



Tracknosis Oil & Gas Edition

White Paper

Forensic Observability, Threat Detection and Regulatory Compliance for the Oil, Gas and Energy Industry

**Making the
Unknown
Known**



Executive Summary

Oil and gas operators run some of the most strategically critical — and most targeted — infrastructure in the world: offshore platforms and drilling rigs, pipelines, refineries, LNG terminals, and storage and distribution networks. They face relentless pressure from nation-state actors, ransomware syndicates, and hacktivists, where a successful cyber attack can halt production, trigger safety and environmental incidents, and disrupt national energy supply. At the same time, regulations and mandates including the TSA Pipeline Security Directives, CIRCIA, NIS2, the EU Critical Entities Resilience (CER) Directive, and API 1164 now require operators to detect, investigate, and report significant incidents within hours — supported by defensible forensic evidence.

Tracknosis is a Forensic Observability platform built for Windows environments — including the engineering workstations, HMIs, historians, and SCADA servers that sit at the IT/OT boundary across upstream, midstream, and downstream operations. It continuously transforms endpoint and server telemetry into trusted forensic evidence, enabling operators to detect threats early, perform rapid root cause analysis, and produce regulatory-ready incident reports — without relying on scarce and costly external forensic specialists.

The Oil, Gas and Energy Cybersecurity Challenge

Oil and gas operators run converged IT and operational technology (OT) estates that span remote and hazardous sites: offshore and onshore production, pipeline SCADA, refinery and terminal control systems, and corporate networks — often blending modern platforms with decades-old equipment. Conventional monitoring tools generate alerts, but rarely answer the question investigators and control-room engineers need most: what actually happened, and did it cross from IT into the systems that keep production safe?



Nation-State Attacks – Advanced persistent threats target rigs, pipelines, and refineries for disruption, espionage, and coercion.



Ransomware – Advanced persistent threats target rigs, pipelines, and refineries for disruption, espionage, and coercion.



Safety System Risk– Tampering with control and safety-instrumented systems can trigger spills, fires, or explosions.



IT/OT Convergence – Attackers pivot from corporate IT into OT via engineering workstations, HMIs, and historians.



Supply Chain Risk – Compromise of vendors, integrators, and remote-access tooling grants a route into operator networks.



Compliance Gap – Without forensic evidence, meeting TSA, CIRCIA, NIS2, CER, and API 1164 windows is very difficult.

Forensic Observability

Tracknosis introduces Forensic Observability – the discipline of continuously transforming telemetry into trusted forensic evidence. Rather than collecting logs and waiting for alerts, Tracknosis analyses what actually changed on disk, attributing every change to a specific user, process, and timestamp.

How It Works

Tracknosis performs sequential forensic scans of Windows NTFS disk structures across IT and OT Windows assets – from corporate endpoints to engineering workstations and historians at remote sites. Each scan captures a complete forensic snapshot. The difference between consecutive scans – the delta – reveals precisely what changed, when, and by whom. This approach detects threats that leave no signature but always leave a forensic trace – including the stealthy tradecraft used to manipulate control-system hosts.

Windows Security Event Logs	Authentication, object access, privilege use, and audit log clearing events
NTFS Master File Table (MFT)	Metadata for every file and directory – timestamps, attributes, allocation status
\$UsnJrnl Change Journal	Complete record of file creates, modifications, deletions, and renames
\$LogFile Transactions	Low-level file system operations independent of Windows auditing
Registry Hive Analysis	Persistence artifacts, configuration changes, and attacker backdoors between scans
SIEM / OT Integration	Forensic enrichment of Splunk, Elastic, Datadog, Cisco XDR, and Microsoft Sentinel

Root Cause Analysis and Threat Detection

Root Cause Analysis

- ▶ Identify patient zero — the first compromised endpoint or account
- ▶ Reconstruct the full attack chain from IT entry to OT impact
- ▶ Attribute every forensic change to a specific user and session
- ▶ Quantify which control-system hosts or operational data were affected
- ▶ Produce an evidence timeline for regulators, safety bodies, and counsel

Threat Detection

- ▶ Ransomware: mass file modification, extension changes, shadow copy deletion
- ▶ OT pivot: unexpected changes on engineering workstations, HMIs, and historians
- ▶ Nation-state: new persistence artifacts and lateral movement between scans
- ▶ Timestamping: SI/FN attribute divergence indicating attacker log evasion
- ▶ Zero-day: behavioral detection without any signature or IoC required

Risk Scoring

Every detected behavioral pattern receives an explainable risk score — fully traceable to the underlying forensic artifacts — so operator security and OT teams can prioritise response effectively. Scores range from Low (routine changes) through Medium (anomalies warranting review) to High and Critical (ransomware staging, active encryption, confirmed control-system tampering).



Regulatory Compliance: TSA, CIRCIA, NIS2, CER and API 1164

Oil and gas operators face mandatory cyber incident reporting obligations that require forensic evidence, structured timelines, and regulator-ready reports — often within 72 hours, and in some cases within 24 hours or sooner. Tracknosis generates this evidence automatically from its continuously maintained forensic repository.

Regulation / Framework	Scope in Government	Key Obligation	Tracknosis Support
TSA Pipeline Security Directives (US)	Owners and operators of designated critical oil and natural gas pipelines	Implement cybersecurity measures; report incidents to CISA, generally within 24 hrs	Forensic evidence of changes to in-scope Windows assets and rapid incident documentation
CIRCIA (US)	US critical infrastructure including oil, gas, and energy operators	Report significant incidents to CISA within 72 hrs; ransomware payments within 24 hrs	Tamper-evident artifact preservation, incident documentation, and response records
NIS2 (EU)	Oil, gas, and energy operators classified as essential entities in EU member states	Early warning within 24 hrs; full notification within 72 hrs; senior accountability	Forensic timeline, evidence preservation, and structured regulatory report within hours
EU CER Directive	Critical entities operating in the oil, gas, and energy sectors	Resilience measures, incident notification, and demonstrable risk management	Continuous forensic monitoring and evidence supporting resilience and notification duties
API 1164 / IEC 62443	Pipeline SCADA security (API 1164) and industrial automation security (IEC 62443)	Secure control systems; manage change; maintain auditable security controls	Forensic evidence of changes to control-system Windows hosts and audit-ready records

Oil, Gas and Energy Use Cases



Ransomware Response

Detect encryption activity through delta analysis; generate forensic evidence package and regulatory report rapidly



Nation-State Intrusion

Detect stealthy persistence and tampering; reconstruct the attack for national authorities



Pipeline & SCADA Protection

Detect tampering and persistence on pipeline and SCADA Windows hosts before operations are impacted



Supply Chain Compromise

Detect tampering introduced via vendors, integrators, and remote-access tooling



IT-to-OT Intrusion

Detect attacker pivots onto engineering workstations, HMIs, and historians; reconstruct the crossover timeline



Safety System Integrity

Detect unauthorised changes to control and safety-system hosts that could endanger people or the environment



Insider & Contractor Risk

Attribute file and configuration changes to specific operator, engineer, or contractor accounts



Post-Incident Analysis

Reconstruct the complete attack chain; quantify impact for regulators, safety bodies, and insurers

Value to CIOs, CISOs, and OT Security Leaders

For oil and gas operators balancing production, safety, environmental responsibility, and national-security obligations, Tracknosis delivers measurable operational assurance. It provides early warning of threats and anomalies, accelerates forensic investigation, supports regulatory reporting, and helps protect the IT/OT boundary — all without replacing existing security investments or disrupting control systems.

Measurable Outcomes:

- ▶ Reduced mean time to detect (MTTD) and mean time to resolve (MTTR) cyber incidents.
- ▶ Rapid root cause identification — reducing reliance on scarce external forensic specialists.
- ▶ Improved uptime and reliability across upstream, midstream, and downstream operations.
- ▶ Regulatory reporting compliance — forensic evidence packages ready within hours, not days.
- ▶ Evidence-based forensic reporting for boards, regulators, and safety authorities.
- ▶ Enhanced collaboration between IT security, OT engineering, HSE, compliance, and operations.
- ▶ Strengthened regulator, investor, and community trust in operational resilience.
- ▶ Reduced cost and duration of cyber incident investigations and regulatory responses.

Benefits for Safety, Environment and Communities

Forensic Observability does not only protect the operator — by safeguarding the systems that control hazardous processes, it directly protects workers, the public, and the environment. When an operator can detect, investigate, and contain incidents in hours rather than weeks, the risk of a cyber-induced safety or environmental event is materially reduced.

Direct Benefits to Safety and the Environment

Process Safety	Early detection of tampering on control and safety-system hosts reduces the risk of spills, fires, or explosions
Environmental Protection	Faster containment limits the chance of a cyber-induced release affecting land, water, and air
Worker Protection	Protecting control systems helps keep on-site personnel safe from process upsets and hazardous events
Energy Supply Continuity	Faster detection and response keep production and distribution flowing, protecting downstream supply
Community Assurance	Rapid, evidenced response reassures regulators and local communities that operations are resilient
Evidence for Inquiry	Tamper-evident timelines support honest, defensible reporting to safety and environmental authorities

Wider Impact

- ▶ Reduced likelihood of cyber-induced safety incidents at hazardous facilities.
- ▶ Lower risk of environmental harm from disrupted or manipulated processes.
- ▶ More reliable energy supply to industry, transport, and households.
- ▶ Transparent, evidence-based engagement with regulators and communities.
- ▶ Greater public confidence in the safe and secure operation of critical energy assets.

Deployment and Governance

Tracknosis deploys rapidly across Windows workstations, servers, engineering hosts, and Citrix environments with no system reboot required. It integrates with existing IT management tooling, requires no dedicated database infrastructure, and supports on-premises, sovereign, segmented, and air-gapped deployments suited to remote and OT-aligned sites.

Supported Platforms	Windows 11; Windows Server 2016–2025; engineering/HMI hosts; Citrix Virtual Apps and Desktops
Deployment Methods	SCCM, Intune, Group Policy, MSI, PowerShell — pilot in minutes, estate-wide in hours
Encryption at Rest	Blowfish 448-bit (forensic repository) and AES-256
Encryption in Transit	TLS 1.3 across all communication channels
Evidence Integrity	Cryptographic hashing of every artifact at acquisition; read-only forensic collection
OT-Aware Deployment	Low-footprint collection suited to segmented OT networks; remote-site, sovereign, and air-gapped support
SIEM Integration	Splunk, Elastic, Datadog, Cisco XDR, Microsoft Sentinel — extends existing investments
Access Control	Granular RBAC and immutable audit logs; data sovereignty and retention controls

Why Tracknosis for Oil, Gas and Energy

Oil and gas operators cannot afford prolonged investigations, regulatory penalties, or the safety, environmental, and reputational consequences of a poorly managed cyber incident. Tracknosis provides the forensic intelligence layer that transforms existing security investments into a platform capable of answering the questions that matter most — and meeting the obligations that regulators, safety authorities, and communities demand.

Forensic Observability

- ▶ Continuous disk-level evidence
- ▶ Delta analysis across IT and OT hosts
- ▶ AI-assisted investigation
- ▶ Evidence independent of log tampering

Regulatory Compliance

- ▶ TSA · CIRCIA · NIS2 · CER · AP I 1164
- ▶ Reports generated within hours
- ▶ Structured evidence for regulators
- ▶ Board and safety-authority outputs

Academic Protection

- ▶ IT-to-OT intrusion detection
- ▶ Pipeline and SCADA protection
- ▶ Safety and environmental assurance
- ▶ Energy supply continuity.

TRACKNOSIS

