



SDL-Powered SIEM for OT

Bring every OT security signal together.
Detect what matters.

What is it?

SDL-Powered SIEM for OT extends the Security Data Lake + SIEM architecture into operational technology environments. It gives OT and SOC teams a common foundation for collecting, normalizing, enriching, storing, correlating and investigating signals from cyber-physical systems (CPS), OT security tools and the IT/OT boundary.

Why it matters

OT security data is often spread across sensors, firewalls, remote-access tools, engineering workstations, historians and existing IT security platforms. When those signals are investigated separately, the relationship between an identity event, a remote session, a workstation anomaly and PLC activity can be easy to miss.

What you get

SDL-Powered SIEM for OT connects OT telemetry to a common security-data and investigation workflow.



Bring OT data together

Onboard signals from PLCs, RTUs, SCADA, DCS, HMIs, historians, engineering workstations, OT firewalls, network sensors, remote access infrastructure and existing IT/OT security products. Use existing sensors and integrations where direct collection from an industrial source is not appropriate.



Normalize, enrich and correlate

The data path is collect → parse → normalize → enrich → store → correlate → detect. OCSF-based normalization creates a common data foundation; asset, network, identity, zone and threat-intelligence context makes the event meaningful.



Detect OT-relevant activity

Detection themes include unauthorized asset and protocol discovery, rogue devices, remote-access anomalies, privileged access, unauthorized PLC communication, abnormal industrial-protocol activity, engineering-workstation anomalies and IT/OT attack paths.



Investigate the attack story

Historical data, timelines, correlation, IOCs, cases and evidence help analysts connect the initial compromise to credential abuse, remote access, OT discovery, engineering-workstation activity, PLC discovery and suspicious commands.

When it makes sense



OT and IT security teams need a shared investigation view.



The organization wants to use existing sensors and security investments rather than replace them.



Security leaders need OT-aware context around identities, assets, zones and communications.



The SOC needs historical search and attack-chain visibility across the IT/OT boundary.



A typical attack story

Initial compromise → credential abuse → remote access → OT discovery → engineering workstation → PLC discovery → suspicious command → attack chain. A single OT alert is a point in time; SDL provides the cross-source and historical context needed to understand the broader path.

An OT security workspace

A customer-facing OT workspace can bring together critical OT assets, threat intelligence, asset risk, vulnerabilities, incidents, attack chains, protocol anomalies, remote-access activity, IT/OT activity, timelines, historical search, IOCs, cases and evidence.

No rip-and-replace starting point

The initial design can focus on selected OT sources and existing security integrations. Validate source connectivity, data ownership, industrial protocol coverage, residency, segmentation and the first investigation scenarios before expanding the rollout.

Technical details

Area	Documented capability
Data onboarding	Industrial assets and OT systems; firewalls; SCADA/DCS; historians; sensors; remote access; existing IT/OT security products.
Data foundation	OCSF-based normalization; raw and normalized security data; historical data; asset, network, identity and threat-intelligence context.
Detection themes	OT discovery; access and identity; industrial activity; IT/OT attack paths; OT/ICS threat intelligence.
Investigation	Timeline; correlation; historical search; IOCs; cases; evidence; attack-chain analysis.
Deployment principle	Specific protocol visibility, source connectivity and architecture depend on the customer's environment and integrations.



Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation.

Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

Gartner®

Infopercept is recognized as a representative vendor in multiple Gartner® reports

- UEMP (Exposure Management)
- AMTD (Preemptive Security)
- AEV (Security Validation)

[Learn More](#) →



Ready to try it out?

Sign up for a demo. Visit infopercept.com/book-a-meeting

Infopercept

Attacker's Mind. Defender's Brain.®

