Managed Detection and Response

Product Description

Document ID	MDR-PD
Document Version	1.4
Last Updated	2025.05

Document Change History

Version	Date	Summary of Changes
1.4	2025.10	Updates to provide structure (versioning, change history) and copyright information. Changes to technology overview to reference, rather than duplicate, content covered in the Arctic Wolf Core Technologies product description.
1.3	2025.05	Minor changes to wording to account for general terms and conditions updates.
1.2	2025.02	Updates to account for the acquisition of the Auora Endpoint Security (fka Blackberry Cylance) products
1.1	2024.11	Addressing terminology inconsistencies with other product description documents
1.0	2024.08	Initial release

Product Description[1]

Arctic Wolf Managed Detection and Response (MDR)

The Arctic Wolf® MDR solution provides 24×7 monitoring of your endpoints, identity, networks, cloud environments, and more, to help you detect, respond, and recover from modern cyber-attacks. The Arctic Wolf Concierge Delivery Model ensures that our purpose-built technology, combined with our extraordinarily talented security delivery teams, help you deliver security outcomes for your organization.

All Arctic Wolf MDR customers have access to the Unified Portal (formerly known as Customer Portal), a web-based self-service application that enables you to configure and tailor the MDR Solution, and provides you with real-time insights to the data, alerts, and tasks related to your security program. As more fully described in the MDR Solution Overview section below, security touchpoints with your Concierge Security® Team (CST) and your Customer Success Manager (CSM) are included as part of the MDR Solution and defined by the Concierge Security Tier (CST Tier) in your subscription, if applicable. Security touchpoints are designed to provide you not only a detailed understanding of current security events and threats but deliver proactive security hardening guidance to improve the security maturity of your security program overall.

Table of Contents

[1] This Product Description was formerly referred to as the MDR Solutions Terms.

Arctic Wolf Technology Overview

In addition to the core technologies offered to all Arctic Wolf solutions that are listed in the Arctic Wolf Core Technologies product description, the below Arctic Wolf Technology Overview sets forth, in general, the Arctic Wolf Technology and the various features and tools that may be included as part of the MDR Solution. The availability and use of any such Arctic Wolf Technology, features, and tools by you is dependent upon the specifics of your subscription and reflected in an ordering document (i.e., Order Form).

Physical Sensor

Our hardware-based network appliances, commonly referred to as a Sensor, allows us to monitor events in your network traffic and identify potential threats.

The Sensors also collect and deliver syslog-forwarded logs from supported third-party product integrations into the Arctic Wolf Platform so that your logs can be parsed, analyzed, and triaged. For more information on Sensor models, see Arctic Wolf Sensors on our Arctic Wolf Help Documentation site.

The Sensor can be deployed in one of the following two modes:

Mode	Description
Mirror/SPAN (Switched Port Analyzer)	• The Sensor passively monitors traffic using a switch. • Network-based containment is unavailable. • Shutting down the Sensor does not affect network connectivity.
Terminal Access Point (TAP)	• The Sensor is installed inline and captures the log traffic that flows through the Sensor itself. • Allows network-based containment for suspicious and malicious activity within the network in which it is installed. • Shutting down the Sensor is likely to affect network connectivity.

***Note**: MDR operates redundantly with your High Availability (HA) specifications to minimize potential service interruptions. The Sensors do not natively provide any HA functionality such as automatic failover for network traffic. For log collection, the Sensors do have built in HA functionality. Additionally, the HA environment must be configured correctly by you to avoid duplication of data. The Deployment Security Team (DST) will assist with this*

configuration during the onboarding phase. Once onboarding is completed, any further configurations are managed and maintained by your internal team or service provider.

Virtual Sensor

MDR includes access to one virtual network appliance commonly referred to as a virtual sensor (vSensor). Access to additional vSensors may be added to your subscription for an additional cost. For more information on the types of virtual network appliances, refer to the table below.

Virtual Network Appliance	Description
Virtual Sensors (vSensors)	vSensors can be used in addition to a physical Sensor to monitor network traffic. The MDR Solution may use one or more vSensor deployments to monitor events in your network and identify potential threats. vSensors also collect and deliver syslog-forwarded logs from supported third-party product integrations into the Arctic Wolf Platform for triage and analysis by the Arctic Wolf Security Operations Center (SOC).
Virtual Log Collector (VLC)	A stand-alone virtualized log collector collects and delivers syslog-forwarded logs from Arctic Wolf supported third-party product integrations into the Arctic Wolf Platform for triage and analysis by the SOC.

Arctic Wolf Agent

The Arctic Wolf Agent ("Agent") is software installed on endpoints. This software initiates system scans to augment the operating system telemetry data, to scan for system misconfigurations through the security controls benchmarking function, and to perform host-based vulnerability assessment scans. The Agent is updated four times daily with the latest vulnerability feeds from Arctic Wolf. The Agent is capable of self-updating, collecting software and asset inventory data, and sends operational metrics and telemetry to the Security Services Team (comprised of your CST and the SOC). The Agent can co-exist with your existing Endpoint Security vendor's tools and for the best possible service, visibility, and coverage, we recommend that the Arctic Wolf Agent be deployed to all devices in your environment alongside Sysmon.

During onboarding, the DST will assist you in the deployment of the Agent at scale within your organization through an appropriate method such as Microsoft Intune, Microsoft System Center Configuration Manager (SCCM), Jamf, or group policy.

Active Directory (AD) Sensor

Arctic Wolf provides technology, an AD Sensor, specifically designed for use on Microsoft AD Domain Controllers within your environment. This AD Sensor provides additional visibility about users, groups, devices, and authentication activity within your AD.

Third-Party Integrations

Arctic Wolf works with your existing security tools, collecting and analyzing telemetry and events from a constantly growing number of log sources, across various attack surfaces. These integrations allow us to further monitor your environment, provide additional detection sources and investigation context.

Arctic Wolf supports integrations covering market-leading products across endpoint, email, identity, network, platform as a service (PaaS), infrastructure as a service (IaaS), application and software as a service (SaaS), and a growing number of industry-specific applications and tools.

The DST will assist with the initial set-up and configuration of your third-party tools during onboarding, provided Arctic Wolf supports integrations to such tools and if such integrations are included in your subscription.

Cloud Detection and Response (CDR)

You may license CDR for Amazon Web Services (AWS), Microsoft Azure, and any such other cloud IaaS and SaaS environments that Arctic Wolf may support. Your election to license such CDR feature will be listed on your Order Form. If licensed, Arctic Wolf will provide detection and response for such IaaS and SaaS environments. Arctic Wolf is not responsible for any software and/or application changes made by such cloud IaaS and SaaS providers which affect or impair the CDR feature.

MDR Solution Coverage

To receive the full benefit of the MDR Solution, the following is a non-exhaustive list of log sources are recommended for all sites, Agents, Sensors, and vSensors. A full list of supported and recommended log sources and integrations can be found at https://docs.arcticwolf.com/

Integration Category	Recommended[2]	Optional[2] (Examples)
Authentication/Identity	Active Directory or Entra ID	Duo, Okta
Cloud	N/A	AWS, AWS WAF, Azure, Azure AD & O365, Defender for Cloud, Google Workspace
Email	N/A	Mimecast, Proofpoint
Endpoint (see Note below)	Agent + Sysmon	Carbon Black, Cisco AMP, Crowdstrike, Arctic Wolf Aurora Endpoint Defense / Cylance, Defender for Endpoint (formerly ATP), Pan Cortex XDR, SentinelOne, Sophos Central, Webroot
Network/Perimeter	Firewall	DHCP, DLP, SD-WAN, VPN
Response Action Integrations	Agent Containment	Duo, Okta, Entra ID, Carbon Black, Crowdstrike, Defender ATP, SentinelOne, Zscaler, External Deny List [Firewall]

Note: *Endpoint is critical to every security program and without coverage the effectivity of your security program will be degraded. It is recommended that you have 85% minimum coverage, or better, across all your endpoints within the environments included with your subscription to get the full benefit of the Solution.*

Note: *Some organizations may be unable to deploy a sensor or virtual sensor due to infrastructure limitations or restricted access. Such organizations may still opt for Arctic Wolf MDR configured in a zero-sensor deployment with access to a restricted set of capabilities and telemetry.*

[2] Product names are subject to change without notice from the appropriate vendor.

Capabilities available in a Zero Sensor MDR deployment	Capabilities not available in a Zero Sensor MDR deployment

• Arctic Wolf security telemetry
  ○ Arctic Wolf Agent, including endpoint containment capabilities
  ○ Account Takeover Risk detection
  ○ External Scanning
• Supported third-party integrations
	• Arctic Wolf security telemetry
	  ○ Arctic Wolf sensor, including Intrusion Detection capabilities and network containment capabilities
	  ○ Arctic Wolf virtual Log Collector (vLC)
	  ○ Arctic Wolf Active Directory sensor, including Active Directory security logs, user, computer, and group information, as well as DNS and DHCP
	• Any third-party security integrations which require a sensor

Arctic Wolf Unified Portal

The Arctic Wolf Unified Portal is a self-service tool that provides a single point of access to your licensed Arctic Wolf products and a channel to collaborate with both your CST and the SOC.

As part of MDR, the Unified Portal allows you to perform the following tasks:

- View Security Alerts (aka Tickets)
- View security focus and any security posture in-depth reviews (SPiDRs[3]) that are available with your subscription or CST Tier, if applicable
- Access dashboards, reports, and, if licensed, Data Exploration capabilities.
- Configure MDR third-party integrations
- Update contacts
- Apply MDR detection suppressions
- Fleet overview of Arctic Wolf sensors, scanners, collectors
- Manage your security policies, permissions, and organizational profile information.

[3] See the Scope of Service document here: https://docs.arcticwolf.com/

Additional Features

Data Retention

Arctic Wolf's standard log retention is ninety (90) days. A longer retention period may be purchased as part of your subscription.

Data Exploration

In the Unified Portal you may have a Data Exploration tab where you can access the Data Exploration components which may include Data Explorer, Data Explorer Lite, Flow Data, and more depending on your subscription.

Flow Data

Flow Data displays the total bytes flowing through your respective devices, protocols, locations, sites, and/or Sensor/vSensor(s). Flow Data is found under the Data Exploration tab of the Unified Portal.

Data Explorer Lite

Data Explorer Lite provides access to very recent (three days) event data.

***Note**: Event data is a collection of analyzed data the Arctic Wolf platform finds to be interesting from a security standpoint*.

Data Explorer

You may license Data Explorer as an additional feature and enable it within the Unified Portal within the Data Exploration tab. Data Explorer allows you to access historical event and observation data for quick, ad-hoc investigations, self-service reporting, and custom alert creation. You may identify and remediate risk in your environment and take appropriate actions when needed depending on results. Depending on your subscription, Data Explorer includes (i) access to the prior 14[4], 30, or 90 days of event and observation data, and (ii) Raw Log Search.

- **For purposes of Raw Log Search and Data Explorer**, raw log data is the data from your environment ingested into the Arctic Wolf platform; analyzed data is parsed, normalized, and enriched data derived from the raw log data and processed by the Arctic Wolf Platform.

  ***Note:** Not all logs ingested by Arctic Wolf are parsed, normalized, or enriched*.

[4] Legacy Data Explorer customers have been grandfathered into the DE-14 tier, increasing their data window from 10 days to 14 days.

- **Raw Log Search**[5] — is a feature of Data Explorer, and a legacy feature of core MDR that is no longer offered outside of Data Explorer. Raw Log Search allows you to search ad-hoc your raw log data in 30-day increments, up to your retention period, such as 90 or 180 days. Raw Log Search enables you to query such data from any ingested source with which the MDR Solution has been integrated, including on-premises systems, cloud, SaaS, and IaaS sources.

- **Self-serve Reporting** – is a feature of Data Explorer that allows you to create one or more dashboards containing one or more visualizations of a given Data Explorer query (widget). Depending on your subscription you may have the ability to create and edit some number of dashboards and widgets to present the data in a way that makes sense to your business.

- **Custom Alerts** – is a feature of Data Explorer which allows you to configure a schedule on which to execute a saved query and a set of recipients to receive a notification if a given run of that query returns non-zero results. Depending on your subscription you may have 10 or more Custom Alerts active at a given time. The results of Custom Alerts that you define are not analyzed by the SOC[6] – the feature is a convenience for you to receive notifications on situations of interest to you.

Active Directory Deception (AD Deception)

With AD Deception, you may create, configure, and maintain Active Directory decoy account(s) intended to act as a deception trap within your network.

The Active Directory decoy account is not intended to participate in normal business activities and should not log into your systems. The Active Directory decoy account is intended to provide a high-fidelity mechanism for detecting abnormal activity yielding no false positives. If you deploy a decoy account, you will be responsible for creating, configuring, and maintaining the decoy account. The naming of the decoy account should follow your account naming conventions. Arctic Wolf will provide reasonable guidance and assistance to you in the configuration of such decoy accounts. Arctic Wolf, with the details of the decoy accounts you provide, will monitor such accounts. Any changes to the decoy account configurations may impact the security of your environment.

[5] Legacy customers licensing Log Search are entitled to Log Search only.

[6] The SOC does have access to all data flowing through the Arctic Wolf pipeline and will appropriately triage this data per the Scope of Service https://docs.arcticwolf.com/

Scanners

Arctic Wolf Scanners ("Scanners") are data collection devices used to capture network device identification and vulnerability data. Scanners are included with your subscription as set forth on your Order Form. The External Vulnerability Assessment Scanners are managed, maintained, and updated with the latest vulnerability feeds by Arctic Wolf.

Scanner	Description
External Vulnerability Assessment (EVA) Scanner	The EVA scanner is hosted on Arctic Wolf cloud infrastructure. It scans customer-provided, public facing assets such as IP addresses, domains, and cloud accounts (if purchased and configured) by performing port detection (for IPs), DNS scan (for domains), followed by vulnerability scanning on all assets (Account Take Over, Web Application, Vulnerability, and CSPM). The schedule for these scans can be defined within the Unified Portal.

The output from the EVA scanning process will be a security risk posture score based on an industry standard and recognized Cybersecurity Framework and Arctic Wolf's proprietary algorithm.

Coverage Score

Your Coverage Score (aka Configuration Score or Security Score) is provided as part of MDR for illustrative and informational purposes only and may be used for internal benchmarking. The Coverage Score is based on certain information related to the results of MDR within your environment and is compiled using the data made available to Arctic Wolf in conjunction with our delivery of the Solution. Your Coverage Score will be communicated in summary reports and/or in the Unified Portal.

Threat Intelligence

You may license Threat Intelligence as an additional feature of your subscription and enable it within the Unified Portal under the Security Bulletins tab in the reporting section. Threat Intelligence is available in a "Plus" version as well as the base offering with the parameters as described below.

Capability / Description	Base	Plus
Threat Reports Security research intelligence reports generated by the Arctic Wolf Threat Research team.	Monthly	Monthly

Video Briefings Security research intelligence briefings across multiple topics and delivered by the Arctic Wolf Threat Research team.	n/a	Quarterly
Downloadable IOC Intelligence Feed of potentially malicious indicators of compromise (IOCs) including, but not limited to, IP's, domains, URL's and file hashes. The data within this feed can be downloaded and used in third party security tools like firewalls and EDR services to block potentially malicious activities.	n/a	Included

Security Expertise: Overview of Security Teams

The Arctic Wolf Security Teams engage with you remotely to support your use of the Solutions and ensure Arctic Wolf has a complete understanding of your unique IT environment. For a full description of the Arctic Wolf Security Teams and the scope of activities performed by each team across all Arctic Wolf Products, please see the Scope of Service document (here). The specific scope of activities handled by the Security Teams related to MDR can be found in the MDR Solution Overview section below.

MDR Solution Overview

By default, the 24x7x365 monitoring of your environment is provided by our global SOC team. If your subscription includes a CST Tier, your CSTs involvement and participation in the Solution will be enhanced in accordance with the specifics of the CST Tier selected by you for your subscription. The following may be included with your MDR subscription:

Working with Arctic Wolf Security Services

During your subscription term, you may regularly engage with your CST and SOC. The level of interaction with your CST will be based on your CST Tier, if applicable. These teams are available to answer questions about MDR, guide you on your Security Journey, and work with you to enhance your security posture.

For all customers, CST is available Monday through Friday from 8:00 a.m. - 5:00 p.m. in the time zone within which your CST is located. The SOC is available 24x7x365. To contact them, call 1-888-272-8429 ext. 2 or email security@arcticwolf.com. If you are calling from

outside of North America, toll-free numbers can be found here: https://arcticwolf.com/toll-free/.

Note: *Arctic Wolf's third-party hosting providers 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 Solution, Arctic Wolf will use commercially reasonable efforts to promptly notify you about the outage and communicate the planned recovery time provided by the hosting provider.*

Solution Delivery Response Times

All actions referred to below will be made by Arctic Wolf Security Services.

All Security Incidents are assigned a severity level[7] as follows:

Severity Level	Description	Example
Urgent	An active threat requiring immediate action. Incidents of this severity pose a high risk of data loss, service disruption, or significant financial/legal consequences.	• Ransomware attack encrypting large portions of critical infrastructure • Zero-day Exploit • Massive Data Exfiltration
High	A considerable threat that could lead to significant compromise or disruption if left unaddressed. Incidents of this severity require immediate attention.	• Malware/Botnet Detected • HTTP Download of Malicious Payload
Medium	Security Incidents with this severity level generally involve a security vulnerability or suspicious activity that may require attention.	• Individual host or Widespread targeting but no sign of compromise
Low	Security Incidents with this severity level involve security posture issues with low impact or benign activities that don't pose a significant threat.	• Individual host or non-critical user

[7] Arctic Wolf reserves the right to adjust the severity of a given Security Incident at our discretion.

The response time service levels for the specified inquiries, Security Incidents, and Emergencies are as follows:

Action	Service Level
Acknowledgement of any schedule request submitted by you to security@arcticwolf.com	One (1) hour from receipt of request.
Acknowledgement of receipt of any Security Incident (inbound) submitted by you to security@arcticwolf.com	One (1) hour from receipt of request; Security Services will follow-up with you with an estimate of response time determined by scope, size, and urgency.
Notification and escalation of any Security Incidents (outbound notice)	Two (2) hours of Arctic Wolf's discovery.
Escalation of any Emergency (outbound notice)	Thirty (30) minutes of Arctic Wolf's discovery.
Emergency escalated via phone to the SOC (inbound notice)	Arctic Wolf will respond within five (5) minutes; you will be required to describe the Emergency. In the unlikely event that your call goes to Voice Mail, the caller must leave a message to receive a reply.

Emergencies generally include any Urgent severity Security Incident and other severity Security Incidents at the discretion of the analyst that could cause degradation or an outage to your systems and infrastructure.

Arctic Wolf's standard Security Incident (as defined below) notification process is through a ticket to your administrator(s); however, we 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.

Note:

- *Solution delivery, including specifically, notification of Emergencies or Security Incidents, will commence once deployment is complete.*

- *Remediation services for Security Incidents, the re-imaging of your systems, or change of policy settings is outside the scope of MDR.*

Escalation Paths and Policies

Escalation paths and policies include details to tell the SOC and CST who should be contacted within your organization, in the event of a Security Incident or Emergency.

You are encouraged to have at least two escalation paths defined and your Deployment Security Team (DST) will help you navigate the right escalation processes for your organization during onboarding. There are no limits to the number of escalation paths that you can define, and you can change, add, or remove them via self-service in the Unified Portal or by collaborating with your CST following onboarding.

Escalation policies may support different escalation paths based on incident type – for example, all endpoint incidents can be routed to one contact, while all email incidents can be routed to another.

Response Action Policies

Response Action policies tell the SOC and your CST when they can contain or action on an identified threat. As part of MDR, Arctic Wolf will use reasonable efforts to perform Response Actions which may include, but are not limited to, the following:

- Host containment
- Enable/Disable user
- Force password
- Close user connections
- Block URL
- Move or delete email
- Retrieve files
- Kill processes
- Execute scripts
- Modify deny lists and IP rules

The default Response Action policy is “always enable Response Actions” to allow the Arctic Wolf SOC to stop threats and threat actors, minimizing the impact of a Security Incident. Your DST (during onboarding) and your CST (after deployment) can help you document the Response Actions policy that is best for your organization.

Should you have multiple technologies deployed within your environment for a given attack surface (e.g. endpoint, identity, network, etc.) in addition to the Arctic Wolf Technologies

such as the Agent, Response Actions will be attempted initially using the Arctic Wolf Technology.

For the SOC to take action you must deploy the Agent or such other agreed upon third party agent, and configure the response integrations, including authentication and permissions for the specific technology as defined in the Arctic Wolf Documentation, appropriate to your environment, through the Unified Portal.

Based on (i) the information you provide to your CST following deployment, (ii) a mutually agreed upon escalation policy, and (iii) your provision of appropriate access to applicable third party security applications, if any, within your environment, the SOC may remotely isolate a your endpoint device(s), network appliance, or user account(s) that show evidence of compromise or other suspicious activity. When the Security Services Team identifies certain indicators of attack on an endpoint, network device, or user account, the Response Action will be initiated in accordance with the agreed upon escalation policy to rapidly quarantine the suspected compromised system or account.

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

The endpoints, network, or user accounts participating in the Response Actions will receive a notification and the Response Actions will be detailed in an incident ticket. If using the Agent, the Unified Portal will display the endpoints that are currently in a contained state. The Security Services Team is available to you to answer questions or provide detailed information on any endpoints, network, and/or user accounts participating in the Response Action.

Incident Investigation, Notification, and Guided Remediation

Security Investigations and Security Incidents

The telemetry data (defined as “Solutions Data” in our Privacy Notice) accepted and ingested by Arctic Wolf that is deemed critical and/or is interesting and relevant from a security perspective, may prompt further analysis by the Arctic Wolf Platform and/or a member of the SOC– this is called a Security Investigation. During the Security Investigation, the SOC may collaborate with you to do further investigation, detail Response Actions, remediate the discovered issue(s), and/or provide a detailed report of the Security Investigation – if these events occur, we identify this as a Security Incident.

You may also request that Arctic Wolf conduct a Security Investigation for data and/or situations that Arctic Wolf does not deem critical and/or interesting and relevant. As part of any Security Investigation, Arctic Wolf will:

- Provide validation of a Security Incident as detected through the Arctic Wolf Platform.
- Participate in calls with your in-house and/or third-party incident response team.
- Provide findings of data captured pertaining to the Security Incident within the Arctic Wolf Platform.
- Provide a report of findings for the Security Investigation upon request.
- Provide recommendations, documentation, and best practices relevant to the Security Investigation.

Notification

The Arctic Wolf SOC is responsible for notifying you of discovered Security Incidents.

The SOC's notification process is done through a security alert ticket via our ticketing system to you, as specified in the escalation paths you have in place within your escalation policies. In the case of an emergency the SOC will also attempt to call customer contacts in priority order and will leave voice mails if necessary.

Security Incident notifications will/may include a description of the Security Incident, the level of exposure, any actions taken prior to the notification, and the suggested remediation steps remaining.

Guided Remediation

The Arctic Wolf SOC and your CST will provide remediation guidance to return your environment to operational status if there is a compromise (e.g., by providing action-oriented guided remediation instructions that you can perform). A typical example of guided remediation would include written or verbal instruction delivered via a security alert or via a call, to remove such malicious applications as persistence mechanisms or malware. If you should require further assistance, you may separately engage Arctic Wolf's Incident Response Team, subject to the terms and scope in an agreed upon statement of work (SOW).

Reporting

Through the Unified Portal, you have access to several pre-defined dashboards as well as the ability to create new dashboards to surface data appropriately for your business. In addition, and if necessary, your CST may assist in the creation of other regular reports based on the data ingested from your environment.

The reports will either be automatically generated and sent to you by the Arctic Wolf Platform, created and reviewed by your CST and issued to you, or available in the Unified Portal as a PDF or as a live dashboard.

***Note**:*

- *Reports on Security Incidents will only contain data within the retention period included with your subscription.*
- *General reports and dynamic dashboards may be constrained to the past 10 days of data.*
- *Reports only include data currently being received from you and parsed by the Arctic Wolf Platform.*

Roles and Responsibilities

To ensure that full value of MDR is received, each party's roles and responsibilities are defined in the table below.

Activity	Arctic Wolf	Customer
Deployment		
Agent installation		X
Essential & optional Log source configuration		X
Escalation path purpose communication	X	
Escalation path definitions		X
Response policy definitions		X
Restricted countries definition		X
Select opt-in alerts		X
Sensor configuration and scan schedule recommendations	X	
Sensor configuration		X
Scanner configuration and scan schedules		X
Site configuration		X
Ingestion integration credentials configuration		X

Response integration credentials configuration		X
Contacts definition		X
Ongoing		
Response Actions configuration		X
Initiate and conduct Response Action(s)	X	
Provide guided remediation	X	
Enact remediation recommendations		X
Alert/ticket remediation		X
Alert tuning	X	
Alert suppressions		X
Custom Alert configuration and remediation		X
Security focus recommendation and execution	X	
External vulnerability scanning	X	
Decommissioning		
Remove physical Sensors from Network and return to Arctic Wolf		X
Remove Solution Data from Arctic Wolf Platform	X	