CASE STUDY

How An Oil Refinery Eliminated Alert Fatigue and Created Contextualized OT Risk Insights

The Challenge

A major oil & gas manufacturer faced critical limitations in its existing OT security infrastructure with false positives and ghost asset alerts, which cluttered security workflows and obscured true threats.

The organization struggled to prioritize risk, lacking the visibility and context to focus on what truly mattered.

Siloed technologies and disconnected data sources made it difficult to understand the full operational environment, hampering both security efforts and compliance readiness.

The Solution

The manufacturer deployed Armis Centrix™ for OT/IoT Security, transforming its ability to detect, prioritize, and respond to risk across its converged OT, IT, and IIoT environment. This included:

- **Data Source Optimization** - Transforming noisy, disjointed data streams into clear, relevant, and actionable alerts focused on high-impact assets.
- **Asset Intelligence & Contextual Enrichment:** Delivered deep asset intelligence enriched with operational context, identified vulnerabilities and other security threats, current security controls, and compliance posture—empowering smarter risk mitigation decisions.

The Results

Identified over 12,000 alerts as ghost assets, external (cloud) assets, and “out-of-working hours” alerts.

A unified risk view of converged OT-IT-IIoT network security systems within its OT environment.

OT security compliance and auditing processes are now automated.

Industry: Oil & Gas

Location: N/A

Size: N/A

Armis Centrix™ for OT/IoT Security

Background

The company is an energy petrochemical refinery with geographically dispersed assets for petroleum refining, logistics, asphalt, renewable fuels, and retail convenience stores. Although it invested in OT cyber security solutions, the company’s security team experienced alert fatigue due to the high volume of false-positive security notifications from its existing Intrusion Detection System (IDS). It also had challenges with its OT cyber security posture because it lacked asset visibility over all of the company’s geographically scattered and unmanned environments. The sheer volume of alerts, combined with an inability to recognize real high-priority security threats with its existing resources, was a major challenge that the team needed to solve.

The company sought to find an efficient and effective solution to:

Reduce Alert Noise - Minimize the volume of low-value or irrelevant security notifications to allow the security team to focus on actionable threats.

Gain Unified Visibility - Establish a comprehensive, 360° view of cyber exposure and security risk across all connected assets, including OT, IT, and IoT devices.

Enhance OT Environment Visibility - Achieve clear, real-time insight into the operational technology landscape to support informed decision-making.

Simplify OT Security Operations - Centralize and streamline cybersecurity management across the OT environment to reduce complexity and operational overhead.

Automate Asset Discovery - Continuously discover, classify, and inventory all assets to build a complete and accurate asset map with relevant pathways.

Identify and Prioritize Risks - Detect vulnerabilities and assess risks in context to support efficient prioritization and mitigation efforts.

The Challenge

The refinery faced significant challenges in its operational security environment, starting with an existing Intrusion Detection System (IDS) that generated an overwhelming volume of ghost assets and false-positive alerts. This constant inaccuracy of alerts made it increasingly difficult for the cybersecurity team to identify and respond to genuine threats, leading to alert fatigue and reduced efficiency. Compounding this issue was the team's inability to effectively prioritize risks, making it hard to determine which alerts required immediate action in order to address actual operational technology (OT) security concerns. Furthermore, they struggled to connect and leverage data sources and existing technologies, which hindered their ability to understand and secure their operational environment comprehensively. These challenges collectively undermined their ability to maintain a proactive and reliable security posture.

The Solution

To address critical visibility, noise, and risk prioritization challenges, the energy company deployed Armis Centrix™ for OT/IoT Security (On-Prem) across its refinery operations. The solution delivered:

- **Automated Event Correlation and Noise Suppression**
  Armis streamlined detection by correlating data from existing security tools including firewalls, OT IDS, SPAN ports, DCS systems, EDRs.
- **Comprehensive Asset Visibility and Enrichment.** Armis enriched OT asset inventory with detailed operational context by leveraging the asset intelligence engine , creating a unified, real-time view of the OT environment.
- **Actionable Insights through Data Integration**
  By ingesting and analyzing data across the refinery's security ecosystem, Armis:
  - **Identified** 12,000+ false-positive alerts as ghost, external, or after-hours activity.
  - **Suppressed** low-priority noise and surfaced only legitimate, high-impact alerts.
  - **Flagged** abnormal and repetitive behavior for investigation and action.
- **Risk-Based Prioritization**
  Leveraging real-time event correlation and asset context, Armis enabled the company to proactively identify exposures, prioritize risk, and assign mitigation resources based on operational impact.

>12,000
false alerts eliminated

100%
Achieved unified visibility across converged OT-IT-IIoT security networks

Automated previously manual OT security compliance and auditing processes

The Results

The deployment of Armis Centrix™ delivered measurable improvements across security posture, operational efficiency, and risk readiness:

Unified Risk Visibility
A single, converged view of OT, IT, and IIoT asset risk thereby eliminating blind spots and improving cross-environment awareness.

Improved ROI from Existing Tools
Integrated Armis with existing security investments to extract more value without additional infrastructure or agents.

Operational Context for Risk Decisions
Security teams now evaluate threats based on asset criticality and process impact, enabling informed, OT-specific responses.

Faster Detection and Response
Significant reduction in Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), with automated insights highlighting true risks and vulnerabilities.

Safe, Continuous Security Assessments
The platform enables ongoing OT posture evaluations without interrupting refinery operations.

Executive-Level Reporting
Delivered comprehensive cyber risk assessments to senior leadership, clearly visualizing the refinery's current OT security posture.

Streamlined Mitigation Playbooks
Provided ready-to-execute mitigation plans tailored to site-specific vulnerabilities and other security issues, helping teams harden their OT network with speed and precision.

Automated Compliance Reporting
OT compliance and auditing processes are now automated, ensuring continuous and proactive adherence to industry regulations and internal standards.