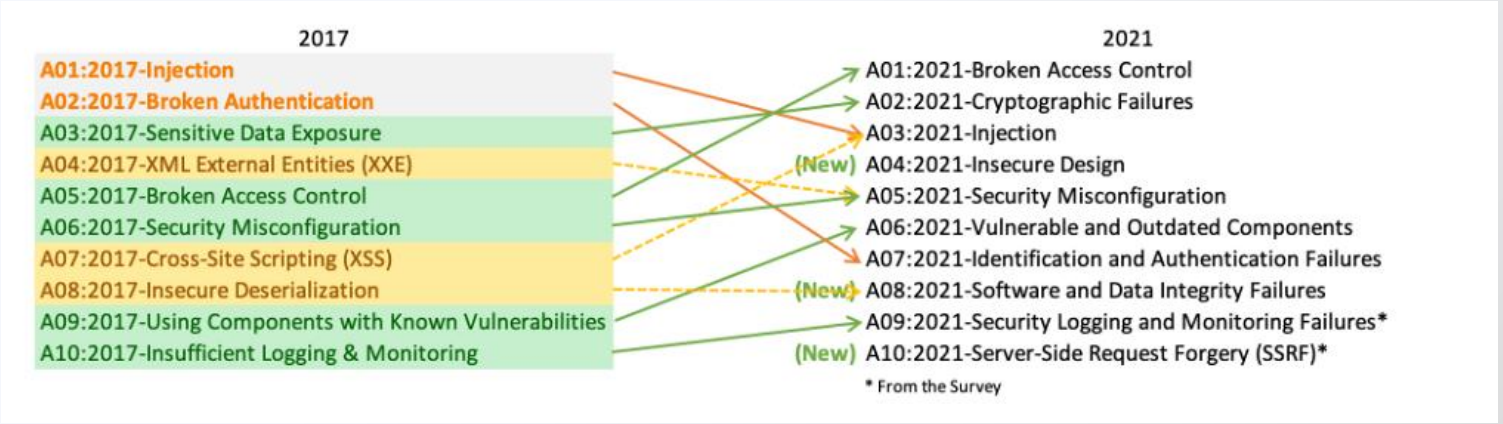
OWASP Top 10 … but for OT?!

Siegfried Hollerer

OWASP - Open Worldwide Application Security Project

- Open community
- Aims to increase (not only) software security
- Free tools and documentation
  - (former OWASP) ZAP
  - JuiceShop

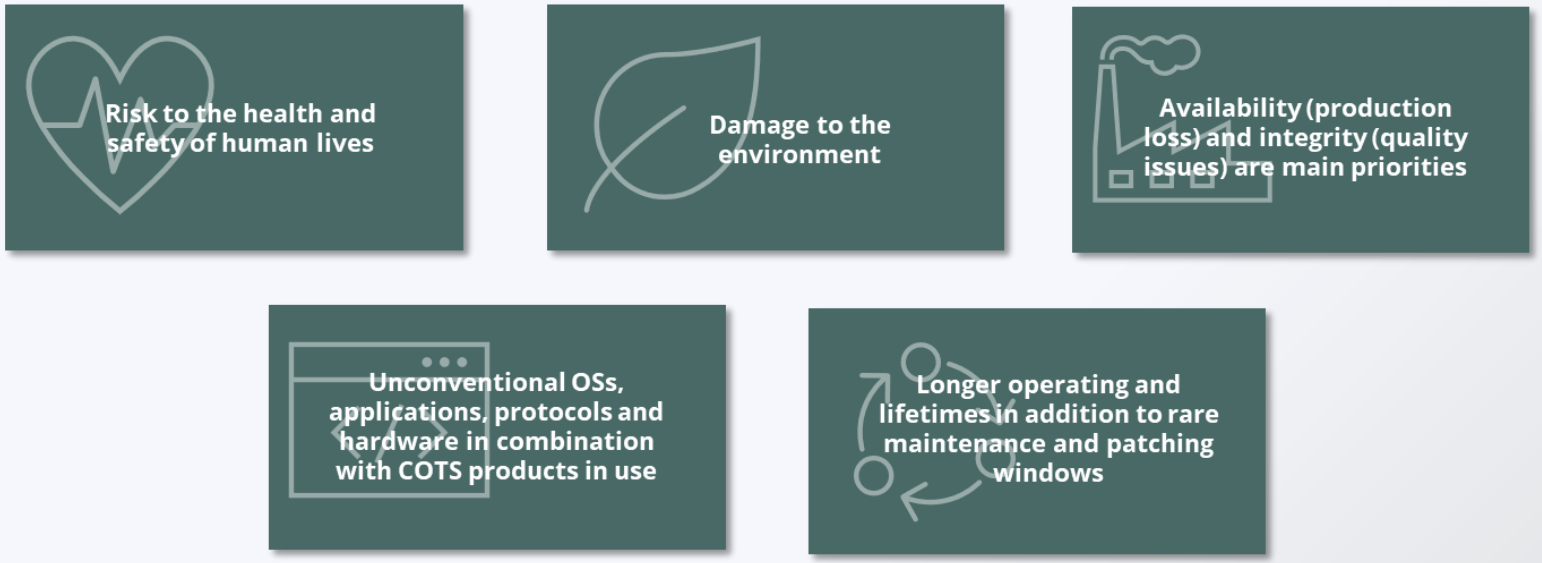
- Well-known through "OWASP Top 10"



What is Operational Technology (OT)?

What is Operational Technology (OT)?

- OT system characteristics differ from traditional IT system characteristics, including additional risks and other priorities



Examples of Cyber Attacks in the Industry

Jahr	Angriff
2008	Agent.bz
2010	Stuxnet
2011	Night Dragon Attacks
2014	Havex
2015	BlackEnergy impacts power supply of Ukraine
2017	TRITON / TRISIS
2018	Ryuk

Examples of Cyber Attacks in the Industry

Jahr	Angriff
2019	LockerGoga
2020	SolarWinds
2021	Cyber attack against US Oil and gas pipeline
2022	Industroyer2
2023	Irrigation systems in Israel attacked
2024	RansomHub

OT vs. IT Security

Security vs. Safety

- Security
  - Protect against threats to technical (IT/OT) systems
  - Raising from humans or the environment
  - e.g.: Hackers/attackers, unintentional error of worker, earthquakes

- Safety
  - Protect against hazards to humans or the environment, including accidents and injuries
  - Raising from technical (IT/OT) systems
  - E.g., emergency stop of nuclear power plants

OT Security vs. IT Security

- Different prioritization of security goals (CIA triad)
  - High focus on availability
  - Example: web shop vs. railway barriers are closing delayed

- Typical worst-case scenario
  - Loss of Safety
  - Loss / Manipulation of Control
  - Loss / Manipulation of View

Focus on Availability

- How to deal with updates?
- Already in product development
  - Plain text network protocols
- When (and how) to test?
- Potential regulations?

Life Cycle

- IT: 2-4 years
- OT: 1-3 decades

- Which security mechanisms did we have 30 years ago?
  - At the asset layer?
  - At the protocol layer?

- Many legacy devices to deal with

Supply Chain

- Asset Owner/Operators, Integrators and vendors/manufacturers

- Only a few vendors/manufacturers available

  - SLAs deny changes on a system including installation of security solutions

To sum up…

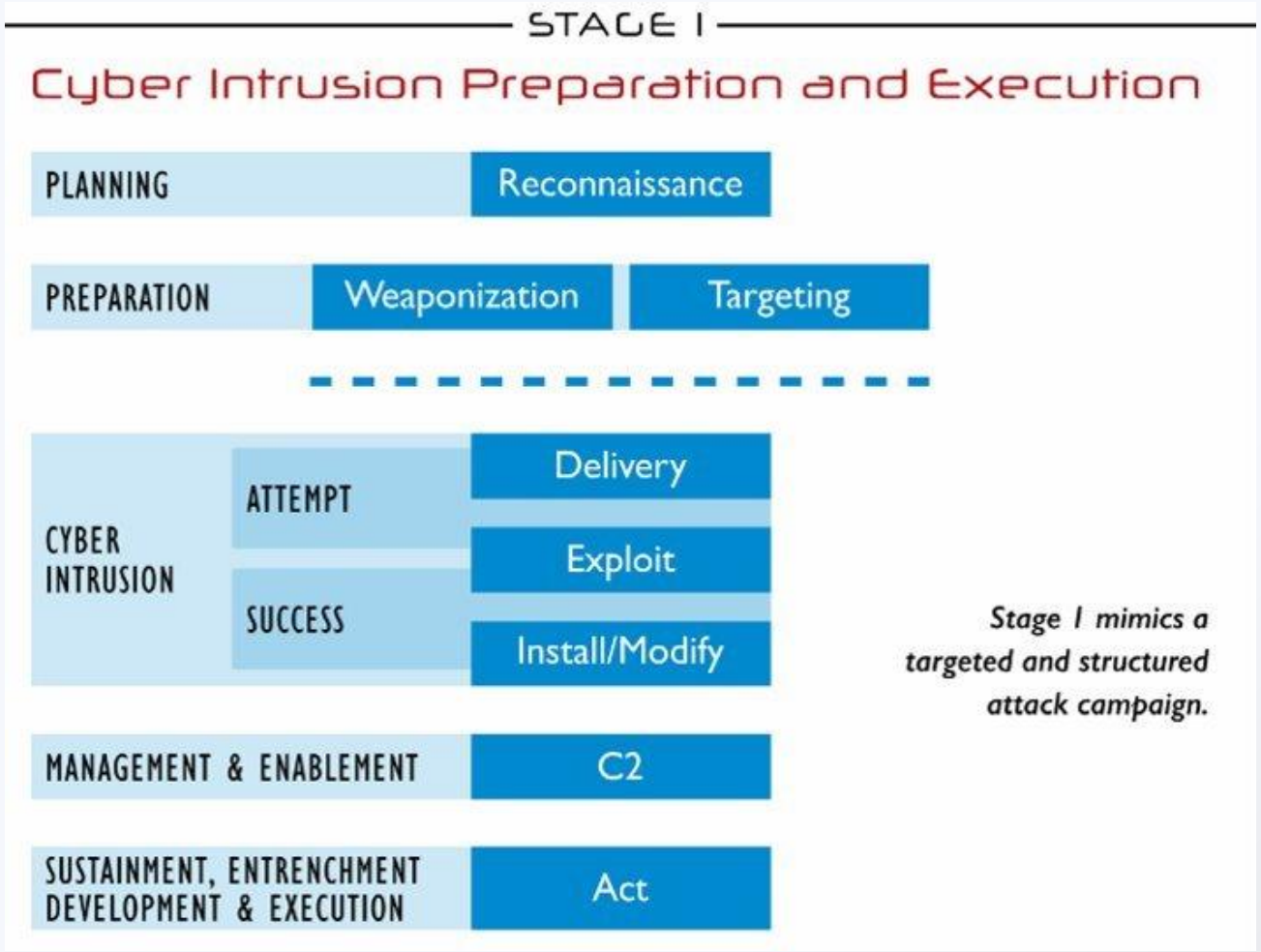
- Focus on safety & availability (not security)
  - Devices are hard to update/patch
- Long life cycles
- Only few vendors

Leads to...

- Devices have to be protected
  - Network segmentation
  - Physical access control
  - Etc.

OT Kill Chain

OT Kill Chain – Stage 1



Source: https://sansorg.egnyte.com/dl/HHa9fCekmc

OT Kill Chain – Stage 1

- Similar to classical IT attack
  - Cf. Cyber Kill chain from Lockheed Martin
- Purpose
  - Information gathering and initial access to the OT system

- Planning
  - **Reconnaissance**: Information gathering
    - Active/Passive (incl. OSINT)
- Preparation
  - **Weaponization**: Generate malicious data
    - E.g., PDFs, Scripts, binaries, etc.
  - **Targeting**: Choose attack vector
    - E.g., Internet-facing firewall for VPN connections, web server, e-mail server

OT Kill Chain – Stage 1

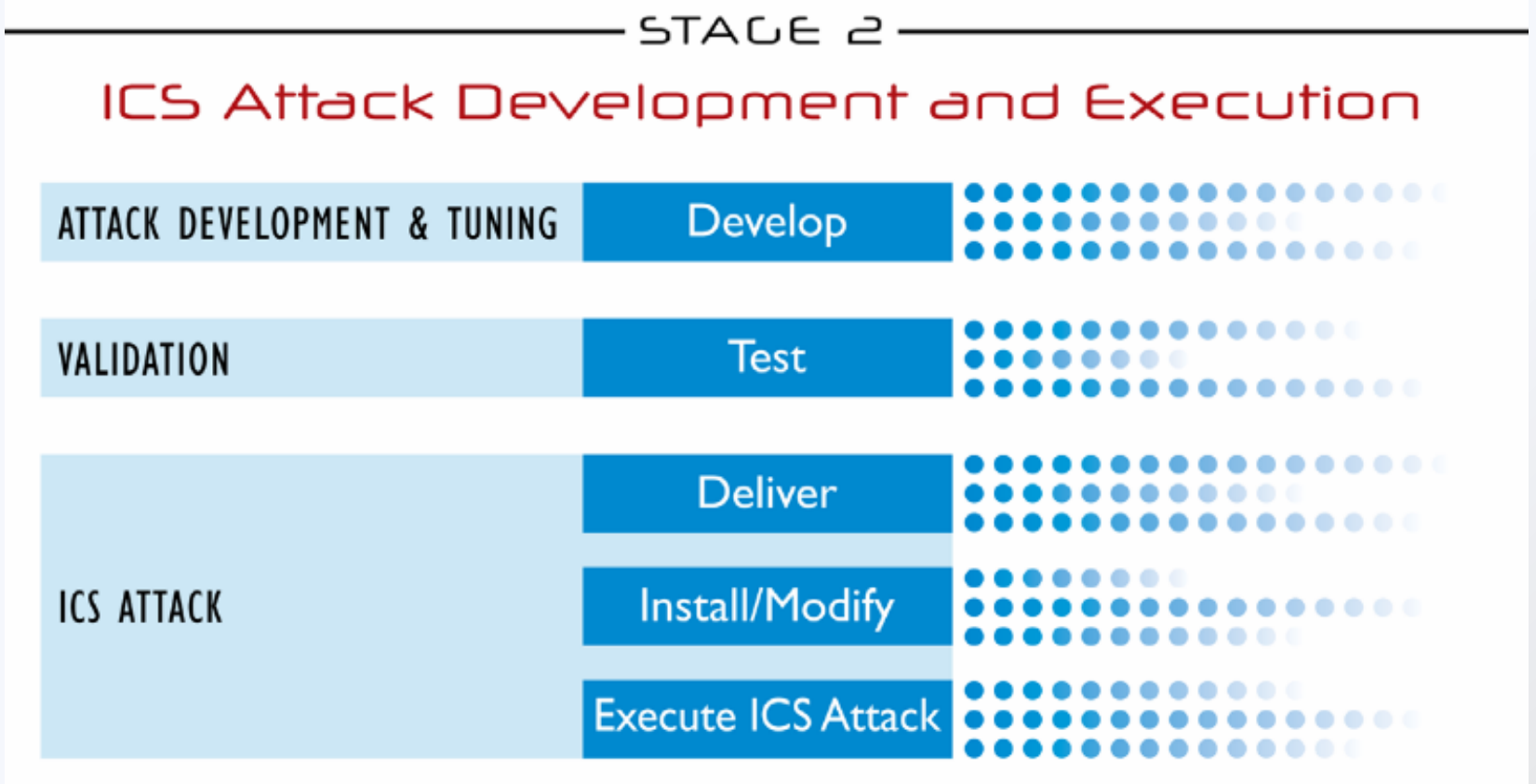
- Cyber intrusion
  - **Delivery**: Interaction with internal network
    - Phishing mail delivers malicious PDF file
    - VPN connection forwards attacker directly to the internal network
  - **Exploit:** Vulnerability gets exploited
    - Malicious PDF file was opened (and unintentionally executed)
    - Use credentials for VPN connections obtained or reconstructed via information gathering
  - **Install/Modify:**
    - Installation of a trojan
    - Use existing on board resources
      - PowerShell, cmd, bash, pyhton, ruby, gcc, etc.

OT Kill Chain – Stage 1

- Management and enablement phase
  - **C2 (command and control):** Initiate persistent access
    - Connection won‘t get lost despite detection and deletion
    - Often hidden in incoming or outgoing communication, existing connections get hijacked
    - Infiltrate equipment (e.g., LAN turtle)

- Sustainment, Entrenchment, Development & Execution
  - **Act:** Accomplish goals of the attack
    - Analyze new systems and data in the network
    - Data theft
    - Lateral movement / post exploitation in the network
    - Encryption of data, placing ransomware

OT Kill Chain – Stage 2



Source: https://sansorg.egnyte.com/dl/HHa9fCekmc

OT Kill Chain – Stage 2

- Attack development and tuning
  - (Process-)specific, individual attack is developed
    - Often offline based on the exfiltrated data of the OT system
    - Hard to detect
    - Significant delay between stage 1 and finishing this phase

- Validation
  - Test the attack against similar or identical configured systems or components (e.g., digital twins)

OT Kill Chain – Stage 2

- ICS Attack
  - cf. stage 1 (deliver, install, execute)
  - Impact
    - Loss of View / Control / Safety
    - Denial of View / Control
    - Manipulation of View / Control / Sensors and Instruments

OWASP OT Top 10

Structure of Each OT Top 10 Item

- Name
- Description
- Rationale
- Known Attacks/Examples
- Mitigations/Countermeasures
- Next Actionable Steps
- References

OT Top 10 - Overview

Unknown Assets and Undocumented Services	Devices with Known Vulnerabilities	Inadequate Supply Chain Management	Loss of Availability
Insufficient Access Control	Missing Incident Detection/Reaction Capabilities	Broken Zones and Conduits Design	Missing Awareness
	Insufficient Security Capabilities	Missing Hardening	

Example: **Unknown Assets and Undocumented Services**

- Not recorded devices or services in the OT system
- These get not updated or managed
  - Are potential vulnerabilities in the system
  - There shouldn‘t be unnecessary processes or devices in OT systems

- Discussed in OT Top 10 item
- 1. Unknown Assets and Undocumented Services

Example: **Loss of Availability**

- Availability in OT
  - Services
  - Processes
  - Real physical devices

- Discussed in OT Top 10 item
- 4. Loss of Availability

Mapping Table

- Links each OWASP OT Top 10 category to standards and regulations
  - IEC 62443 (inkl. 62443-2-1:2019, 62443-3-2:2020, 62443-3-3:2020, 62443-2-4:2024, 62443-4-1:2018, 62443-4-2:2020)
  - NIST SP 800-82:v3
  - NIST CSF 2.0
  - MITRE ATT&CK Framework
  - EU NIS2 Implementing regulation C(2024) 7151 - Annex
  - ISO27001 Annex (only section 6)

Emergence and Contribution

Methodology Behind Owasp OT Top 10

- Based on public reports and analysis
  - ENISA threat landscape 2024 and CI sector landscapes
  - Threat reports from different vendors/manufacturers
  - Best practices and experiences from the industry
  - Pentest census from Limes Security
  - Analyse report from OMICRON Energy
  - …

Methodology Behind Owasp OT Top 10

- Experience of the contributors
  - OT penetration testing and security testing
  - OT security architect
  - OT security analyst
  - OT security management
  - OT vulnerability research
  - OT incident / response
  - Academic research
- Living project

List of Contributors

Andreas Happe (Co-Leader)

Siegfried Hollerer (Co-Leader)

University of Applied Sciences St. Pölten

Bundesministerium Inneres

Simon Rommer (Co-Leader)

OMICRON

Nino Fürthauer

LIMES SECURITY

Felix Eberstaller

LIMES SECURITY

Sixtus Leonhardsberger

LIMES SECURITY

And others...

Thank you for Listening

- Release was in October 2025
- Release cycles not yet fixed
  - Maybe every two years?

- https://ot.owasp.org
  - Managed on github
  - Open for All
  - Pull-Requests Welcome!

$ whoami

Siegfried Hollerer

Security Architect & Analyst @ BMI

Lektor @ FH STP

siegfried.hollerer@bmi.gv.at

linkedin.com/in/siegfried-hollerer-1ab397162

scholar.google.com/citations?user=DOVpGMUAAAAJ