AT&T Business

AT&T USM Anywhere Advisors

Augment your threat detection and response program with expert support

AT&T USM Anywhere Advisors help to improve your threat detection and response program by providing reactive security support to your internal security teams from our expert AT&T Cybersecurity Consultants. Our USM Anywhere Advisors serve as an extension of your in-house staff, helping with day-to-day operations while allowing your security team to learn industry best practices and the latest techniques for threat detection and incident response from our cybersecurity experts.

The AT&T USM Anywhere Advisors' reactive incident response services help to identify and triage potential security incidents within your environment. Based on their security expertise, the team evaluates your environment for signs of suspicious activity that have been missed by existing security controls and that could potentially impact confidentiality, integrity, and availability of your environment. When an incident occurs, the team is available to help investigate and deliver an analysis of findings and recommendations for remediation or further investigation.

With this service, we can help take some of the burden off your existing security team without the cost and complexity of bringing on additional staff.

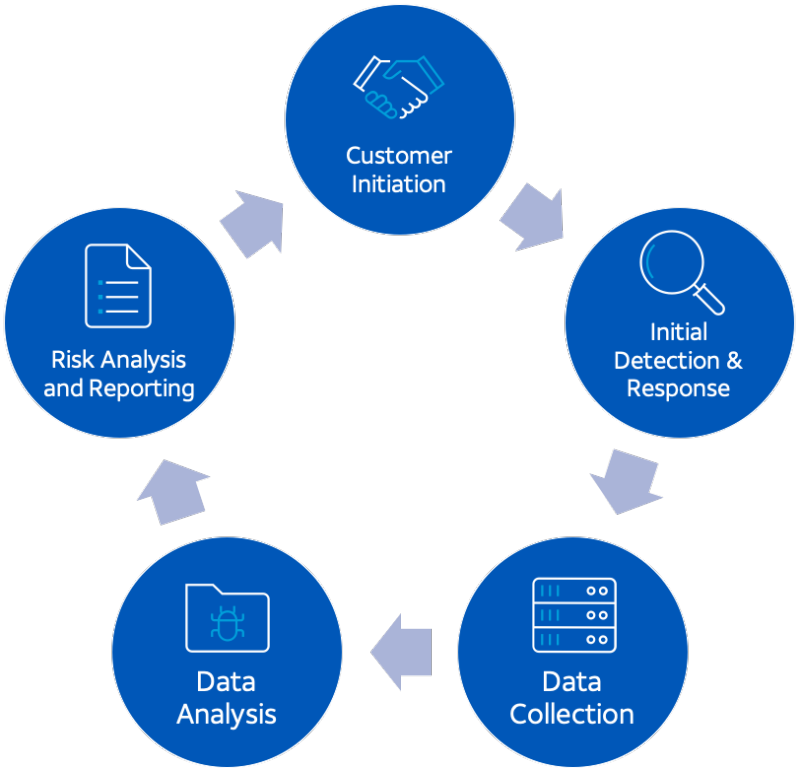
Potential benefits:

- Easily bring on additional staff to help with security operations
- Gain access to cybersecurity experts with an advanced skillset to help resolve more complex situations
- Streamline incident response activities with expert guidance
- Reduce some of the burden on your security team

Service features:

- Reactive cybersecurity operations support
- Help to identify and triage potential security incidents within your environment
- Evaluation of your environment for signs of suspicious activity

How it works



AT&T USM Anywhere Advisors work with your internal team to help improve your security posture and help you get the most out of USM Anywhere. The reactive support is available for a pre-defined set of monthly hours, ranging from 4-40 hours, which expire at the end of each calendar month. When support is needed, your team can send an email to engage the team. The hours can be used to help with a range of security operation activities from platform tuning to incident investigation and response. Platform onboarding and tuning includes general tuning, sensor deployment, enabling asset discovery, AlienApp configuration, and more.

Investigations overview

During an investigation, the USM Anywhere Advisors will investigate your environment for indicators of compromise to determine if rogue users or malicious actors have gained a foothold in your environment. The team will begin each investigation by evaluating all actionable alarms and events in USM Anywhere and creating a specific hypothesis. If all of the required information is not available, they will work with your team to identify any additional systems, applications, and networks to include in the scope of the investigation.

The team will utilize the Investigations feature in USM Anywhere to track all investigative activities, including initial detection and response, data collection, data analysis, and impact analysis and reporting.

Initial Detection and Response

In this phase, the AT&T USM Anywhere Advisors work with your internal team to identify potential areas where computer and network security incidents have occurred previously or are likely to occur in the future. This may be based on specific indicators or through the hypothesis statements for the investigation. You can escalate specific issues for investigation, or target areas may be identified by either team while performing other activities.

Data Collection

In this stage, the AT&T USM Anywhere Advisors will perform the initial investigation by gathering facts about the suspected incident. If the team is not able to find all the information required for the investigation in USM Anywhere, the USM Anywhere Advisors may request access to additional systems to gather more data and perform analysis.

Typically, the initial response will involve the following:

- Investigating actionable alarms and/or events present within USM Anywhere
- Interviewing system administrators or other internal resources who would have the technical insights into the systems or networks
- Reviewing network topologies and data flows
- Reviewing logs from various systems including IDS, firewall, and Syslog data
- Creating forensic images

Data Analysis

As the data artifacts related to an investigation become available, the USM Anywhere Advisors will begin to triage the data, update investigation priorities based on their analysis, and address any investigation-related questions your team may have. This is an iterative process which may include the following actions:

- Utilizing threat intelligence tools, customer-defined policies, and malware forensic tools to determine if the detected behaviors are indicative of an "actionable" security threat that requires an investigation
- Group Actionable Alarms and/or Events with supporting threat intelligence, related Alarms and Events, conclusions, relevant files, and analyst recommendations in an investigation
- Updating the investigation as additional information is gathered and analyzed, including increasing or decreasing the Severity (Critical, High, Medium, Low), changing the status (Open, In Review, Closed), and adding an "Assignee"
- Informing the customer of user policy violations for in-scope systems, making recommendations for security control updates, updating a security control on behalf of the customer, advising the customer to reset a machine to known good state, and more

All of these response activities can be captured in playbooks in USM Anywhere using custom Response Action Rules to automate the actions taken in response to specific threats and are customized based on your unique incident response needs. Custom Notification Rules can also be configured to increase threat visibility and help reduce time to response of similar incidents in the future.

Risk Analysis and Reporting

During the Analysis and Reporting phase, the AT&T USM Anywhere Advisors analyze all of the information gathered and document the findings and any recommendations in USM Anywhere. Near-real-time communications and debriefs will be provided by the team to provide that you understand the full scope and impact of the incident, the results and recommendations of the investigation, and any recommendations for next steps to both recover from the current incident and help reduce risk of future occurrences.

About AT&T Cybersecurity

AT&T Cybersecurity's edge-to-edge technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning — helping to enable our customers around the globe to anticipate and act on threats to protect their business.