CYMANII

the cybersecurity manufacturing innovation institute

Better Plants: Cyber Security Bootcamp 2025 - Thursday, April 24th

Inside a Cyber Intrusion – End-to-end Workflow Example (Vulnerabilities, Risk, Exploitation)

Rima Asmar Awad, PhD
Cybersecurity Software Engineer // ORNL
Rima.Awad@cymanii.org // awadrl@ornl.gov

Jennifer Sims
Cyber Security Professional// ORNL
Jennifer.Sims@cymanii.org // simsja@ornl.gov

Objectives

After attending this session, you will able be to:

- Understand threat actors specific to manufacturing
- Identifying risks: financial, operational, and regulatory
- Develop a threat profile
- Analyze cyber intrusion workflows
- Identify insider threats and ICS vulnerabilities
- Map cyber attacks to real-world exploits
- Apply best practices for cyber defense

The Rising Threat of Cyberattacks in Manufacturing

- Cyberattacks on manufacturing are rising due to the IT-OT convergence, legacy systems, and insecure industrial protocols
- Cyber intrusions can cause:
  - Financial losses
  - Production downtime
  - Intellectual property theft
  - Safety risks
- This session will walk through an end-to-end cyber intrusion workflow using a real-world threat profile for a manufacturing company

What are threat profiles?

- A structured analysis that identifies:
  - Threat actors
  - Attack vectors
  - System vulnerabilities
  - Potential impacts
- Threat profiles help organizations understand specific cyber threats and improve incident response & risk mitigation

Threat Profile for Manufacturing Industry

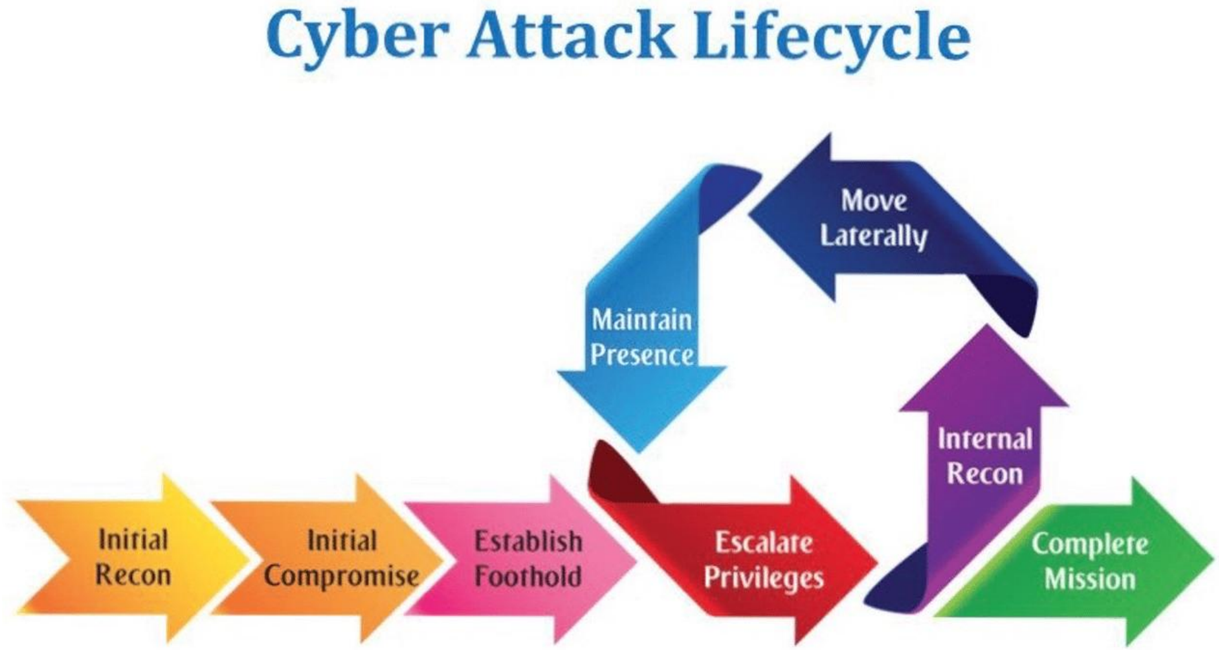
- Common risks in the manufacturing sector:
  - Legacy systems with weak security
  - Third-party dependencies (suppliers, contractors)
  - ICS and SCADA vulnerabilities
- Threat actors:
  - Nation-state actors targeting intellectual property
  - Cybercriminals deploying ransomware
  - Insider threats (disgruntled employees, unintentional negligence)

MITRE ATT&CK

- ATT&CK is a knowledge base of adversary tactics and techniques
- Organized into tactics, techniques, and procedures (TTPs)
- Helps in understanding attack behavior
- CWEs classify common software and hardware weaknesses
- Helps organizations identify and mitigate vulnerabilities
- Tied to attack patterns from MITRE ATT&CK

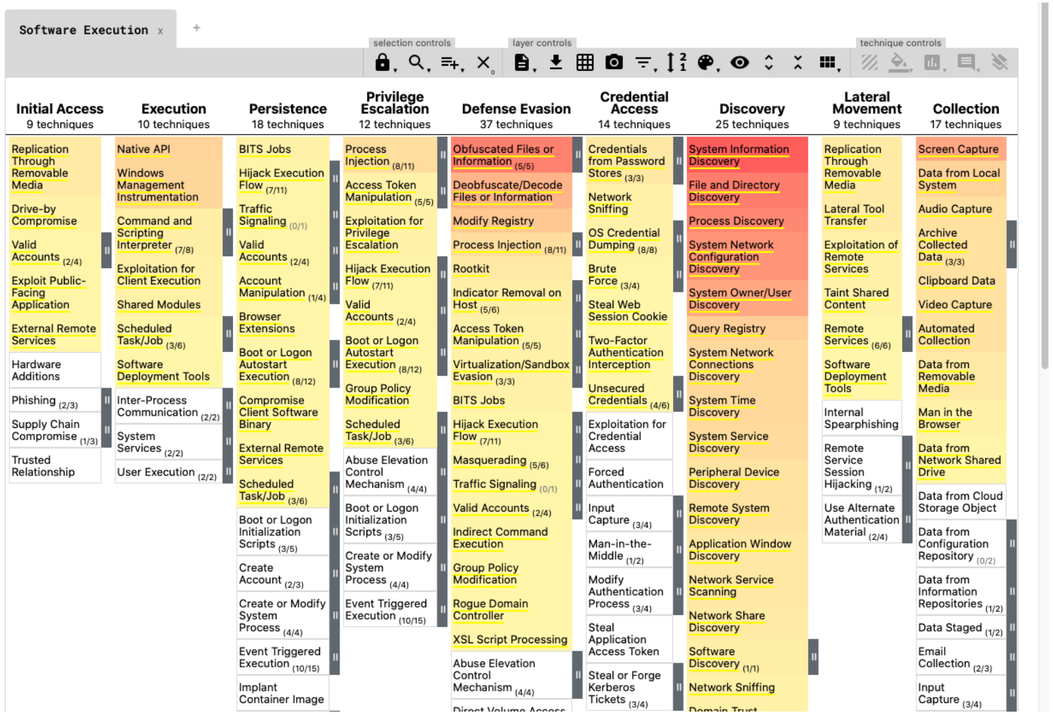
Cyber Intrusion Workflow – Attack Lifecycle

- Each phase aligns with MITRE ATT&CK tactics and techniques
  - Reconnaissance (TA0043) – Gather intelligence
    - T1598: Phishing for info
    - T1595: Active scanning
  - Initial Access (TA0001) – Gaining entry
    - T1566: Spear phishing
    - T1190: Exploit web apps
  - Exploitation (T1203) – Exploiting vulnerabilities
    - CWE-89: SQL Injection
    - CWE-269: Privilege misuse



Cyber Intrusion Workflow – Attack Lifecycle

- Privilege Escalation (TA0004) – Gaining higher access
  - T1068: Exploit misconfigurations
  - T1548: Bypass security controls
- Persistence (TA0003) – Maintaining access
  - T1543: Modify system processes
  - T1078: Use valid accounts
- Lateral Movement (TA0008) – Spreading internally
  - T1021: Exploit remote services
  - T1003: Credential dumping
- Impact (TA0040) – Causing damage
  - T1486: Ransomware
  - T1490: Disable backups



Developing a Threat Profile

1. Define the scope and objectives
2. Identify critical assets
3. Identify potential threat actors
4. Analyze attack vectors and vulnerabilities
5. Assess risk levels and potential impact
6. Create and document the threat profile
7. Implement mitigation strategies
8. Continuous Monitoring and updating

Define the scope and objectives

- Define the Scope:
  - A clear scope ensures targeted and manageable efforts
- Key Questions to Consider:
  - What is the purpose of the profile?
  - Who are the stakeholders?
  - Which systems, processes, and data are included?

Understand and Prioritize Asset Protection

- Identify Key Assets:
  - Determine what needs protection and focus on the most valuable and vulnerable assets.
- Key Questions to Consider:
  - What assets are crucial for operations?
  - Which assets, if compromised, would cause major damage?
  - Which assets have historically exhibited vulnerabilities?

Identify Potential Threat Actors

- Determine who might target assets and why
- Types of actors:
  - Cybercriminals
  - Nation-State Actors
  - Insider Threats
  - Hacktivists
  - Competitors

Insider Threats

- An insider threat is the *potential* for an insider (intentional, unintentional) to use their authorized access or understanding of an organization to harm that organization
  - Intentional Threats – actions taken to harm the organization for personal benefit or personal grievance
  - Unintentional threat
    - Negligence – exposes an organization to a threat through carelessness
    - Accidental – mistakenly causes an unintended risk

Analyze Attack Vectors and Vulnerabilities

- Vulnerability Assessment:
  - Identify and evaluate potential weaknesses:
    - Outdated software or unpatched systems
    - Weak security configurations
    - Known and emerging vulnerabilities
- Common Attack Vectors:
  - Social Engineering:
    - Tactics such as phishing, pretexting, and baiting
    - Exploitation of human error to bypass security measures

MITRE ATT&CK framework analysis can help map known Tactics, Techniques, and Procedures (TTPs) of relevant threats

Assess Risk Levels and Potential Impacts

- Prioritize Threats & Vulnerabilities:
  - Identify and rank them by likelihood and impact

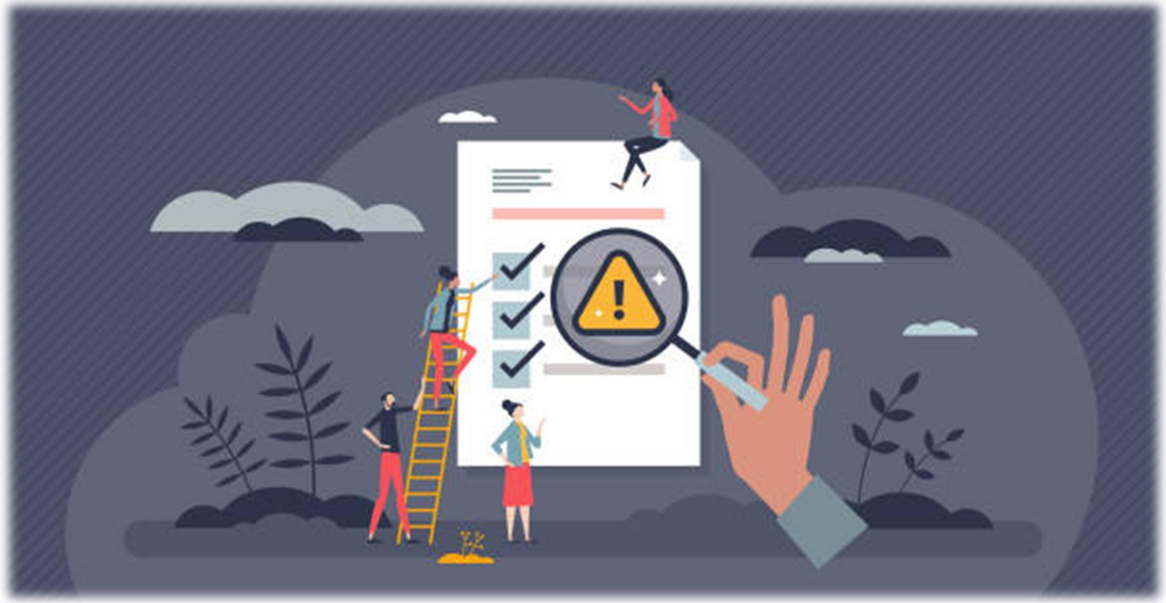
Evaluate Likelihood:

  - Use threat models to map out attack scenarios and assess feasibility

- Analyze Impact:
  - Determine criticality to gauge potential operational, financial, and reputational damage
- Mitigation:
  - Focus on high-risk areas for targeted response and continuous monitoring

Create and Document Threat Profile

- Compile everything into structured threat profile
  - Overview
    - Scope, assets, key findings
  - Threats
    - Threat actors, motivations, attack vectors
  - Vulnerabilities and Risks
    - Risk assessment results
  - Mitigation Recommendations
    - Strategies for risk reduction



Implement Mitigation Strategies

- Foundation Based on Findings:
  - Develop strategies directly from threat profile insights and risk assessments
  - Focus on addressing the most critical vulnerabilities identified
- Apply Targeted Security Controls:
  - Deploy controls specifically designed to mitigate high-risk areas
  - Regularly update and refine measures as threats evolve
- Align with Business Priorities:
  - Ensure strategies support overall business objectives and fit within budget constraints
  - Engage stakeholders to integrate security with operational goals
- Practical Examples:
  - Conduct comprehensive cyber awareness training sessions.
  - Enforce two-factor authentication (2FA) for all remote access

Continuous Monitoring and Updating

- Regular Reviews:
  - Conduct periodic threat assessments and reviews of existing controls
- Integrate Emerging Intelligence:
  - Update profiles based on new threats and vulnerabilities
- Adaptive Mitigation:
  - Refine mitigation strategies to address evolving risks
- Real-Time Alerts:
  - Utilize monitoring tools for prompt detection and response
- Compliance Updates:
  - Ensure alignment with current regulatory and industry standards

ICS-Specific Vulnerabilities

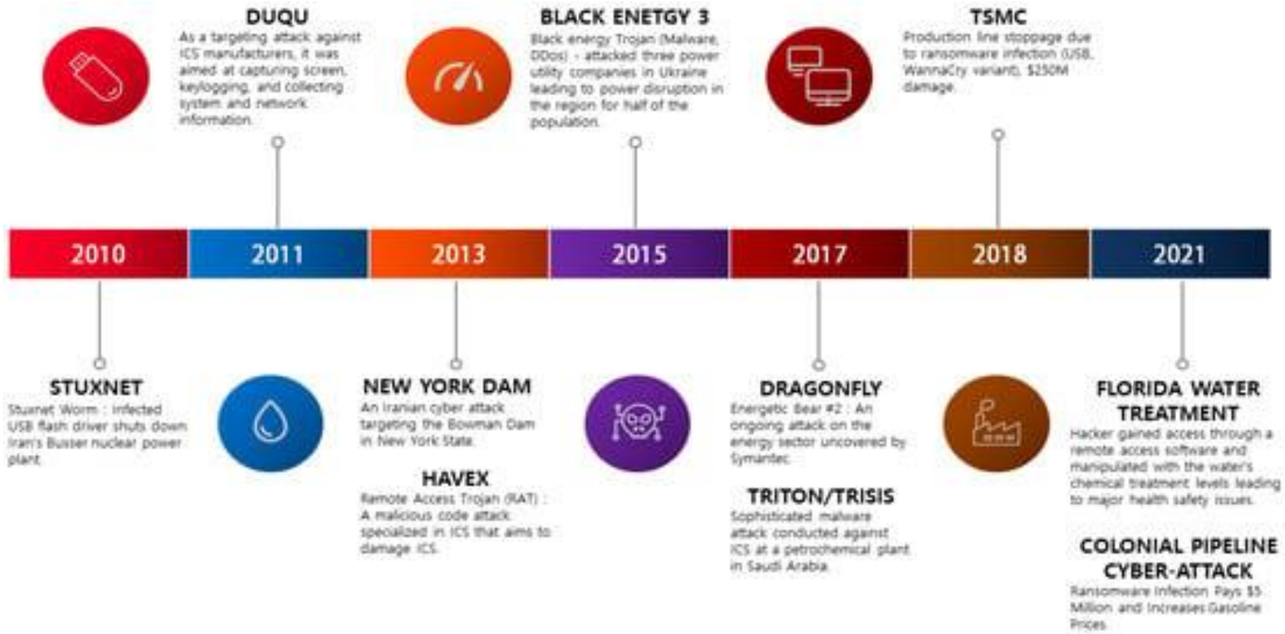
- Legacy Systems & Authentication Issues:
  - Weak Authentication in PLCs:
    - Legacy PLCs often use weak authentication mechanisms, making them susceptible to attack
- Remote Access Exploits:
  - Poorly Secured VPNs and RDP:
    - Inadequate configuration of remote access tools can provide attackers with a direct entry point
- Unencrypted Industrial Protocols:
  - Protocols such as MODBUS and DNP3 often lack encryption
- Third-Party and Vendor Risks:
  - Remote access granted to vendors or third parties without robust security measures can become a backdoor for attackers

Insider Threats in Manufacturing

- Types of Insider Threats:
  - Malicious Insiders (Intentional)
    - Data theft (stealing intellectual property, trade secrets)
    - Sabotage (modifying ICS settings to disrupt operations)
  - Negligent Insiders (Unintentional)
    - Misconfigured security (open RDP ports, weak passwords)
    - Untrained employees (falling for phishing attacks, mishandling credentials)
- Real-World Example:
  - An employee plugs in an infected USB drive, spreading malware to ICS
  - Attackers exploit weak security policies (no USB restrictions, lack of monitoring)

Exploits Targeting ICS Systems

- CS-specific attacks:
  - Industroyer2
  - Stuxnet (exploitation of PLCs)
  - TRITON malware (targeting industrial safety systems)
- Potential attack vectors:
  - Modifying controller logic
  - Man-in-the-middle attacks on SCADA communications



Industroyer2 (2022) – Ukraine Power Grid Attack

- Original Industroyer malware was found in 2016 designed to disrupt ICS and succeeded in causing power outages in Kiev, for an hour
- 2022 – New variant used to attack Ukraine's power grid
- Attributed to APT- Sandworm
- Attackers used malware to interact directly with ICS devices responsible for controlling electricity substations
  - At the same time, a disk-wiping malware was deployed to erase data across various operating systems

Defending Against Cyber Intrusions

- Strong Authentication & Access Controls:
  - Enforce multi-factor authentication and robust password policies
- Secure Industrial Protocols:
  - Encrypt communication channels to safeguard data
- Monitor & Detect Anomalies:
  - Utilize advanced monitoring tools for real-time threat detection
- Regular Patching & Incident Response:
  - Ensure timely updates and develop a proactive incident response plan
- Network Segmentation & Micro segmentation:
  - Isolate network segments and apply micro segmentation to minimize lateral movement

Frameworks and Tools

- MITRE ATT&CK for ICS
  - Mapping real-world attack techniques
- NIST Cybersecurity Framework (CSF)
  - Risk mitigation and management
- Common Vulnerability Scoring System (CVSS)
  - Assessing vulnerability severity
- ISO 27005
  - Risk management framework for information security
- Cyber Kill Chain (Lockheed Martin)
  - Understanding cyber attacker tactics

Threat Profile - Example

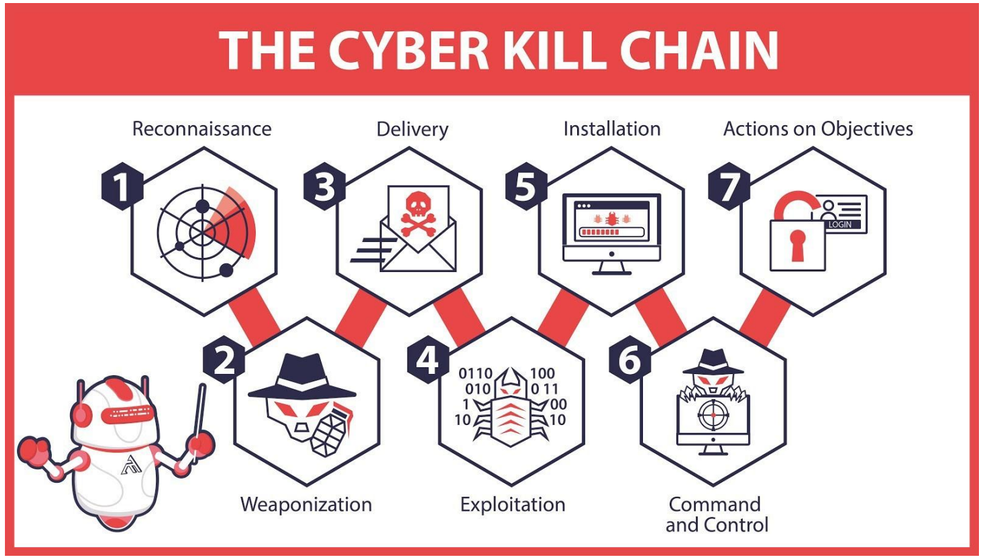
- Threat actors targeting Ghost Manufacturing
  - Ransomware Groups
  - Insider threat
  - Nation-State Actors
  - Hacktivists
  - Third-Party Vendors

Threat Profile - Example

- Company overview
  - Industry: Semiconductor manufacturing (Ghost Manufacturing)
  - Assets: High-precision equipment (wafer processing machines), PLCs, Raw materials (photoresists)
  - Technology: Uses IIoT-enabled production lines and cloud-based remote monitoring
  - Weaknesses: Legacy Systems, poor network segmentation, remote access risks

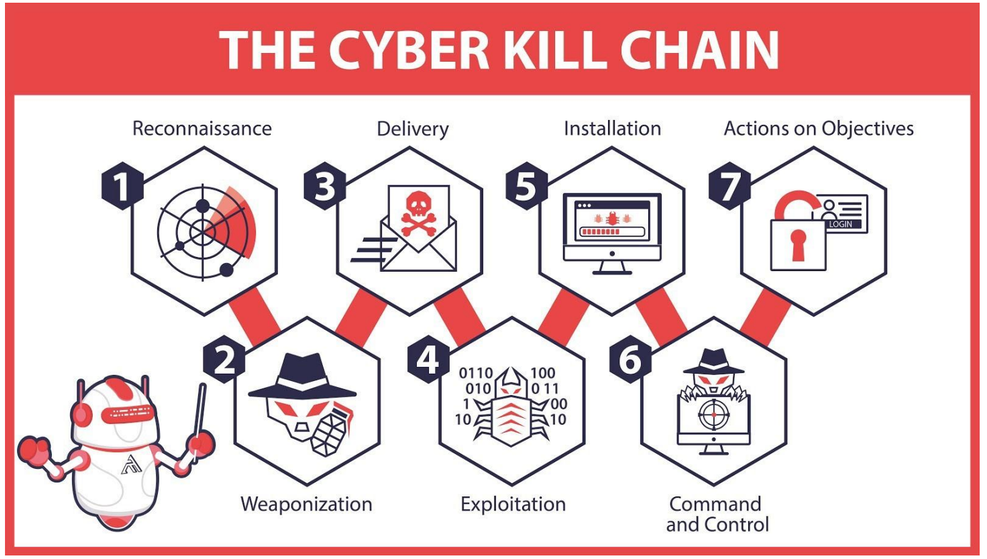
Attack Patterns and Vulnerabilities

- Initial Access: Phishing Email with Malicious Attachment
  - Overview: Emails crafted to appear legitimate, prompting users to open harmful attachments
  - Attack Details:
    - Vector: Malicious attachment delivers malware upon opening
    - MITRE ATT&CK: T1566.001 – Spearphishing Attachment
    - CWE: CWE-200 – Exposure of Sensitive Information



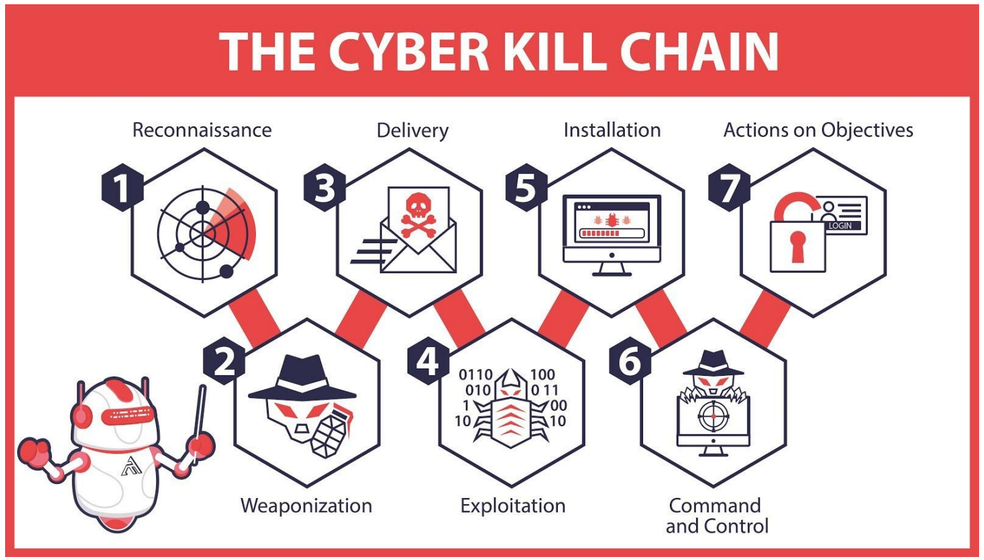
Attack Patterns and Vulnerabilities

- Execution and privilege escalation
  - Attack Vector:
    - Exploiting unpatched Windows ICS workstations via Remote Desktop Protocol (RDP) to gain unauthorized access
  - MITRE ATT&CK Technique:
    - T1078 – Valid Accounts (Weak Credentials)
    - Attackers leverage weak or default credentials to escalate privileges
  - Common Weakness Enumeration (CWE):
    - CWE-798 – Hardcoded Credentials in Software
    - Use of hardcoded credentials increases the risk of exploitation if systems are not updated



Attack Patterns and Vulnerabilities

- Lateral movement and ICS exploitation
  - Attack Vector:
    - Moving from the IT to the OT environment by exploiting a lack of network segmentation
  - MITRE ATT&CK Technique:
    - T1570 – Lateral Movement via Network Pivoting
    - Attackers traverse the network to compromise Industrial Control Systems
  - Common Weakness Enumeration (CWE):
    - CWE-284 – Improper Access Control
      - Inadequate access controls enable unauthorized movement between network segments



Summary

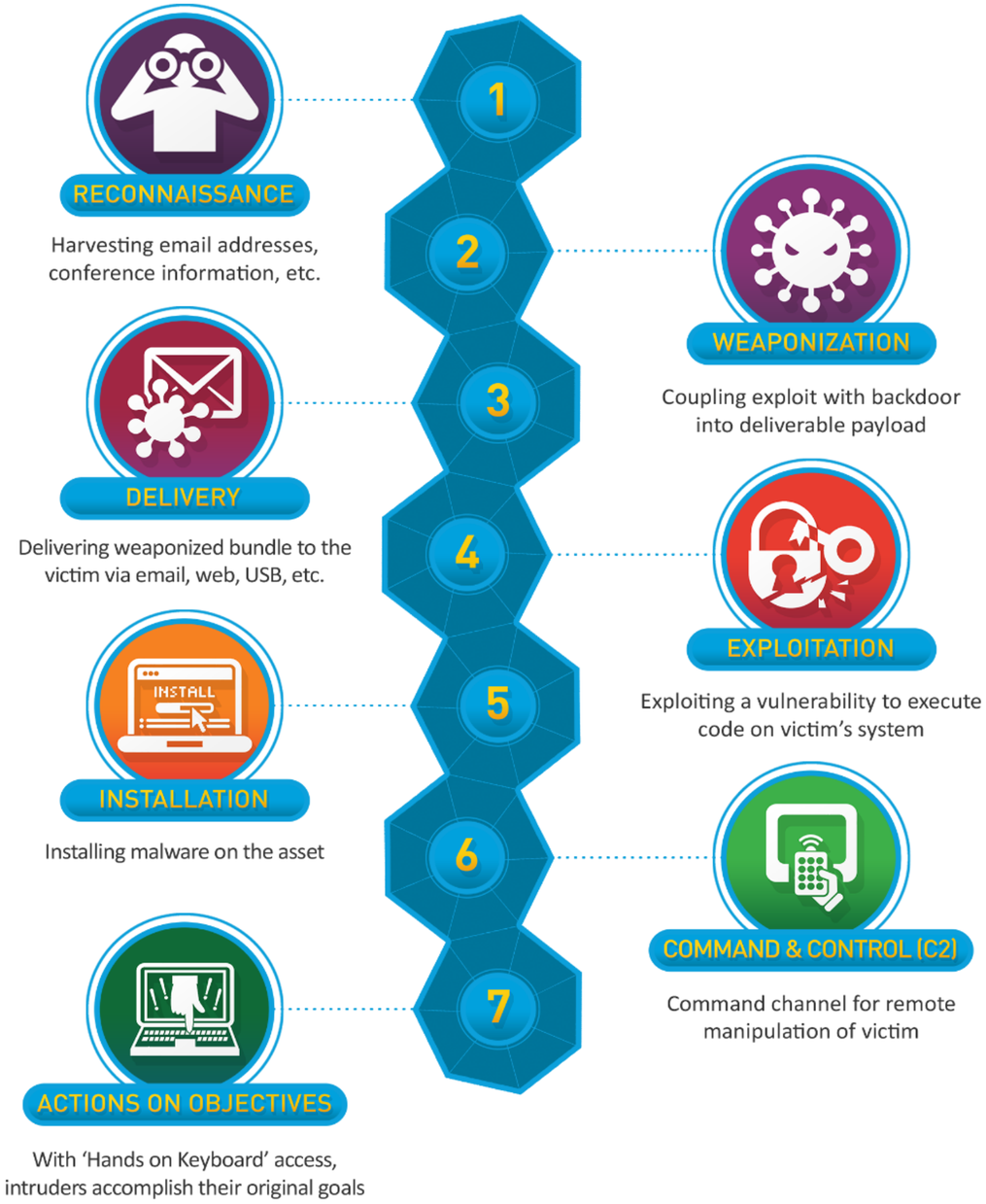
- Developing a threat profile is an essential practice for understanding risks in manufacturing and industrial environments.
- By identifying threat actors, vulnerabilities, and attack vectors, organizations can prioritize defenses and improve resilience against cyberattacks.

ACTIVITY

Threat Profile for Phantom Manufacturing

- Scope
  - Medium-sized aerospace manufacturer
  - Uses CNC machines, robotic arms, PLCs
  - Hybrid IT/OT network, remote vendor access

Cyber Attack Kill Chain Review



Phantom Manufacturing Scenario

Phantom Manufacturing fell victim to a coordinated cyber attack due to multiple security vulnerabilities A nation-state actor APT group, with the aid of a disgruntled insider, exploits phishing vulnerabilities, weak VPN security, and unpactched ICS software to sabotage production and exfiltrate sensitive design data.

Reconnaissance

Hacker's Action	Failure	MITRE ATT&CK ICS
APT group uses open-source intelligence to gather information on Phantom's employee's LinkedIn profiles, press releases, and corporate job postings.	No external attack surface monitoring	T0866: Gather Victim Identity Info T0869: Network Info

Weaponization

Hacker's Action	Failure	MITRE ATT&CK ICS
Attacker's craft a spear-phishing email targeting the engineering team. Embedded malware has been disguised as an MES update.	No email security filtering, sandboxing.	T0868: Spear-phishing link T0885: Supply Chain Compromise

Delivery and Exploitation

Hacker's Action	Failure	MITRE ATT&CK ICS
• An engineer (unintentional insider threat) falls for the phishing email and executes the payload, giving attackers initial access. • Stolen VPN credentials (weak passwords, no MFA) to allow remote access.	No MFA, no endpoint detection	T1078: Valid Accounts T0860: Remote Services

Installation & C2

Hacker's Action	Failure	MITRE ATT&CK ICS
• The attacker's deploy backdoors and pivot into the ICS network. • Attacker's exploit unpatched PLC firmware to install unauthorized control logic	No anomaly detection, no firmware integrity checks	T0833 Modify Controller Logic, T0867 C2 Over Web Protocols

Actions on Objectives

Hacker's Action	Failure	MITRE ATT&CK ICS
• ICS logic is manipulated to overheat CNC machines, causing material defects. • Sensitive aerospace part designs are exfiltrated via remote shell.	No network segmentation, no ICS-specific IDS.	T0807: System Firmware Corruption T0852: Data Destruction

Impact of Attack

- 4-day production outage
- $2.5 million in financial losses
- Regulatory scrutiny and loss of customer trust

Lessons Learned

- Implement two-factor MFA & privileged access management
- Conduct regular security awareness training
- Segment IT/OT networks
- Deploy ICS-specific threat detection
- Use MITRE ATT&CK ICS to map attack surfaces

QUESTIONS?

Contact Us

https://cymanii.org/cymanii-training/

Follow us on social media:

Content Partners and Training Provided By:

CYMANII Officially Endorsed Educational Content

UTSA Cybersecurity for Manufacturing

INL Idaho National Laboratory

NIST

References

- https://www.klogixsecurity.com/blog/strategic-guide-to-mitre-attck-framework
- https://attack.mitre.org/matrices/ics/
- https://www.nist.gov/cyberframework
- https://attack.mitre.org/resources/attack-data-and-tools/
- https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats
- https://time.com/7008613/ukraine-russia-power-sector-frontline/
- https://www.welivesecurity.com/2022/04/12/industroyer2-new-sandworm-malware-targeting-ukrainian-energy-sector/
- https://www.isa.org/standards-and-publications/isa-iec-62443-series
- https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
- https://www.cisa.gov/resources-tools/resources/securing-industrial-control-systems