Mandiant

SECURITY TECHNOLOGIES THAT MANAGED DEFENSE SUPPORTS

The following tables list the supported security technologies, required Google Security Operations parsers, and supported alert types from each vendor that are processed as part of providing security event monitoring and threat hunting services.

> Indicators of Compromise (IOCs) and signatures created by customers are not within the scope of Managed Defense service delivery. Managed Defense does not generally escalate rules where activity has been blocked. For instance, an email may be quarantined before you receive it or traffic may be dropped by an inline network security device. This escalation is only possible if the activity is related to other malicious activity.

Corelight

Product	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Open NDR	Suricata alerts and Zeek logs are supported by Managed Defense.	Alerts and Telemetry: **CORELIGHT** (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/corelight-changelog)	• Suricata Alerts

CrowdStrike

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
CrowdStrike Endpoint Security	CrowdStrike Falcon Enterprise or higher	CrowdStrike Falcon Enterprise, Elite, and Complete are supported for Endpoint Protection Platform (EPP) alerts.	**CS_ALERTS** (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/cs-alerts-changelog)	Endpoint Protection (EPP) alerts
CrowdStrike Falcon Next-Gen Identity Security	CrowdStrike Falcon Next-Gen Identity Security	Managed Defense supports ingestion and monitoring of alerts from the CrowdStrike Falcon Identity Protection (IDP) module.	**CS_ALERTS** (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/cs-alerts-changelog)	Identity Protection (IDP) alerts
Falcon Endpoint Telemetry	Falcon Data Replicator license	CrowdStrike Falcon Enterprise, Elite, and Complete are supported by Managed Defense. Falcon Data Replicator is required for service.	**CS_EDR** (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/cs-edr-changelog)	N/A

Microsoft

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Defender for Endpoint	One of the following: • Endpoint Plan 2 • Defender for Business • Defender for Identity license	Microsoft Defender for Endpoint Plan 2 or Defender for Business is required for service delivery. Managed Defense uses the **Endpoint Detection and Response (https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-endpoint-detection-response?view=o365-worldwide)** features of the platform.	Alerts: **MICROSOFT_GRAPH_ALERT (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/microsoft-graph-alert-changelog)** Telemetry: **MICROSOFT_DEFENDER_ENDPOINT (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/microsoft-defender-endpoint-changelog)**	• Antivirus • Endpoint Detection and Response (EDR)
				The following signatures are monitored in real-time by the Managed Defense SOC. All other signatures are leveraged for hunting and do not adhere to Managed Defense Service Level Objectives. • Suspected over-pass-the-hash attack (forced encryption type) • Suspicious additions to sensitive groups • Data exfiltration over SMB • Suspected Golden Ticket usage (forged authorization data) • Malicious request of Data Protection API master key • Suspicious service creation • Suspected Kerberos SPN exposure • Suspected Golden Ticket usage (ticket anomaly) • Suspected Golden Ticket usage (nonexistent account) • Suspected SID-History injection • Suspected overpass-the-

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Defender for Identity	One of the following: • Endpoint Plan 2 • Defender for Business • Defender for Identity license	Microsoft Defender for Identity alerts is supported for customers who have provided Managed Defense access to Microsoft Security Graph.	Alerts: **MICROSOFT_GRAPH_ALERT (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/microsoft-graph-alert-changelog)**	hash attack (Kerberos) • Suspected Skeleton Key attack (encryption downgrade) • Suspected DCShadow attack (domain controller replication request) • Suspicious VPN connection • Suspected DCShadow attack (domain controller promotion) • Suspected use of Metasploit hacking framework • Suspected Brute Force attack (SMB) • Suspected NTLM authentication tampering • Suspected WannaCry ransomware attack • Suspected NTLM relay attack • Suspected SMB packet manipulation (CVE-2020-0796 exploitation) • Suspected Golden Ticket usage (ticket anomaly using RBCD) • Suspected rogue Kerberos certificate usage • Suspected exploitation attempt on Windows Print Spooler service • Suspected AS-REP Roasting attack • Exchange Server Remote Code Execution (CVE-2021-26855) • Suspicious modification of a sAMNameAccount attribute (CVE-2021-42278 and CVE-2021-42287 exploitation) • Suspicious modification of the Resource Based Constrained Delegation attribute by a machine account • Suspicious disable of

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
		audit filters of AD CS		

Operational Technology applications

Product	Description	Required SecOps Parser	Managed Defense Supported Alert Types
Claroty CTD	Alerts from Claroty CTD are supported by Managed Defense.	**CLAROTY_CTD (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/claroty-ctd-changelog)**	• Alerting events `blocked` or `not blocked` are informational and passed on in the alert context as one of the following: ◦ `attempted` ◦ `failed` ◦ `succeeded`
Claroty xDome	Alerts from the Threat category are supported by Managed Defense.	**CLAROTY_XDOME (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/claroty-xdome-changelog)**	• Events in the Threat category, malicious addresses, or infected devices
Forescout eyeInspect	Alerts from Forescout eyeInspect are supported by Managed Defense	**FORESCOUT_EYEINSPECT (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/forescout-eyeinspect-changelog)**	N/A
Nozomi Guardian	INCIDENT and SIGN alerts are supported by Managed Defense.	**NOZOMI_GUARDIAN (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/nozomi-guardian-changelog)**	• All alerts are forwarded to the SOC based on Severity

Palo Alto Networks

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Next Generation Firewall	N/A	Palo Alto Next Generation Firewalls (PAN NGFW) threats that are not blocked are supported by Managed Defense. Managed Defense can integrate with a WildFire Free or Advanced license for additional detection of malware. Data Filtering logs can optionally provide additional context for investigations.	Alerts: **PAN_FIREWALL (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/pan-firewall-changelog)**	• Threats • WildFire • Data Filtering***

SentinelOne

Product	License requirement	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Singularity	Cloud Funnel license	SentinelOne Singularity Complete is supported by Managed Defense. A Cloud Funnel license is required for Managed Defense service delivery.	Alerts: **SENTINELONE_ALERT (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/sentinelone-alert-changelog)** Telemetry: **SENTINELONE_CF (https://docs.cloud.google.com/chronicle/docs/ingestion/parser-list/sentinelone-cf-changelog)**	• Threats • Storyline Active Response (STAR)™****

Trellix

Product	Minimum Version	Maximum Version	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Email Security (EX)*	9.1	10.0	Trellix Email Security Server Edition on-premises.**	N/A	• Trellix Alert Type: ◦ Malware Object
Email Security Cloud	N/A	N/A	Trellix Email Security Cloud Edition is software as a service application.	N/A	
Endpoint Security (HX)*	5.3	10.0	Trellix Endpoint Security can be deployed in on-premises, cloud, or virtual appliance configuration for Managed Defense service delivery.**	N/A	• Real-Time IOCs • Malware Protection*** • Malware Guard*** • Exploit Guard

Product	Minimum Version	Maximum Version	Description	Required SecOps Parsers	Managed Defense Supported Alert Types

Helix Security Platform	N/A	N/A	Trellix Helix Enterprise can be connected to Managed Defense service delivery by granting Managed Defense access to the instance through Trellix IAM.	N/A	• Helix alerts with the following tags:
					  ◦ MD-ACTION
					  ◦ MD-INFO
					• Helix alerts with the following tags are also covered for MD for OT customers:
					  ◦ ICS-ACTION
					  ◦ ICS-INFO

Network Forensics Packet Capture (PX)*	6.1	6.2	Trellix Network Forensics can be deployed on-premises or virtual appliance for Managed Defense service delivery.**	N/A	• Suricata Alerts (Mandiant rule package enabled)

Product	Minimum Version	Maximum Version	Description	Required SecOps Parsers	Managed Defense Supported Alert Types
Network Security (NX)*	9.1	10.0	Trellix Network Security can be deployed in on-premises, cloud, or virtual appliance configuration in either inline or passive modes for Managed Defense service delivery.**	N/A	• Trellix Alert Types: ◦ Domain Match ◦ Malware Callback ◦ Malware Object ◦ Web Infection ◦ Infection Match • Suricata Alerts (with optional Mandiant NTAP feature enabled)

* *Managed Defense follows the* ***End of Life Policy for Trellix Supported Technology (https://thrive.trellix.com/s/article/000013145)****. In general, this End of Life Policy typically means that the most recent two software revisions for each product are supported.*

** *Connection to the Managed Defense VPN is required for service delivery.*

*** *Alerts are leveraged for hunting and/or for additional context and do not adhere to Managed Defense Service Level Objectives*

*noted in the **Managed Defense Service Description** (https://docs.mandiant.com/home/md-service-description).*

Trellix Appliance VPN requirements

Managed Defense uses a Virtual Private Network (VPN) to connect to Trellix appliances. The following prerequisites must be met for Trellix appliances to connect to the Managed Defense VPN:

- The appliance is set up and connected to the network according to the *System Administration Guide* of the appliance.
- Secure Shell (SSH) or Intelligent Platform Management Interface (IPMI) access is configured on the appliance and accessible by an administrator. Refer to Using the IPMI Interface in the *System Administration Guide* of the appliance for directions on setting up IPMI.
- The appliance can initiate a connection to the network and port range corresponding to the country from which the service of your organization is delivered. Mandiant requires connectivity to the following TCP port ranges for United States:

Network Range	TCP Port Ranges
205.233.0.0/26	443 and 1200-1220

- Network Forensics and Network Security appliances must be configured to resolve public DNS.