AT&T Managed Threat Detection and Response

Threat Model Workshop

Anyone who has deployed managed security solutions at scale can tell you how quickly you'll begin to encounter problems with a "one-size-fits-all" approach. Threat detection and response technology implementations specifically should not immediately jump to deploying IDS sensors or endpoint agents. They should start with a thorough analysis of the customer's environment and the broader business context. Many security tool implementations go awry because no one stopped to understand how the business that they're trying to protect actually operates from a technical perspective, and the ways in which this architecture should inform the deployment and future priorities of a managed security service.

At AT&T Cybersecurity, we take the time to get to know our customers and their business. Every AT&T Managed Threat Detection and Response service begins with an on-site or remote threat model workshop led by AT&T Cybersecurity Consulting. This workshop helps enable AT&T to document vital business functions and resources, define infrastructure scope, confirm deployment requirements, diagnose existing security program gaps, and establish ongoing security program objectives. The in-depth knowledge of the customer systems gained through the workshop allows our SOC analysts to determine the most effective strategy for monitoring the customer's environment as we begin the deployment of the USM platform.

Potential benefits:

- Meet the AT&T Cybersecurity team that will be deploying USM and working to help protect your enterprise
- USM Security Analysis training seats included
- Dedicated workshop time spent with the AT&T team
- Threat Model Document outlining your critical resources, threat surface area, and any identified likely threat vectors
- Technical Provisioning Document outlining all integrations, data feed, and customizations required for deployment
- Allows for development of a cybersecurity monitoring and response strategy that's tailored to the unique needs of your business
- Enables the AT&T team to gain an in depth understanding of the customer's environment and more effectively deploy the USM platform

Initial Kickoff

An initial kickoff call is held between the AT&T team and the customer five business days after the contract is finalized and the fulfillment process is complete. During the call, the team discusses the scope of the deployment, assignment of roles, customer expectations, timelines, and schedules follow up action items and meetings.

The goal of the meeting is to:

- Introduce the customer's team and your AT&T Cybersecurity Consulting team.
- Establish the points of contact from the Customer's Engineering and Incident Response teams to facilitate future communication between AT&T and the customer for the duration of the contract.
- Answer any questions from the customer, set expectations for reporting, and establish cadence of communication, escalations, and associated next steps and timelines.

Threat Model Workshop

Following the initial kick off, an AT&T Cybersecurity consultant will conduct a threat model workshop with the customer. The consultant will work with the customer's teams to complete a Threat Model Document, identifying and documenting the customer's critical resources, the associated Threat Surface Area, and Identified Likely Threat Vectors. Following the Threat Model Document, a Technical Provisioning Document is completed to guide platform deployment. At the conclusion of the workshop, the AT&T team will provide both documents back to the customer's team for review. Using the analysis from the Threat Model Workshop and other onboarding activities, the assigned threat hunter will work with the customer to generate the first version of the Incident Response Plan. This plan is customized to the security operations and management model deemed best fit for the customer and is a living document that can be revisited throughout the lifecycle of the service.

Threat Model Document

The Threat Model Document guides the AT&T Managed Threat Detection and Response (MTDR) service. It provides context and helps establish priorities within the network infrastructure for the customer. This helps to provide that the USM platform is appropriately implemented and the security analysts understand the customer's environment.

This Threat Model will focus on three primary components:

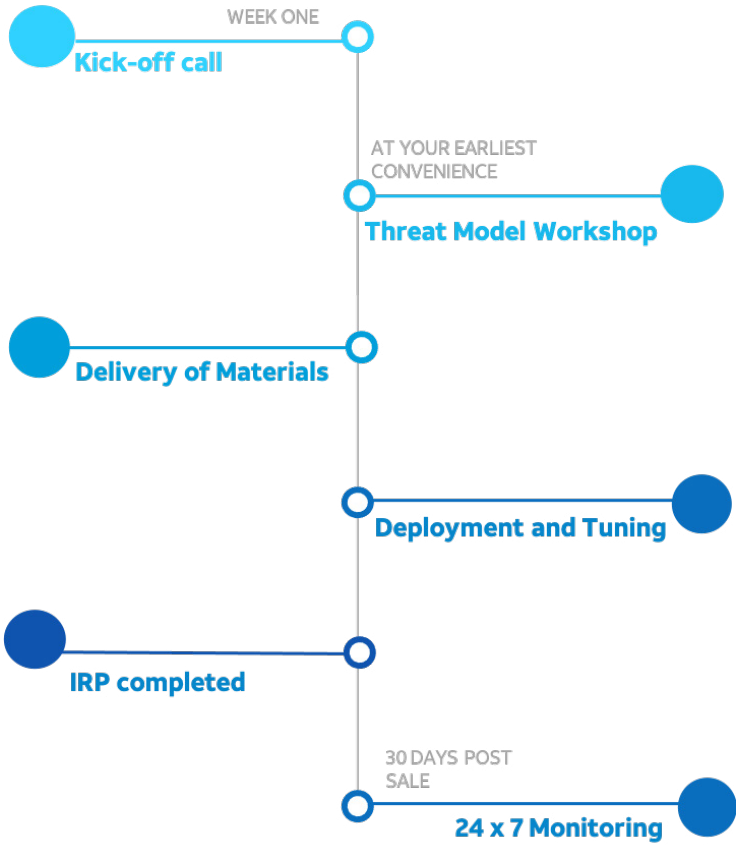
- **Critical Resources:** Resources that maintain sensitive data, that if breached, would require significant incident response to remediate. This can include PHI or PCI data, as well as data that is proprietary or secret to the organization, such as intellectual property. In addition, critical resources may not have sensitive information, but if unavailable would have a direct business impact.

- **Threat Surface Area:** Describes the exposed surfaces limited to the scope of the Critical Resources. Surfaces include, but are not limited to, web servers, firewalls and network infrastructure, operating systems, and in-house or third-party developed code.

- **Identified Likely Threat Vectors:** Describes the consultant's assessment of the most relevant threats to the customer's Critical Resources given their Threat Surface Area. These are classified as external threats, coming from outside the organization, or Internal, attacks coming from within the organization.

Technical Provisioning Document

The Threat Model Document is then used to confirm the technical requirements for deployment, which are then codified into a Technical Provisioning Document. This document outlines all integrations, data feeds, and any customization required for specialized ingestion of data or unique data feeds. The security engineering team then uses this document to begin the USM platform deployment.



Onboarding Timeline

Kick-off call - Five days after your contract is signed, the MTDR project manager schedules a kickoff call with an AT&T Cybersecurity Consultant

Threat Model Workshop - AT&T Cybersecurity Consultant works with your teams to identify Critical Resources and customize your deployment plan

Delivery of Materials - Consultant and SOC Support (Security Engineer) delivers your Threat Model and Technical Provisioning Document

Deployment and Tuning - Working with a Security Engineer, we deploy USM, integrate data sources, and tune the instance to best fit your Threat Model

IRP Completed - The AT&T team and the customer's team complete a custom Incident Response Plan

24 x 7 Monitoring - Onboarding completed, and the customer handed off to 24x7 monitoring

About AT&T Cybersecurity

AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange,™ and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.