

BEYOND DETECTION: THE OIL AND GAS SOC GUIDE

Oil and gas cybersecurity teams are not short on alerts. What they lack is confidence in the decisions those alerts lead to.

In a recent Anomali survey of oil and gas cybersecurity leaders, 30% said that the failure they feared most was making a security decision that could not be fully explained or audited.

That fear maps directly onto how this sector is actually getting breached, and onto the very specific bind the CISO sits in when it happens.

Two things make oil and gas different from almost every other vertical a SOC guide gets written for. First, the attack surface is physical: refineries, pipelines, well pads, and offshore platforms run on operational technology (OT) that was never designed to be internet-connected, and it is now converging with IT faster than most security programs can secure it. Second, the person accountable for that convergence, the CISO, is being asked to carry personal, board-level, and increasingly regulatory liability for a risk surface that is only partly theirs to control.

The risk is real. Independent OT threat research puts poor IT/OT network segmentation at the top of the list of findings in oil and gas environments — the highest share of any sector analyzed — and flat network architectures mean that once an adversary lands, ransomware and other malware

can move laterally with very little resistance.¹ Analysts increasingly point to one scenario as the dominant risk for 2026: ransomware that starts in IT and crosses into OT, because operational downtime in this sector is not just lost revenue — it is safety risk, environmental exposure, legal liability, and regional supply disruption, all of which give extortion actors outsized leverage.²

The CISO carries this differently than other executives, and the audit is where that shows up. Ask most CISOs what actually keeps them up at night and the answer isn't the next breach, but the next audit and what happens to them personally if the evidence doesn't hold up. Splunk's 2026 CISO Report found that 78% of CISOs are now personally worried about being held liable for security incidents, up from 56% just a year earlier, a 22-point jump in twelve months.³ The same report found one in five say they've been pressured not to report a compliance issue at all. That's the backdrop every audit in this sector plays out against.

For oil and gas specifically, the audit isn't a once-a-year event with a consultant and a PowerPoint. It's a standing evidentiary obligation, and in this sector it comes from the TSA. Operators of TSA-designated critical hazardous liquid and natural gas pipelines and LNG facilities work under the Security Directive Pipeline-2021-01 and 2021-02 series, revised and reissued annually since the Colonial Pipeline attack.⁴

¹Dragos, 2026 OT/ICS Cybersecurity Year in Review — IT/OT segmentation findings in oil and gas, dragos.com.

²Telesoft, "The Biggest Oil & Gas Cybersecurity Risk in 2026 — and How CISOs Can Protect IT, OT and Critical Infrastructure."

³Splunk, 2026 CISO Report, as cited in Cyberbase AI, "The 10 Biggest CISO Challenges in 2026," cyberbase.ai.

⁴TSA, Security Directive Pipeline-2021-01 series and Security Directive Pipeline-2021-02 series, issued after the May 2021 Colonial Pipeline incident and reissued with revisions each year (SD Pipeline-2021-02F effective May 3, 2025; SD Pipeline-2021-01F effective Oct. 25, 2025), tsa.gov.

The series requires a TSA-approved Cybersecurity Implementation Plan naming the specific measures in place, an incident response plan for designated critical cyber systems, a Cybersecurity Assessment Plan submitted every year for approval with the prior year's results attached, records sufficient to demonstrate compliance, a cybersecurity coordinator available around the clock, and notification to CISA no later than 24 hours after a cybersecurity incident is identified.⁵ Refineries, marine terminals, and LNG facilities with marine transfer operations carry a second set of obligations under the Coast Guard's Cybersecurity in the Marine Transportation System rule, effective July 16, 2025, whose Cybersecurity Plan, Cybersecurity Officer, and assessment requirements phase in through July 16, 2027.⁶ When CISA finalizes the CIRCIA rule, 72-hour incident reporting and 24-hour ransom-payment reporting will apply on top of that.⁷

The dollar penalties look modest next to other regulated sectors. TSA's own sanction guidance tops out at \$14,602 per violation for surface transportation modes.⁸ The real exposure is the plan itself. A TSA-approved implementation plan is a document an operator can be held to measure by measure, and the operator who cannot show that one of its own named measures actually operated is the one explaining that to an inspector, and then to a board carrying its own SEC disclosure obligations. When a regulator asks why a decision was made, "the tool flagged it" is not an answer, and "we're pretty sure we were covered" is not a defense.

At the same time, IT/OT convergence blurs the boundary between security and operations, so the CISO increasingly needs both technical depth and the strategic standing to influence business goals. It's a role that has quietly expanded from "protect the network" to "defend every call, in front of an auditor, with evidence, on infrastructure you don't fully own — and increasingly, with your own name on the finding."

SOC leadership feels a parallel version of this pressure, just lower on the org chart and closer to the noise. Tines'

2026 Voice of the SOC Analyst report found 71% of SOC analysts report burnout tied to alert fatigue, and some SOC managers or directors aren't only fighting the threat landscape, they're fighting to keep a trained team in their seats long enough for that training to pay off. Both problems trace back to the same root cause: too much unfiltered noise, and not enough context arriving with it.

There is a way through, and it runs in order. Fix the data the decisions rest on, then build up from clean data to governed action. The five moves below climb that path, and each one maps to a real, current failure mode in this sector, not a generic SOC problem.

1. START WITH THE DATA: THE GAPS ARE REAL, NOT THEORETICAL

The obstacle most oil and gas SOC's face is the data feeding the tools they already have. Analysts review intelligence from multiple sources carrying the same observables (IP addresses, file hashes, and the like) with contradictory severity assessments. Vendor feeds go stale, overlap, and sit in silos, and every source arrives in its own schema. Most SIEMs keep full-fidelity data hot for only 30 to 90 days, and cold-storage retrieval costs make historical investigation painful.

This matters more here than elsewhere because of how oil and gas infrastructure is actually built: geographically distributed well pads, pipelines stretching hundreds of miles, and refineries that cannot tolerate unplanned downtime for patching. Known vulnerabilities routinely coexist with internet exposure and remote-access pathways for extended periods, not because teams don't know about them, but because patching is constrained by operational continuity requirements, vendor qualification processes, and the sheer difficulty of managing assets spread across remote sites. Fragmented, noisy data on top of that reality slows triage and hides the exposure a CISO will eventually have to explain. Anomali ingests every source, normalizes it to a single open schema (OCSF),

⁵TSA, *SD Pipeline-2021-01 series* (Cybersecurity Coordinator available to TSA and CISA 24/7; report cybersecurity incidents to CISA as soon as practicable and no later than 24 hours after identification) and *SD Pipeline-2021-02 series* (TSA-approved Cybersecurity Implementation Plan, Cybersecurity Incident Response Plan, annual Cybersecurity Assessment Plan and prior-year results, recordkeeping), [tsa.gov](https://www.tsa.gov). The original May 2021 directive set a 12-hour reporting window; later revisions moved it to 24 hours.

⁶U.S. Coast Guard, *Cybersecurity in the Marine Transportation System*, final rule, 90 Fed. Reg. 6298 (Jan. 17, 2025), effective July 16, 2025; applies to facilities with security plans under 33 CFR parts 104-106.

⁷Cyber Incident Reporting for Critical Infrastructure Act of 2022. The 72-hour incident and 24-hour ransom-payment windows are statutory; reporting obligations begin on the final rule's effective date. CISA published its proposed rule in April 2024 and listed the final rule for September 2026 in the July 2026 Unified Agenda.

⁸TSA, *Enforcement Sanction Guidance Policy* (updated Jan. 24, 2025): up to \$14,602 per violation for surface transportation modes, up to \$17,062 for other persons; see also 49 CFR 1503.401 for per-action ceilings. Amounts are adjusted for inflation.

⁹Tines, *Voice of the SOC Analyst Report* (2026), tines.com.

removes duplicates before they ever become alerts, and fuses vetted intelligence into each event as it lands, so context arrives with the data instead of as a lookup an analyst runs later. It installs without a rip-and-replace, deploying on top of the SIEM you already run, which matters when regulators expect continuity of monitoring and operations can't absorb a platform migration on top of everything else.

Why it matters to the CISO: *when an auditor or a board member asks how a known vulnerability sat exposed for months, "the patch was operationally deferred" is a real answer, but only if the CISO can also show the compensating context and monitoring that were in place around it. Clean, fused data is what makes that second half of the answer possible.*

Why it matters to SOC leadership: *the average security team fields thousands of alerts a day, and industry research puts the false-positive share at close to half¹⁰, all noise a SOC manager has to staff against, shift after shift. Deduplication and fused context at ingest isn't just an audit-readiness play; it's the lever that keeps a triage queue from becoming a retention problem.*

2. SEE ACROSS IT AND OT: THE ADVERSARY IS BUILT TO WAIT

Some intrusions are built to wait, and oil and gas is where that patience pays off best for the attacker. The traditional air gap between IT and OT has eroded as companies modernize field operations with IoT sensors, cloud analytics, and remote engineering access¹¹; threat researchers have documented adversaries deliberately exploiting the distributed, remote-access-dependent nature of oil and gas infrastructure to gain persistent, long-lived footholds. A dormant foothold in an OT environment such as a compressor station, a historian, or a SCADA gateway can sit for months before it moves, well outside the 30-to-90-day hot window most SIEMs default to.

This is also where the CISO's job gets structurally harder than a typical enterprise security leader's: OT and IT are usually owned by different teams with different priorities

(uptime and safety vs. confidentiality and patch cadence), often on different reporting lines. The CISO is expected to have visibility and influence across both, without always having formal authority over OT engineering decisions. A visibility gap is more than a monitoring problem in this context; it's a governance problem the CISO has to answer for even when the asset in question was never fully theirs to secure.

A modern security data lake changes the economics of closing that gap: it ingests terabytes and searches years of structured and unstructured data in seconds, without the cold-storage retrieval fees and timeouts that make legacy historical search impractical. Because compute and storage are decoupled, you pay when analytics run rather than for idle capacity — which is what finally makes full-fidelity, long-term retention across both IT and OT affordable enough to actually happen. The measure that matters is Mean Time to Prioritized Remediation (MTPR), and the target is seconds. "Are we impacted, and where," across both networks, should not take days, and it should not require asking OT engineering for a special export.

Why it matters to SOC leadership: *every minute an analyst spends manually pivoting between the IT SIEM, the OT historian, and a separate cold-storage export is a minute not spent on the actual investigation, and that kind of repetitive, low-value toil is what analysts cite as a top driver of burnout and turnover.*

3. MOVE FROM DETECTING TO DECIDING: THE AUDIT, NOT THE INCIDENT, IS WHAT CISOS ACTUALLY FEAR

Every investigation starts with the same question: is this a threat, and are we affected? Is the actor known? What's the vector? Is our infrastructure at risk? Raw signal tells you what happened. Context tells you what it means, already attached to the event,

But in oil and gas, "deciding" is the beginning of a paper trail someone else is going to inspect. The TSA model runs on an annual cycle built around proving that a measure worked rather than that it was written down: the assessment plan goes in for approval, last year's assessment results go in with it, changes to the implementation plan have to be approved before they

¹⁰Microsoft, SOC 2026 report, as cited in World Informatix, "Alert Fatigue in the SOC: 2026 Causes, Costs & Fixes."

¹¹Hydrocarbon Processing, "How Oil and Gas Operators Can Strengthen OT Security in 2026."

count, and the records have to be there when an inspector asks.¹² A gap found in your own assessment is only step one. You then need months of new, compliant evidence before the next submission closes. There is no partial credit for “we’re confident this happened” without the record to show it.

This is why the 30% of survey CISOs who fear an unexplainable decision are describing something much more concrete than it sounds. SEC cyber-incident disclosure rules have pushed real accountability for cyber risk management up to the board, and boards in turn push the evidentiary burden straight back down to the CISO.¹³ The TSA directives require operators to document the specific measures protecting their infrastructure and to hold the evidence that those measures operate. “The tool flagged it” was never a sufficient answer to an auditor; it is now closer to a personal liability exposure than an operational gap, and one reason a growing share of CISOs are negotiating D&O coverage and indemnification language into their own employment contracts.¹⁴

When intelligence is fused at ingest, an alert arrives already attributed, already mapped to MITRE ATT&CK, and already scored, so when the CISO has to show the basis for a decision, the reasoning already exists as a record instead of something to be reconstructed under pressure, months later, from someone’s memory of a Tuesday in March. Compliance evidence gets produced from the operational data itself instead of assembled by hand for each submission. Anomali brings full-fidelity telemetry, the context that gives it meaning, agentic judgment that reasons across it, and governed action into one system, so that record exists by default rather than by heroic effort the week before an inspection.

Why it matters to the CISO: an unexplainable decision eventually becomes an inspection response with your name on it. In a regulatory environment where personal liability worry has jumped 22 points in a single year, the ability to show your reasoning is what separates a defensible answer from a personal exposure.

Why it matters to SOC leadership: today, assembling that evidence trail usually falls on whichever analyst is still around when the request lands, adding hours of manual log-pulling stacked on top of an already full queue. Evidence generated automatically, at the point of decision, gives that time back to the team instead of taking it away.

4. CONSOLIDATE ON ONE INTELLIGENCE-FIRST PLATFORM: THIRD-PARTY RISK ISN'T OPTIONAL TO OWN

Most SOC stacks in this sector are an archaeology of single-purpose tools bought over a decade, running alongside a supply chain the CISO didn’t choose and can’t fully audit: oilfield services vendors, contractors connecting from outside the perimeter, and OT equipment vendors who control their own patch cycles. Industry research consistently flags supply-chain vulnerability remediation as one of the top priorities energy-sector CISOs are actively trying to fix¹⁵: every third party with system access shares in the risk, but the CISO is usually the one who has to measure their maturity and hold them accountable, without owning every downstream decision they make.

A point-tool strategy compounds this rather than fixing it: a team running eight to twelve disconnected products is also running eight to twelve separate integration points for third-party risk to hide in. Intelligence is the layer that makes consolidation worth it: Managed Intelligence as a Service (MlaaS), powered by ThreatStream Next-Gen, keeps the data lake continuously enriched with threat actors, TTPs, and campaigns, and operationalizes that intelligence in minutes rather than the days a manual TIP-to-SIEM handoff takes.

For critical infrastructure specifically, peer sharing closes a gap no single vendor relationship can, and in this sector it works through an analyst team rather than directly between companies. In the ONE-ISAC model, a member submits what it is seeing in its own environment to the ISAC’s Threat Intelligence Center, where analysts anonymize the submission, enrich it with their own background

¹²TSA, SD Pipeline-2021-02 series: Cybersecurity Implementation Plan approval, annual Cybersecurity Assessment Plan submission with the previous year’s results, and recordkeeping obligations, tsa.gov; see also TSA’s information collection notice for the SD Pipeline-2021-02 series (comments due Feb. 2, 2026).

¹³KPMG, Cybersecurity Considerations 2025: Energy and Natural Resources Sector — SEC disclosure liability, board accountability.

¹⁴Cyberbase AI, “The 10 Biggest CISO Challenges in 2026” — D&O coverage / indemnification trend.

¹⁵EY, “How Energy Sector CISOs Can Show Cybersecurity’s Value” — third-party/supply-chain risk priority

and sends it out to the membership under Traffic Light Protocol. Members decide whether to be identified or to stay anonymous. The company that submits gets analytic work it did not have to staff, and every other member gets early warning about something already sitting inside a peer's network, which matters in a sector where state-aligned actors and long-horizon espionage campaigns are known to target the same infrastructure across multiple operators. Membership is not free. Member companies pay annual dues, and Anomali user licenses are part of the member benefits those dues buy.

Why it matters to the CISO: board risk reports work better and hold up better under scrutiny when third-party and supply-chain risk is measured continuously against one consistent data set, instead of surfaced only when a vendor's breach becomes your incident.

5. ADOPT AI ON A GOVERNED PATH — BECAUSE THE SKILLS GAP IS THE REAL CONSTRAINT, AND RETENTION IS THE METRIC NOBODY BUDGETS FOR

The industry is short on qualified analysts, and the ones on staff are stretched across an attack surface that keeps expanding: IT, OT, cloud, identity, and now AI-driven threats aimed squarely at the humans in the loop. For SOC leadership specifically, the math is brutal: Tines' 2026 Voice of the SOC Analyst report found 71% of analysts report burnout tied to alert fatigue, and some SOC's are seeing turnover cycles under 18 months¹⁶, which means a SOC manager can spend months training an analyst only to be back at the staffing table before that investment pays off. Adversaries are already using AI to scale phishing and identity attacks faster than traditional perimeter defenses can adapt, which raises the stakes on a staffing gap oil and gas has been living with for years.

AI is part of the answer, but governance is the precondition, not an afterthought. Natural language processing lowers the bar for triage; an analyst who

can ask a question in plain language instead of writing a complex detection query can take on work that used to require a senior analyst, narrowing the skills gap without a multi-year ramp. AI also absorbs first-pass triage load, enriching telemetry in real time and escalating only what needs a person.

This is also where the CISO's role has expanded again: beyond architecture and audits, energy-sector security leaders are increasingly expected to act as internal evangelists¹⁷ by building digital awareness and buy-in across a workforce (and an OT engineering culture) that didn't grow up assuming everything is a target. Governed AI adoption gives the CISO something concrete to point to when making that case: a way to close the skills gap that doesn't require asking the board for a headcount increase the budget won't support.

Why it matters to SOC leadership: AI-assisted triage is a retention lever. Every hour of rote first-pass triage that shifts to an assistant is an hour an analyst gets back for the higher-judgment work that actually keeps them engaged, which is the difference between an 18-month tenure and a career.

¹⁶Tines, Voice of the SOC Analyst Report (2026), tines.com.

¹⁷KPMG, Cybersecurity Considerations 2025: Energy and Natural Resources Sector — CISO as internal evangelist.

PAY LESS, GET MORE

Storage is one of the largest and least examined line items in the SOC. Traditional SIEMs charge for full ingest and make long retention expensive, and many depend on additional paid tools to feed and analyze the data they hold.

A serverless data lake changes the math. Full-fidelity data is stored at cloud-object-storage cost, years of retention become viable, and because compute runs only when analytics do, cost aligns to usage instead of peak provisioning.

See Everything.

Know What Matters.

Act With Confidence.

THE FOUNDATION THE AGENTIC SOC REQUIRES

Anomali delivers an AI-powered platform built on an Intelligent Unification Layer, with Managed Intelligence as a Service as its foundation and governed agentic operations on top. Detection was never the hard part in oil and gas. Deciding — and being able to defend that decision to a board, a regulator, or a jury of one's own OT engineering team — is. Anomali gives CISOs, SOC leaders, and their teams the context, intelligence, and governance to act with confidence and defend every call, built on more than a decade of intelligence work.

SEE ANOMALI IN ACTION

[Request a Demo](#)