Cyber Kill Chain for OT

Understanding attack methodologies in industrial environments

OT Security Learning Series

Document 421 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction **3**

2 Lockheed Martin Cyber Kill Chain **3**

3 SANS ICS Kill Chain **4**
3.1 Stage 1: IT/Corporate Intrusion 4
3.2 Stage 2: ICS Attack Development 4

4 Real-World Examples **5**
4.1 Stuxnet Kill Chain 5
4.2 Ukraine Power Grid (2015) 5

5 Defensive Strategies by Stage **5**

6 MITRE ATT&CK for ICS **6**

7 Summary **6**

8 Further Reading **6**

1 Introduction

Information

The Cyber Kill Chain is a framework for understanding the stages of a cyberattack. Originally developed for IT environments, specialized models have emerged for OT/ICS that account for the unique characteristics of industrial control systems.

Why kill chains matter for OT:

- **Structured defense** – Identify where to detect and disrupt attacks
- **Threat intelligence** – Map adversary behavior to stages
- **Gap analysis** – Find weaknesses in defensive coverage
- **Incident response** – Understand attack progression

Warning

OT attacks typically require more stages than IT attacks because adversaries must understand physical processes before causing impact. This extended timeline provides more opportunities for detection.

2 Lockheed Martin Cyber Kill Chain

The original Cyber Kill Chain, developed by Lockheed Martin, defines seven stages of an intrusion:

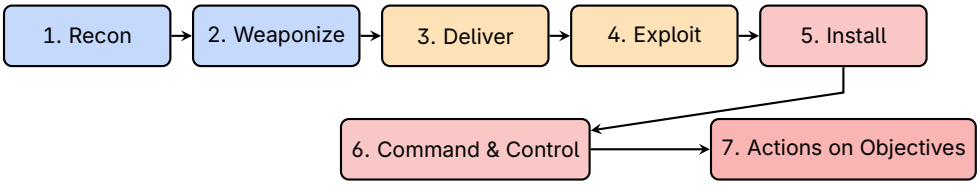

Figure 1: Lockheed Martin Cyber Kill Chain

Stage	Description	OT Example
1. Reconnaissance	Gather information about target	Research SCADA vendors, job postings
2. Weaponization	Create malware/exploit	Develop PLC-specific payload
3. Delivery	Transmit weapon to target	Spear phishing, USB drop
4. Exploitation	Trigger vulnerability	Exploit unpatched HMI
5. Installation	Install persistent access	Deploy RAT on engineering WS
6. Command & Control	Establish communication	C2 via encrypted tunnel
7. Actions	Achieve objectives	Manipulate process, steal data

Table 1: Kill Chain Stages with OT Examples

3 SANS ICS Kill Chain

Two-Stage Model

The SANS ICS Kill Chain recognizes that attacks on industrial control systems require two distinct phases: initial intrusion (similar to IT) followed by ICS-specific attack development and execution.

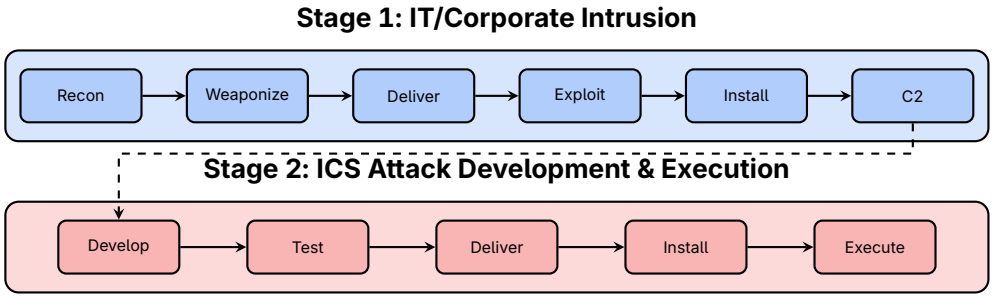

Figure 2: SANS ICS Kill Chain (Two-Stage Model)

3.1 Stage 1: IT/Corporate Intrusion

Follows the traditional kill chain to gain access to the corporate network:

- Target IT systems, email, corporate network
- Goal: Establish foothold and pivot toward OT
- May take weeks to months

3.2 Stage 2: ICS Attack Development

Step	Description
Develop	Create ICS-specific attack capability (requires process knowledge)
Test	Validate attack in lab environment or simulator
Deliver	Transfer attack tools to ICS network
Install/Modify	Deploy on ICS components, modify control logic
Execute	Trigger attack to cause physical impact

Table 2: Stage 2 ICS Attack Steps

Key Point

Key insight: Stage 2 requires significant ICS knowledge. Attackers must understand the physical process, control logic, and potential impacts. This typically requires reconnaissance within the OT environment, extending the attack timeline.

4 Real-World Examples

4.1 Stuxnet Kill Chain

Stage	Stuxnet Activity
Reconnaissance	Years of intelligence gathering on Iranian nuclear program
Weaponization	Custom malware with 4 zero-days, Siemens S7 payloads
Delivery	USB drives, possibly via contractors
Exploitation	Windows vulnerabilities, WinCC database exploit
Installation	Rootkit on Windows, inject code into PLCs
C2	Peer-to-peer updates, limited external C2
ICS Attack	Modified centrifuge speeds while hiding from operators

Table 3: Stuxnet Mapped to Kill Chain

4.2 Ukraine Power Grid (2015)

Stage	Attack Activity
Reconnaissance	Months of network mapping, learning SCADA systems
Weaponization	BlackEnergy malware, KillDisk wiper
Delivery	Spear phishing with malicious Word documents
Exploitation	Macro execution, credential theft
Installation	Persistent access on corporate and SCADA networks
C2	VPN connections using stolen credentials
ICS Attack	Remote HMI access, opened breakers, wiped systems

Table 4: Ukraine Attack Mapped to Kill Chain

5 Defensive Strategies by Stage

Stage	Defensive Measures
Reconnaissance	Limit public information, monitor for scanning
Weaponization	Threat intelligence, malware analysis
Delivery	Email filtering, USB controls, web filtering
Exploitation	Patching, application whitelisting, hardening
Installation	Endpoint detection, integrity monitoring
C2	Network monitoring, DNS analysis, egress filtering
ICS Attack	Process monitoring, anomaly detection, safety systems

Table 5: Defenses Mapped to Kill Chain Stages

Warning

Defense in depth: No single control stops all attacks. Implement detection and prevention at multiple stages to increase the chances of disrupting an attack before impact.

6 MITRE ATT&CK for ICS

Information

MITRE ATT&CK for ICS provides a more detailed framework with specific tactics, techniques, and procedures (TTPs) observed in real ICS attacks. It complements kill chain models with actionable threat intelligence.

Key ICS-specific tactics:

- **Initial Access** – How attackers enter OT networks
- **Execution** – Running malicious code on ICS
- **Persistence** – Maintaining access
- **Evasion** – Avoiding detection
- **Discovery** – Learning OT environment
- **Lateral Movement** – Moving through OT network
- **Collection** – Gathering process data
- **Command & Control** – Maintaining communication
- **Inhibit Response** – Preventing operator action
- **Impair Process** – Disrupting physical operations
- **Impact** – Causing damage or safety incidents

7 Summary

Key Takeaways

- **Traditional kill chain** – 7 stages from recon to actions
- **ICS kill chain** – Two-stage model (IT intrusion + ICS attack)
- **Extended timeline** – OT attacks require process knowledge
- **Detection opportunities** – More stages mean more chances to detect
- **Defense in depth** – Layer controls across all stages
- **MITRE ATT&CK** – Detailed TTPs for threat-informed defense

8 Further Reading

Frameworks

- **MITRE ATT&CK for ICS**
  https://attack.mitre.org/techniques/ics/
- **Lockheed Martin Cyber Kill Chain**
  https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Resources

- **SANS ICS Kill Chain Paper**
  https://www.sans.org/white-papers/36297/
- **CISA ICS Security**
  https://www.cisa.gov/topics/industrial-control-systems

Part of the OT Security Learning Series