Solutions Terms: Managed Detection & Response

Last Updated: June 28, 2023

This Managed Detection and Response – Solution Terms sets forth the terms and conditions of the Managed Detection and Response Solution (the "Solution"). The Solution, if purchased by Customer as evidenced by Customer's election on an Order Form, will be provided in accordance with the terms set forth herein and the Solutions Agreement (the "Agreement") made by and between Customer and Arctic Wolf Networks, Inc. ("Arctic Wolf"). Any capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement.

The Solution is delivered by the Security Services team (which was formerly referred to generally as the Concierge Security™ Team) which is comprised of two (2) teams: (1) the Concierge Security™ Team ("CST"), and (2) the Security Operations Center ("SOC").

The Solution. Specific features and functionality provided as part of the Solution include:

- collection of Solutions Data[1], including Customer's system logs, from Customer's systems using Equipment,
- analysis by Arctic Wolf Security Services of both Equipment and log data through the correlation of Solutions Data with threat and vulnerability information,
- scanning of Customer's internal and external systems,
- escalation of Security Incidents (as defined below) in need of attention by Customer as set forth herein,
- advisory recommendations intended to improve Customer's security robustness,
- calculation of Customer's Security Score, as more fully described below,
- Data Exploration module, if licensed by Customer as reflected on an Order Form (as more fully described below)[2].
- Host Containment Actions (as more fully described below), and
- regular summary Executive Dashboard reports, as described herein and the Documentation.

NOTE: The performance of the Solution, including specifically, notification of Emergencies or Security Incidents, as defined below, will not commence until after initial deployment is complete. The performance of (i) remediation services for Security Incidents (as defined below), (ii) the re-imaging of Customer's systems, or (iii) change of policy settings is outside the scope of the Solution.

[1] Solutions Data also may be referred to in the Agreement as Customer Data.

[2] Existing Arctic Wolf MDR Customers may be, subject to authorization by Arctic Wolf, eligible to license Log Search capabilities only. In such event, Log Search will be included on an Order Form.

Data Transfer. Any Equipment provided by Arctic Wolf to Customer is physically or virtually deployed to monitor Customer's system traffic. Such system traffic is augmented with additional sources of log data, as required, to deliver Managed Detection and Response. All such system traffic information is deemed Solutions Data. Essential log sources will be determined by Customer and Arctic Wolf during the onboarding process preceding the Order Form Effective Date.

Any Solutions Data will be securely transmitted to Arctic Wolf. The Solution operates redundantly with Customer's High Availability (HA) specifications in order to minimize potential service interruptions. Hosting providers used by Arctic Wolf to deliver the Solution may experience service interruptions and service outages outside the control of Arctic Wolf. If such a hosting provider issues an outage notice that could materially impact delivery of the Solutions, Arctic Wolf will use commercially reasonable efforts to promptly notify Customer about the outage and communicate the planned recovery time provided by the hosting provider.

Solutions Data may include personal or confidential information. Customer will provide any such personal or confidential information in accordance with the terms of the Agreement.

Data Retention. Arctic Wolf will store Solutions Data for the Data Retention period specified in Customer's then-current Order Form. Solutions Data may be returned to Customer in accordance with the terms of the Agreement.

Data Storage. Arctic Wolf will store Solutions Data in the hosting provider location set forth on an Order Form.

Updates & Upgrades. Automated maintenance and update cycles to the Equipment will be performed remotely by Arctic Wolf Security Services. Arctic Wolf will provide any services related to the replacement or upgrades of the Equipment. Any costs related to such Equipment replacement or upgrades will be in accordance with the Agreement.

Security Incidents. The CST supporting Customer is available 8:00 am to 5:00 pm (based on the time zone within which the CST is located), Monday through Friday (excluding holidays). The SOC is available 24 hours a day, 7 days a week, including holidays. Customer may schedule specific activities with their CST by contacting the Arctic Wolf SOC at security@arcticwolf.com. Arctic Wolf Security Services will acknowledge any schedule request submitted by Customer to security@arcticwolf.com within one (1) hour of receipt of such request. Arctic Wolf Security Services will provide an estimate of response time determined by scope, size, and urgency.

Arctic Wolf Security Services will notify and escalate to Customer any Security Incidents, the definition of which will be agreed upon by Customer and its CST during the Subscription Term after transition from the deployment team, discovered by Arctic Wolf within two (2) hours of Arctic Wolf's discovery of such Security Incident. Arctic Wolf standard Security Incident notification process is through a ticket to the Customer; however, Arctic Wolf and Customer may agree to alternate notification processes. Security Incident notifications will include a description of the Security Incident, the level of exposure, and a suggested remediation strategy. Customer is responsible for implementing, in its sole discretion, any remediation strategies identified by Arctic Wolf. Customer may request validation by Arctic Wolf that any such implemented remediation strategies are working as expected.

Emergencies. Following transition from the deployment team to the CST, Customer and the CST will agree on and document which Security Incidents will be defined as an "Emergency". Emergencies will typically include the discovery of ransomware and other alerts that could cause degradation/outage to Customer's infrastructure security. Arctic Wolf will escalate Emergencies to Customer within thirty (30) minutes of Arctic Wolf's discovery of the Emergency.

Any Emergency identified by Customer can be escalated to Arctic Wolf's Security Services by calling: 1-888-272-8429, option 2. Customer must describe the Emergency in the initial call and Arctic Wolf will respond within 5 minutes. In addition, with respect to any urgent inquiries, Customer may contact Arctic Wolf's Security Services by calling: 1-888-272-8429, option 2.

Scans. On a monthly basis, Arctic Wolf will use the Solution to conduct external vulnerability assessment scans of Customer's environment. As part of these scans, vulnerability and exploit information will be normalized and correlated with other data sources in order to determine Customer's Security Score and prioritization of any identified remediation strategies. Arctic Wolf will deliver to Customer a summary security report that includes Security Incident and Emergency notification activities on a monthly and quarterly basis.

Coverage Score (fka Configuration Score or Security Score). Customer's Coverage Score is provided as part of the Solution for illustrative and informational purposes only and may be used by Customer for internal benchmarking. The Coverage Score is based on certain information related to the results of the Solution within Customer's environment and is compiled using the Solutions Data made available to Arctic Wolf in conjunction with its delivery of the Solution. Customer's Coverage Score will be communicated in Customer's summary reports in addition to being available on Customer's online Executive Dashboard. Customers may elect to compare their Coverage Score against industry averages from organizations in the same industry vertical to assess how Customer is performing against industry norms.

Host Containment Actions. Arctic Wolf may, if agreed with Customer, using commercially reasonable efforts, perform host containment actions, including removal of host containment, as described below (collectively, "Host Containment Actions"), provided that Customer has deployed the Arctic Wolf Agent or such other agreed upon third party agents. In the event Customer has deployed multiple agents, including the Arctic Wolf Agent, within its environment, Arctic Wolf will contain using the Arctic Wolf Agent. Based on (i) information provided by Customer to its CST following initial deployment, (ii) a mutually agreed upon escalation process set forth in Customer's onboarding document, as updated upon agreement by Customer and its CST during the Subscription Term, and (iii) Arctic Wolf is provided appropriate access to applicable third party security applications, if any, within Customer's environment, the Security Services team may remotely isolate a Customer endpoint device(s) that shows evidence of compromise or other suspicious activity. When the Security Services team identifies certain indicators of attack on an endpoint, the Host Containment Action will be initiated systematically, in accordance with the agreed upon escalation process, and subject to the requirements set forth herein, to rapidly quarantine the suspected compromised system.

The indicators of attack that may drive Host Containment Actions include those relating to ransomware (and other types of advanced malware), malicious command-and-control (C2) activity, or active data exfiltration attempts.

The endpoints under containment will receive a containment notification and the Host Containment Actions will be detailed in an incident ticket. If using the Arctic Wolf Agent, the Customer Portal will display the Customer endpoints that are currently in a contained state. Security Services team is available to Customer to answer questions or provide detailed information on any contained endpoints.

Pre-requisites for Host Containment Actions – Customer must:

- Complete a checklist in partnership with its CST, which will include further definition, including but not limited to the scenarios where Arctic Wolf will and will not perform Host Containment Actions including specific information regarding which endpoints/servers where Host Containment Actions will and will not be performed, the times of day for Host Containment Actions to occur, notification and escalation preferences related to Host Containment Actions;
- Provide Arctic Wolf with technical permissions to allow Arctic Wolf to perform Host Containment Actions within Customer's environment (Customer understands that should Arctic Wolf have invalid access or is blocked from initiating Host Containment Actions, Arctic Wolf will be unable to provide the agreed upon Host Containment Actions);
- Implement appropriate internal procedures and oversight to the extent Customer utilizes the configuration of workflows and processes, including but not limited to Host Containment Actions and other similar functionalities; and
- Enable software or services, in Customer's discretion, to permit necessary visibility into Customer's environment to perform Host Containment Actions.

Active Directory Deception. If licensed and implemented by Customer either as a standalone or bundled feature within the Solution, Customer may deploy Active Directory Deception ("AD Deception"). With AD Deception, Customer creates, configures and maintains Active Directory decoy account(s) intended to act as a deception trap within Customer's network.

The Active Directory decoy account is not intended to participate in normal business activities and should not log-in to Customer's system. The Active Directory decoy account is intended to provide a high-fidelity mechanism for detecting abnormal activity yielding no false positives. If a decoy account is deployed by Customer, Customer is responsible for creating, configuring, and maintaining the decoy account. The naming of the decoy account should follow Customer's account naming conventions. Arctic Wolf will provide reasonable guidance and assistance to Customer in the configuration of such decoy accounts. Customer will provide Arctic Wolf details of the decoy account to Arctic Wolf for monitoring. Customer understands that any changes to the decoy account configurations may impact the security of Customer's environment.

Microsoft US Government Community and High US Government Community Environment Monitoring. In the event Arctic Wolf monitors applications for Customer within the Microsoft US Government Community environment or US Government Community High environment (each a "GCC environment") as part of the delivery of the Solutions, Customer understands and agrees as follows:

1. Only Arctic Wolf supported, and integrated applications will be monitored in the GCC environment.
2. Solutions Data (i) may be accessed by Arctic Wolf, its Affiliates, and any third-party providers, from locations outside the United States, and (ii) may be accessed by persons who are not United States citizens;
3. Arctic Wolf does not require access to or delivery of Customer's Controlled Unclassified Information;
4. Arctic Wolf will provide reasonable cooperation to Customer in the event of a data breach involving Solutions Data including, but not limited to assistance in responding to any government or regulatory inquiries;
5. Certain Microsoft log sources may be in beta and, consequently, Arctic Wolf makes no representations as to the delivery of the Solutions related to any such beta Microsoft log sources; and
6. Customer will immediately notify Arctic Wolf of non-consent or any change in consent and any monitoring of Customer's GCC environment will immediately cease without further liability to Arctic Wolf.

Additional Modules.

- **Cloud Detection and Response ("CDR").** Customers may license CDR for Amazon Web Services (AWS), Microsoft Azure, and any such other cloud IaaS and SaaS environments that Arctic Wolf may agree to monitor at a frequency agreed upon with Customer. Customer's election to license such CDR feature will be set forth on an Order Form. If licensed as part of the Solution, Arctic Wolf will provide detection and response for the respective IaaS and SaaS environments as described herein.

- **Data Exploration.** Customers may license Data Exploration. Customer's election to license such Data Exploration feature will be set forth on an Order Form. Data Exploration allows Customer to work with its CST to identify and remediate risk in Customer's environment. Customer may access historical and analyzed data for quick, ad-hoc investigations and self-service reporting while working with its CST to understand the results and take actions when needed. Data Exploration includes (i) Data Explorer which includes pre-defined workflows to address common security questions and (ii) Log Search which permits Customer to query its retained Solutions Data in 30-day increments.