Mandiant

ONBOARDING RESPONSIBILITIES

The table defines the responsibilities of the Managed Defense team and customers during onboarding:

Onboarding Phase	Managed Defense	Customer
Initialization		
Conduct Managed Defense Kick-Off Meeting	✔	
Provide user information for Mandiant Advantage Portal account creation		✔
Create new Mandiant Advantage Portal Users	✔	
Provision Managed Defense Portal API Clients (Optional)	✔	
Integrate with Managed Defense Portal API (Optional)		✔
Provide Managed Defense Service Documentation	✔	
Technology Enablement		
Deploy Supported Technologies for Managed Defense		✔
(Google Security Operations Only) Grant Managed Defense analysts access to Google Security Operations		✔
(Google Security Operations Only) Grant Managed Defense access to monitor data ingestion details by linking Google Cloud Project to Managed Defense		✔
(Microsoft Defender for Endpoint Only) Configure Azure Storage to receive data from Microsoft Defender for Endpoint (Customer is responsible for costs associated with the Azure Storage and data transfer)		✔
(Microsoft Defender for Endpoint Only) Configure Azure API permissions for Managed Defense as an MSSP for Microsoft Defender for Endpoint		✔
(SentinelOne Singularity Only) Provision and maintain Amazon S3 or Google Cloud Storage to export endpoint telemetry with Cloud Funnel		✔
(SentinelOne Singularity Only) Create API tokens for Managed Defense at Global or Account level		✔
(CrowdStrike Falcon Only) Create CrowdStrike Support ticket to make Managed Defense a parent of your CrowdStrike deployment		✔
(CrowdStrike Falcon Only) Create API key for Managed Defense access to Falcon tenant(s)		✔

Onboarding Phase	Managed Defense	Customer
Configure Supported Technologies for Managed Defense		✔
Provision Supported Technology for Managed Defense	✔	
Test Supported Technology Alerts	✔	✔
Endpoint Agents		
Install endpoint agent software on supported operating systems		✔
Configure Endpoint Groups and Services		✔
Perform Endpoint Services Testing	✔	✔
Authorize Managed Defense to Contain Endpoints (Optional)		✔
Finalization		
Confirm Onboarding Complete	✔	✔

Connectivity

This section summarizes customer roles and responsibilities for connectivity of supported technology.

- Provide information and remote access to enable the deployment of Managed Defense Supported Technology.
- Provide and maintain network connectivity between Managed Defense and Managed Defense Supported Technologies.
- Permit Managed Defense to access supported technologies to retrieve Security Alerts and Events.
- Address issues pertaining to lack of visibility within the monitored environment, such as loss of endpoint agent visibility, loss of network visibility, or unknown system traffic.

Mandiant recommends implementing strong network segmentation on security technologies connected to Managed Defense. Outbound connectivity from security technologies should be restricted to the minimum ports and protocols necessary.

Maintenance

This section summarizes customer roles and responsibilities for the maintenance of supported technology.

Managed Defense support for security technologies is currently categorized by the partnership agreements in place with various security vendors. The partnership agreements facilitate deep collaboration between the Managed Defense team and the vendor that can allow for deeper response and orchestration actions to be taken on behalf of customers. For example, host containment and file acquisition. These partnership agreements also clarify which alert, event, and log sources will be fully supported by Managed Defense.

- Customers must have an active software license and support contract for all Managed Defense Supported Technologies.
- Customers are responsible for ongoing maintenance, deployment, and management of Supported Technologies.
- Customers shall provide Managed Defense Consultant with at least 24 hours notice for planned network maintenance that may affect communications of Supported Technology with Managed Defense.
- Customers must identify and notify Managed Defense when changes within the environment may impact Managed Defense visibility and coverage. Managed Defense has no obligation to provide services for network segments and endpoints that are not visible to Managed Defense Supported Technology.
- Mandiant does not maintain backups of any supported security technologies connected to the Managed Defense service. Customers are responsible for all backups of all supported technologies connected to the Managed Defense service.

Customers are responsible for the rotation of credentials in authentication tokens provided to Managed Defense and must notify their Managed Defense Consultant (MDC) before changing any credentials. Failure to inform Managed Defense of new credentials may lead to a service delivery outage.