



Hacking Industrial Control Systems

*Insights on **IT/OT Security**, (Legacy) **Protocols**
and **Security Advisories** at **Siemens***

ACSC 2026 – CoE Event Siemens

Rechtlicher Haftungsausschluss

Die Inhalte dieser Präsentation dienen ausschließlich zu Bildungs- und Informationszwecken. Alle in dieser Vorführung gezeigten oder besprochenen Hacking-Techniken und Cybersecurity-Methoden sind auf kontrollierte Umgebungen und legale, autorisierte Tests ausgelegt.

Wichtige Hinweise:

1. **Keine illegale Aktivität:** Jede Form von unautorisiertem Zugriff auf Computer- oder Netzwerksysteme, die nicht Ihnen gehören oder für die Sie keine ausdrückliche Genehmigung zur Durchführung von Tests erhalten haben, ist rechtswidrig. Cyberkriminalität ist eine ernste Straftat und kann zu strafrechtlichen Konsequenzen führen.
2. **Verantwortung des Nutzers:** Wir übernehmen keine Haftung für Schäden, die aus der, insbesondere unsachgemäßen oder illegalen, Anwendung der in dieser Vorführung gezeigten Informationen resultieren. Zuschauer sind dafür verantwortlich, die gesetzlichen Vorschriften zu kennen und einzuhalten.
3. **Keine Beratung:** Diese Vorführung stellt keine Rechts- oder Sicherheitsberatung dar. Konsultieren Sie bei rechtlichen oder sicherheitsrelevanten Fragen immer Fachleute.
4. **Professionelle Anwendung:** Die in dieser Vorführung gezeigten Techniken sollten ausschließlich von professionellen Cybersecurity-Expert*innen im Rahmen von Penetrationstests, ethischem Hacking oder ähnlichen legalen Aktivitäten verwendet werden.

Durch das Ansehen dieser Vorführung oder das Testen einer der angebotenen Simulationen erklären Sie sich damit einverstanden, diese Regeln einzuhalten und die in dieser Vorführung bereitgestellten Informationen nur in Übereinstimmung mit dem Gesetz zu nutzen.

Attack Target?



oil refinery



port logistics



hydropower plant

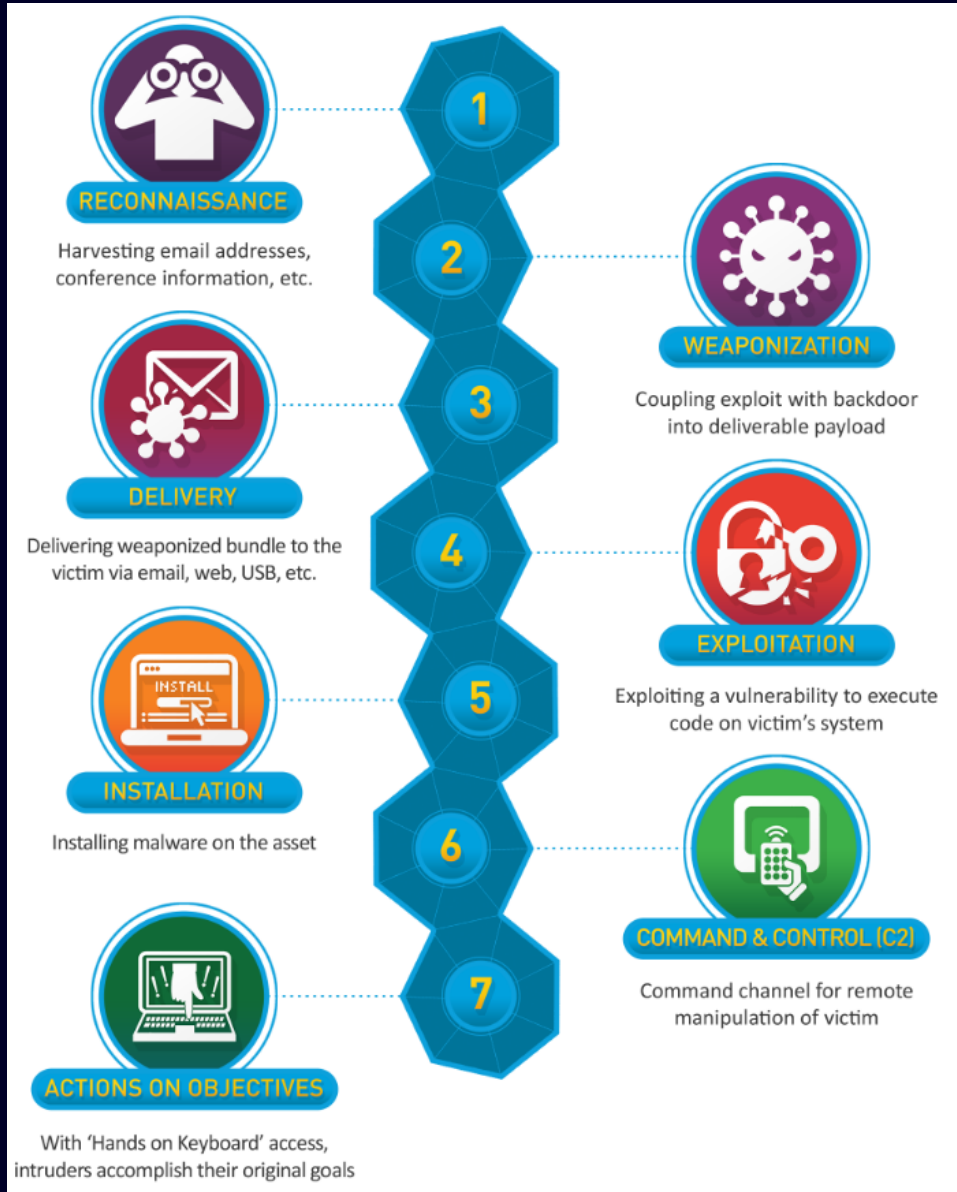


car manufacturer

Images <https://www.pexels.com/>

Why?

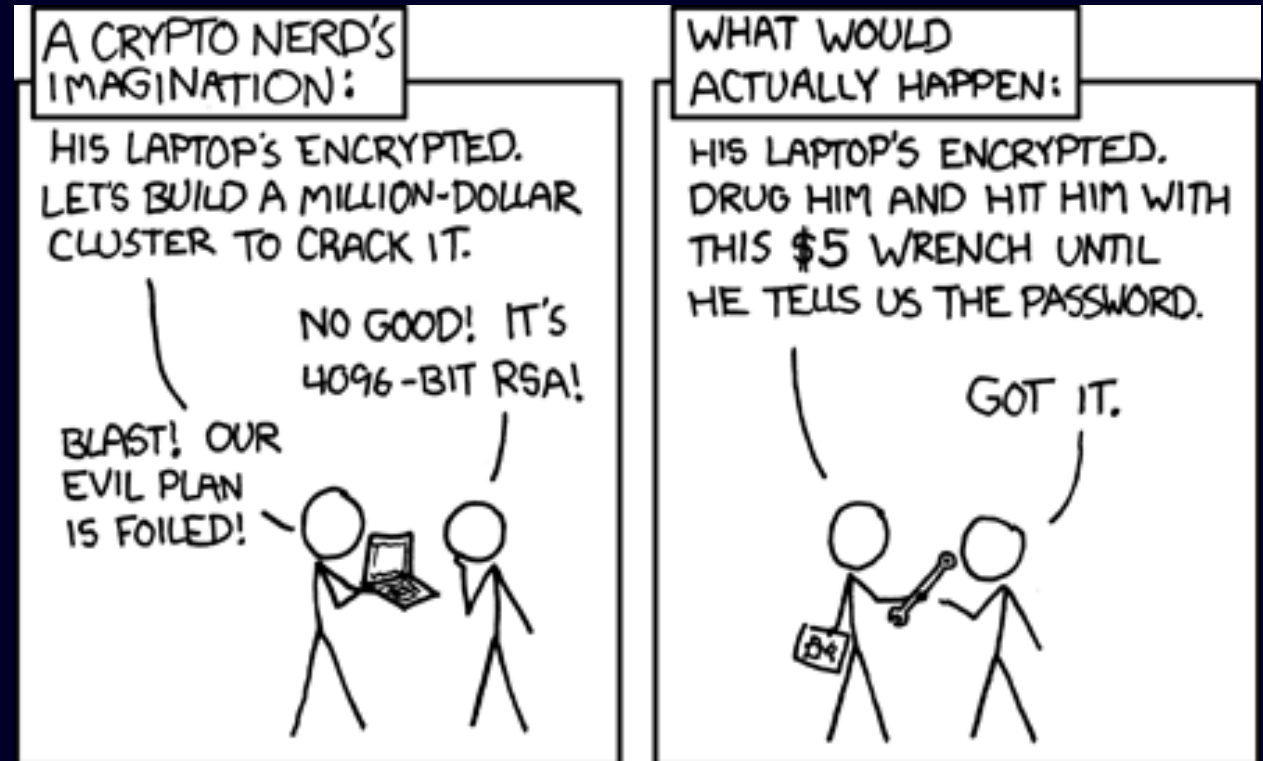
First Steps?



- Cyber Kill Chain
- ... models sequential stages of a cyber attack

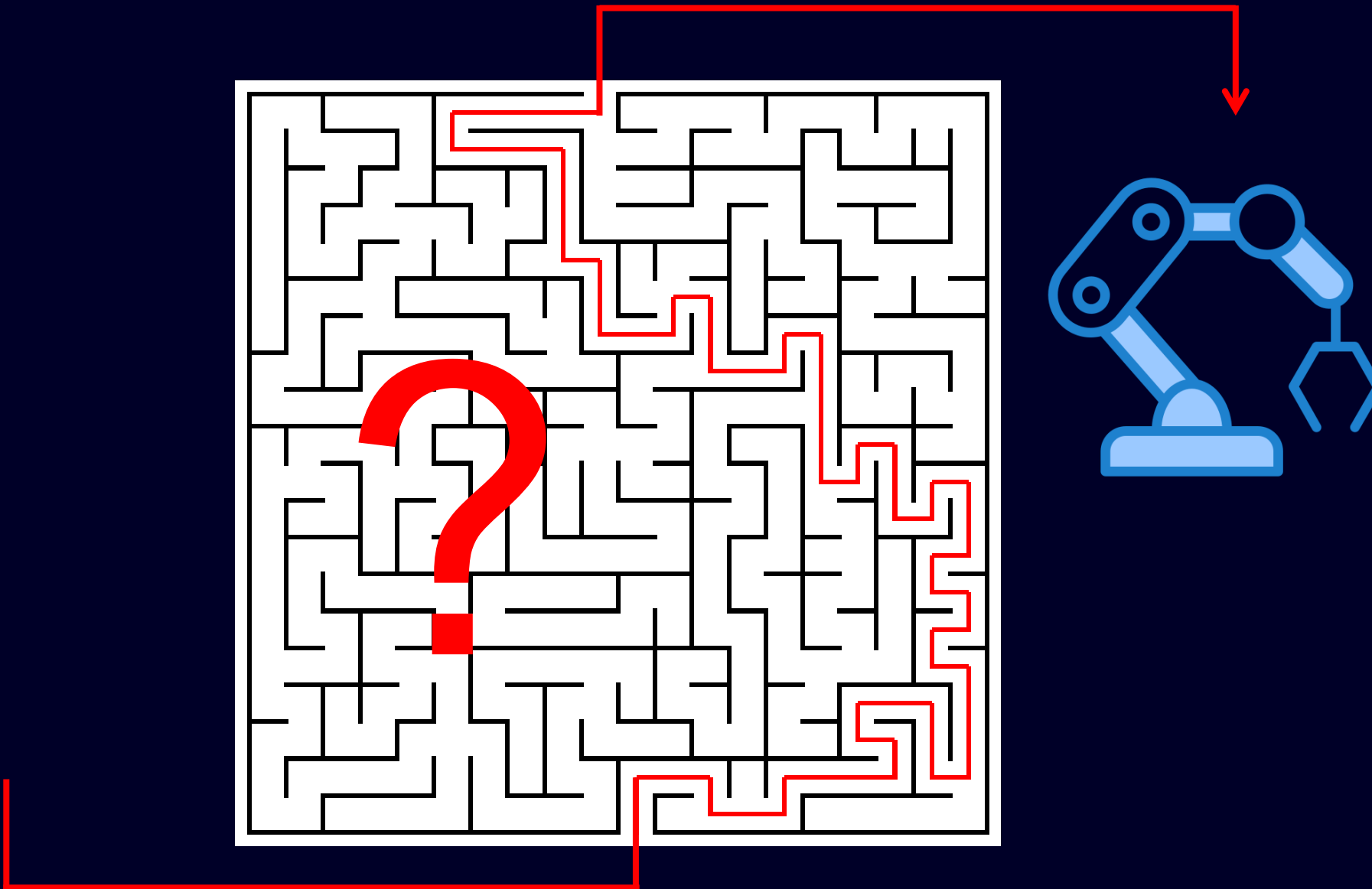
Initial Access?

- Physical Access
- Insider Threat
- Phishing, Social Engineering
- Exploiting Public-Facing Applications
- Guest WiFi
- Stolen Credentials
- Supply-Chain-Attacks
- 5 Dollar Wrench
- ...



<https://xkcd.com/538/>

Initial Access ✓



Topic 1: IT/OT Network Segmentation

DMZ
(Demilitarized Zone)

IT

(Information Technology)

OT

(Operational Technology)



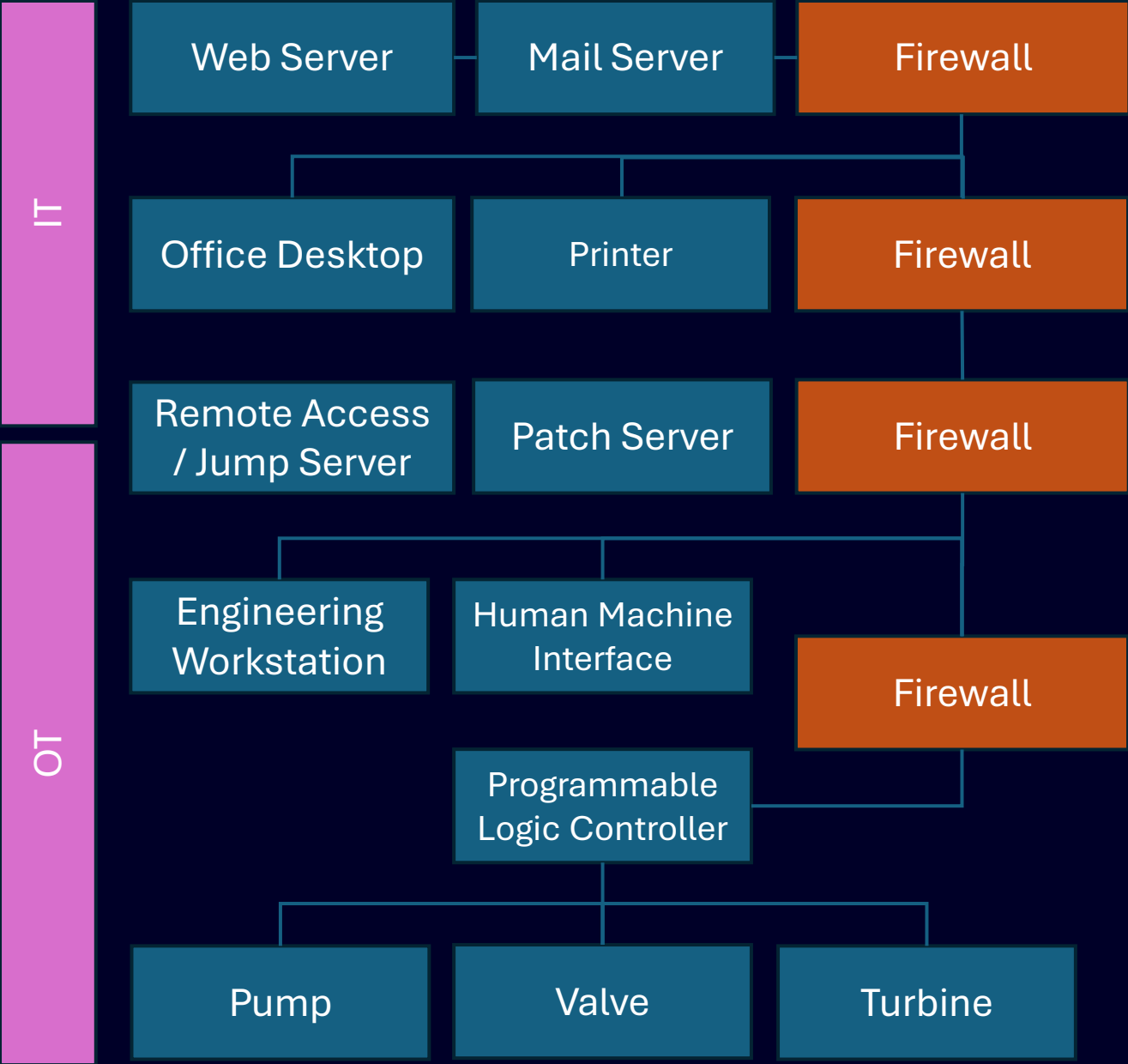
IT/OT?

Network Layout of a hydropower plant



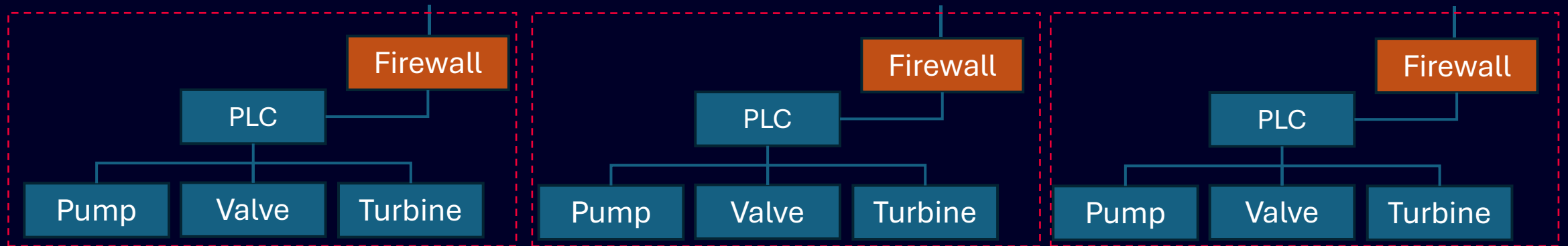
<https://www.pexels.com/photo/massive-water-flow-on-a-dam-2796964/>

DMZ



Cell Protection Concept

- Most important: Separation between production and office networks
- Shouldn't result in production being one flat network
- Subdivision of production into protected cells
- **Protected Cell**: Self-Contained, (semi-)automated production unit to perform a specific task
- Reduce attack surface and prevent lateral movement if one cell is compromised
- Prevent a local incident from becoming a plant-wide shutdown



A Cell In Practice

A Cell In Practice

1. Power Supply

Depending on the components in an automation cell.

Global standard for control and sensor systems (PLCs, Relays, ...) -> 24V DC



A Cell In Practice

2. Industrial Router

Key component in segmentation of industrial network

Compared to home router: Rugged housing for harsh environments, support of OT protocols, ...



3. Industrial Switch

A cell in practice

3. PLC

„Brain“ behind the automation

Continuously monitors inputs from sensors and execute pre-programmed logic to control outputs

Cycle Time: Time it takes for a PLC to read physical inputs, execute user program, update outputs

Depends on implemented application and components

Typically 10-20ms for common industrial logic



A cell in practice

4. (Decentral) I/O System

Sensors (inputs) and Actuators (outputs) a PLC needs to control might be spread across longer distances and result in complex, expensive wirings

Put I/O System closer to field devices and connect to PLC using single ethernet cable.



A cell in practice

Siemens SCALANCE S
(firewall at boundary of network cell)

Cell 1



Siemens SCALANCE X
(managed switch to connect within cell components)



Siemens ET200
(I/O System)



Sensors / Actuators

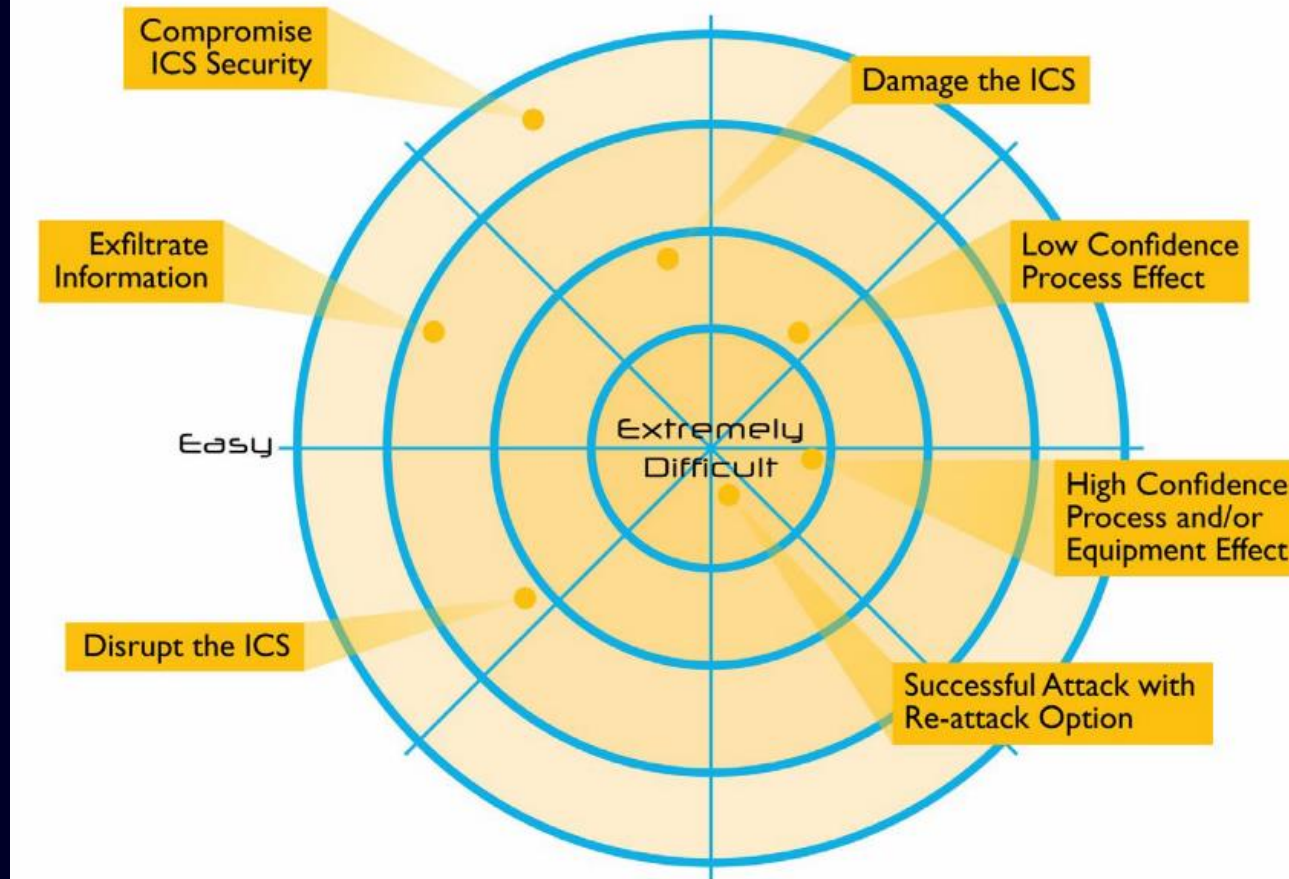


Siemens PLC
(Controller with program logic)

Cell 2



ICS Attack Difficulty



"The Industrial Control System Cyber Kill Chain", Michael J. Assante and Robert M. Lee, October 2015: <https://sansorg.egnyte.com/dl/k7gJ2gVBj5>

Stuxnet

- Attack on Iran nuclear program, discovered in 2010
- Self-replicates through auto-execution from USB drives
- Spreads via network exploiting multiple Windows vulnerabilities (SMB, Print Spooler, ...)
- If host with Siemens Step7 Software is found:
 - Fingerprints a specific industrial control system (ICS)
 - Modifies code transferred to Siemens PLCs



<https://www.theguardian.com/world/2021/apr/12/natanz-nuclear-facility-sabotage-iran-vulnerability-to-cyber-attacks>

 View Report

 Download Results

 Historical Trend

 View on Map

 Advanced Search

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

2026-06-15T05:44:48.335590

SNMP:

Uptime: 1

Description: Siemens, SIMATIC, S7-1500, CPU 1515-2 PN, HW: 3, FW: V2.9.4

Service: 72

Versions:

1

3

Engineid.Format: octets

Contact:

Engine Boots: 2

2026-06-14T15:31:12.615855

S7 Protocol (S7comm+) - Siemens SIMATIC S7-1500 CPU Firmware V3.1.1.0\r\n

2026-05-30T01:29:48.240647

SNMP:

Description: Siemens, SIMATIC S7-1500, CPU 1516-3 PN/DP, HW Rev: 4, FW: V3.1.2,

Versions:

1

Next Steps?

`(root@kali)-[/tmp]`

`# nmap -v ...`

Starting Nmap 7.98 (<https://nmap.org>) at 2026-06-15 16:04 +0200

Initiating SYN Stealth Scan at 16:04

Scanning localhost (...) [1000 ports]

Discovered open port 22/tcp on 127.0.0.1

Discovered open port 80/tcp on 127.0.0.1

`...`



Topic 2: (Legacy) OT Protocols

Secure / Insecure?

`(root@kali)-[/tmp]`

`# nmap -v ...`

Starting Nmap 7.98 (<https://nmap.org>) at 2026-06-15 16:04 +0200

Initiating SYN Stealth Scan at 16:04

Scanning localhost (...) [1000 ports]

Discovered open port 22/tcp on 127.0.0.1

Discovered open port 80/tcp on 127.0.0.1

`...`

Completed SYN Stealth Scan at 16:04, 0.04s elapsed (1000 total ports)

- TCP 23 → Telnet
- UDP 69 → TFTP
- TCP 102 → S7
- UDP 161 → SNMP
- TCP 502 → Modbus
- UDP 514 → Syslog
- TCP 4840 → OPC-UA
- UDP 34964 → PROFINET
- TCP 44818 → Ethernet/IP
- ...

Telnet

TCP/UDP Port: TCP/23

Part of Nmap Top 1000 ports: Yes

Purpose: CLI for remote access to a server or network device

Characteristics:

- Client-server architecture
- Uses a virtual terminal connection
- Transmits data in plain text
- Supports basic authentication (username/password)

Security:

Confidentiality	Integrity	Authenticity
none	none	weak

Successor / Alternative: SSH

TFTP

TCP/UDP Port: UDP/69

Part of Nmap Top 1000 ports: Yes

Purpose: Lightweight protocol for transferring files between network devices

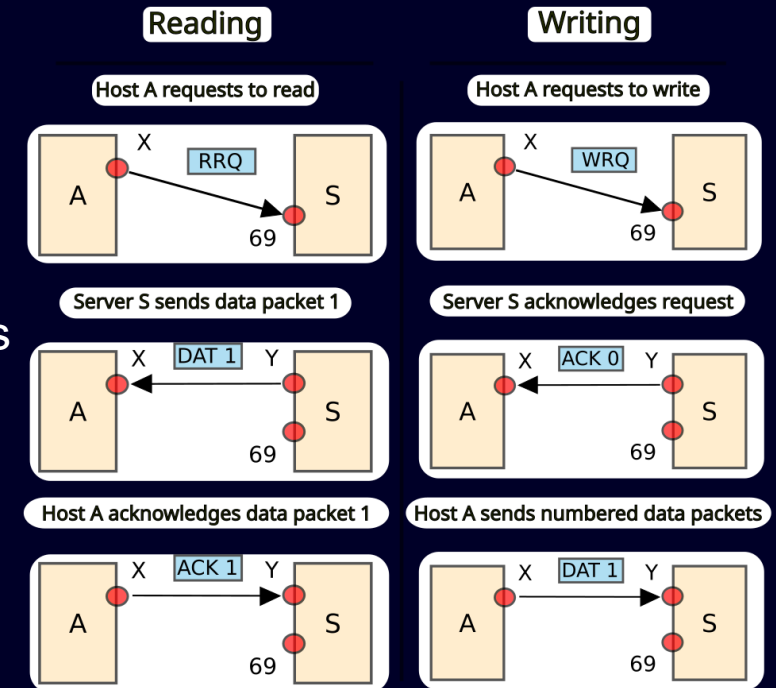
Characteristics:

- Client-server architecture
- Uses UDP, making it connectionless and unreliable
- Limited functionality compared to FTP

Security:

Confidentiality	Integrity	Authenticity
none	none	none

Successor / Alternative: SFTP



From one of our product manuals ...

Device management

4.5.2 Uploading/downloading files using a TFTP client

4.5.2 Uploading/downloading files using a TFTP client

To upload or download a file using a TFTP client, do the following:

NOTICE

Security hazard – risk of unauthorized access and/or exploitation

TFTP does not define an authentication scheme. Any use of the TFTP client or server is considered highly insecure.

SNMP v1/v2c

TCP/UDP Port: UDP/161,162
Part of Nmap Top 1000 ports: Yes

Purpose: Managing and monitoring of network devices

Characteristics:

- Uses Management Information Bases (MIBs) to define managed objects
- Supports "Get," "Set," and "Trap" operations
- Versions: SNMPv1, SNMPv2c (authentication with “community strings”), SNMPv3

public /
private

Security:

- v1/v2c

Confidentiality	Integrity	Authenticity
none	none	weak

Successor / Alternative: SNMPv3

Syslog

TCP/UDP Port: UDP/514

Part of Nmap Top 1000 ports: Yes

Purpose: Standard for sending system log or event messages to a central server.

Characteristics:

- Supports various message severities and facilities
- Originally used UDP, making it unreliable (messages can be lost)
- RFC 5424 defines an updated syslog protocol with more features

Security:

Confidentiality	Integrity	Authenticity
none	none	none

Successor / Alternative: Syslog over TLS (RFC 5425) for encryption and authentication

S7 (PUT/GET)

TCP/UDP Port: TCP/102

Part of Nmap Top 1000 ports: Yes

Purpose: Programming, monitoring, and controlling SIMATIC S7 PLCs

Characteristics:

- Proprietary to Siemens
- Used extensively in industrial control systems (ICS) and SCADA environments
- Can operate over various network layers, including TCP/IP

Security:

Confidentiality	Integrity	Authenticity
none	weak	weak

Successor / Alternative: S7Plus / OMS+



Modbus/TCP

TCP/UDP Port: TCP/502

Part of Nmap Top 1000 ports: Yes

Purpose: Used in industrial control systems for communication between devices.

Characteristics:

- Client-server architecture
- Simple, open, and widely adopted
- Supports various data types (coils, discrete inputs, input registers, holding registers)

Security:

Confidentiality	Integrity	Authenticity
none	weak	none

Successor / Alternative: Modbus/TCP over TLS, OPC UA, PROFINET

Recap

Protocol	Confidentiality	Integrity	Authenticity
Telnet	None	none	weak
TFTP	none	none	none
S7 (PUT/GET)	none	weak	weak
SNMP v1/v2c	none	none	weak
Modbus/TCP	none	weak	none
Syslog	none	none	none

Why These Protocols Pose Challenges

- **Lack of Authentication/Encryption**

Many were designed for isolated networks where physical security was the primary concern, not cybersecurity threats.

- **Proprietary Nature**

Some are proprietary, making it harder for third-party security tools to inspect or secure them.

- **Deeply Embedded**

Replacing these protocols often means replacing critical, long-lived hardware, which is expensive and can cause significant downtime.

- **Real-time Requirements**

Introducing security measures like encryption can sometimes add latency, which is unacceptable in time-sensitive control systems.

Best Practices for Dealing with Legacy (OT) Protocols

- **Network Segmentation**
Isolate OT networks from IT networks and use segmentation with VLANs.
- **Protocol Gateways**
Implement secure gateways that translate legacy protocols to secure ones.
- **Secure Remote Access**
For remote access, use VPNs (with MFA) rather than direct connections.
- **Continuous Monitoring**
Implement robust network monitoring to detect unusual traffic patterns (IDS/IPS).
- **Patching and Updates**
Apply security patches and firmware updates to devices and systems where possible.



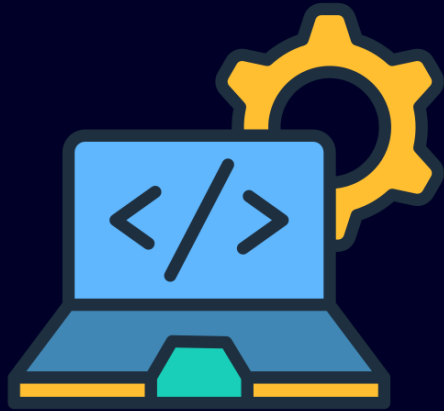
PROFINET < V2.5

Security:

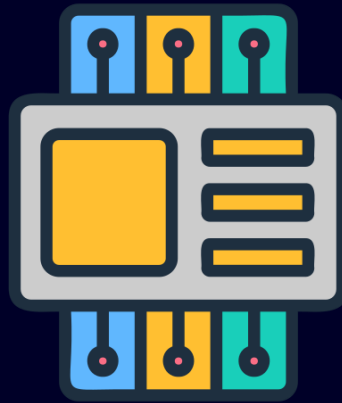
Confidentiality	Integrity	Authenticity
weak	weak	weak

PROFINET Device Types

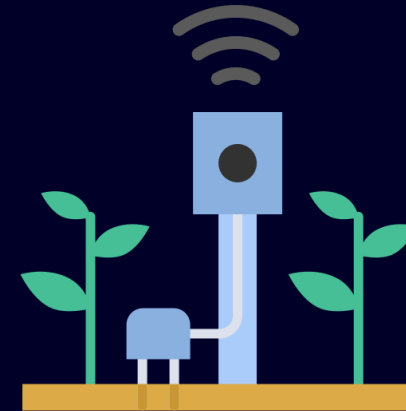
I/O Supervisor
(e.g. TIA Portal v20)



I/O Controller
(e.g. Simatic S7-1500 PLC)

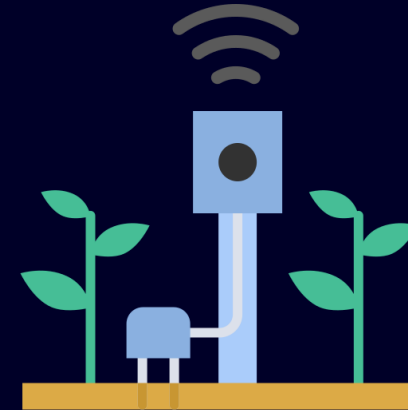
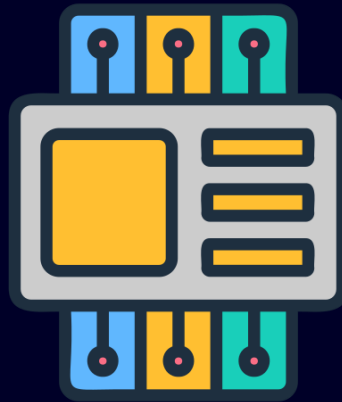
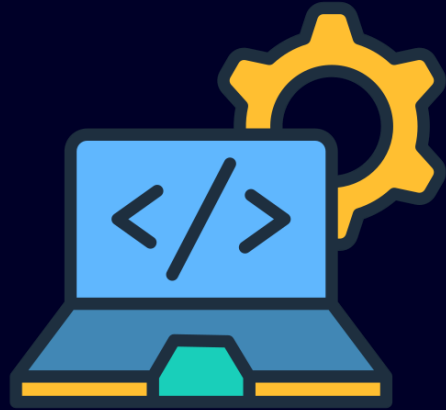


I/O Device
(e.g. Sensors, Drives, etc.)



PROFINET communication

PROFINET Communication Channels



Cyclic Data: IO Data

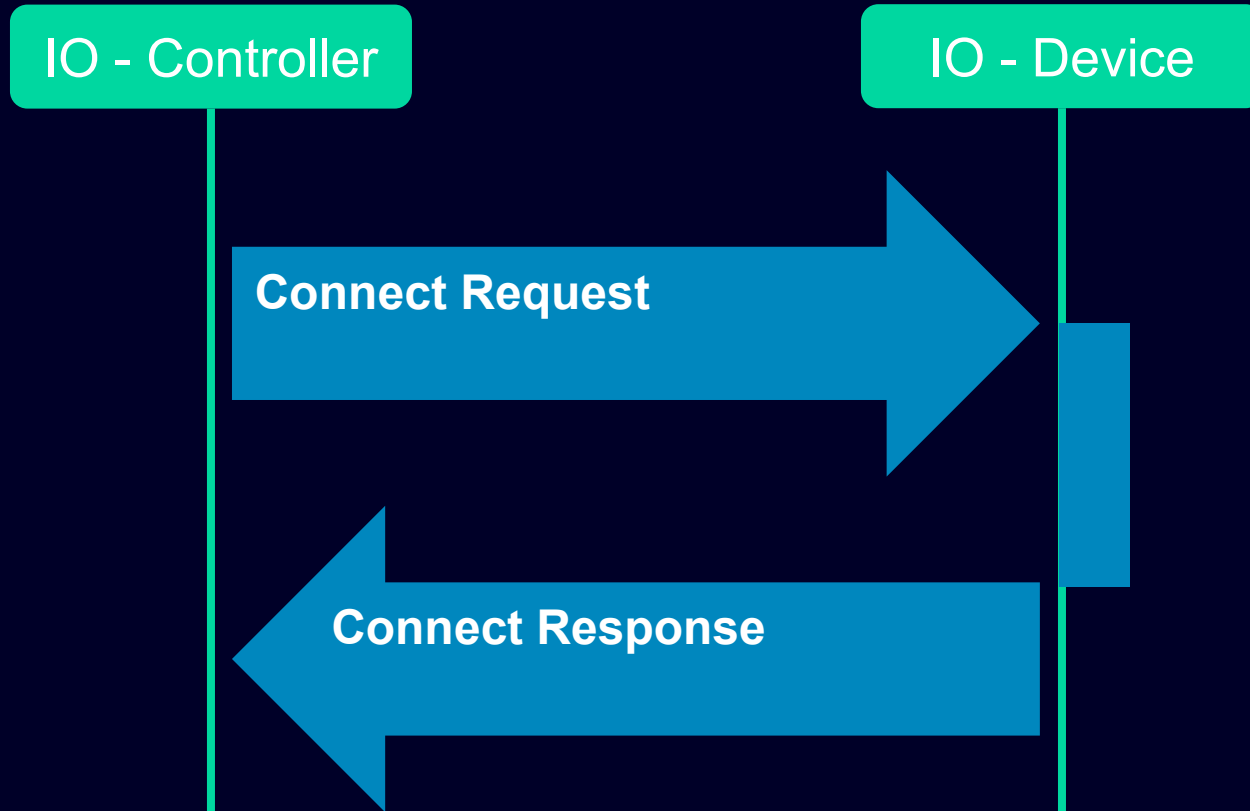


Acyclic Data: Records



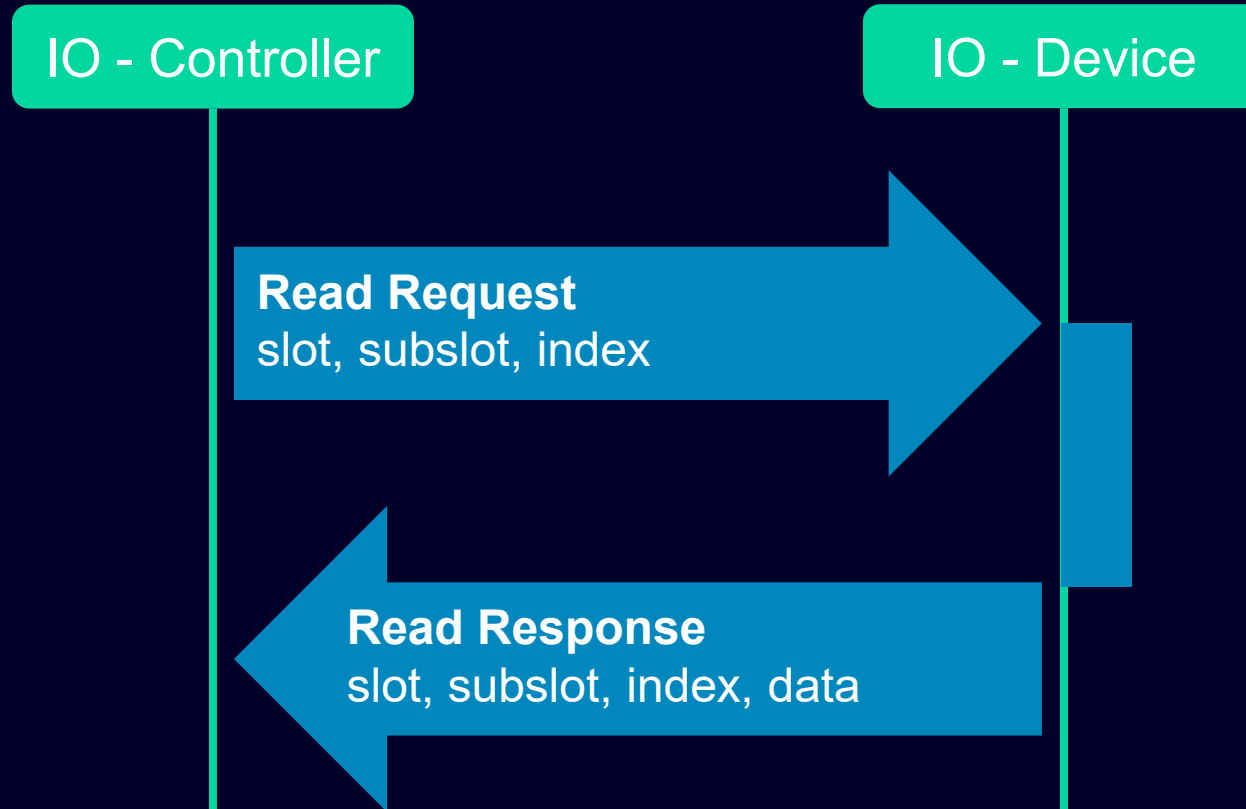
Acyclic Data: Alarms

Application Relation (AR)



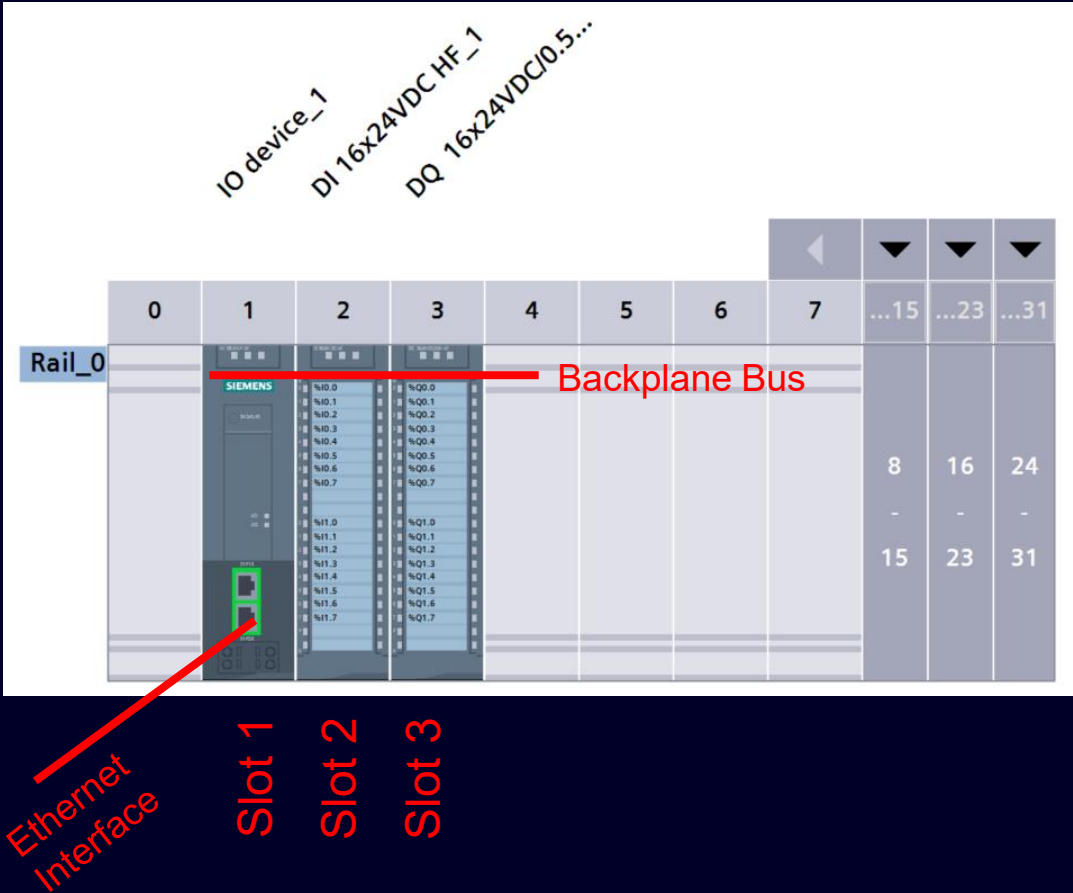
- Communication initialized by establishing AR
- Content of Request:
 - Cyclic Communication Relations (+Timing)
 - Input
 - Output
 - Expected Submodules
 - Alarm Communication Relations
- Content of Response:
 - OK / Not OK
 - Diff between expected vs present modules

Read Record



```
# IODReadRe{q,s}
class IODReadReq(Block):
    """IODRead request block"""
    fields_desc = [
        BlockHeader,
        ShortField("seqNum", 0),
        UUIDField("ARUUID", None),
        XIntField("API", 0),
        XShortField("slotNumber", 0),
        XShortField("subslotNumber", 0),
        StrFixedLenField("padding", "", length=2),
        XShortEnumField("index", 0, IOD_WRITE_REQ_INDEX),
        LenField("recordDataLength", None, fmt="I"),
        StrFixedLenField("RWPadding", "", length=24),
    ]
```

Slots, Indices, ...



Index	Name
0x800A	Diagnosis channel subslot
0x800B	Diagnosis all subslot
0x800C	Diagnosis maintenance subslot
0xAFF0	I&M 0 manufacturer data
...	...

PROFINET V2.5



- Important Update for conformity with EU Cyber Resilience Act (CRA)
- New SXP (Service Exchange Protocol) for Layer-2 and Layer-3 communication
- Secure Access, secure communication from outside of cell with IO-Controller and IO-Devices (e.g. when applying firmware updates)
- Secure Realtime, adds encryption and authenticity for cyclic and acyclic RT communication between IO-Controller and IO-Device

Security:

Confidentiality	Integrity	Authenticity
present	present	present

EtherNet/IP



TCP/UDP Port: TCP/44818, UDP/2222
Part of Nmap Top 1000 ports: No

Purpose: Used for real-time control, configuration, and data acquisition in industrial automation.

Characteristics:

- Leverages the Common Industrial Protocol (CIP) for application-layer messaging
- Supports cyclic (real-time I/O) and acyclic (messaging) messaging
- Open standard managed by ODVA (Open DeviceNet Vendors Association)

Security:

Confidentiality	Integrity	Authenticity
weak	weak	weak

Successor / Alternative: EtherNet/IP with CIP Security

EtherNet/IP with CIP Security



TCP/UDP Port: TCP/44818, UDP/2222
Part of Nmap Top 1000 ports: No

Purpose: Used for real-time control, configuration, and data acquisition in industrial automation.

Characteristics:

- Uses TLS for acyclic data, DTLS for cyclic data
- Can either be used with Preshared-key or Public-key infrastructure

Security:

Confidentiality	Integrity	Authenticity
present	present	present

Successor / Alternative: -

OPC UA



TCP/UDP Port: TCP/4840

Part of Nmap Top 1000 ports: No

Purpose: Secure, reliable, and platform-independent framework for data exchange in industrial automation.

Characteristics:

- Service-oriented architecture (SOA)
- Supports complex data models and semantic information

Security:

Confidentiality	Integrity	Authenticity
present	present	present

Successor / Alternative: -

Result?



<https://www.flaticon.com/free-icons/coffee-break>

Topic 3: Security Advisories

How do you keep up to date
with new CVEs?

CVE Databases – cve.org

- Allows searching for:
 - CVE ID
 - CWE ID (= Common Weakness Enumeration, e.g. CWE-416 “Use After Free”)
 - Date and Date Range
 - Exact phrases
- For products use exact phrase (e.g. „SCALANCE“)
- Returns relevant entries including:
 - Unique CVE ID
 - Publisher: CNA (= CVE Numbering Authority)
 - Description

Search Results

Showing 1 - 25 of 32 results for "SCALANCE WAM763"

Show:

25

Sort by:

CVE ID (new to old)

CVE-2025-40833

CNA: Siemens

The affected devices contain a null pointer dereference vulnerability while processing specially crafted IPv4 requests. This could allow an attacker to cause denial of service condition. A manual restart is...

[Show more](#)

CVE-2025-24532

CNA: Siemens

A vulnerability has been identified in SCALANCE WAB762-1 (6GK5762-1AJ00-6AA0) (All versions < V3.0.0), SCALANCE WAM763-1 (6GK5763-1AL00-7DA0) (All versions < V3.0.0), SCALANCE WAM763-1 (ME) (6GK5763-1AL00-7DC0) (All versions < V3.0.0), SCALANCE WAM763-1...

[Show more](#)

CVE-2025-24499

CNA: Siemens

A vulnerability has been identified in SCALANCE WAB762-1 (6GK5762-1AJ00-6AA0) (All versions < V3.0.0), SCALANCE WAM763-1 (6GK5763-1AL00-7DA0) (All versions < V3.0.0), SCALANCE WAM763-1 (ME) (6GK5763-1AL00-7DC0) (All versions < V3.0.0), SCALANCE WAM763-1...

[Show more](#)

CVE-2025-15467

CNA: OpenSSL Software Foundation

SADP

Issue summary: Parsing CMS AuthEnvelopedData or EnvelopedData message with maliciously crafted AEAD parameters can trigger a stack buffer overflow. Impact summary: A stack buffer overflow may lead to a crash,...

[Show more](#)

CVE Databases – cve.org

- Each record provides more detailed information:
 - Publication date
 - Description
 - Corresponding CWE
 - Severity: CVSS (= Common Vulnerability Scoring System)
 - List of affected products
 - Affected firmware versions
 - References



Updated: 2026-05-12
Published: 2026-05-12

Description

The affected devices contain a null pointer dereference vulnerability while processing specially crafted IPv4 requests. This could allow an attacker to cause denial of service condition. A manual restart is required to recover the system.

CWE 1 Total

[Learn more](#)

- [CWE-476: : NULL Pointer Dereference](#)

CVSS 2 Total

[Learn more](#)

Score	Severity	Version	Vector String
7.5	HIGH	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
8.7	HIGH	4.0	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Product Status

[Learn more](#)

Vendor

Siemens

Product

SCALANCE WAM763-1

Versions 1 Total

Default Status: unknown

Affected

- affected from 0 before V3.2.0

References 1 Total

- <https://cert-portal.siemens.com/productcert/html/ssa-392349.html>

CVE Databases – nvd.nist.gov

- By NIST (= National Institute of Standards and Technology)
- Supports similar search options to cve.org
- Search for exact phrase:

Identifier	CISA Kev Info	Published Date	CNA	Description
CVE-2025-24532	✖	2025-02-11	Siemens AG	A vulnerability has been identified in SCALANCE WAB762-1 (6GK5762-1AJ00-6AA0) (All versions < V3.0.0), SCALANCE WAM763-1 (6GK5763-1AL00-7DA0) (All versions < V3.0.0), SCALANCE WAM763-1 (ME) (6GK5763-1AL00-7DC0) (All versions < V3.0.0), SCALANCE WAM763-1 (US) (6GK5763-1AL00-7DB0) (All versions < V3.0...
CVE-2025-24499	✖	2025-02-11	Siemens AG	A vulnerability has been identified in SCALANCE WAB762-1 (6GK5762-1AJ00-6AA0) (All versions < V3.0.0), SCALANCE WAM763-1 (6GK5763-1AL00-7DA0) (All versions < V3.0.0), SCALANCE WAM763-1 (ME) (6GK5763-1AL00-7DC0) (All versions < V3.0.0), SCALANCE WAM763-1 (US) (6GK5763-1AL00-7DB0) (All versions < V3.0...

CVE Databases – nvd.nist.gov

- Or search for products using CPE (= Common Platform Enumeration)

Vendor	Product
cpe:2.3:h:siemens:scalance_wam763-1:-:*:*:*:*:*:*	View CVEs
siemens	scalance_wam763-1

- Format:
 - CPE Version
 - Part: h(ardware), o(operating system), a(pplication)
 - Vendor
 - Product
 - Version
 - Update, Edition, Language, Software Edition, Target Software, Target Hardware, Other

CVE Databases – euvd.enisa.europa.eu



- EU vulnerability database
- Collaboration with cve.org and other databases
- Acts as a CNA for vulnerabilities discovered by European CERTs

Rated critical →

Known exploited →

Filter by CVSS score ⓘ

Filter by EPSS score ⓘ

Filter by vendor

Filter by product

Filter by assigner ⓘ

Filter by publication date

Filter by updated date

Show only exploited vulnerabilities ⓘ

Apply

Reset filters ↺

Minimum score 0

Maximum score 10

0

10

Minimum score 0

Maximum score 100

0

100

Siemens

SCALANCE WAM763

Search by assigner

Filter by publication date

Filter by updated date

☐ Exploited

ID	Alternative ID	Exploitation	CVSS	Product	Vendor	Changed
EUVD-2025-209778	GHSA-9483-pcvr-wj53 CVE-2025-40833	0.32%	v4.0: 8.7	SCALANCE X204-2	Siemens	1 month ago
The affected devices contain a null pointer dereference vulnerability while processing specially crafted IPv4 requests. This could allow an attacker to cause denial of service condition. A manual restart is required to recover the system.						
EUVD-2023-48727	GHSA-86gv-6g4q-x856 CVE-2023-44373	1.35%	v4.0: 9.4	SCALANCE W786-2IA RJ45	Siemens	2 months ago
Affected devices do not properly sanitize an input field. This could allow an authenticated remote attacker with administrative privileges to inject code or spawn a system root shell. Follow-up of CVE-2022-36323.						
EUVD-2022-39041	GHSA-9r25-j996-8h38 CVE-2022-36325	0.79%	v3.1: 6.8	SCALANCE XC206-2SFP G EEC	Siemens	2 months ago
Affected devices do not properly sanitize data introduced by an user when rendering the web interface. This could allow an authenticated remote attacker with administrative privileges to inject code and lead to a DOM-based XSS.						
EUVD-2022-39040	CVE-2022-36324 GHSA-hm3h-qvm3-r8qv	1.44%	v3.1: 7.5	SCALANCE XC206-2SFP	Siemens	2 months ago
Affected devices do not properly handle the renegotiation of SSL/TLS parameters. This could allow an unauthenticated remote attacker to bypass the TCP brute force prevention and lead to a denial of service condition for the duration of the attack.						

Where do they originate from?

- References link to information page from publisher
- For Siemens: Security Advisory

Updated: 2026-05-12
Published: 2026-05-12

Description

The affected devices contain a null pointer dereference vulnerability while processing specially crafted IPv4 requests. This could allow an attacker to cause denial of service condition. A manual restart is required to recover the system.

CWE 1 Total

Learn more

CWE-476: : NULL Pointer Dereference

CVSS 2 Total

Learn more

Score	Severity	Version	Vector String
7.5	HIGH	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
8.7	HIGH	4.0	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Product Status

Learn more

Vendor

Siemens

Product

SCALANCE WAM763-1

Versions 1 Total

Default Status: unknown

Affected

affected from 0 before V3.2.0

References 1 Total

https://cert-portal.siemens.com/productcert/html/ssa-392349.html

Restricted | © Siemens 2026 | Hennerbichler, Krisper, Sadek | DI FA DSP SEN PS | 2026-06-23

SIEMENS

Siemens Security Advisories

- Provides information on ...
 - The publication date
 - Severity ratings (e.g., using CVSS scores).
 - Summary of the vulnerability and current mitigations.

Siemens Security Advisory by Siemens ProductCERT

SSA-392349: Denial of Service Vulnerability in Industrial Devices

Publication Date: 2026-05-12
Last Update: 2026-05-12
Current Version: V1.0
CVSS v3.1 Base Score: 7.5
CVSS v4.0 Base Score: 8.7

▼ SUMMARY

Multiple industrial devices contain a vulnerability that could allow an attacker to cause a denial of service condition.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

Siemens Security Advisories

- Provides information on ...
 - The affected products and versions.
 - Recommended patches/updates.

▼ **KNOWN AFFECTED PRODUCTS**

[Un-/Collapse All](#)

Affected Product and Versions	Remediation
IE/PB LINK HA (6GK1411-5BB00) All versions affected by CVE-2025-40833	Currently no fix is planned See further recommendations from section Mitigations
IE/PB link PN IO (incl. SIPLUS NET variants) ↓	Show more details
SCALANCE M-800 family (incl. S615, MUM-800 and RM1224) ↓	Show more details
SCALANCE SC-600 family ↓	Show more details
SCALANCE W-700 IEEE 802.11ax family ↑	Show more details
SCALANCE WAB762-1 (6GK5762-1AJ00-6AA0) All versions < V3.2.0 affected by CVE-2025-40833	Update to V3.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109992747/ See further recommendations from section Mitigations
SCALANCE WAM763-1 (6GK5763-1AL00-7DA0) All versions < V3.2.0 affected by CVE-2025-40833	Update to V3.2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109992747/ See further recommendations from section Mitigations

Siemens Security Advisories

- Provides information on ...
 - Recommended mitigations or workarounds.
 - General security recommendations.

▼ MITIGATIONS

Siemens has identified the following specific mitigations that customers can apply to reduce the risk:

- Restrict access to the affected systems to trusted IP addresses only

Product-specific remediations or mitigations can be found in the section [Known Affected Products](#). Please follow the [General Security Recommendations](#).

▼ GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: <https://www.siemens.com/cert/operational-guidelines-industrial-security>), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: <https://www.siemens.com/industrialsecurity>

Siemens Security Advisories

- Provides information on ...
 - The addressed vulnerabilities
 - Might contain multiple CVEs if:
 - Similar impact and products
 - Similar mitigations and fixes

▼ **VULNERABILITY DESCRIPTION**

[Un-/Collapse All](#)

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

▼ **Vulnerability CVE-2025-40833**

The affected devices contain a null pointer dereference vulnerability while processing specially crafted IPv4 requests. This could allow an attacker to cause denial of service condition. A manual restart is required to recover the system.

CVSS v3.1 Base Score 7.5

CVSS v3.1 Vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Base Score 8.7

CVSS v4.0 Vector CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE CWE-476: NULL Pointer Dereference

Siemens Security Advisories

- Subscribe via Mail: productcert@siemens.com (subject line “[Advisory Mailing List] Subscribe”)
- Or consume CSAF or RSS Feeds:
 - <https://cert-portal.siemens.com/productcert/csaf/ssa-feed-tlp-white.json>
 - <https://cert-portal.siemens.com/productcert/rss/advisories.atom>
 - <https://cert-portal.siemens.com/productcert/rss/alerts.atom>
- Or use the search functionality:
 - <https://www.siemens.com/en-us/content/cert-services/?s=product>

Search Security Advisories

Filter by Date ▾

Reset

ID ▾ ▴	CVSS Score ▾ ▴	Document Title	Info	Version	Last Update ▾ ▴	Download
SSA-723487	9.0	RADIUS Protocol Susceptible to Forgery Attacks (CVE-2024-3596) - Impact to SCALANCE, RUGGEDCOM and Related Products	/	V2.0	2026-06-09	HTML CSAF PDF TXT
SSA-434797	9.8	Buffer Overflow Vulnerability in OpenSSL affecting Siemens Products	/	V1.0	2026-06-09	HTML CSAF PDF TXT
SSA-392349	7.5	Denial of Service Vulnerability in Industrial Devices	/	V1.0	2026-05-12	HTML CSAF PDF TXT

Siemens CERT and Siemens ProductCERT

- Computer Emergency Response Team
 - Siemens has own CERT, that cooperates with CERTs of other organizations, companies, countries
 - Responsible for handling cybersecurity incidents in Siemens infrastructure
 - Mail: cert@siemens.com
 - PGP Public Key: <https://cert-portal.siemens.com/cert/pgp/cert-siemens-com.asc>
-
- **Product** Computer Emergency Response Team
 - Responsible for coordinating the handling of product-related cybersecurity vulnerabilities
 - Central point of contact for customers, researchers, and internal teams regarding product security incidents
 - Mail: productcert@siemens.com
 - PGP Public Key: <https://cert-portal.siemens.com/productcert/pgp/productcert-siemens-com.asc>
 - Publishes **Security Advisories** to inform customers about vulnerabilities and recommended actions.
 - E.g. <https://cert-portal.siemens.com/productcert/html/ssa-392349.html>

Siemens Vulnerability Handling and Disclosure Process

1. Discovery & Reporting: Vulnerabilities are identified internally or reported by external researchers/customers. Should contain (preferably as encrypted email):
 - Vulnerability description with Proof-of-Concept code
 - Affected product or infrastructure including affected version
2. Validation & Analysis: ProductCERT verifies the vulnerability and assesses its potential impact.
3. Remediation Planning: Collaboration with product development to create fixes (patches, updates, workarounds).
4. Communication (**Security Advisory**): Timely and clear advisories are published, detailing the vulnerability and recommended actions.
5. Distribution & Implementation: Customers receive and apply the provided remedies.

<https://www.siemens.com/en-us/content/cert-services-vulnerability-process>

Hall of Thanks

- Acknowledgments of external pentesters and researchers
- For ethical and confidential disclosure
- <https://www.siemens.com/en-us/content/cert-services/hall-of-thanks/>

Acknowledgements

Each name represents an individual or organization who has privately reported one or more security vulnerabilities in Siemens' products, solutions, services, or infrastructure and worked with Siemens to mitigate the issue.

2026

2025

2024

AES Corporation
Organization

Aashutosh Devkota
Individual

Achmea Security Assessment Team
Organization

Adrián Tirado García
Individual

Albert Spruyt
ENCS

Amar Djebbara
Individual

Amr Alaa
NexaSec

Andreas Kolbeck
SEC Consult Vulnerability Lab

Restricted | © Siemens 2026 | Hennerbichler, Krisper, Sadek | DI FA DSP SEN PS | 2026-06-23

SIEMENS

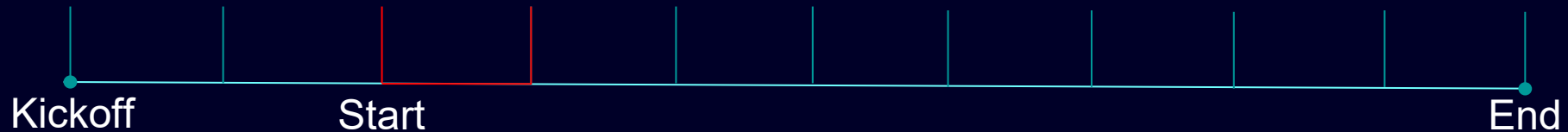
Pentesting

1. Kickoff meeting with product owners / developers:
 - Communication of new features
 - Reception of firmware / hardware



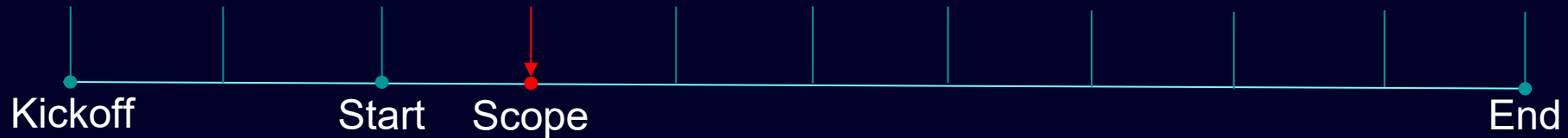
Pentesting

1. Kickoff meeting with product owners / developers
2. Reconnaissance:
 - Analysis of target product
 - Port Scan
 - Relevant features
 - ...
 - Familiarizing with documentation, specifications, etc.



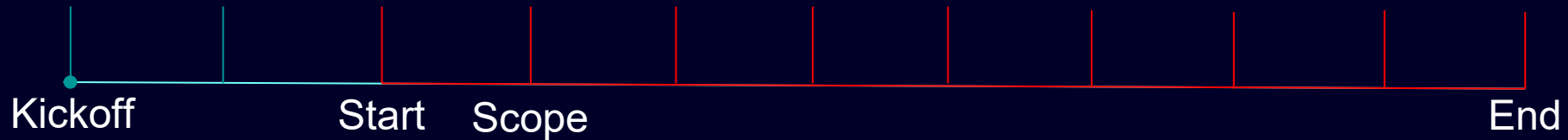
Pentesting

1. Kickoff meeting with product owners / developers
2. Reconnaissance
3. Scope meeting with product owners / developers:
 - Proposal and discussion of relevant features / components



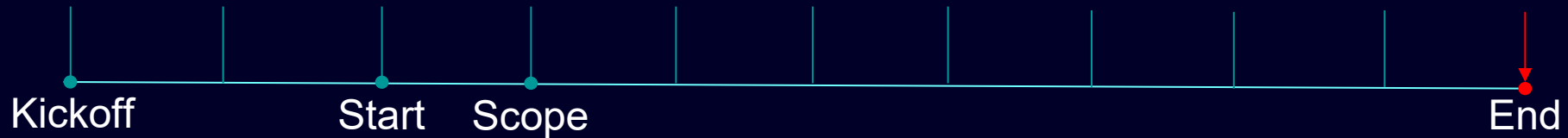
Pentesting

1. Kickoff meeting with product owners / developers
2. Reconnaissance
3. Scope meeting with product owners / developers
4. Pentest:
 - Testing of in-scope items
 - Usage of appropriate tools:
 - Burp Suite: Web
 - Ghidra: Firmware / Binary Analysis
 - Python: POCs, Scripting
 - Wireshark: Packet Analysis
 - Fuzzers
 - AI-powered tools: Code / Configuration File Analysis
 - ...



Pentesting

1. Kickoff meeting with product owners / developers
2. Reconnaissance
3. Scope meeting with product owners / developers
4. Pentest
5. Finalization:
 - Summary of findings in a report
 - Rating of findings via CVSS 4.0
 - Packaging of POC scripts
 - Confidential disclosure of report



Pentesting

1. Kickoff meeting with product owners / developers
2. Reconnaissance
3. Scope meeting with product owners / developers
4. Pentest
5. Finalization
6. Next Pentest:
 - Retest of previous findings
 - Repetition of steps 1-5

Security Testing Services

- External pentesting for companies / factories:
 - SiSSI – Siemens Security Scanning for Industry
- Similar steps in shorter duration with more caution (1-2 days)
- Process:
 - Discussion of relevant network segments
 - Analysis of IT / OT network:
 - Traffic analysis
 - Device discovery & Service enumeration
 - Analysis of exposed services:
 - Weak cryptography
 - Default credentials
 - Vulnerable versions
 - Report



© <https://flux-image.com/image/the-coders-focus>



https://www.freepik.com/free-photo/builder-uniform-wooden-background-flat-lay_32846488.htm



https://www.freepik.com/free-photo/group-multiethnic-diverse-hands-raised_19133490.htm

Quiz