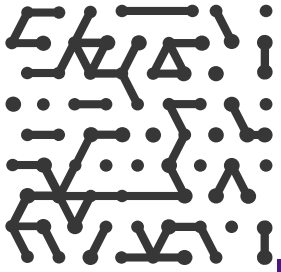
SOLUTION BRIEF

Armis Managed Threat Services: OT Operationalization



Overview

Extending visibility into Operational Technology (OT) networks and connected assets is crucial for optimizing cyber resiliency, and securing critical business capabilities. However, the attack surface of OT networks is growing rapidly, and there are multiple active threats targeting them. In addition, Security Operations Center (SOC) teams are typically overwhelmed, making it challenging to extend their visibility, or establish an optimized SOC in response to the growing risk.

Armis offers a platform that provides a powerful and flexible toolset to unlock the full potential of centralized, business-based asset intelligence. The platform is designed to support optimal resilience-based programs, and can be contextually optimized to meet the unique needs of customers' security-operations programs. Armis also offers Managed Threat Services (MTS) that can quickly optimize and maintain a high-efficacy SOC in alignment with the evolving threat and business landscapes.

To accelerate the customer's OT security operationalization efforts, Armis MTS enables highly-optimized threat-based continuous monitoring and alerting capabilities offered through the Armis platform. With industry expertise and an emphasis on optimizing the SOC around centralized, business-aligned asset intelligence, Armis is uniquely positioned to help organizations strengthen their cyber resiliency, and safeguard critical business capabilities.

Outcomes

The Armis Managed Threat Services (MTS) team will act as an extension of your security team to help operationalize, and continually optimize your global Armis implementation around your cyber resiliency priorities and the following key outcomes:

Baseline Customer Tenant

The customer tenant will be baselined around the following areas:

a. Current active threats

b. High-risk areas of concern

c. Cyber hygiene areas of concern

Continuous Policy Creation

Experts will be regularly recommending new policies to proactively identify threats in your constantly changing cybersecurity landscape.

MTS OT Dashboard

A dashboard will be populated for MTS OT customers to include dashlets commonly utilized to measure the efficacy and efficiency of the MTS program.

Threat and Risk-Based OT Policy Tuning

Experts will provide recommendations for tuning your platform to optimize the output. and ensure you receive contextually prioritized alerts based on their potential impact on the business.

Manual Threat Hunting

Manual expert-conducted threat hunting in the customer tenant on a regular schedule. Threat hunting includes random times of day, as well as historical data of up to 90 days for all suspicious and/or malicious activity.

Regular Operational Meetings

As part of the service, the customer is entitled to a weekly operational meeting with an expert, lasting up to 60 minutes. This meeting provides a comprehensive review of the previous week's operations, and allows the customer team to ask questions, and receive additional information as required.

OT Insight Report

The customer will be provided with one (1) OT insight report weekly, that describes all noted findings, including critical threat notifications with recommendations for controls and remediations/mitigations where applicable. The report will also outline any additional compensating information relevant to the findings based on additional research conducted by our experts.

MTS Monthly Executive Summary

The customer will be provided with a monthly executive review summarizing the monthly accomplishments, critical issues, major risks, and next steps. The report will also outline the look ahead for the next 30 days.

Scope

The scope of the service includes all sites and assets in scope for coverage by the existing Armis contract(s), as of the current date of signed contract. The period of service will be included in your purchase order, and is a minimum of one (1) year. The customer may elect to extend this service, purchase additional services, or elect to purchase a new service.

Description of Service

Through a combination of named, experienced threat hunters backed by world-class research and intelligence, support resources, and custom technical capabilities, the Armis Managed Threat Services (MTS) team will deliver the following:

Baseline Customer Tenant

The Armis MTS team understands the importance of protecting your business' critical assets from evolving cyber threats. With our expertise in the industry, and your insights into your priorities and assets, we can tailor our services to provide you with the best protection possible.

To begin, we will conduct a comprehensive baseline assessment of all sites across your tenant. This will help us to gain a deep understanding of what normal activity looks like within your organization, and to identify any anomalies or potential risks.

Our baseline assessment will involve analyzing a range of factors, including network traffic, activities, ip connections, and other relevant data points. We will use this information to establish a clear picture of your organization's baseline activity, and to pinpoint any assets that may be operating outside of normal parameters.

Once we have established a baseline, we will use this information to inform our threat-hunting activities. By focusing our efforts on potential areas of weakness or abnormal activity, we can proactively identify and mitigate potential threats before they have a chance to cause damage.

The Armis Managed Threat Services (MTS) team prides itself on its ability to provide customized solutions that are tailored to the unique needs of each client. With our baseline assessment and threat-hunting services, you can rest assured that your critical assets are protected from cyber threats.

Continuous Policy Creation

The Armis MTS team prides itself on its proactive and dynamic approach to cybersecurity. One of the key components that set us apart is our commitment to continuous policy creation, driven by the insights gathered through our robust threat-hunting activities.

Our expert team of security analysts constantly monitors your network and systems for potential threats, and emerging risks. By analyzing the data collected from these threat-hunting operations, we gain invaluable knowledge about the ever-evolving threat landscape. This intelligence serves as the foundation for the development of tailored, and up-to-date security policies, ensuring that your organization remains resilient against the latest cyber threats. Through this proactive strategy, we can swiftly adapt and implement necessary security measures, providing you with a comprehensive and proactive security posture that safeguards your critical assets in today's ever-changing cybersecurity landscape.

Threat and Risk-Based OT Policy Tuning

The Armis MTS team can provide valuable recommendations to customers to help them tune their security platform so that they are only focusing on actionable alerts with the highest priority. We understand that many companies receive a high volume of security alerts on a daily basis, which can be overwhelming and make it difficult to identify the most critical threats. By analyzing the customer's existing security infrastructure, we can provide guidance on how to configure and optimize their security systems to reduce noise and false positives, while prioritizing alerts based on their potential impact on the business. This not only helps our customers save time and resources, but also ensures that they are effectively managing their security risks, and protecting their critical assets.

MTS OT Dashboard

One of the key aspects of our service is to provide a dashboard that allows our clients to monitor and track the efficiency and efficacy of both the tuning and threat-hunting processes. Our dashboard presents an OT view of the security posture of our client's environment, highlighting any potential risks, threats, or vulnerabilities that may require immediate attention. Our team of security experts continuously enables the client's monitoring of systems, and performs monthly threat-hunting exercises to detect any potential security breaches before they can cause damage. The dashboard provides data on the performance of our security measures, giving our clients the confidence that the service is working effectively. By providing this level of transparency and visibility, our service helps clients stay ahead of potential threats and mitigate any risks to their business.

Threat and Risk-Based OT Policy Tuning and Recommendations

The Armis MTS team will provide valuable recommendations to customers to help them tune their security platform so that they are only focusing on actionable alerts with the highest priority. We understand that many companies receive a high volume of security alerts on a daily basis, which can be overwhelming and make it difficult to identify the most critical threats. By analyzing the customer's existing security infrastructure along with their Operational Technology (OT) landscape, we can provide guidance on how to configure and optimize their security systems to reduce noise and false positives, while prioritizing alerts based on their potential impact on the business. This not only helps our customers save time and resources, but also ensures that they are effectively managing their security risks and protecting their critical assets.

Manual Threat Hunts

The Armis Managed Threat Services (MTS) team understands the importance of staying ahead of the ever-evolving threat landscape. That's why we offer manual threat hunts as an integral part of our service, focused on optimizing your threat response, and risk management efforts.

Our named expert threat hunters will conduct random manual threat hunts, customized to address the highest priority risk scenarios and corresponding hunt hypotheses. We will continually review and update these hypotheses throughout the course of our service, ensuring that we remain proactive in our approach to threat hunting.

We understand that the threat landscape can change rapidly, and that new risks can emerge at any time. That's why we remain agile in our approach, customizing our hypotheses and operational priorities in response to zero-day threats, and any other relevant factors. Our mission is to ensure that you can proactively, and reactively, safeguard and act on what matters most, against active threats that exploit the intricate web of asset-based exposures in today's complex business environments.

The results and findings from each hunt will be used to support a range of recommendations, including the creation of policies, risk management recommendations, service reporting, and even the Armis product dashboard, where applicable. By leveraging the insights gained from our manual threat hunts, we can provide you with a more holistic view of your threat landscape, and help you to take proactive steps to mitigate any potential risks.

Regular Operational Meetings With Your Team

Armis Managed Threat Services (MTS) resources will meet with your team on a regular basis (usually every 1 to 2 weeks) to discuss recent findings, risk mitigation or remediation recommendations, policy changes, threat hunt priorities, business context details, and more. These meetings are designed to support the continuous optimization of your operational needs, and ensure that all aspects of the service are aligned with your specific requirements.

Regular OT Insight Report

The Armis MTS team understands the importance of regular reporting to keep our customers informed and up-to-date on the latest threats and trends. Our weekly OT customer report is designed to provide valuable insights into threat hunt findings, research findings and trends, priorities, and recommendations for mitigation or controls. This report includes detailed information on recent threat hunts, including any findings, recommended actions, and suggested controls or mitigation strategies. Additionally, we provide research findings and trends, ensuring our customers are aware of emerging threats and risks. Our report also highlights priorities, enabling our customers to focus on the most critical issues affecting their OT environments. With our regular reports, we aim to provide our customers with the information they need to make informed decisions, and continuously improve their security posture.

MTS Monthly Executive Summary

The Armis Managed Threat Services (MTS) team provides a monthly executive summary that compiles an overview of the past month's accomplishments, critical issues, and major risks. This summary is designed to provide executive-level insights into the performance of the service and help our customers understand the impact of our work. Additionally, the summary outlines the next steps we plan to take over the next 30 days, ensuring that our customers are aware of upcoming initiatives, and can plan accordingly. The executive summary is a valuable tool for executives and other key stakeholders, enabling them to stay informed and engaged in the ongoing management of the organization's security posture. By providing a comprehensive summary of the past month's activities and future plans, we help our customers make informed decisions, and continuously improve their security posture.

Delivery Timeline

The below timeline is based on our baseline delivery plan. This timeline along with corresponding outcomes are reviewed in the initial onboarding session. The Managed Threat Services (MTS) team is able to accelerate or decelerate the timeline based on business needs and availability. Where applicable, we will capture, adjust, and execute overall short and long-term plans accordingly.

Months 1 - 3

Onboard to Threat Services

Complete Asset and Application Survey

Align Policy Tuning

Start Critical Policy Tuning

Start Weekly Insight Reports

Months 4 - 5

Critical Policies Tuned

Review of All Policies Starts

Manual Threat Hunting Starts

Threat Hunting Hypothesis Start

Regular Operations Meetings Start

Months 6 - 12

Regular Review of Insights

New Hunting Areas Identified and Classified

Regular Review of New Policies

Regular and Ongoing Detailed Information Sharing (via Shared Repo)

Staffing

The service will be delivered through a combination of support resources. The breakdown of resources that will be supporting the account can be found below.

Armis Personnel	Description
Named Armis Threat Hunter(s)	Threat hunts and recommendations
Secondary Threat Hunter(s)	Threat hunts and recommendations
Peer Review Threat Hunter(s)	Qualification of findings/hypothesis
Research Analyst(s)	Analyst specializing in threat intelligence and threat research

Core Deliverables

- Customer tenant baseline across all sites
- Regular expertly-performed, contextually-aligned OT threat hunts
- MTS OT dashboard
- OT Threat and risk-based, hygiene priority insights and recommendations report
- Continuous creation and tuning of contextualized threat and risk-based Armis policies
- Establishment and maintenance of business relationship
- Live sessions with an Armis MTS expert every 1 to 2 weeks
- Incident response team/process integrations and enablement

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial