verizon

# AUTONOMOUS THREAT HUNTING +



## 1. GENERAL

1.1 **Service Definition.** Autonomous Threat Hunting + (ATH) is a Verizon cloud-based offering that proactively searches for threats and potential security incidents using patented machine learning technology to a select set of threat intelligence indicators and Customer log data. The Autonomous Threat Hunting service applies data science concepts and machine learning technologies to automate the hunt for compromised or infected assets and to transform gigabytes of log data, multiple threat intelligence feeds, and varied raw threat indicators into a prioritized list of high-quality alerts with reduced false positives. Customer can integrate the ATH service through an Application Programming Interface **(**API) with several Security Information and Event Management (SIEM), log management, incident response and other security and IT operations platforms.

1.2 **Service Features.** The following service features are included with Autonomous Threat Hunting:

1.2.1 **Threat Hunting Leads Reports.** Alert results will be made available on daily and/or hourly reports that will contain the outbound communications deemed suspicious. Alerts will also contain contextual information such as:

- a numeric confidence score, which indicates on a scale of -100 (least confident) to 100 (most confident) how confident the machine learning models are that an alert is worth investigating by an analyst;
- direct or indirect matches on threat intelligence; and,
- optional tags that indicate a tentative and probabilistic indication of the possible nature of the threat involved.

1.2.2 **Customer portal.** The Customer portal provides access to threat hunting leads reports, ability to provide feedback on threat hunting leads, and the ability to view or change set policies and options that control the way Autonomous Threat Hunting operates.

1.2.3 **REST API**. API allows Customer to programmatically access the ATH alerts, for example, to build integration with its SIEM, log management, incident response and other security and IT operations platforms. Customer will have access to threat hunting leads, ability to provide feedback on threat hunting leads, and ability to view or change set policies and options that control the way Autonomous Threat Hunting operates.

1.2.4 **Security Services Advisor (SSA).** Customer is assigned a SSA, who will host a quarterly service review meeting. The SSA is assigned to multiple ATH customer accounts and is not a dedicated resource to any 1 customer. The SSA provides training on the use of the Customer portal, manages Customer communications, and manages service issues.

1.2.5 **Security Operations Center (SOC) Support.** Where applicable, SOC support for the Service will be provided remotely from Verizon SOC locations in the United States, Europe and Asia on a 24x7x365 basis.

1.2.6 **Data Availability and Retention.** Alerts will remain available on the customer portal for 1 year.

1.3 **Service Activation and Implementation**. Verizon will assign a project manager to Customer who will schedule a kick off meeting to introduce the Verizon service delivery team, identify the Authorized Contacts for Customer, discuss the scope of the Autonomous Threat Hunting service and its business impacts, provide a questionnaire for the Deployment Kit, and obtain any required information from Customer. Upon receipt from Customer of a completed Deployment Kit, Verizon will create a proposed project plan with high-level milestones and timelines. Verizon will only provision Autonomous Threat Hunting after Customer has approved the project plan.

## 2. SUPPLEMENTAL TERMS

### 2.1 Customer Responsibilities

2.1.1 **Deployment Kit**. Where applicable, Customer must complete a Verizon deployment kit and provide such deployment kit to Verizon within 15 Business Days of the kick off meeting or Verizon may terminate Customer's Service Order. Verizon may charge Customer for any expenses incurred by Verizon (including labor fees) through the date of termination.

2.1.2 **Customer Log Collection**. Customer is responsible for providing the Data Sources according to the requirements and supported device list provided by the project manager at Service Activation and Implementation. Customer will also maintain a consistent and steady flow of Data during the Service Term.

2.1.3 **Overutilization**. If the volume of Data logs submitted by the Data Sources exceeds the Service Tier purchased, the ATH processing will be suspended until (a) a higher Service Tier is purchased, or (b) the start of a new billing period, whichever occurs earlier.

2.1.4 **Maintenance Contracts.** Where required, Customer will (a) at its own expense, procure and maintain with each applicable vendor adequate maintenance contracts and all licenses necessary for the Data Sources to enable Verizon to properly perform Service; (b) comply with Service prerequisites and operational procedures as set forth in the applicable terms; and (c) promptly inform Verizon of any changes in Customer Environment and any changes to the nomination and/or authorization level of the Authorized Contacts responsible to oversee, monitor or evaluate the provision of Service.

2.1.5 **Interoperability.** Where applicable, Customer acknowledges that modifications or changes to the Data Sources (such as future releases to the Data Source's operating software) or to the Customer Environment may cause interoperability problems, inability to transmit data to Verizon, or malfunctions in a Data Source and/or the Customer Environment. Customer will give Verizon written notice (notice via email is acceptable) of any modifications or changes within 5 Business Days after making any such changes. Customer acknowledges that it is Customer's responsibility to maintain, at its sole cost and expense, the Customer Environment to ensure that the Customer Environment is interoperable with each Data Source.

2.1.6 **Service Equipment.** Where applicable, Verizon may require certain collection equipment to collect Log data from Data Sources and to forward such Log data records to the SMC (e.g., Connection Kits). If Verizon determines that such collection equipment is needed on Customer's Site, Customer must provide the necessary equipment subject to Verizon's specifications, either: (a) through direct procurement from equipment provider, or (b) through Verizon as a separate CPE procurement. Verizon will configure and access such equipment remotely.

2.1.7 **User Interface.** In connection with the provision of Service, Verizon may provide Customer with one or more user Logins to access a User Interface. Customer will at all times keep its Login strictly confidential and will take all reasonable precautions to prevent unauthorized use, misuse or compromise of its Login. Customer agrees to notify Verizon promptly upon learning of any actual or threatened unauthorized use, misuse, or compromise of its Login. Verizon is entitled to rely on Customer's Login as conclusive evidence of identity and authority. Customer will be liable for all activities and charges incurred through the use of Customer's Login, and will indemnify, defend and hold Verizon Indemnitees harmless from all liabilities, losses, damages, costs and expenses (including, without limitation, reasonable attorneys' fees and costs) incurred by Verizon to the extent resulting from the use and/or compromise of Customer's Login, unless the unauthorized use, misuse or compromise of Customer's Login is solely attributable to Verizon's gross negligence or willful misconduct.

2.1.8 **Installation Sites and Equipment.** For premise based ingestion, Customer will prepare any installation site in accordance with Verizon's instructions to ensure that any equipment that interfaces with Customer's computer system is properly configured as required for the provision of Service and operates in accordance with the manufacturer's specifications. All Customer premise based Data Sources must have a routable network path to and be compatible with the Connection Kit. Customer will install and maintain software agents required for the provision of Service to Data Sources on Customer network, at its cost. If Customer fails to make any preparations required herein and this failure causes Verizon to incur costs during the implementation or provision of Service, then Customer agrees to reimburse Verizon promptly for these costs.

2.1.9 **Additional Customer Obligations.** Customer understands that, in addition to the other Customer obligations described in this Service Attachment, Customer must ensure that Customer contacts are available to Verizon, for the kick-off call, and at other times as required throughout the term of the Service Order.

2.2 **Warranties**

2.2.1 **Verizon's Disclaimer of Warranties.** Verizon does not warrant that any network, computer systems, or any portions thereof, are secure. Verizon does not warrant that use of Autonomous Threat Hunting will be uninterrupted or error-free or that any defect in Autonomous Threat Hunting will be correctable or that incidents will be fully contained. Customer acknowledges that impenetrable security cannot be attained in real-world environments and that Verizon does not guarantee protection against breaches of security, or the finding or successful prosecution of individuals obtaining unauthorized access. Verizon does not warrant the accuracy of information provided to Customer hereunder.

2.2.2 **Customer Warranty.** Customer represents and warrants that Customer (a) has and will continue to have all rights, power, permissions and authority necessary to have Verizon provide Autonomous Threat Hunting services including, without limitation, consent of all authorized network end users located in the European Union ("EU") or other countries and where applicable (i) consulting all European Works Councils with respect to the operation of Autonomous Threat Hunting for EU based end users, and (ii) complying with all Data Protection regulators notifications and/or registration obligations with respect to the operation of the Autonomous Threat Hunting for all end users; (b) will use the Autonomous Threat Hunting services, including all reporting, deliverables, documentation, and other information provided in connection with the Autonomous Threat Hunting service solely for purposes of protecting Customer from abusive, fraudulent, or unlawful use or access to its information, systems and applications including public internet service provided by Verizon and Customer will not market, sell, distribute, lease, license or use any such deliverables, documentation or information for any other purposes; and (c) will comply with all applicable laws and regulations. Customer will indemnify and hold harmless Verizon from any end user or other third party claims related to these Customer warranties.

verizon

2.2.3 **Third Party Warranties.** For any third party products and/or services incorporated as part of Service, Customer will receive only the warranties offered by such third party to the extent Verizon may pass through such warranties to Customer.

2.3 **Use of Data.** As part of Customer's use of the Services, Customer will be providing certain (i) Network Data, (ii) User Data, and/or (iii) Feedback. Some Network Data is necessary for the essential use and functionality of the Services. Network Data is also used to provide associated services such as technical support and to continually improve the operation, security, efficacy and functionality of the Service.

2.3.1 **User Data.** Customer grants Verizon a worldwide, royalty-free, sublicensable license to use, modify, reproduce, publicly display, publicly perform, and distribute the User Data only as reasonably required to provide the Service.

2.3.2 **Network Data.** Customer hereby grants to Verizon a non-exclusive, irrevocable, worldwide, perpetual, royalty-free and fully paid-up license to use (i) the Network Data that is aggregated and de-identified so that it does not identify Customer for the purpose of enhancement of the Services, and (ii) any information that Verizon learns in evaluating Network Data to create the Statistical Data for the purpose of enhancing, developing, and/or promoting the Services.

2.3.3 **Feedback**. De-identified Feedback may be incorporated into the Services, and Customer hereby grants Verizon a non-exclusive, irrevocable, worldwide, perpetual, royalty-free and fully paid-up license to use de-identified Feedback for any purpose whatsoever, including, without limitation, for purposes of enhancing, developing and/or promoting products and services, including the Services.

3. **FINANCIAL TERMS.** Customer will pay the applicable monthly recurring charge (MRC) for the Service as shown in the Agreement.

4. **DEFINITIONS.** The following definitions apply to Autonomous Threat Hunting, in addition to those identified in the Master Terms of your Agreement.

| Term | Definition |
|---|---|
| **Authorized Contacts** | Customer personnel authorized by Customer to access the product portal and to interact with Verizon for the Autonomous Threat Hunting service. |
| **Customer Environment** | The network and/or information technology infrastructure in which Customer Data Sources reside. |
| **Data** | Machine-generated information that can be digitally transmitted and processed. |
| **Data Source** | Any source of logs data that represent a record of stateful connections initiated by machines on Customer networks with a destination on the Internet. This includes but is not limited to perimeter firewalls and URL filtering solutions. |
| **Feedback** | Any suggested changes, clarifications, additions, modifications or recommended product improvements to the Services that Customer provides as part of technical support or otherwise by direct entry into a product user interface, phone conversation, email or otherwise. |
| **Login** | IDs, account numbers, personal identification numbers or codes, passwords, digital certificates or other means of authentication. |
| **Network Data** | Any technical data and related information about Customer's computer network generated as part of Customer's usage of the Services, including, but not limited to the operating system type and version; network host data; origin and nature of malware, endpoint GUID's (globally unique identifiers); Internet Protocol (IP) addresses; MAC addresses; log files; network configurations; network security policies; information related to the usage, origin of use, traffic patterns, and behavior of the users on a network; and any aggregate, demographic or network traffic data. |

| | |
|---|---|
| **Service Tier** | The volume of Data logs your organization feeds the system. |
| **Statistical Data** | Any information or data that is created from the Network Data, provided that such information or data is aggregated and de-identified or otherwise cannot be used to identify Customer's network. |
| **User Data** | All information and materials, including personal information, that Customer provides in connection with Customer's use of the Services, but does not include Network Data. |
| **User Interface** | A web-based portal, dashboard, or other electronic means to share information and reports with Customers that pertains to Security Incidents that are identified and escalated to Customer. |