



MITHRYL SYSTEMS

UNIFIED DEFENSE FOR CRITICAL SYSTEMS

EXECUTIVE BRIEF

YOUR SOC WASN'T BUILT FOR OT

Why OT MDR Is the Missing Layer Between IT Security and Critical Operations

Extend your existing SOC with OT-native expertise, Augmented Intelligence, and Operational Intelligence so you can make confident decisions before cyber risk becomes operational impact.



THE GAP



The SOC Has

- Telemetry
- Tools
- Analysts
- Alerts
- Threat Intelligence



THE SOLUTION

Mithryl Systems OT MDR

- OT-Native Expertise
- Augmented Intelligence
- Continuous Cyber Fusion
- Integrated Compliance
- Operational Intelligence



THE OUTCOME

Operations Gets

- Context
- Investigation
- Operational Impact
- Recommendations
- Confidence



CYBER INTELLIGENCE.
OPERATIONAL DECISIONS.



Protect Critical Operations.
Operate With Confidence.

Contents

Executive Summary	3
The Gap Between the Soc and Operations	3
What the SOC Has	4
What Operations Needs	4
The Missing Layer: Operational Intelligence.	4
IT Response and OT Response Are Not the Same	4
Why the Gap is Becoming More Urgent	5
Your SOC Does Not Need to Become an OT SOC	6
Augmented Intelligence Changes the Economics of OT Security	6
From Alerts to Operational Intelligence	7
Compliance Becomes Part of the Operation	8
Every Investigation Should Make the SOC Better	8
What Changes With OT MDR	9
The Question for IT Leaders	9
Your SOC Doesn't Need to Become an OT SOC	10



Executive Summary

Your Security Operations Center is not failing. In fact, it may be doing exactly what it was designed to do.

Your SOC monitors enterprise infrastructure, correlates telemetry, investigates alerts, identifies threats, protects identities and endpoints, and coordinates response across an increasingly complex technology environment. You have invested in analysts, SIEM, EDR, firewalls, identity security, threat intelligence, cloud security, and perhaps dedicated OT monitoring technology.

The problem is not that your SOC lacks cybersecurity capability. **The problem is that industrial operations create an entirely different decision environment.**

When a cyber event crosses into Operational Technology, the question changes from, **"Is this malicious?"** to **"What does this mean to operations, and what should we do about it?"**

That question requires operational context, OT expertise, industrial threat intelligence, knowledge of engineering processes, safety awareness, regulatory understanding, and the ability to evaluate cyber risk against production consequences.

Most enterprise SOC's were never designed to provide that. That is the gap OT Managed Detection & Response is designed to close.

The Gap Between the Soc and Operations

Most industrial organizations already possess enormous amounts of cybersecurity information. The enterprise SOC has telemetry. It has alerts. It has analysts. It has threat intelligence. It has security platforms. Increasingly, it also receives information from OT monitoring technologies deployed across industrial environments.

But visibility is not the same as understanding. An alert originating from an engineering workstation, historian, HMI, jump host, industrial firewall, or OT monitoring platform may tell the SOC that something happened. It does not necessarily tell the analyst what that activity means to the industrial process, whether production is at risk, whether the activity

is expected engineering behavior, or what operational consequences could result from taking action.

That creates a critical gap between **cybersecurity information and operational decision-making**.

What the SOC Has

Security telemetry, alerts, SIEM and XDR platforms, EDR, threat intelligence, security analysts, enterprise playbooks, incident response processes, and increasingly OT security telemetry.

What Operations Needs

Operational context, validated investigations, understanding of production impact, engineering-aware recommendations, compliance evidence, OT threat expertise, response guidance, and confidence in the decisions being made.

The Missing Layer: Operational Intelligence.

Operational Intelligence transforms cybersecurity telemetry into the context, evidence, analysis, and recommendations organizations need to understand what is happening, why it matters to operations, and what should happen next.

IT Response and OT Response Are Not the Same

Traditional IT incident response is often designed around rapid containment. Compromised endpoints can be isolated. Accounts can be disabled. Connections can be blocked. Systems can be reimaged.

Those same actions can have very different consequences in an industrial environment. Isolating an engineering workstation could affect an active maintenance process. Blocking communications could interfere with an industrial application. Taking a system offline could affect production availability. Responding to suspicious behavior without understanding the underlying industrial process could introduce greater operational risk than the original event.



That is why OT cybersecurity requires a different operating model. The objective is not slower response. It is **informed response**.

Before action is taken, organizations need to understand the cyber event, the affected assets, their relationship to industrial processes, the potential operational consequences, and the safest available response.

Cybersecurity identifies the threat. Operational Intelligence helps determine the decision.

Why the Gap is Becoming More Urgent

The separation between enterprise IT and industrial operations is disappearing. Digital transformation, remote access, cloud connectivity, enterprise applications, connected supply chains, third-party access, industrial IoT, and centralized identity are creating more connections between IT and OT environments.

Attackers understand those connections. An incident that begins with a compromised identity, endpoint, vendor account, remote access system, or enterprise application can become an operational problem as attackers move toward the systems supporting production.

At the same time, security teams are managing increasing volumes of telemetry and alerts. Industrial environments continue to introduce specialized technologies and operational constraints. Regulatory expectations are expanding. Boards and executives increasingly expect security leaders to demonstrate operational resilience rather than simply report cybersecurity activity.

Artificial intelligence is accelerating the environment further. Attackers can operate faster, while defenders have an opportunity to dramatically accelerate correlation, enrichment, evidence collection, investigation, and analysis.

The organizations best prepared for this environment will not simply be those with the most cybersecurity technology. They will be the organizations capable of turning that technology into **Operational Intelligence before cyber risk becomes operational impact**.



Your SOC Does Not Need to Become an OT SOC

Building a completely separate OT Security Operations Center may sound like the obvious answer. For many organizations, it is not.

Creating another SOC can mean another team, another operating model, additional technology, duplicated processes, separate workflows, and another organizational silo between IT and OT.

There is a better approach. **Extend the SOC you already have.**

Mithryl Systems OT Managed Detection & Response augments the existing Security Operations Center with the specialized capabilities required to understand and protect industrial environments. Your SOC continues doing what it does well.

Mithryl Systems adds OT-native expertise, continuous investigation, industrial threat intelligence, Detection Engineering, Threat Hunting, Digital Forensics and Incident Response, integrated compliance, Augmented Intelligence, and operational decision support.

The result is not two disconnected security organizations. It is a stronger security operation capable of understanding risk across both enterprise and industrial environments.

Augmented Intelligence Changes the Economics of OT Security

The volume and complexity of cybersecurity information make purely manual investigation increasingly difficult to scale. Mithryl Systems uses Augmented Intelligence to accelerate the investigative work machines perform best while preserving human judgment for the decisions that require operational expertise.

Augmented Intelligence accelerates telemetry correlation, evidence collection, threat enrichment, relationship analysis, investigation timelines, case preparation, compliance documentation, and reporting. Instead of spending valuable analyst time assembling



information from multiple systems, experienced OT analysts can focus on understanding what the evidence means. But AI does not make operational decisions.

Experienced OT professionals validate findings, interpret operational context, evaluate potential business and production impact, and develop recommendations appropriate for the customer's environment.

Operations retains authority over actions affecting production. **AI accelerates. Experts investigate. Operations decides.** This combination allows the existing SOC to gain specialized OT capability without requiring every enterprise analyst to become an industrial cybersecurity expert.

From Alerts to Operational Intelligence

Mithryl Systems OT MDR changes the endpoint of the security workflow. The objective is no longer simply:

Alert → Triage → Close

The objective becomes:

Telemetry → Correlation → Investigation → Operational Context → Recommendation → Operational Decision → Continuous Improvement

Every meaningful event is investigated within its operational context.

- What happened?
- Which systems and processes are involved?
- Is the activity malicious, suspicious, expected, or operational?
- What could happen if it continues?
- What could happen if we respond?
- What regulatory or compliance implications exist?
- What should the organization consider doing next?



Those are the questions that turn cybersecurity information into Operational Intelligence.

Compliance Becomes Part of the Operation

Regulatory compliance should not begin when an auditor arrives. OT MDR integrates compliance into ongoing cybersecurity operations by continuously producing the evidence, investigative records, response documentation, decision history, and reporting needed to demonstrate cybersecurity program effectiveness.

Rather than treating compliance as a separate reporting exercise, Mithryl Systems helps organizations make regulatory readiness an outcome of everyday security operations.

This approach can support organizations working within frameworks and requirements such as NERC CIP, IEC 62443, NIST SP 800-82, NIST Cybersecurity Framework, TSA Security Directives, NIS2, and applicable sector-specific requirements.

Security operations generate the evidence. Operational Intelligence provides the context. Compliance gains the documentation. Executives gain greater confidence in organizational readiness.

Every Investigation Should Make the SOC Better

Traditional MDR can become transactional. An alert arrives, an analyst investigates it, a ticket is closed, and the process begins again. Mithryl Systems takes a different approach.

Every investigation contributes intelligence that can improve future security operations. Investigation findings inform Detection Engineering. Detection gaps create new detection content. Threat intelligence informs new hunts. Hunting uncovers additional visibility requirements. Incident findings improve response playbooks. Compliance evidence improves regulatory readiness. Operational knowledge strengthens future investigations.



The result is a continuous improvement cycle. The SOC does not simply process today's events. **It becomes better prepared for tomorrow's.**

What Changes With OT MDR

With Mithryl Systems OT MDR, the enterprise SOC gains specialized OT capabilities without replacing its existing technology, people, or processes. Security teams gain deeper investigations and operational context. Engineering and operations teams receive recommendations grounded in the realities of industrial environments. Compliance teams gain stronger evidence and continuous regulatory support. Executives gain clearer visibility into operational cyber risk and resilience.

Existing investments in SIEM, EDR, OT monitoring, firewalls, identity, threat intelligence, and other security technologies become more valuable because the information they generate contributes to a broader Operational Intelligence capability. The result is not simply more security coverage. It is a more capable security organization.

The Question for IT Leaders

The question is no longer whether OT belongs within the cybersecurity strategy. It already does. The question is whether the existing security operation can answer the questions that matter when cybersecurity reaches operations:

1. **What happened?**
2. **What does it mean to production, safety, reliability, and compliance?**
3. **What should we do next?**

If those answers depend on assembling the right people after an incident begins, the organization has an Operational Intelligence gap. And during an operational cyber event is the wrong time to discover it.

Your SOC Doesn't Need to Become an OT SOC

It needs an OT MDR partner.

Mithryl Systems extends your existing SOC with OT-native expertise, Augmented Intelligence, Continuous Cyber Fusion, integrated compliance, and Operational Intelligence so your organization can understand what is happening, determine what it means to operations, and make confident decisions before cyber risk becomes operational impact.

**Your SOC has the data. Mithryl Systems delivers the Operational Intelligence.
CYBER INTELLIGENCE. OPERATIONAL DECISIONS.**

Mithryl Systems transforms cybersecurity telemetry into Operational Intelligence, enabling industrial organizations to Protect Critical Operations and Operate With Confidence.

Learn more about *Mithryl Systems OT Managed Detection & Response* at MithrylSystems.Com



About Mithryl Systems

Mithryl Systems exists to protect what powers the world. We help organizations responsible for critical operations reduce cyber risk, strengthen operational resilience, and make confident decisions across increasingly connected IT and OT environments. Our approach brings together operational technology expertise, cybersecurity, engineering, intelligence, governance, and experienced human judgment around a shared understanding of operational risk.

At the center of Mithryl is a simple belief: cybersecurity should protect business outcomes, not simply generate alerts. Through OT Managed Detection & Response, OT Detection Engineering, Incident Response, Threat Hunting, Digital Forensics, Red Team Assessments, vCISO Services, and OT Cyber Fusion Strategies, we turn security telemetry into operational intelligence that helps organizations understand what is happening, what matters, and what to do next.

Our purpose is **Unified Defense for Critical Systems**. Our promise is **Operate With Confidence**. That means protecting production without unnecessary complexity, breaking down the barriers between security and operations, and giving leaders the clarity they need to keep the systems their organizations and communities depend on running.

For more information, visit <http://www.mithrylsystems.com>.

Disclaimer. © Copyright 2026 by Mithryl Systems. All Rights Reserved. All product and company names herein may be trademarks of their respective owners. The information and content in this document is provided for informational purposes only and is provided “as is” without any warranty, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. PhishCloud is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, PhishCloud makes no claim, promise, or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. PhishCloud makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document. If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as possible.

Reproducing, copying, or making adaptations, or compilation works based on this content without prior written authorization from PhishCloud, Inc., is prohibited by law.