EXECUTIVE BRIEF

MITHRYL SYSTEMS

UNIFIED DEFENSE FOR CRITICAL SYSTEMS

TRADITIONAL SOCs WEREN'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 SOLUTION	THE OUTCOME
The SOC Has • Telemetry • Tools • Analysts • Alerts • Threat Intelligence	**Mithryl Systems OT MDR** • OT-Native Expertise • Augmented Intelligence • Continuous Cyber Fusion • Integrated Compliance • Operational Intelligence	**Operations Gets** • Context • Investigation • Operational Impact • Recommendations • Confidence

CYBER INTELLIGENCE.
OPERATIONAL DECISIONS.

Protect Critical Operations.
Operate With Confidence.

Contents

Executive Summary 3
The Gap Isn't Visibility. It's Operational Understanding. 4
The Human Middleware Problem 5
IT Response and OT Response Are Not the Same 6
A Traditional SOC Does Not Need to Become an OT SOC 7
From Alert to Operational Intelligence 8
Augmented Intelligence Accelerates the Investication. Experts Determine What it Means. 10
OT MDR Should Not Stop When The Ticket Closes 10
Compliance Becomes Part of Security Operations 12
Why This is Becoming More Urgent 13
What Chanes with Mithryl Systems OT MDR 14
The Question Every IT Leader Should Ask 15
Not Another Security Silo 15
About Mithryl Systems 17

Executive Summary

The traditional Security Operations Center is not failing. In fact, it may be doing exactly what it was designed to do. The modern enterprise SOC monitors infrastructure, correlates telemetry, investigates alerts, protects identities and endpoints, identifies threats, and coordinates response across an increasingly complex technology environment. Organizations have invested heavily in SIEM, EDR, identity security, firewalls, threat intelligence, cloud security, and, increasingly, dedicated OT monitoring technology. Those investments are essential, and they should remain at the center of the cybersecurity program.

The challenge begins when a cybersecurity event crosses into an industrial environment. An enterprise analyst may know that a vendor account authenticated to an OT jump host at 2:13 a.m. after several failed attempts. The analyst may know the source address, account, endpoint, authentication history, and associated threat intelligence. But that information alone does not tell the organization whether the activity threatens production, whether the vendor was performing authorized work, what industrial systems can be reached from that jump host, or whether disabling the account could interrupt an active engineering or maintenance activity.

At that point, the question is no longer simply, **“Is this malicious?”** The more important question becomes, **“What does this mean to operations, and what should we do about it?”**

Answering that question requires capabilities most enterprise SOCs were never designed to provide: OT expertise, engineering awareness, industrial threat intelligence, operational context, understanding of production and safety consequences, regulatory knowledge, and the ability to evaluate the cyber risk of an event against the operational risk of the response.

That is the gap OT Managed Detection & Response is designed to close. Mithryl Systems extends the existing SOC with OT-native expertise and Augmented Intelligence, transforming security telemetry into Operational Intelligence that helps cybersecurity and operations teams understand what is happening, determine what it means to critical operations, and make the right decision without unnecessarily disrupting production.

The Gap Isn't Visibility. It's Operational Understanding.

Industrial organizations have more cybersecurity visibility than ever. Enterprise SOCs collect telemetry from SIEM, EDR, identity platforms, firewalls, remote-access systems, cloud infrastructure, threat intelligence, and other security technologies. Many organizations have also deployed specialized OT monitoring platforms across industrial environments. Together, these technologies can provide substantial visibility into activity across the enterprise and operational environment.

But visibility and understanding are not the same thing. An alert from an engineering workstation, historian, HMI, jump host, industrial firewall, or OT monitoring platform can tell the SOC that something happened. It does not automatically tell the analyst what that activity means to the industrial process, what operational dependencies exist, or what the consequence of taking action might be.

Consider a suspicious privileged login to an OT jump host. Before deciding how to respond, the organization may need to determine:

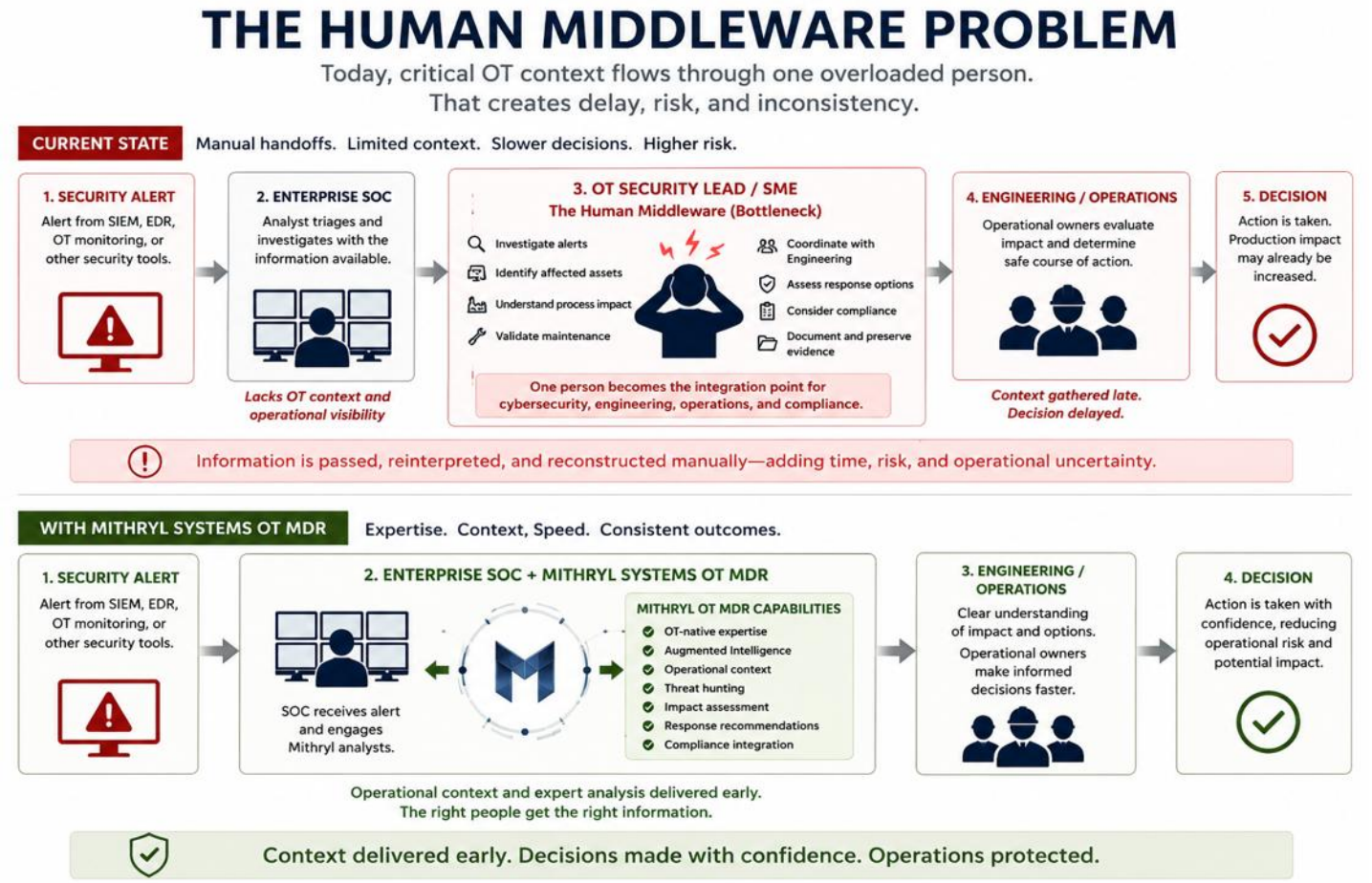
- Was the access expected and was there an approved maintenance window?
- Which industrial assets, applications, and processes can be reached through the jump host?
- Could the account reach systems capable of changing the process?
- Was engineering or maintenance activity underway?
- Could disabling the account interrupt legitimate operational activity?
- Could isolation affect production, operator visibility, safety, or recovery?
- Does the event create regulatory, evidence, or reporting implications?
- Who has the authority to make the operational decision?

Those are not simply cybersecurity questions. They are operational questions triggered by a cybersecurity event, and they are the questions that ultimately determine whether the organization can respond quickly without creating additional risk.

The Human Middleware Problem

In many industrial organizations, the connection between the enterprise SOC and plant operations is still largely manual. The SOC investigates what it can and, when an event requires industrial context, escalates to an OT security lead, engineer, plant resource, or other individual who understands the environment. That person becomes the human integration layer between cybersecurity and operations.

The process often looks like this:



The OT resource determines what the affected asset actually does, identifies the appropriate operational owner, establishes whether maintenance activity is underway, evaluates the consequences of containment, coordinates with engineering or compliance, and helps determine what can safely be done. The process can work, but it depends heavily on individual knowledge, availability, relationships, and the ability to reconstruct operational context while an investigation is already underway.

That model becomes increasingly difficult to scale as IT and OT become more connected, third-party access expands, industrial telemetry increases, regulatory expectations grow, and cybersecurity teams are expected to operate continuously. The organization does not need another alert queue. It needs a repeatable operating model for turning cybersecurity alerts into informed operational decisions.

IT Response and OT Response Are Not the Same

Traditional IT incident response frequently prioritizes rapid containment. A compromised endpoint may be isolated, a suspicious account disabled, a malicious connection blocked, or an affected system taken offline and rebuilt. In an enterprise environment, those actions can be both appropriate and necessary.

In OT, however, the response itself can become part of the risk. An engineering workstation may be supporting an active maintenance activity. A jump host may provide the only approved engineering path into a critical process area. Blocking communications may interfere with an industrial application. Isolating a system may reduce operator or engineering visibility. Taking an asset offline may affect production availability or complicate recovery.

This does not mean OT response should be slower. It means the response must be informed by the operating environment. Before taking action, the organization needs to understand the event, the affected assets, their relationship to the industrial process, the potential consequence of the threat, the potential consequence of the response, and the safest available course of action.

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

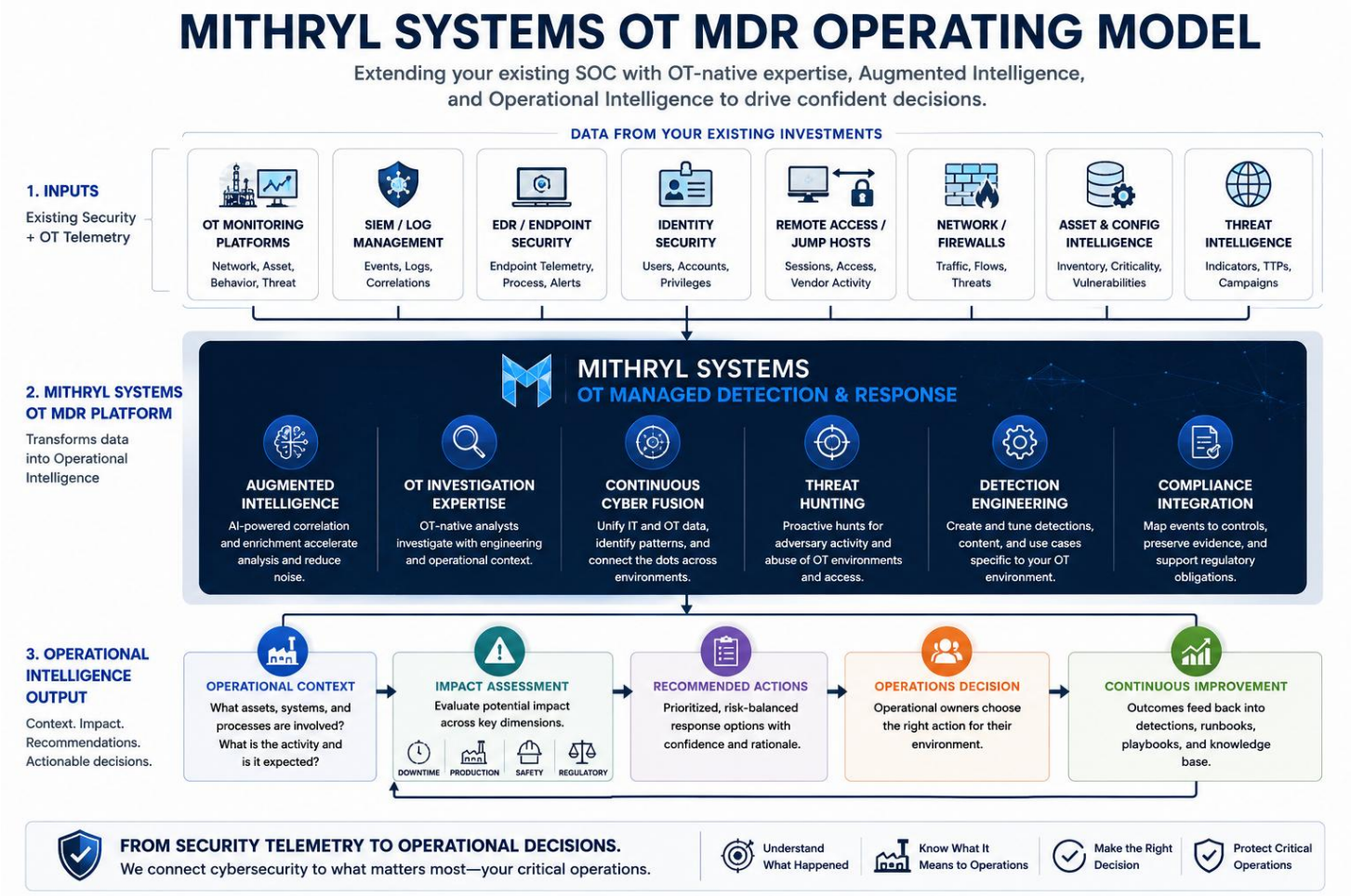


A Traditional SOC Does Not Need to Become an OT SOC

The answer to this challenge is not necessarily to build another SOC. A separate OT SOC can introduce another team, another workflow, another technology stack, and potentially another organizational boundary between enterprise security and operations. For many organizations, the stronger model is to extend the SOC they already have with specialized OT capabilities.

Mithryl Systems OT Managed Detection & Response is designed around that model. Existing investments in SIEM, EDR, OT monitoring platforms, firewalls, identity, remote access, threat intelligence, asset visibility, and SOC workflows remain in place. Mithryl works across that environment to provide the specialized investigation and operational interpretation required when cybersecurity reaches OT.

The operating model connects the capabilities that already exist rather than replacing them:



The objective is not to replace the enterprise SOC or remove decision authority from operations. It is to eliminate the point at which the SOC reaches OT and suddenly has to assemble the rest of the investigation manually.

From Alert to Operational Intelligence

Traditional security operations often follow a familiar path from alert to triage, investigation, and closure. That workflow is effective for many enterprise security events, but an OT event should not end simply because the alert has been investigated. The organization still needs to understand what the event means to the operation and what decision should follow.

Mithryl Systems extends the workflow from telemetry through operational decision-making:



For a meaningful OT event, the investigation should establish:

- What happened and what evidence supports that conclusion?
- Which assets, systems, and industrial processes are involved?
- Is the activity malicious, suspicious, expected, or operational?
- What could happen if the activity continues?
- What could happen if the organization takes containment action?
- Could production, safety, reliability, recovery, or regulatory obligations be affected?
- What is known, what is estimated, and what remains uncertain?
- What action should the organization consider next?

The difference is significant. The endpoint of the process is no longer simply a closed security ticket. It is a better-informed operational decision. **That is Operational Intelligence.**

Augmented Intelligence Accelerates the Investigation. Experts Determine What it Means.

Industrial cybersecurity environments generate more information than analysts can reasonably correlate manually. Mithryl Systems uses Augmented Intelligence to accelerate the portions of an investigation where automation can add meaningful value, including telemetry correlation, evidence collection, enrichment, relationship analysis, timeline construction, case preparation, documentation, and reporting.

That allows experienced OT analysts to focus on the work that requires judgment and operational understanding. They can evaluate whether activity is expected in the environment, determine what industrial process may be affected, assess whether a proposed response could create production consequences, identify additional evidence requirements, and determine which operational stakeholders should participate in the decision.

AI does not decide whether a production system should be isolated. It does not own the decision to interrupt an engineering connection, disable an operational account, or remove a system from service. Those decisions require people who understand the process, the environment, and the consequences.

Augmented Intelligence accelerates the investigation, OT experts interpret the evidence, and operations retains decision authority.

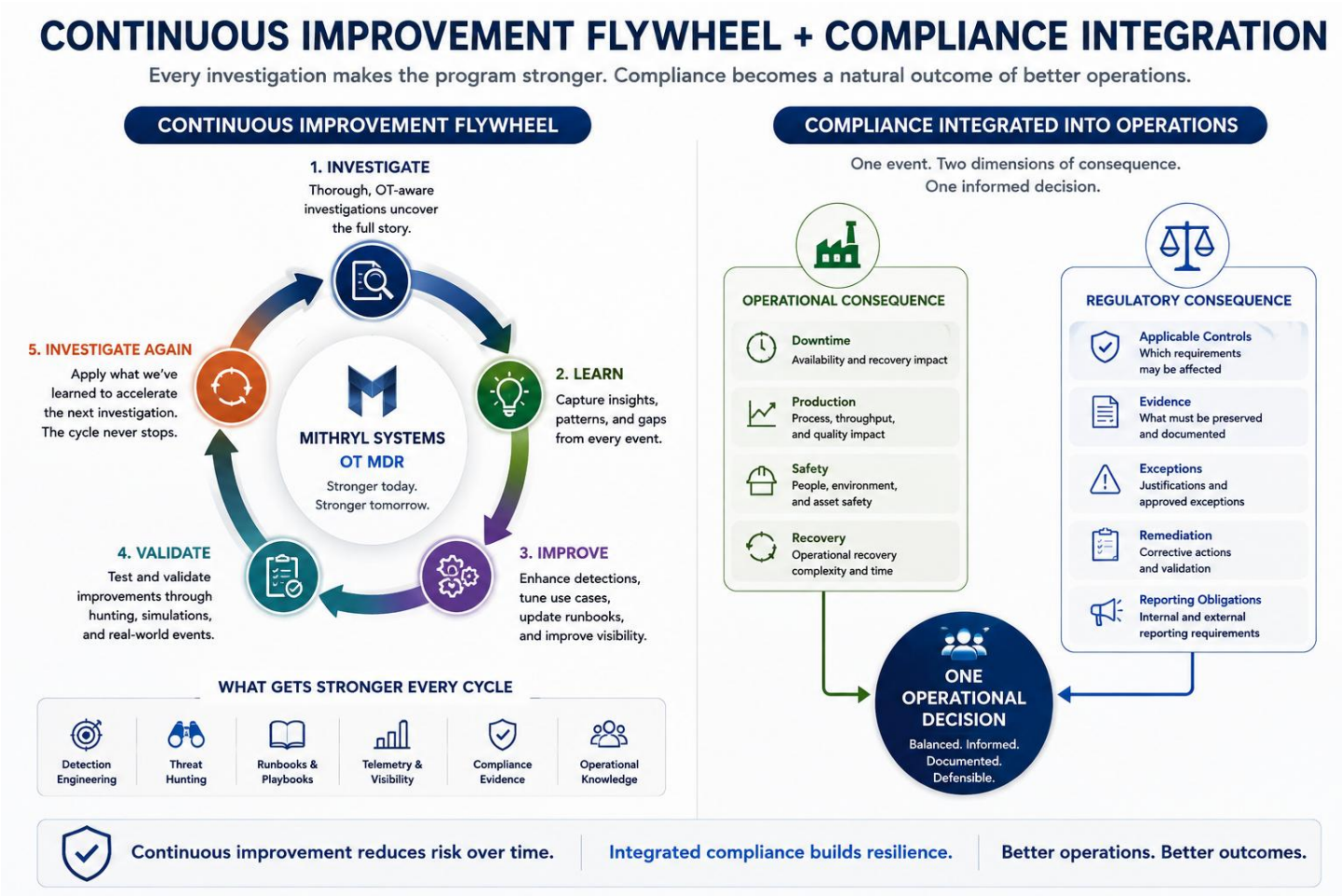
OT MDR Should Not Stop When The Ticket Closes

One of the limitations of a transactional MDR model is that the organization can spend enormous effort investigating individual alerts without materially improving its underlying

ability to detect or respond to the next event. An alert arrives, an analyst investigates, the case is closed, and the process begins again when the next alert appears.

OT MDR should create a different outcome. Every meaningful investigation should leave the security program stronger than it was before the event occurred. An investigation that exposes a detection gap should result in improved detection logic. Missing telemetry should drive visibility improvements. Newly observed attacker behavior should inform Threat Hunting. Weaknesses in response should change runbooks. New operational knowledge should become part of future investigations rather than remaining with the individual who happened to work the incident.

The result is a continuous improvement cycle:



This matters particularly in OT because the operating environment is constantly changing. Assets, processes, vendors, remote-access pathways, maintenance practices, threat activity, and regulatory requirements all evolve. A runbook written during a point-in-time consulting engagement may be useful, but a runbook that is continuously exercised, validated, updated, and improved becomes an operational capability.

Mithryl Systems OT MDR is designed to provide that capability continuously.

Compliance Becomes Part of Security Operations

Compliance should not begin when an auditor requests evidence. In a mature OT security program, the evidence created during normal security operations should contribute directly to regulatory readiness. Investigations, response actions, decision history, control context, and supporting evidence should be preserved as part of the operating process.

This is particularly important because the same cyber event can create both operational and regulatory consequences. Suspicious privileged access to an OT environment, for example, may create a potential pathway to critical operations while also raising questions about applicable access controls, monitoring requirements, evidence, reporting obligations, or remediation requirements.

Those should not become two unrelated investigations. Mithryl Systems incorporates regulatory context into the OT investigation so the organization can evaluate operational risk and compliance implications as part of the same event. This approach can support environments operating under requirements and frameworks including NERC CIP, IEC 62443, NIST SP 800-82, NIST Cybersecurity Framework, TSA Security Directives, NIS2, and applicable sector-specific requirements.

The specific regulatory implications will always depend on the environment, asset classification, applicable requirements, and facts of the event. The objective is not

compliance instead of resilience. It is to provide the organization with a more complete understanding of both.



Why This is Becoming More Urgent

The boundary between enterprise IT and industrial operations continues to become more permeable. Remote access, third-party connectivity, centralized identity, cloud services, enterprise applications, connected supply chains, Industrial IoT, centralized security platforms, and digital transformation all create business and operational value. They also create new pathways through which an enterprise cybersecurity event can reach operational environments.

At the same time, attackers can operate faster, security teams are processing more telemetry, industrial environments remain highly specialized, and executives

increasingly expect cybersecurity leaders to explain risk in terms of business and operational resilience rather than cybersecurity activity alone.

The organizations best positioned for this environment will not necessarily be those with the largest collection of security tools. They will be the organizations capable of answering three questions quickly and confidently:

- What happened?
- What could it mean to critical operations?
- What should we do about it?

That ability is becoming a core operational resilience capability.

What Chanes with Mithryl Systems OT MDR

Mithryl Systems does not replace the enterprise SOC, remove authority from operations, or require organizations to abandon the security technologies they have already deployed. Instead, OT MDR provides the specialized layer required to connect security telemetry, OT expertise, engineering context, regulatory considerations, and operational decision-making.

The result is a different experience for each stakeholder:

- **The SOC gains** deeper OT-aware investigations, industrial threat expertise, Detection Engineering, Threat Hunting, DFIR support, and better context for escalation.
- **Operations gains** validated information, operationally appropriate recommendations, clearer understanding of potential consequences, and confidence that cybersecurity response considers production realities.
- **Compliance gains** investigation evidence, decision history, control context, response documentation, and stronger continuous regulatory readiness.
- **Executives gain** a clearer understanding of cybersecurity risk in terms of production, safety, reliability, regulatory exposure, and operational resilience.

Most importantly, the security technologies the organization already owns become more valuable because their telemetry contributes to better decisions rather than simply generating more information.

The Question Every IT Leader Should Ask

The question is no longer whether OT belongs in the cybersecurity strategy. In organizations with critical operations, it already does. The more important question is whether the existing security operation can move from a cybersecurity alert to an informed operational decision without having to assemble the necessary expertise, context, relationships, and decision process after the incident has already begun.

When a cybersecurity event reaches operations, the organization should be able to answer:

- **What happened?** Do we understand the event and have sufficient evidence to support the assessment?
- **What does it mean?** Can we explain the potential consequences to production, safety, reliability, recovery, and regulatory exposure?
- **What should we do next?** Can cybersecurity and operations make an informed decision that balances cyber risk with operational risk?

If answering those questions requires finding the right OT expert, locating the appropriate engineer, reconstructing asset relationships, determining maintenance status, identifying decision authority, and assembling operational context while the incident is already unfolding, the organization has an Operational Intelligence gap.

During an operational cyber event is the wrong time to discover that gap.

Not Another Security Silo

Mithryl Systems extends the existing Security Operations Center with OT-native expertise, Augmented Intelligence, Continuous Cyber Fusion, integrated compliance,

and Operational Intelligence. The goal is not to create another security silo. It is to connect cybersecurity and operations so the organization can understand what is happening, determine what it means to critical operations, and make the right decision before cyber risk becomes operational impact.

Your SOC may already have much of the data it needs. What it may not have is the OT-specific expertise, operational context, and decision framework required to turn that data into action.



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. Mithryl Systems 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, Mithryl Systems 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. Mithryl Systems 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 Mithryl Systems is prohibited by law.