Secureworks

Secureworks® Taegis™ ManagedXDR Elite

Note: **See this version of the ManagedXDR service description if Customer purchased this Service prior to February 2, 2023.**

Overview

The Taegis™ ManagedXDR Elite Service ("**Service**") provides Customer with security monitoring and Investigations within Secureworks® Taegis™ XDR ("**XDR**") 24 hours a day, 7 days a week ("**24x7**"). The Service includes Threat detection and Investigations, Threat and proactive response actions, 24x7 access to Secureworks® Security Analysts from within XDR, Elite Threat Hunting, and additional support and features as described below. All capitalized words and phrases shall have the meanings set forth herein, as defined in the Glossary, or within the Secureworks-applicable agreement, such as the Customer Relationship Agreement.

Notes:

- "Endpoint" and "asset" are used interchangeably in this service description.
- **For customers with more than one XDR tenant (i.e., Additional Managed Tenant)**, service components and Service Level Agreements ("**SLAs**") are applicable across all of Customer's tenants, unless otherwise specified below.

Service Components

24x7 Access to Security Analysts

Security Analysts are available 24x7 through the XDR in-application chat or ticket system, or through telephone.

Secureworks Services for Taegis™ ManagedXDR

Taegis™ ManagedXDR customers are entitled to purchase Service Units—upon initial ordering of the Taegis™ ManagedXDR subscription or at any time during the Services Term—for an additional fee. Service Units can be used for Proactive Services or Emergency Incident Response ("EIR"). See the Addendum - Secureworks Services for Taegis™ ManagedXDR and the Secureworks Services for ManagedXDR Catalog for information.

Threat Detection and Investigations

Secureworks will review and investigate Threats detected within XDR. Threats requiring further analysis as determined by Secureworks will result in creation of an Investigation within XDR. Secureworks will notify Customer through XDR, email, or supported integrations after enough evidence is collected and a Threat is deemed malicious, or if Secureworks requires further input from Customer to proceed with the Investigation.

Secureworks makes routine updates and changes to Taegis to proactively improve the services and Taegis experience for all customers; therefore, Customer may see customized suppression rules, event filter modifications, and alert tuning within XDR that is designed to minimize low-value alerts and focus time on high-value alerts.

Note for Customers with more than one XDR tenant (i.e., Additional Managed Tenant): Threats will be monitored, and investigations will be created separately for each of Customer's XDR tenants. Threat detection and investigations will not be performed across multiple tenants together.

Response

Secureworks will perform supported Threat response actions within Taegis™ XDR on behalf of Customer, after receiving written authorization from Customer, which may come in the form of Proactive Response as described below. The most current list of supported actions can be provided to Customer upon request. For some supported actions, Customer may optionally authorize Secureworks to perform proactive response actions (also known as pre-authorized containment actions) using Customer-created playbooks within Taegis™ XDR. For Customers with Proactive Response, see https://docs.ctpx.secureworks.com/mxdr/connectors_proactive_response/ for information.

Note for customers with more than one XDR tenant (i.e., Additional Managed Tenant): Threat response actions will be performed separately for each of Customer's XDR tenants. Threat response actions will not be performed across multiple tenants together.

If malicious activity is observable within Taegis and has been confirmed by Secureworks as an active threat, then Secureworks will take additional response actions – referred to as Unlimited Response. Activity related to Customer-authorized penetration, vulnerability, or technical testing does not qualify for Unlimited Response All of the following criteria must be met when Secureworks is determining whether Unlimited Response is required:

- Observed activity in Customer's environment, which is occurring on active reporting assets in scope for Customer's Secureworks ManagedXDR subscription, is indicative of human adversary presence (e.g., evidence of successful lateral movement, data exfiltration, credential access, privilege escalation)
- Adversary activity or Security Incident originates from an Investigation created by Secureworks
- Endpoints are actively sending telemetry data to Taegis through a supported EDR agent

Unlimited Response includes only the following activities:

- Endpoint analysis for telemetry that located within Taegis
- Network analysis from network sensors that are integrated with Taegis
- Malicious code analysis for malware discovered as a result of a Secureworks response engagement
- Log analysis for data collected from supported integrations available within Taegis
- Triage data for endpoints actively sending telemetry data to Taegis
- Response actions supported within Taegis (https://docs.ctpx.secureworks.com/mxdr/connectors_proactive_response/)

Note: The utilization of unlimited response cannot be applied to matters requiring privileged engagements with Customer's legal counsel or involvement with cyber insurance carriers. For these types of matters, please contact Security Analysis via chat to start an Incident Response engagement.

Secureworks will provide Customer with written updates on Security Incident status, including information about activities performed and any notable findings. Findings will be communicated with Customer upon discovery. Upon completion of activities for Unlimited Response, Secureworks will send to Customer an Investigation report containing Investigation details and recommendations. This report is delivered to Customer within the Investigation in XDR, and upon delivery of the report, the Investigation is considered closed. If Customer makes multiple requests for Unlimited Response due to activity with the same root cause, then Customer must implement Secureworks-recommended security posture changes to continue qualifying for Unlimited Response.

Elite Threat Hunting

Secureworks will conduct human-driven Threat Hunting, and relevant findings will be made available to Customer within Investigations in XDR. Lead by a Named Threat Hunter assigned to Customer, the Secureworks proprietary methodology, expertise, threat analytics, and threat intelligence will be used to identify unknown Threats and undiscovered threat actors through their tactics, techniques, and procedures ("**TTPs**"), as well as to identify deficiencies in visibility, misconfiguration, or missing data sources discovered as a result of human-driven Threat Hunting. Further, the Threat Hunter will inspect collected Customer telemetry to detect activity such as anomalous user activity, network communications, and application usage; and persistence mechanisms.

The Secureworks Threat Hunting team is generally available Monday – Friday, 7 a.m. – 10 p.m. UTC, for support that is specific to Threat Hunting; however, Customer must contact the Secureworks Security Operations Center ("SOC") for all support inquiries, and the SOC will engage the Threat Hunting team if needed. If Customer contacts the Secureworks SOC for support during a time that is not within the above-listed time frame, and Threat Hunting-specific input is required to resolve Customer's issue, then the Threat Hunting team will be engaged as soon as possible during the above-listed hours.

Elite Threat Hunting includes the following:

- Assignment of a Named Threat Hunter who will collaborate with Customer to gain a thorough understanding of Customer's environment for purposes of effectively conducting Threat Hunting
- Continuous human-driven Threat Hunting across Customer's telemetry in XDR in search of undetected Threats and security exposure that jeopardizes Customer's security posture
- Up to two (2) touchpoint meetings each month with the Threat Hunter at a time as agreed with Customer, to discuss previously shared threat hunt findings and discuss and agree upon the tailored threat hunts to align with Customer's risks and objectives.
- Up to four (4) tailored threat hunts performed each month (maximum of one (1) per week and a minimum of 3 business days processing time to begin the requested hunt). These hunts can include, but are not limited to:
    - Artifact-Driven Threat Hunting
    - Cloud and Network Threat Hunting
    - Hypothesis-Driven Threat Hunting
    - Threat Intelligence-Driven Threat Hunting
- Analysis and escalation to Customer via Taegis Investigation of all activity discovered during Threat Hunting that is deemed critical and could represent a confirmed Security Incident or Threat (e.g., misconfiguration, visibility deficiency)

Notes:

- **Note to Customers with more than one XDR tenant (i.e., Additional Managed Tenant):** Investigations created from Elite Threat Hunting activities as described above will be presented in the corresponding Customer XDR tenant. The maximum number of tailored threat hunts provided each month is four (4) regardless of the number of tenants. The maximum number of touchpoint meetings with the Named Threat Hunter is provided is two (2) regardless of the number of tenants.

  For clarity, if a Customer has four individual tenants, performing the same tailored threat hunts on each individual tenant counts as four tailored threat hunts, not one.

- Elite Threat Hunting cannot begin until after the specified Onboarding activities are completed (https://docs.ctpx.secureworks.com/legal/mdr_service_description/#onboarding). In addition, Secureworks highly recommends that Customer completely deploy supported Endpoint Agents on all endpoints—up to Customer's Licensed Volume—to maximize the effectiveness of this Service. Until completely deployed on all endpoints, Customer understands, agrees, and accepts the risk that this Service will have reduced capabilities for Customer's environment.
- ManagedXDR Elite customers who want to use CrowdStrike Endpoint must purchase the standard Falcon Data Replicator (FDR) directly from CrowdStrike or a CrowdStrike-authorized reseller.

Secureworks Threat Intelligence

XDR is powered by Secureworks Threat Intelligence. Customer network and endpoint telemetry is continually compared against network, endpoint, and behavioral indicators to identify Threats within Customer's IT environment.

Continuous Improvements

Secureworks will recommend continuous improvements to Customer's security posture. For ManagedXDR customers, Secureworks will provide quarterly threat trends, program goals, notable activity in XDR, and provide recommendations for improvement. On an ad-hoc basis, Secureworks, in its sole discretion, may engage additional Secureworks experts to provide the support outlined in this section.

Note to customers with more than one XDR tenant (i.e., Additional Managed Tenant): Customer will receive unified reports and recommendations at the Customer level rather than a specific tenant-level review. However, notable activity in XDR including alerts, investigations, and threat hunts will be provided for each of Customer's XDR tenants.

Service Phases

There are two primary phases for delivering the Service: **Onboarding** and **Steady State**.

Onboarding

Prior to onboarding and deployment, Secureworks will activate Customer's Service by provisioning access to Customer's instance of XDR, which will also provide Customer with access to: 1) online documentation; and 2) instructions to access and deploy the Taegis/Red Cloak Endpoint Agent.

Customer is responsible for deployment of the Taegis/Red Cloak Endpoint Agent or other supported third-party Endpoint Agent, as well as the Taegis™ XDR Collector in Customer's environment. Instructions for downloading the XDR Collector are located in the online documentation. Secureworks will assist Customer remotely through teleconference with questions during this process, as needed.

While Secureworks considers onboarding complete and the Security Investigation service level set forth below to apply when Customer has deployed at least 40% of its Licensed Volume (e.g., deployed compatible Endpoint Agents to endpoints) **and** Customer has acknowledged completion of the training videos within parts one and four of the ManagedXDR Onboarding Overview (https://docs.ctpx.secureworks.com/training/mxdr_onboarding/introduction/), Secureworks highly recommends that Customer completely deploy the Taegis/Red Cloak Endpoint Agent (or other compatible Endpoint Agent) on all endpoints—up to Customer's Licensed Volume—to maximize the effectiveness of the ManagedXDR Elite service. Until completely deployed, Customer understands, agrees, and accepts the risk that the ManagedXDR Elite service will have reduced capabilities for Customer's environment. See the ManagedXDR Elite Onboarding Guide (https://docs.ctpx.secureworks.com/mdr/onboarding/) for more details on these limitations.

Note to Customers with more than one XDR tenant (i.e., Additional Managed Tenant): Secureworks will provision access to each instance of Customer's XDR tenants. Customer is responsible for deploying Endpoint Agents and data collectors for each of Customer's XDR tenants. To reach Steady State for each tenant, at least 40% of the allocated Licensed Volume for that tenant must be deployed **and** Customer representative **for each tenant** must acknowledge completion of the training videos within parts one and four of the ManagedXDR Onboarding Overview (https://docs.ctpx.secureworks.com/training/mxdr_onboarding/introduction/). During onboarding, Secureworks will work with Customer to determine and document the initial allocation of Licensed Volume for each tenant. After Steady State is reached, Customer has the flexibility to re-allocate the total amount of Endpoint Agents (according to Customer's Licensed Volume) across each of Customer's XDR tenants at their discretion. Secureworks strongly recommends Premium Onboarding to support the complexity and project management required to onboard more than one tenant.

Steady State

Steady State monitoring and Elite Threat Hunting for Customer's environment commences when Customer deployed at least 40% of its Licensed Volume (i.e., deployed compatible Endpoint Agents to endpoints) **and**

Customer has acknowledged completion of the training videos within parts one and four of the ManagedXDR Onboarding Overview (https://docs.ctpx.secureworks.com/training/mxdr_onboarding/introduction/).

Phase	Activities

Onboarding	***Timing: From XDR activation until Steady State begins***
	• Collect details about Customer including the following:
	  ○ IT environment
	  ○ Endpoint Agents deployed
	  ○ XDR integrations
	  ○ Primary points of contact and other users
	  ○ Physical locations
	  ○ Critical assets (endpoints) and high-value targets
	• Customer completes the training videos within parts one and four of the ManagedXDR Onboarding Overview (https://docs.ctpx.secureworks.com/training/mxdr_onboarding/introduction/)
	• Facilitate the Elite Threat Hunting introductory teleconference to discuss with Customer the following:
	  ○ Overview and deliverables
	  ○ Roles, responsibilities, and scope
	  ○ Bi-weekly (every two weeks) operational teleconference

Initial Baseline Meeting	***Timing: Approximately four (4) weeks after Steady State monitoring begins*** • Define shared program goals to establish a plan for continuous improvement • Review and discuss Customer profile responses to understand Customer's IT environment, security controls, and any other relevant context • Provide guidance on current detection mechanisms in XDR and how they can be applied to Customer • Review notable Alerts, Investigations, and Threat Hunts created for Customer
Quarterly Updates	***Timing: Quarterly after the baseline meeting is conducted*** • Review and evaluate program goals and plan • Review current topics in the threat landscape • Review Investigations and Alert trends • Provide security posture guidance •

Customer Obligations

Customer is required to perform the obligations listed below and acknowledges and agrees that the ability of Secureworks to perform its obligations hereunder, including meeting the Service Level Agreements ("**SLAs**") listed further below, are dependent on Customer's compliance with these obligations. Noncompliance with Customer obligations relative to this Service may result in limitations and reduced service capabilities, suspension of managed components of the Service and/or SLAs, or a transition to monitor-only components of the Service.

Note to Customers with more than one XDR tenant (i.e., Additional Managed Tenant): The Customer Obligations listed below are required and applicable to **each** of Customer's XDR tenants.

Customer will do the following:

- Ensure that Customer's IT environment has a compatible Endpoint Agent installed on each endpoint that will be licensed for the Service
- Deploy a compatible Endpoint Agent on each endpoint (as explained above, once at least 40% of Licensed Volume is deployed, the transition to Steady State can begin)

- Obtain licenses and/or support for third-party Endpoint Agents from authorized sources
- Ensure availability of sufficient network bandwidth and access to perform the Service
- Perform ongoing monitoring of active integrations and Customer's associated health to ensure the Service is operating optimally
- Provide appropriate access to Secureworks for integrations as required by XDR
- Ensure its security controls are operating on versions supported by Secureworks integrations
- Manage credentials and permissions for integrations with XDR
- Ensure list of Customer's authorized contacts remains current, including permissions and associated information
- Provide information and assistance (e.g., files, logs, IT environment context) promptly during Investigations that Secureworks conducts for Threats against Customer
- Schedule reports and conduct ad-hoc reporting within XDR
- Ensure internal support for creation and management of custom rules (i.e., custom alert detection and analysis) as these will vary from customer to customer and will not be supported by Secureworks

Service Level Agreements ("SLAs")

The ability of Secureworks to perform an Investigation and decide whether a Threat is malicious is dependent on a compatible Endpoint Agent being installed on a licensed endpoint in Customer's IT environment. The service levels below apply to endpoints that are licensed as part of the Service and are actively communicating with the Secureworks infrastructure.

Note: The only type of Investigation for which Secureworks provides an SLA is the Security Investigation; no SLA is provided for any other type of Investigation.

Service Level	Definition	Measure	Target	Credit
Security Investigation	Secureworks will monitor XDR for Threats. When malicious activity is detected, Secureworks will perform an Investigation, provide an analysis, and notify Customer. Secureworks will notify Customer electronically which may include using XDR, email, or supported integrations. Subsequent related activity identified as part of the ongoing Investigation or monitoring will be appended to an existing Investigation.	Time from Investigation-created timestamp to Customer-notified timestamp as measured by Secureworks	Less than 60 minutes	1/100th of the monthly Service fee if difference between the timestamps is 60-240 minutes 1/30th of the monthly Service fee if difference between the timestamps is greater than 240 minutes Maximum of one credit will be given per calendar day (based on US Eastern time zone)

Service Level	Definition	Credit
Unlimited Response	Urgent requests for Unlimited Response submitted through the IR Hotline, the XDR in-application chat, or the ticketing system within XDR will be acknowledged by the Secureworks team within four (4) hours.	1/100th of the monthly Service fee for each calendar day (based on US Eastern time zone) that the SLA is not met

1.1 Warranty Exclusion

While this Service is intended to reduce risk, it is impossible to completely eliminate risk, and therefore Secureworks makes no guarantee that intrusion, compromises, or any other unauthorized activity will not occur on Customer's network.

Additional Information

Billing for the Service begins at the same time as billing for XDR, which occurs when the login credentials for XDR are sent to Customer through email. Contact account manager or refer to the official terms as stated on Customer's Transaction Document from purchase for the most up-to-date details.

See the documentation within XDR (https://docs.ctpx.secureworks.com/) for information about compatible browsers, integrations, detectors, dashboards, and training. Other information is also available, including release notes.

Glossary

Term	Description
Additional Managed Tenant	An add-on service for ManagedXDR and ManagedXDR Elite that provides Customer with more than one XDR tenant.
Alert	Prioritized occurrences of suspicious or malicious behavior detected by a detector within XDR.
Endpoint Agent	An application installed on an endpoint that is used to gather and send information about activities and operating system details of the endpoint to XDR for analysis and detection of Threats. Use this link to access the list of Endpoint Agents that are compatible with XDR: https://docs.ctpx.secureworks.com/at_a_glance/#endpoints.
Integration	Application Programming Interface ("**API**") calls or other software scripts for conducting the agreed-upon Services for the connected technology.
Investigation	A central location within XDR that is used to collect evidence, analysis, and recommendations related to a Threat that may be targeting an asset in a Customer's IT environment. Investigations are categorized into types, such as Security and Incident Response.
Security Analyst	A Secureworks security expert who analyzes alerts deemed High and Critical for customers, and creates and escalates Investigations. ***Note:*** A Security Analyst may also be referred to as a ManagedXDR analyst or an MXDR analyst across other Secureworks documentation.
Security Incident	An XDR-generated circumstance in which a compromise or suspected compromise has occurred involving a Customer's environment.
Security Investigation	A type of Investigation that is conducted for a Critical or High alert or event in XDR after a Security Analyst completes preliminary investigative procedures to determine whether a Threat is valid.
Service Level Agreements ("**SLAs**")	A binding agreement to meet defined Service delivery standards.
Services Term	Period of time identified in the Transaction Document during which Services will be delivered to Customer.
Threat	Any activity identified by XDR that may cause harm to an asset in a Customer's IT environment.

Term	Description
Threat Hunter	A designated Secureworks security expert focused on Threat Hunting.
Threat Hunting	To proactively and iteratively discover current or historical threats that evade existing security mechanisms and to use that information to develop future countermeasures and increase cyber resilience.