ICS / OT Incident Detection & SOC Engineering

SIEM telemetry · detection engineering · IT↔OT correlation

● LIVE · CTX_LOADED
REV 2026.05 · v1.0
SCOPE · DEFENSIVE · BLUE TEAM

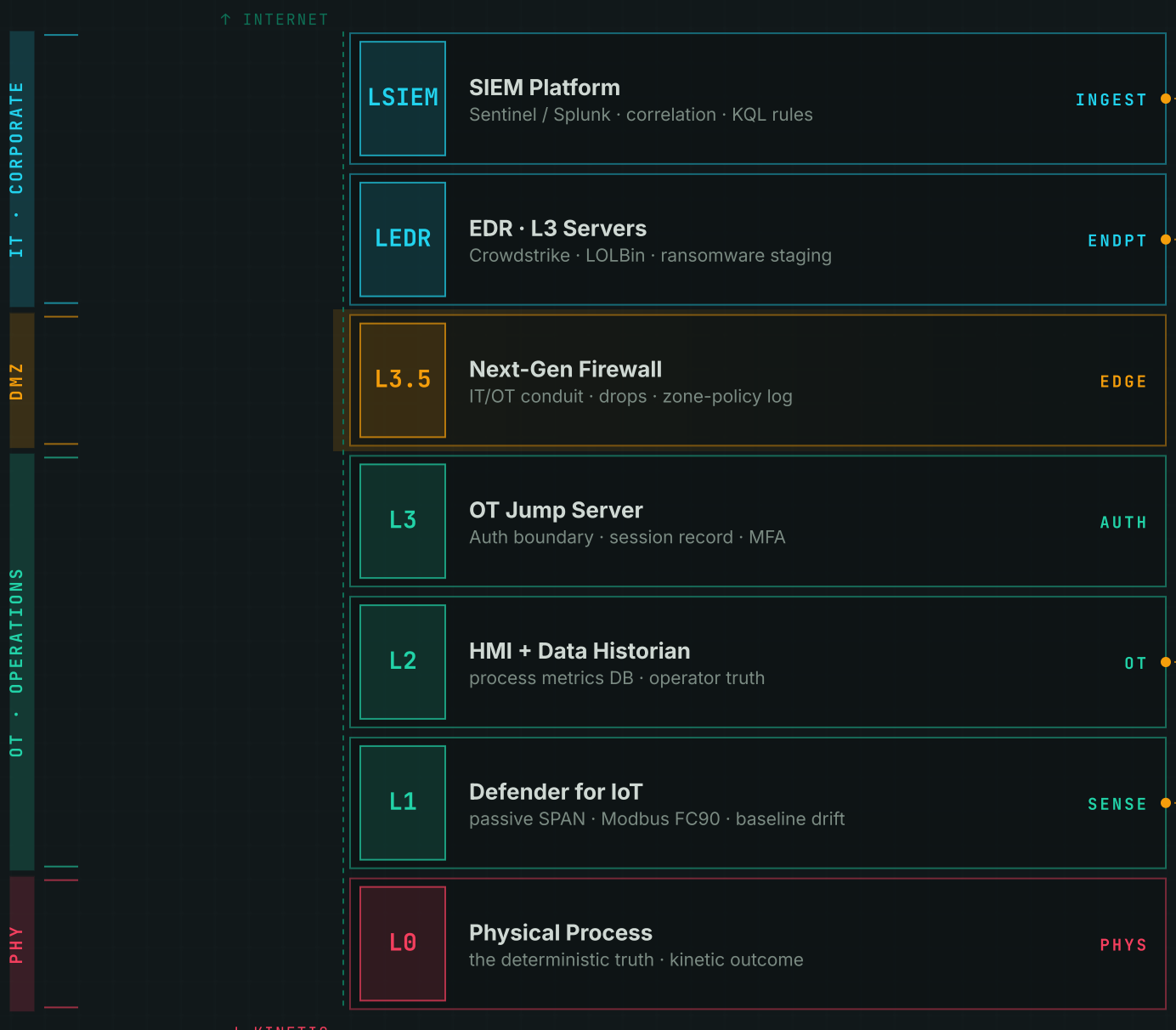
01

WHAT IT IS
Ingestion, parsing and alerting on OT-specific telemetry to identify cyber-physical threats before they reach the process.

WHY IT MATTERS
Attackers dwell in IT networks for months; bridging the gap to OT takes time — robust detection engineering stops them at the boundary.

WHERE
Centralized IT/OT SOCs integrating raw network taps with advanced SIEM platforms.

§02 SOC Telemetry Stack · ingest layers · weak points · detection seams



⚠ WEAK POINTS

W1 · LEVEL SIEM
Log forwarding gaps · switch configs, firewall drops and jump-host auths often never reach the SIEM

W2 · LEVEL EDR
Ransomware staging on L3 servers · rapid encryption + vssadmin delete shadows precedes detonation

W3 · LEVEL 2
Indicator removal on HMI · attackers clear Windows Event logs before disruptive payload (T0872)

W4 · LEVEL 1
Spoofed reporting · replayed normal Modbus while process driven critical (Stuxnet · T0856)

IT · L4-5 | DMZ · L3.5 | OT · L1-3 | Physical · L0

Telemetry without forwarding is invisible · baseline drift is the highest-fidelity OT alert

§03 Attack Surface · where IT becomes OT

Data Historian
Attackers target the database recording process metrics to manipulate sensor data — blinding operators (Stuxnet masked centrifuge speeds).

Lateral Movement
Pivoting through SMB or WMI from a compromised IT domain controller into the OT domain — flat trust = full kill chain.

Log Forwarding
Critical OT telemetry (switch configs · firewall drops · jump-host auth) often never reaches the SIEM — invisible attacker.

KILL CHAIN

01 IT phish + AD foothold → 02 SMB/WMI lateral to DC → 03 Pivot to OT jump server →
04 Clear HMI event logs → 05 Spoof reporting → kinetic

§04 MITRE ATT&CK · ICS · techniques most-used in OT compromise

T0872	**Indicator Removal on Host** — Clearing Windows Event logs on the HMI prior to executing a disruptive payload.
T0856	**Spoof Reporting Message** — Intercept network traffic and replay 'normal' status to the HMI while the physical process is driven critical.
T0859	**Valid Accounts** — Engineer credentials used to traverse the boundary — risky IT sign-in must elevate every OT command they issue.

§05 Detection & Monitoring · signals · why active scans break OT

◉ **Ransomware Deployment**
EDR on Level-3 servers for rapid file encryption or mass shadow-copy deletion (vssadmin delete shadows).

◉ **Logic Manipulation**
Defender for IoT → SIEM rule on Modbus Function Code 90 (Program Download) outside approved maintenance windows.

◉ **Boundary Crossing**
Any successful authentication to an OT jump server from an IP outside the dedicated IT secure-access subnet.

§06 Mitigation & Hardening · what to actually deploy

\+ **Dynamic Asset Inventory**
You cannot protect what you cannot see. Passive baseline of normal OT communications — A→B is law.

\+ **Reliable Log Forwarding**
Switch configs, firewall drops, jump-host auths all forwarded to SIEM — close the visibility delta first.

\+ **IT↔OT Correlation**
Risky Azure AD sign-in for engineer X auto-elevates severity on every OT command issued by user X within a window.

§07 Red Team · offensive · what actually works

01 Map the passive sensors first — then keep malicious traffic in-band between devices that already normally communicate, blending into baseline noise.

02 Compromise the historian instead of the PLC — if operators can't trust their screens they will not respond to physical alarms in time.

03 Pivot via SMB / WMI from a compromised IT domain controller — most environments still share trust between IT AD and OT AD.

§08 Blue Team · defensive · what most teams miss

01 Baseline first. OT is deterministic — any deviation from yesterday's traffic pattern is a high-confidence alert, not a noisy one.

02 Correlate identity with kinetic. An IT risky sign-in + an OT 'write register' from the same user within minutes = critical, page someone.

03 Treat the historian as crown-jewel. Tamper-evident logging + read-only replicas — operators must always trust their screens.

§09 Quick Commands · passive only on production OT

```
› KQL DeviceNetworkEvents | where RemotePort in (502,102,20000,44818) ⟶ Catch OT protocol traffic from non-OT subnets
› KQL | where LocalIP !startswith "10.OT.Subnet" ⟶ Filter to crossings outside the OT block
› FQL event_simpleName=ProcessRollup2 FileName IN (powershell,wmic) ⟶ LOLBin on hostnames *HMI* / *EWS*
› Sentinel rule: ModbusFC=90 AND NOT in_maintenance_window ⟶ Program Download outside change windows
```

§10 Memory Hooks · commit these to muscle memory

HOOK
OT is Deterministic
If A normally talks to B, A talking to C is an immediate red flag — not noise to be tuned out.

HOOK
Boundary + Inside
Firewalls protect the DMZ; passive sensors catch what gets through. You need both, not either.

HOOK
Historian = The Truth
Protect the historian at all costs — if operators cannot trust their screens, the plant cannot function.