Unifying IT, OT and AI-Driven Detection for Collective Defence

Jeff Yeo, CCSP, CISSP, CISM, ITIL, COBIT
Leader, Solution Engineering Cisco-Splunk

The Threat Is Already Here

4x increase in APT activity
targeting Singapore,
2021 to 2024
(CSA Singapore Cyber Landscape 2024)

UNC3886 – confirmed active
inside all four Singapore major
telco operators, July 2025

Not opportunistic: a deliberate,
patient campaign targeting
communication backbone infrastructure

Attacker objective:
persistence inside CII,
pre-positioned for disruption
or intelligence collection

The question has changed:
Not: will a sophisticated adversary attempt entry?
But: will defenders see them before they reach OT systems?
For most OT environments today – the honest answer is: probably not, in time.

The Visibility Gap:
Why OT Environments Blind Defenders

Industrial telemetry is generated but rarely analysed

- PLCs (Programmable Logic Controllers), RTUs (Remote Terminal Units), and HMIs (Human-Machine Interfaces) generate rich network traffic — it is simply never sent to a SIEM
- OT protocols (Modbus, DNP3, IEC 61850, OPC-UA) are invisible to standard IT security tools

Organizational silos make correlation impossible

- IT SOC monitors enterprise infrastructure; OT operations team monitors process stability
- Neither team sees both sides of a lateral movement that crosses the IT/OT boundary

Dwell time advantage belongs to the attacker

median dwell time(reconnaissance/staging) in ICS environments before an attack exceeds 185 days*

PIPEDREAM/INCONTROLLER: designed to operate undetected in OT for extended periods

Goal: unified visibility – without disrupting sensitive industrial processes

*Source*intelligence-Driven Active Defence Report 2026*

Unified IT and OT Telemetry

SIEM (IT Security Layer)

- **Authentication Mapping:** Tracking identity, remote logins, and credential handshakes across corporate segments.
- **Endpoint Behaviors:** Detecting process spawning, registry changes, and lateral pivoting sequences.
- **Enterprise Correlation:** Evaluating suspicious jumps across corporate network nodes.

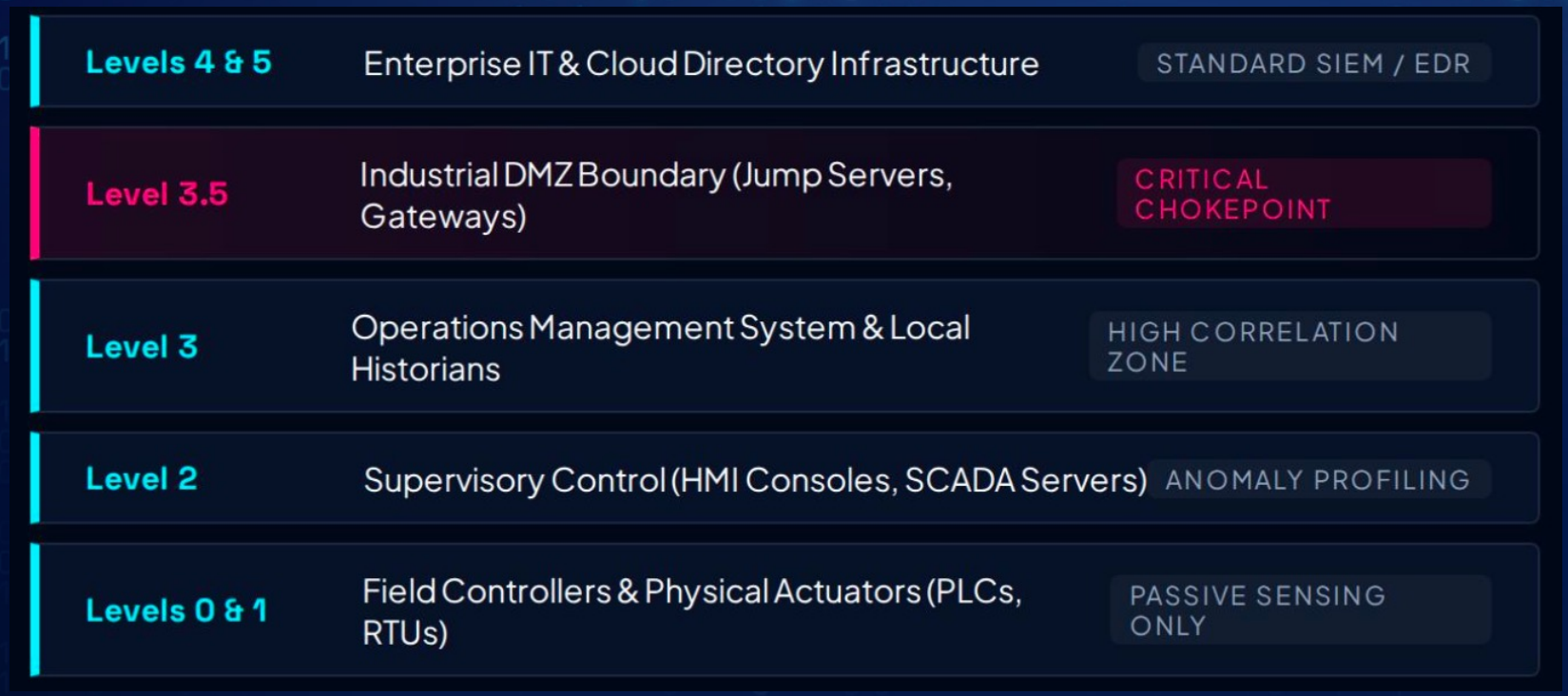
Passive Sensors (OT Network)

- **Deep Packet Inspection (DPI):** Decoupling and analyzing process control frames completely out-of-band.
- **Zero Interruption Baseline:** Passive-only tracking. Strictly avoids injecting active scans on live process controls.
- **Command Profiling:** Flagging anomalies, unscheduled firmware edits, or illegal device write instructions.

Data Normalization via Common Information Model (CIM)
The primary challenge in IT/OT convergence is that IT logs (JSON, Syslog) and OT protocols (Modbus, DNP3, OPC-UA) speak different languages.

SIEM Role: Using the Common Information Model (CIM), maps these disparate data sources into a unified schema. Whether it is a Windows Event ID 4624 (IT login) or a Modbus Function Code 16 (OT write), a SIEM normalizes these into common fields like src_ip, dest_ip, and action. This allows you to write a single detection rule that triggers regardless of the underlying protocol.

Purdue Model Detection Placement



- **Key insight: adversaries cross Purdue levels deliberately and gradually**
  - UNC3886 pattern: IT compromise → credential theft → jump server → OT SCADA access
  - Detection must span levels — a single-layer view misses the full kill chain
- **Critical constraint: detection in OT must not impact process availability**
  - Active scanning in OT is dangerous — passive-only monitoring is non-negotiable below Level 3

SIEM's Role: provides a framework to map detection logic directly to the MITRE ATT&CK for ICS matrix. You can build "Notable Events" that are tagged with the specific MITRE technique ID (e.g., T0831 - Manipulation of Control). This provides the "shared language" required for communication between the SOC and OT operations teams.

MITRE ATT&CK for ICS: From Framework to Detection Logic

STANDARDS

Complements IEC 62443

Positioned alongside IEC 62443 as a companion standard — 62443 defines security levels and zones/conduits architecture; ATT&CK for ICS supplies the adversary behavior layer on top.

ECOSYSTEM

OT Vendor-wide adoption

Widely adopted across the OT threat-intel and detection vendor ecosystem map their own content back to this taxonomy, so it's a shared vocabulary, not a proprietary one.

Why this framework specifically?

- International adoption: used by CISA (published directly in its ICS eviction strategies guidance), referenced alongside IEC 62443 as a complementary standard, widely adopted across the OT threat intel/vendor ecosystem

? What is IEC 62443 ?
An internationally recognized series of standards that defines requirements and processes for implementing and maintaining secure Industrial Automation and Control Systems (IACS) and operational technology (OT). It serves as a foundational cybersecurity playbook for protecting critical infrastructure like power plants, manufacturing facilities, and chemical processing plants.

MITRE ATT&CK for ICS: How It Works In Practice

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command & Control	Inhibit Response	**Impair Process Control**	**Impact**

Attacker objective progresses left to right — each tactic answers "what is the adversary trying to accomplish right now?"

EACH TECHNIQUE MAPS TO AN OBSERVABLE

Every technique under a tactic ties to something you can actually see — a specific pattern in OT network traffic or endpoint logs. That's what makes the framework operational rather than academic.

EXAMPLE

T0831 — Manipulation of Control

Tactic: Impact

Covers unauthorized changes to setpoint values, tags, or control parameters — the technique describes the attacker's objective, not a specific sensor signature.

How a detection engineer might operationalize it:

An unexpected write to a PLC register outside a normal operating window.

MITRE ATT&CK for ICS: Coverage Gaps

01	**Known TTPs only**	The framework catalogs documented tactics and techniques. Novel techniques specific to your OT environment aren't in the matrix by definition — they require custom detection engineering, not a framework lookup.
02	**Physical process knowledge is a prerequisite**	Defenders must understand what “normal” looks like in their own process — setpoints, timing, sequencing — before “abnormal” is detectable. The framework describes adversary behavior; it doesn't teach you your own plant.
03	**Protocol coverage is uneven**	Not all ICS protocols have equal community-developed detection content. Modbus and DNP3 coverage is comparatively mature; less common or proprietary protocols have much thinner published detection logic.

Detection Engineering: Translating TTPs to Alerts

1. INITIAL ACCESS

Common Vector:

- Spearphishing Attachment
- Enterprise IT VPN exploit
- Dual-homed system pivot

2. LATERAL PIPING

TTP Focus:

- Remote Service Session
- Valid credentials reuse
- Engineering Workstation

3. MANIPULATE CONTROL

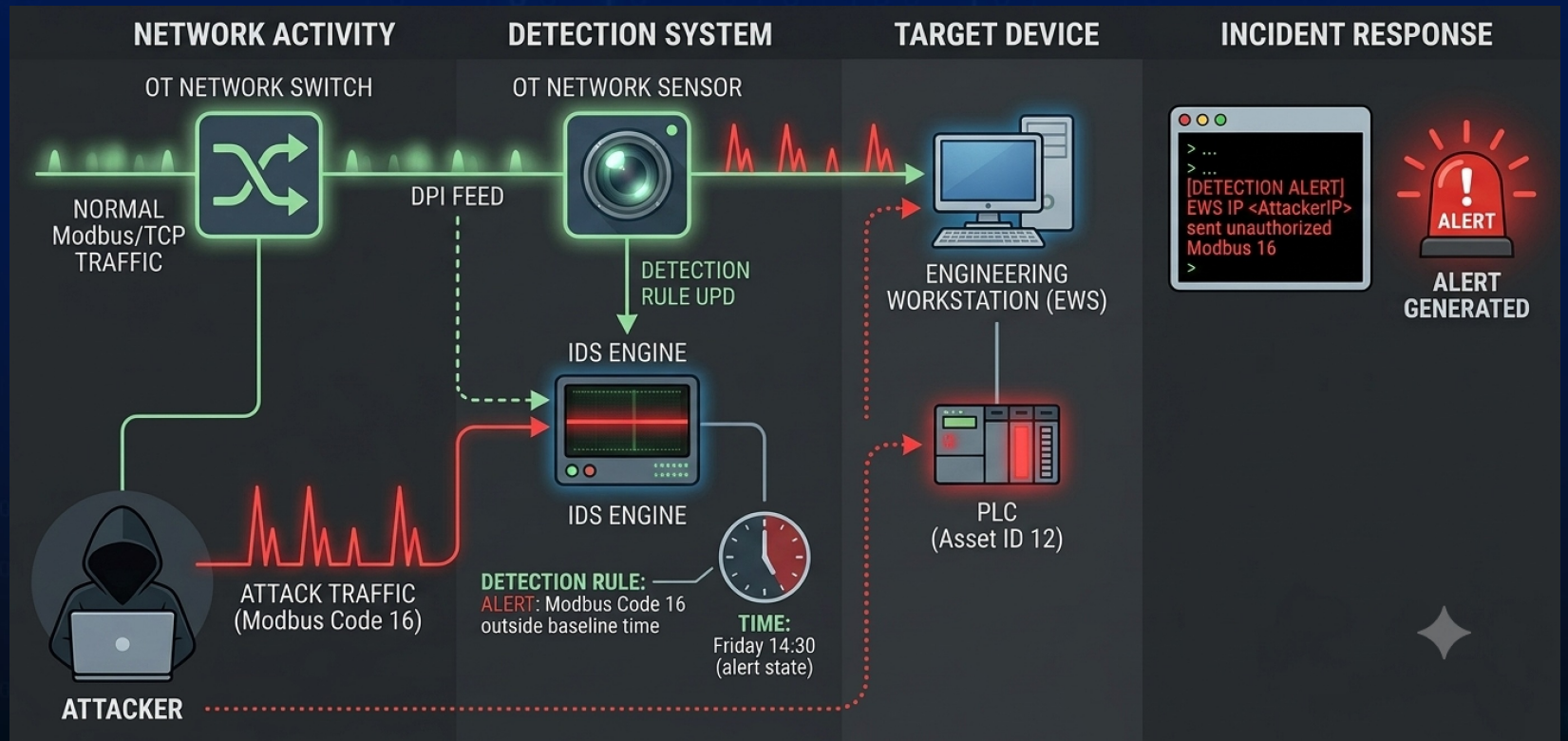
TTP Focus:

- Unauthorized Modbus/TCP
- Device firmware update
- PLC register changes

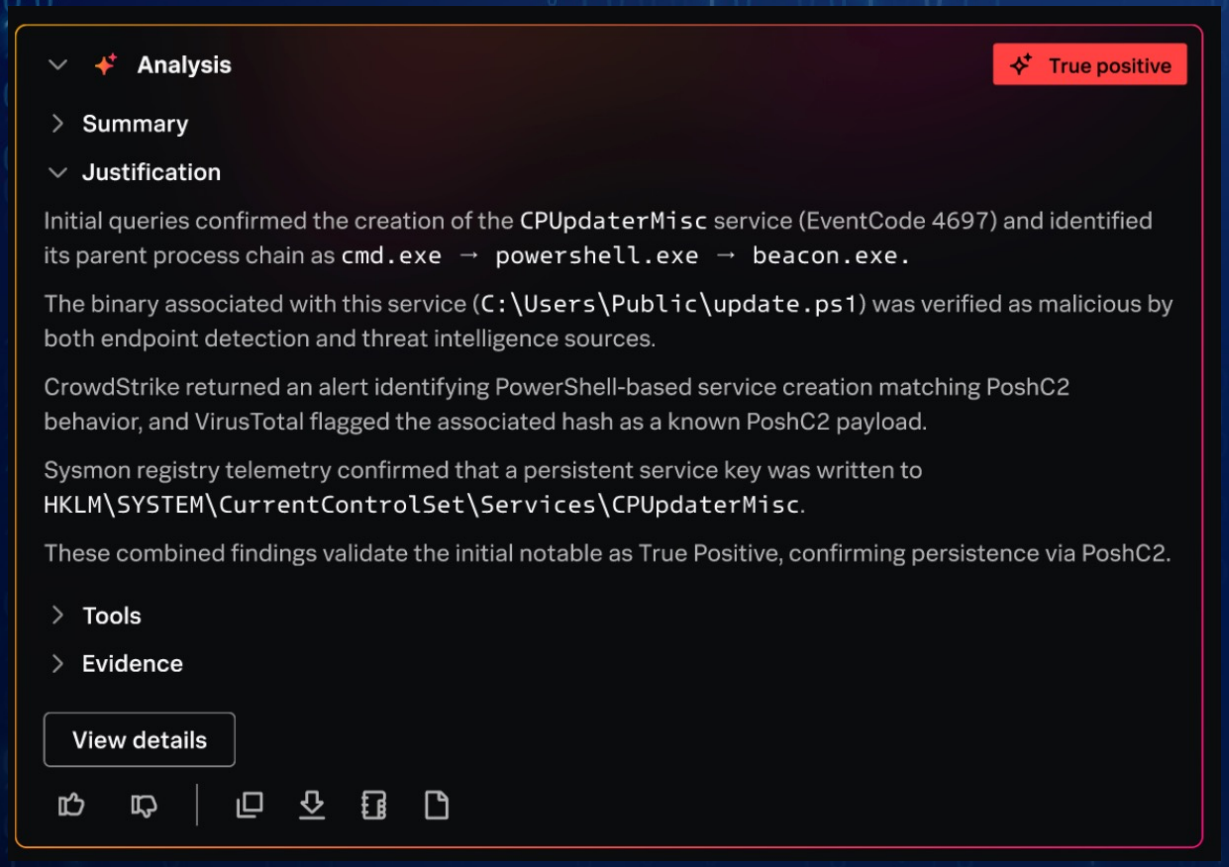
4. ULTIMATE IMPACT

Critical Risks:

- Denial of physical view
- Manipulation of safety
- Equipment damage



Ai-Assisted Triage



- **Where AI genuinely reduces analyst burden today (IT layer)**
  - Alert correlation across large IT telemetry volumes: AI identifies related events a human would miss in noise
  - IOC enrichment and initial triage: automated context-gathering from threat intel reduces time-to-investigate
  - SPL / query generation: natural language to detection logic reduces skill barrier for new analysts
- **Where AI adds value in OT — with strict constraints**
  - Anomaly scoring: AI can flag statistical deviations from OT baseline — but human review is mandatory before any action
  - Cross-domain correlation: AI correlating IT lateral movement with OT anomaly timing can surface campaigns faster
- **Where AI must never operate autonomously**
  - AI must NOT automatically initiate any response action in OT environments
  - Isolating an OT asset or blocking a network path can cause physical process disruption or safety incidents
  - Human-in-the-loop is non-negotiable for all OT response decisions — this is not a technology limitation, it is a governance requirement

Establishing the Governance Framework Before You Deploy AI

SECURITY DOMAIN	AI AUTHORIZATION AND ROLE	GOVERNANCE & OVERSIGHT BOUNDS
IT Domain Enrichment Alerting correlation & Splunk SPL formulation	AUTONOMOUS TRIAGE	Allowed to gather contextual metadata, deduplicate alerts, and suggest queries autonomously.
Cross-Domain Correlation Tying enterprise credentials to OT anomalies	CO-PILOT / ENRICHMENT	Permitted to build cross-domain anomaly scores. **Strictly requires human analyst confirmation.**
OT Control Decisions **PLC Isolation, network block, or port downing**	STRICTLY PROHIBITED	No automated physical disruption permitted. **Human-In-The-Loop mandatory for safety integrity.**

CSA Singapore OT Master Plan 2024 explicitly requires documented human oversight for automated security decisions in CII

The Practitioner's Checklist: Before the Next Campaign Begins

- **Deploy Passive Visibility Sensors:**
  Deploy non-intrusive monitoring appliances to capture and baseline communication loops down to Purdue Levels 1 and 2.
- **Normalize via Unified CIM:**
  Map diverse OT protocols and IT directories into a common, normalized schema inside your SIEM for seamless queries.
- **Profile Attack Paths to MITRE ICS:**
  Prioritize mapping threat models against high-risk actions, specifically targeting credential abuse and access pivots.
- **Formulate Joint IT/OT Runbooks:**
  Establish joint operational processes signed by security executives and physical plant engineers to ensure safe recovery steps.
- **Configure Maintenance Window Muting:**
  Interconnect scheduled maintenance logs with the alert engine to automatically silence false alarms during scheduled system updates.
- **Enforce Manual Action Guardrails:**
  Draft formal boundaries restricting where AI systems may triage automatically vs. where human approval is required.

Closing: Collective Defence Is Not a Destination

1. UNIFIED TELEMETRY

SIEM + Passive OT Sensor

This combination stands as the absolute minimum viable architecture required to reliably defend Critical Information Infrastructure (CII) environments.

2. MITRE ATT&CK FOR ICS

Cross-Domain Context

Translates complex industrial protocol anomalies into structured adversary tactics, ensuring enterprise SOC analysts instantly comprehend operational process risks.

3. GOVERNED AI TRIAGE

Human-in-the-Loop Boundaries

Provides high analytical value inside IT layers. However, an absolute human validation line must be structurally enforced prior to deployment near physical OT control actions.