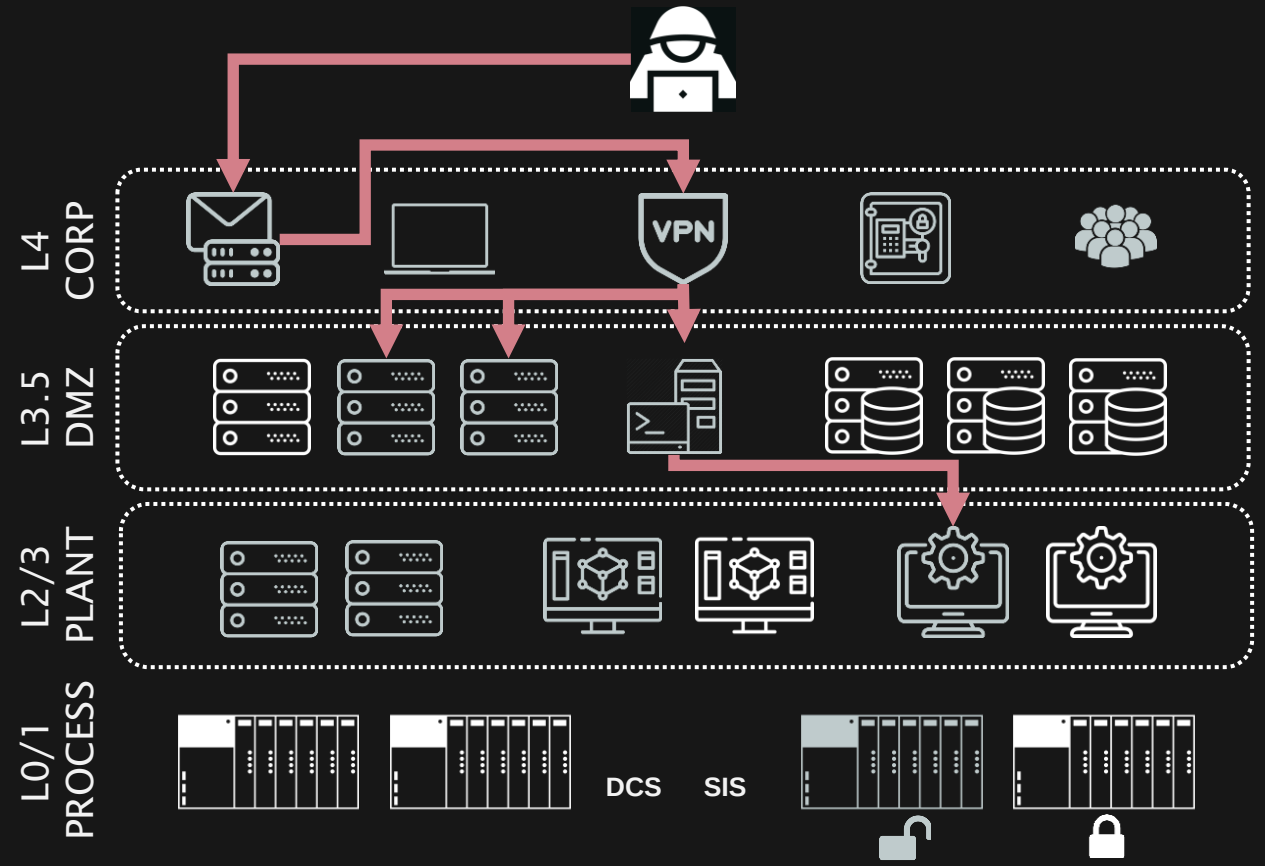
Key priorities

- Safety
  - Zero operational impact
  - No risk to human safety
- Efficiency
  - Constrained timeframes
- Value
  - Output needs to be accurate and actionable

Methodology & Alignment with the ICS Cyber Kill Chain

OT Pentest Methodology

Methodology and Kill Chain Alignment



Stage 1: Access

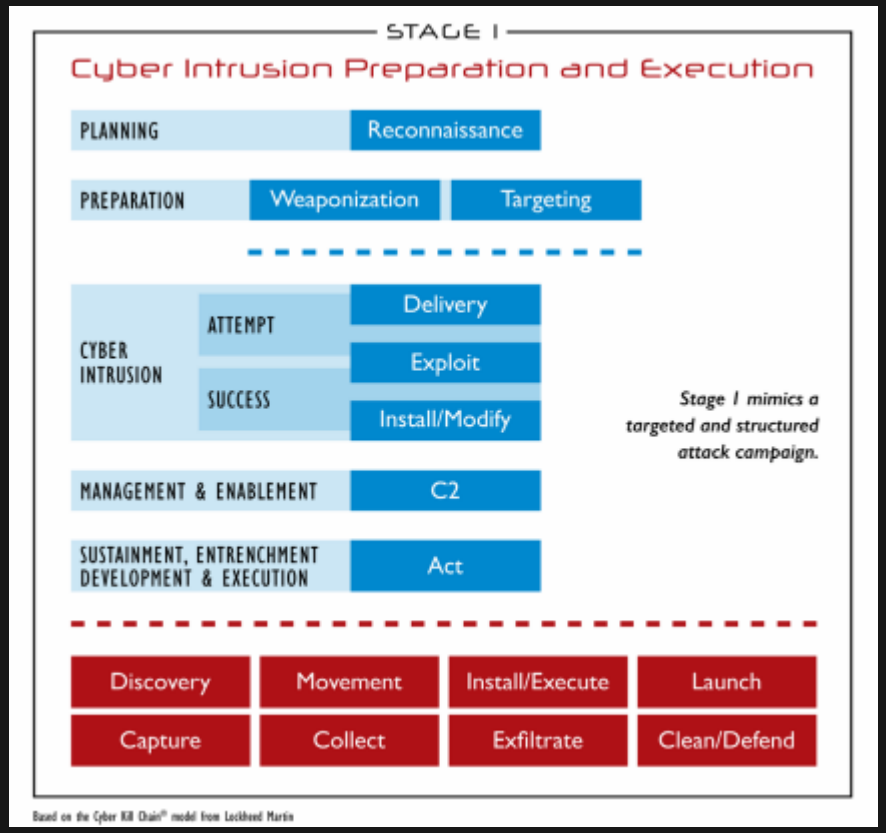
Stage 2: ICS Attack (Impact)

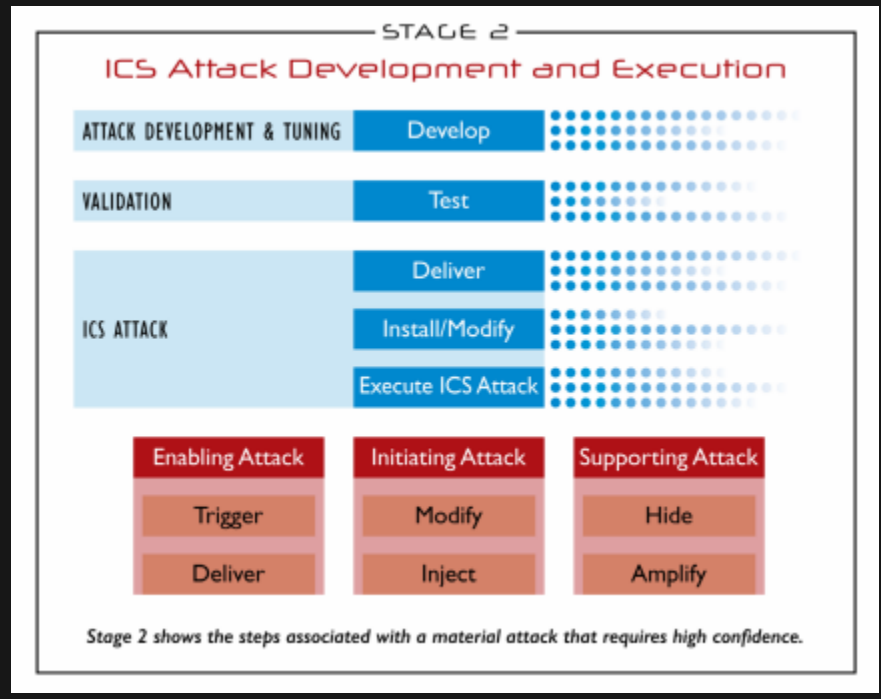
The ICS Cyber Kill Chain provides:

- Appropriate context
- Actionable prioritization
- Relevant objectives and goals to align testing activities with adversary capabilities and intent.

OT Pentest Methodology

Methodology and Kill Chain Alignment





OT Pentest Methodology

Methodology and Kill Chain Alignment

1. Scoping & Information Gathering (Our chance to do *Reconnaissance*)
2. Crown Jewel Analysis (Our opportunity to do *Targeting*)
3. Assumed Breach Access (Our chance to skip the extensive *Cyber Intrusion* process)
4. Command & Control
5. Action
    1. Enumerate
    2. Exploit
    3. Move
    4. Manage
    5. Repeat
    6. Enumerate the Process
6. ICS Attack Development (Our chance to make the output relevant to OT)
7. Reporting (Our chance to make the output actionable)

OT Pentest Methodology

Planning/Scoping

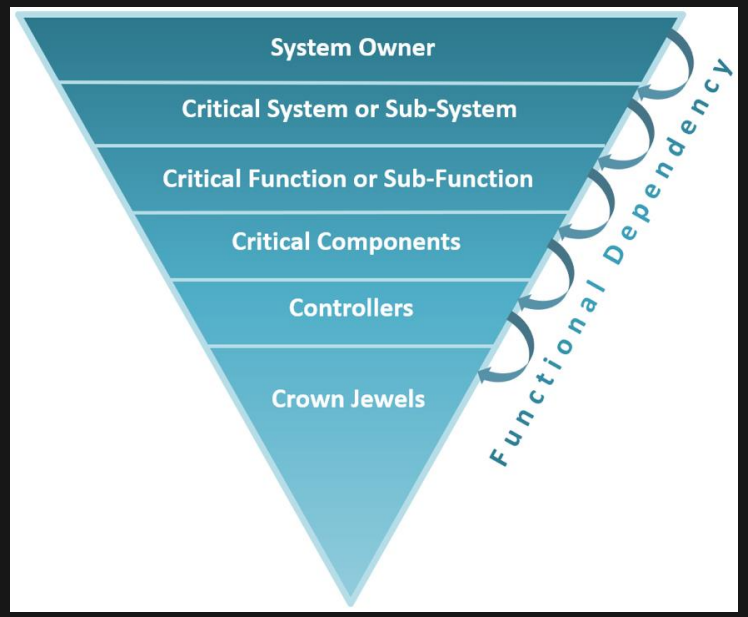
Engagement scoping and information gathering activities are aligned with the *Planning phase* of Stage 1 of the ICS Cyber Kill Chain. This is our chance to do what an adversary does when they perform *Reconnaissance* activities.

- Customer needs
  - Cybersecurity maturity, assessment type, industry, etc.
- Threat Landscape
  - Relevant TTPs, threat capabilities
- Rules of Engagement (ROE)
  - Scope, objectives, goals, etc.
- Request for Information
  - *Whitebox Reconnaissance*

OT Pentest Methodology

Crown Jewel Analysis

Crown Jewel Analysis (CJA) is aligned with the *Preparation phase* of Stage 1 of the ICS Cyber Kill Chain. This is our chance to perform *Targeting* like an adversary.



OT Pentest Methodology

Access Validation/Initial Foothold Prep

In almost all cases, the most effective OT pentest will be done from an assumed breach, whitebox perspective. This effectively represents the *Cyber Intrusion phase* of Stage 1 of the ICS Cyber Kill chain.

- Relevance
  - What story are we trying to tell?
- Remote access
  - Test ahead of time
- Permissions
  - Test ahead of time

OT Pentest Methodology

Action

In an assumed breach OT penetration test, the active assessment really begins in the *Sustainment, Entrenchment, Development & Execution phase* of Stage 1 of the ICS Cyber Kill chain.

Enumerate > Exploit > Move > Manage > Repeat > Enumerate The Process

The key is that we remain focused on gaining access to systems or information that help us understand the industrial process.

OT Pentest Methodology

ICS Attack Scenario Identification

After we've demonstrated methods of accessing the Control Network, we stop active testing and pivot to a *bottom-up* approach.

Referring to our CJA and collaborating with customer stakeholders, we start theory-crafting what an effective ICS attack would need to cause a significant and predictable process or equipment impact.

Unless we have a lab environment with equipment mirroring the production environment, this phase should rely on standalone demos or POC, or just discussion with stakeholders.

Value Optimization

Value Optimization

Key priorities

- Safety
  - No operational impact
  - No physical harm
- Efficiency
  - Compressed timeframes
- Value
  - Must be OT-focused
  - Must be actionable

Value Optimization

Key supporting strategies

- Planning & Preparation (Safety, Efficiency, Value)
  - ROE
  - RFI
- Assumed breach (Efficiency)
- Avoid EDR evasion (Efficiency, Value)
  - Quiet, then Loud
- Multiple mitigation options (Value)
  - Architectural
  - Configuration
  - Monitoring

Value Optimization

Rules of Engagement (ROE)

- Scope
- Objectives
- Goals
- Foothold
- AV/EDR Evasion Expectations
- Timeframe
- Key contacts
- Communication plans

Value Optimization

Request for Information (RFI)

- Network diagrams
- Asset Inventory
- PCAPS
- Firewall/switch configs
- Remote access information
- Third-party dependencies
- Test account provisioning

Value Optimization

Assumed Breach

- Initial access takes a long time – assumed breach lets us focus on testing the other layers of defense in depth.
- More efficient and valuable to assume a bad day and inquire what an adversary could do once they have a foothold.
- Develop realistic scenarios (IT compromise, trusted OT vendor compromise, etc.).

Value Optimization

Avoid EDR Evasion

- AV/EDR is a key security control
- We should test for AV/EDR misconfigurations
- But… it's very inefficient and not at all valuable to spend most of an engagement trying to bypass modern EDR
  - Cat and mouse game
  - Only one layer of defense-in-depth
- Apply the same assumed breach approach
  - EDR can and will be bypassed, so let's imagine that it has been – what now?
- Quiet, then Loud

Value Optimization

Multiple mitigation options

- Architectural vs. Configuration vs. Monitoring
- Strategic vs. Tactical
- Sometimes there aren’t patches…
- Monitoring is a valid mitigation!
  - Monitoring needs to be tested
  - Detections need to be tuned
  - Response needs to be practiced

Value Optimization

Less Red, More Purple

- A trend from the Red Team mindset towards Purple Team paradigms supports all three priorities:
  - Safety
  - Efficiency
  - Value

Value Optimization

Story Time

Less Red, More Purple

- OG&E + Dragos Purple Team NPT

Q&A

Ask us anything!

Thank you!

Please take a moment to complete the survey

https://www.surveymonkey.com/r/MROSACPENtest