



Invinsense OT Deception

Detect earlier. Understand the attacker. Build OT-specific intelligence.



What is it?

Invinsense OT Deception adds controlled decoys to the OT environment so unauthorized interaction becomes a high-confidence signal. Instead of waiting for an attacker to reach a production asset, teams can observe reconnaissance, credential abuse, lateral movement and industrial targeting around carefully designed deception assets.

Why it matters

Attackers may spend time discovering assets, testing credentials and moving through the environment before they touch a critical PLC, HMI or engineering workstation. Ordinary alerts can be difficult to prioritize. Interaction with a controlled decoy is different: it is activity that should not normally happen and therefore deserves immediate attention.

What you get



A controlled deception layer

Deploy deception assets such as decoy PLCs, SCADA or server systems, HMIs, services, network paths, engineering workstations and credentials. The exact decoy types and protocols should be selected for the target OT environment.



High-confidence interaction signals

Unauthorized interaction with a deception asset can reveal the source, target, service or protocol touched, credentials attempted, systems discovered and the sequence of activity. The signal becomes more valuable when correlated with surrounding telemetry.



Threat intelligence from your environment

Combine deception-derived observations with OT assets, network telemetry, identity events, remote-access activity, vulnerability context, historical behavior and approved external intelligence. This creates intelligence relevant to the customer's own environment—not just a list of generic indicators.

When it makes sense



The security team wants earlier warning of OT reconnaissance or lateral movement.



The organization needs a high-confidence signal before an attacker reaches production systems.



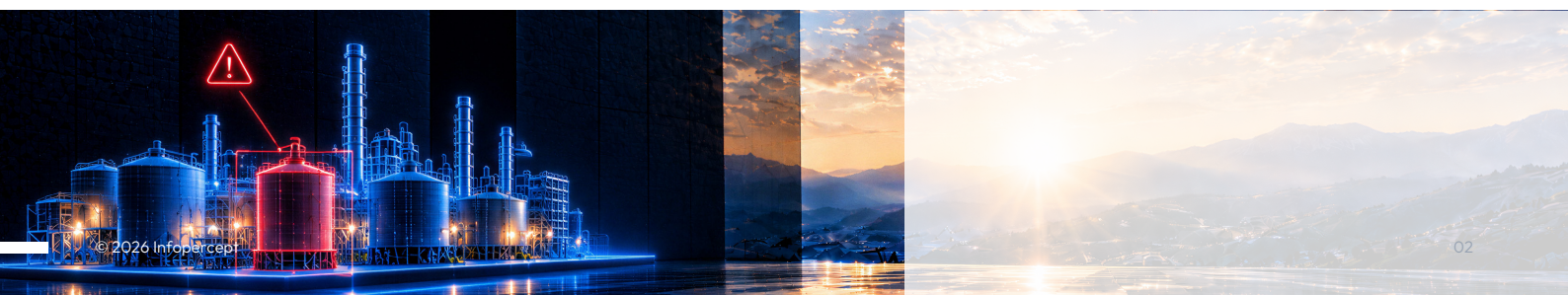
IT and OT activity needs to be connected into an attack story.



The SOC wants richer evidence for threat hunting and incident investigation.

A typical attack story

Initial compromise → credential abuse → OT discovery → interaction with a decoy → engineering workstation targeting → PLC discovery → attack chain generated. The deception event is not meant to stand alone; its value increases when surrounding identity, network, endpoint, asset, vulnerability and historical data are available.



Deception with SDL and OT SOC

A deception event can flow into SDL for OCSF normalization and enrichment, receive asset context, and be used in the OT SOC investigation workflow. The resulting record can include the critical alert, source and target context, attempted credentials or services, related activity, ATT&CK for ICS mapping where configured, and historical correlation.

Technical details

Area	Documented capability
Deception assets	Decoy PLC; decoy SCADA/server; decoy HMI; decoy services; decoy network paths; decoy engineering workstation; decoy credentials.
Detection themes	Reconnaissance, credential and access activity, lateral movement, industrial targeting and early intrusion/Industrial ransomware indicators.
Intelligence	Entry point, reconnaissance behavior, systems discovered, movement, techniques, attempted credentials, protocol/service interaction and potential objective.
Operations	OT deception → high-fidelity telemetry → SDL → normalization/enrichment → attack chain → OT SOC.

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.®