Ontinue

ONTINUE ION
SERVICE DESCRIPTION

Ontinue

Table of Contents

1. ABOUT THIS DOCUMENT

This service description of Ontinue ION provides you with a comprehensive overview of how the ION service helps you mitigate threats and reduce risk, leveraging the security tools you already own. This Service Description is part of and incorporated into the Master Services Agreement available at www.ontinue.com/msa or the agreement executed by and between Ontinue and Customer for ION Services ("MSA"). Notwithstanding anything to the contrary, Customer acknowledges and agrees that Ontinue may modify or update the ION Service over time to accurately reflect the services being provided, provided that any such modifications or updates do not materially degrade the security or function of the Services. Specifically, this document covers the following:

Section	Description
ION Components	An explanation of the component parts of the ION MXDR service, covering both the platform and the human teams.
ION Technology	The technology deployments and licenses that are either prerequisites or recommendations for using the service.
ION Service Launch	The details of how the service is operationalized for customers, designed to deliver value from the start.
ION Service Operations	How ION runs security operations, including the roles and responsibilities in daily, as well as emergency, scenarios.

2. ION COMPONENTS

ION Platform

The cloud-native platform that supports the ION MXDR service. The ION Platform contains the following key components:

- **ION for Microsoft Teams**: The Microsoft Teams interface through which customers interact with the ION service, including the ION Cyber Defense Center and Cyber Advisory.
- **ION Web Interface**: The web interface provides an alternative way to view ION dashboards and interact with the service, outside of ION for Microsoft Teams.
- **ION Automate**: The automation engine that is designed to auto close benign positives and automatically investigate and resolve true positives, to the extent possible.
- **ION IQ:** ION's proprietary artificial intelligence (AI), that serves both customers and Ontinue teams in executing and managing security operations more efficiently and effectively.
- **ION Cyber Defender Workbench:** an Ontinue tool that leverages ION IQ, automation, and more to increase efficiency and effectiveness of Ontinue's Cyber Defenders.

ION Cyber Defense Center

The ION Cyber Defense Center (CDC) is the 24/7 global security operation that supports the ION service. The CDC uses a "follow-the-sun" model to help ensure better responsiveness and customer satisfaction. Through such a model, all Cyber Defenders work during their daytime hours, with 24/7 coverage seamlessly shifting between different locations.

The CDC currently runs multiple Security Operation Centers (SOCs) as detailed on this page: https://www.ontinue.com/ion-mxdr-service/cyber-defense-center/

The CDC includes the following teams:

- **Cyber Defenders**: The security experts responsible for day-to-day incident handling and containment. These personnel are comparable to Tier 2/3 security analysts and engineers.
- **Advanced Threat Operations**: The Advanced Threat Operations team consists of threat intelligence (TI) specialists and expert threat hunters (TH).
    - **Threat Intelligence (TI)**: TI specialists monitor known and emerging threats to customers, keeping on top of the continuously changing threat landscape. As part of their mandate, the TI team curates the threat feeds that are used to drive better prevention and detection.
    - **Threat Hunters (TH)**: The TH team is tasked with running proactive threat hunts in customer environments.
- **Data Science**: The Data Science team consists of PhDs and other experts who build and train AI models on defender behavior. This team continuously identifies opportunities for process optimization and automation to make the Cyber Defense Center and the ION Platform faster, more effective, and more efficient.
- **Threat Detection**: The Threat Detection team designs and maintains the coverage model to help ensure customer environments are comprehensively protected. The team curates each control that ION leverages for threat detection and investigation, to ensure robust coverage while minimizing noise and costs.
- **Automation Engineers**: The Automation Team works closely with the Data Science, Threat Detection, and Cyber Defense teams to build and improve automation in the ION Platform.

ION Cyber Advisory

- **Cyber Advisors:** The Cyber Advisory team complements the CDC by providing ION customers with a trusted advisor to partner with on improving their security posture and maximizing the value of their security services.
- **Cyber Advisory Architects**: Cyber Advisor Architects bring deep technical expertise, in the Microsoft security space and beyond. They oversee Cyber Advisor processes and take the lead on key advisory activities.
- **Project Managers:** The Project Management team takes charge of the project coordination for the activation of the ION service. They work closely with the designated Cyber Advisor from kick-off through to the operational start of the ION MXDR service.
- **Vulnerability Management Team**: The Vulnerability Management team serves customers who purchase the Managed Vulnerability Mitigation add-on service. The team monitors customer environments, reporting on high-risk vulnerabilities given the specifics of the customer's IT environment.

3. ION TECHNOLOGY

The ION MXDR service uses a variety of technologies and security controls to effectively protect customer environments. Some of these are requirements, while others are recommended but not strictly required. It is the responsibility of the customer to procure the technology licenses and deploy the technologies listed as required below.

Technology License Requirements for ION

Technology required for ION	License and pricing	Comments
Active **Microsoft Azure** Tenant		Can be an Enterprise Agreement, "Pay as you go", or CSP.
Microsoft Sentinel	The details of Microsoft Sentinel pricing are available on the Microsoft Sentinel pricing page.	
Microsoft Azure Log Analytics	Details of Log Analytics pricing can be found on the Microsoft page.	
Microsoft Defender for Endpoint	Defender for Endpoint Plan 2 license	There are many Microsoft licensing SKUs that include the Microsoft Defender for Endpoint License Microsoft Defender for Server Plans 1 and 2 includes Microsoft Defender for Endpoint Plan 2. The full list of possibilities is detailed here.
Microsoft Entra ID [1]	Entra ID Plan 2 license	At a minimum, Entra ID P2 is required for a single user for Ontinue to access the M365 Defender console. Our recommendation is to have Entra ID P2 for all users. The details of this license are here.
Microsoft Teams	Included in many regions as a part of M365. If not, specific licenses for Teams are available.	Please note that a Shared Teams channel is required to operate the service and enable collaboration with Ontinue.

[1] formerly known as Azure AD

Technology Deployment Requirements for ION

Technology deployments required for ION
Endpoint Sensors: for the activation of the ION service, customers are responsible for the deployment of Defender for Endpoint on a sufficient number of endpoints to conduct initial baselining, estimated to be 80% coverage of Microsoft Defender for endpoints, or as otherwise agreed. Additionally, if endpoint sensors are not deployed on all endpoints (including servers) at the time of service launch, then it is required to have a clearly documented plan on how the deployment will be completed to 100% and share this with the Ontinue team.

Technology Recommendations for ION

Licenses	Comments
Microsoft Defender for Cloud	The details of pricing are available on the Defender for Cloud pricing page.
Microsoft 365 E5	Enables the ingestion of additional, recommended M365 security log sources/connectors, including Microsoft Entra ID Protection, Defender for Office 365, Defender for Identity, and Defender for Cloud Apps. These can also be licensed individually.

Technology Deployment Recommendations for ION

Technology deployments recommended for ION
Azure Monitor agent installed and configured on all customer Active Directory Domain Controllers

Microsoft Sentinel access permissions	
Enabling Microsoft Sentinel	Customers need **contributor** permissions to the subscription in which the Microsoft Sentinel workspace resides.
Using Microsoft Sentinel	Customers need either **contributor** or **reader** permissions on the resource group that the workspace belongs to.
Additional permissions may be needed to connect specific data sources.	

Note: Microsoft costs (including ingestion costs) are billed directly by Microsoft (or the CSP) and are not part of the ION service costs. Ontinue works with customers to analyze these costs (especially daily ingestion costs, which are a key factor) and make recommendations on how to optimize Azure consumption.

ION data residency and resiliency

ION is hosted in the Microsoft Azure availability zone of Switzerland North. For more details on Azure availability zones please see: https://azure.microsoft.com/en-us/explore/global-infrastructure/availability-zones

Azure Tenants and Workspaces

ION runs security operations based on a single customer tenant. To support customers who have multiple Azure tenants, ION onboards each of the customer tenants separately. This means, each tenant will have:

- A distinct set of Teams and Channels in Microsoft Teams.
- A distinct ION Web Interface with data and reporting specific to the individual tenant.

ION currently supports one Sentinel Workspace per tenant.

Security Controls and Log Sources Summary

The following table summarizes key security controls and log sources used by ION.

Category	Mandatory	Best-practice
Endpoint	**Defender for Endpoint – Plan 2 (Alerts)**	Defender for Endpoint device logs
Identity		Active Directory logs Microsoft Entra[1] logs Microsoft Entra ID Protection[2] Defender for Identity Critical identity logs
Cloud	**Azure Activity logs** **Office 365 logs**	Defender for Office 365 - Plan 2 Defender for Cloud Apps Defender for Cloud Critical cloud apps logs
Network		Any ASIM supported IDS, Proxy, DNS, and Firewall – includes security controls from Palo Alto, Zscaler, Cisco, Vectra, Checkpoint, ForcePoint, and more

[1] formerly known as Azure AD

[2] formerly known as Azure AD Identity Protection

Note: ION collects the minimum data types needed to effectively deliver the MXDR service. For details on precisely which data types are used currently, please contact the Ontinue team.

For more information on Sentinel entity types, please see: https://learn.microsoft.com/en-us/azure/sentinel/entities-reference

Log Sources

The ION service takes an approach where signal-to-noise ratio is prioritized, rather than total log sources. Log sources are categorized in the following manner:

Type	Purpose
Investigative	The high-fidelity log sources on which detection is based
Contextual	All other log sources, leveraged for context in threat hunting and investigations, but not directly for detection.

Investigative Log Sources

Investigative log sources are a foundational element of ION. These are the "sources of truth" on which detection logic is based.

Endpoint: A valuable investigative log source for the service is the endpoint. Microsoft Defender for Endpoint is the main source of endpoint telemetry. It provides visibility for fast analysis, operating continuously and reporting suspicious events. Defender for Endpoint can be configured to stop suspicious processes instantly or isolate a compromised machine, to prevent any kind of lateral movement. In addition, ION increases visibility with additional detection coverage using the raw device logs from Defender for Endpoint. When needed, these logs can also be searched for past incidents, increasing the effectiveness of response. Defender for Endpoint supports Windows, Mac OS and Linux, thus covering everything from desktops to servers. Microsoft Sentinel comes with an out-of-the-box connecter to 365 Defender, providing immediate integration with Defender for Endpoint.

Identity: Active Directory (AD) and Microsoft Entra (formerly known as Azure Active Directory) logs are highly recommended log sources for the service. They provide the needed visibility on identity, as well as to reinforce monitoring of domain controllers, which are critical assets. Additionally, Ontinue also recommends Microsoft Entra ID Protection and Defender for Identity, for the advanced identity coverage they provide. To enable log forwarding customers need to: update/confirm AD audit policy on all Domain Controllers (Ontinue will provide best practices for this), install and configure the Azure Monitor agent (AMA) using any relevant filtering provided by Ontinue.

Cloud, Apps, Email: Azure Activity and Office Activity logs are mandatory log sources, required to maximize visibility and ensure effectiveness of the service. Defender for Cloud is recommended to strengthen the security posture of customer cloud resources. Defender for Cloud Apps, as well as the raw logs of critical cloud apps (if there's a native connector to Microsoft Sentinel), are also recommended.

Working With Additional Log Sources

AAA Framework - Log Sources

To maintain solid signal-to-noise ratio, ION bases detection logic on a carefully curated set of log sources from Microsoft and other vendor security controls. This framework is termed "Triple A" and is used to assess all potential log sources. The framework assess:

Applicability: Does the source contain security relevant events and apply to the assets customers deem valuable?

Actionability: Does the source provide information that can guide responses?

Accuracy: Does the source have a high degree of accuracy?

Once a log source has been determined to meet the AAA standard, the next steps can be taken to ingest it's logs for use in security operations. The use of a log source can vary from serving as a contextual source or for threat hunting, through to serving detection use cases. Beyond the log source, every new detection use case also needs to meet the AAA standard.

Log Ingestion - Responsibilities

There are various ways, including REST APIs, to connect log sources with Microsoft Sentinel. Ontinue relies on customers to properly connect and maintain log sources. Customers are responsible for all setup work in their environment, including the deployment and configuration of agents. Once log data reaches Ontinue ION Log Analytics, Ontinue assumes responsibility for operationalizing the log data (subject to prior validation with the AAA methodology, the *Microsoft Sentinel Connectors* section of this document and the ION product roadmap).

Log Ingestion – Initial Set Up

If support is needed with connecting additional log sources at service launch, Ontinue Consulting Services can assist, at an extra cost. The costs of Ontinue Consulting Services for connecting additional log sources in customer environments are one-time costs at the time of service launch; there is no additional monthly cost from the ION service for additional log sources. This activity is quoted on a Time and Materials basis.

Log Ingestion – Ongoing Maintenance

Note that any custom log ingestion implementations will likely require ongoing maintenance, which if executed by Ontinue Consulting Services, will be billable as well.

Log Ingestion – Microsoft Sentinel Connectors

Changes to the log sources feeding into Microsoft Sentinel via connectors and parsers is often required. Microsoft, the community, and Ontinue release new connectors on a rolling basis. Customers can request assistance from Ontinue to implement new connectors. New connectors fall into these categories:

Deployment Effort Category	Description	Implementation and pricing
Easy	Native Azure log sources or CEF log sources	**Included in the ION service**
Medium	Syslog sources, API with an existing parser, community releases	**Included (on a best effort basis) in the ION service**, with the support of the customer, if the deployment effort is no more than 1 day
Challenge	Log sources that require custom parsers, Logic Apps, Rest API, or any connector requiring > 1 day of implementation effort	**Not included in the ION service** - These connectors are not included in the standard ION services and billed on a time and materials basis.

Log Ingestion - Optimization

ION provides visibility into Microsoft Sentinel consumption-related costs via dashboards. The service includes recommendations on how to optimize the data ingested into Microsoft Sentinel based on observations in monitoring the customer environment and the security relevance of the log data. Ontinue will implement AMA filters to support these observations for deployment in the customer environment. Any filtering activity that exceeds one day of implementation effort will be quoted on a time and materials basis.

ION Browser Compatibility

Ontinue recognizes ION users may have various Internet Browsers and Operating Systems. The aim is to provide the best possible experience when using the ION Web Interface, in a way that works consistently, efficiently, and effectively across the below listed web browsers.

Compatible Web Browsers
Microsoft Edge
Google Chrome
Apple Safari
Mozilla Firefox

For all the browsers listed above, the current and preceding browser versions are supported. If not listed above web browser compatibility is not ensured.

4. ION SERVICE LAUNCH

ION Service Launch Key Parties and Responsibilities

Key Party	Contact / Entity	Responsibilities
Ontinue ION	Project Managers	Ensures that the ION service launch advances swiftly, with key milestones successfully completed in a timely manner.
	Cyber Advisors	Ensures the correct technical implementation of the service, including guiding customers on configuration and setup. Jointly reviews with customer the applicable IT risks. Leads the guided technical setup call. Leads the process and procedures setup call. Provides a 1-hour ION Platform training session. Provides initial set of security observations, and recommendations, if applicable.
	Threat Hunters	Runs onboarding threat hunt to identify security hygiene issues, misconfigurations, and indicators of threat activity.
	Detection Engineers	Execute customer configurations, deploy analytic rules, and perform fine-tuning through to SLA handover. Evaluate requests for new log sources and/or use cases. Serve as Subject Matter Experts on maximizing the value of log sources.
Customer	CISO or Head of Security	Serves as the security strategy and IR policy owner. Provides approvals and drives onboarding forward from the customer side. Onboards third-party providers, e.g. legal advisors. Ensures all required technology is licensed and deployed.
	IT Security Operations	Ensures accuracy of Critical Asset inventory. Ensures accuracy of Escalation Matrix.
	IT Team or designated MSP/CSP	Serves as the Azure Global Admin for technical onboarding with Cyber Advisors and for access package approvals. Provides detailed information of the customer security environment for the ION service launch.

ION Service Launch Phases

Deployment of the Microsoft Sentinel workspace and onboarding is done with automation using the Ontinue CI/CD pipeline, Azure Marketplace, and an Azure Resource Manager (ARM) template. From a technical perspective, the ION service can be up and running with minimal effort and disruption to customer security teams or users by leveraging Azure Lighthouse. An onboarding guide provides detailed instructions to set up permissions, deploy Azure resources, and enable a select number of cloud-native connectors. On-premises log sources are connected to Log Analytics as described in the Log Ingestion section of this document.

Service launch typically takes 1 to 5 days to reach *Operational Start* of MXDR protection, from which it takes on average 10 business days to enter the fully operational phase of the service in which the Service Level Agreement is available (*SLA-start)*. ION launch milestones are as follows:

Phase	Description
Pre-kick-off Information Collection:	This can begin as soon as the contract is signed and involves collecting key information about the customer environment, including critical assets and log sources, as well as defining operational procedures, including the Rules of Engagement.
Kick-off & Platform Setup:	At the project Kick-Off, the Ontinue Sales Engineer will introduce the customer to the Ontinue Cyber Advisor. Together, the ION platform is connected to the customer environment and key operational parameters, such as lines of communication in case of an incident, are defined. **Outcome**: Both teams are introduced to each other, the service scope is clear, stakeholders are identified, communication lines are established. The customer's Microsoft Sentinel instance is created and connected to Ontinue ION through Azure Lighthouse. ION Access to the MS Defender for Endpoint is set up. ION for Microsoft Teams is connected to the customer environment.
Service Setup	Service parameters, such as the Rules of Engagement, Escalation Matrix, Asset Inventory and Governance setup are configured in an initial version. The Active Directory audit policy is potentially updated to conform to best practices. Log ingestion from DCs to Microsoft Log Analytics is validated and critical Microsoft log connectors are enabled. Additional configuration and installation occurs in the backend without need for customer interaction. **Outcome**: Service Setup is completed, and the customer's environment is ready for Operational Start.
Onboarding Threat Hunt	Onboarding threat hunts have been designed to drive immediate improvements to a new customer's security posture. The output produced is a hunt report, representing the first ION deliverable every customer receives. The report details identified security hygiene issues, highlights misconfigurations, and, most importantly, searches for any malicious activity that might be indicative of an ongoing compromise or threat activity.

	Outcome: Key opportunities to improve security posture are identified and reported on. Checks done in an effort to ensure customer is not in a state of breach. Note: To ensure effective baselining, it is important that customers are not in the middle of a significant, ongoing incident. If this is the case, it is required that customers engage appropriate professional services (not included in Ontinue ION), for the Ontinue ION Service Launch to continue.
Operational Start	The Cyber Advisor validates that ION is working as expected. **Outcome**: The customer environment is now under protection of Ontinue ION. In case of distress, the customer may raise critical incidents to the Ontinue Cyber Defense Center 24/7 through ION Engage. ION Threat Hunting begins proactively surfacing threats. The customer is included in briefings & alerts issued by the Ontinue Threat Intelligence Team. The Threat Detection Team commences work on continuous detection optimization & localization. The Cyber Defense Center responds to incidents triggered by the Threat Hunting and Threat Detection teams, as well as critical incidents raised through ION Engage.
Special Detection Optimization & Localization **Part 1 of 2**	Over the course of approximately 10 business days, alerts generated by the Microsoft Defender stack are optimized with respect to their signal to noise ratio to enable accurate and relevant detection of threats. Additional detection use cases leveraging further signal, such as Active Directory log data are configured and localized to the customer's individual environment. The Cyber Advisor coordinates localization efforts with the customer in weekly 1-hour calls. The customer provides feedback to questions on their environment to this end. **Outcome:** Curated set of use cases deployed and baselined. Escalation Matrix, Rules of Engagement, and Asset Inventory set up. The customer's environment is stable and ready for SLA (Service Level Agreement) start.
SLA-start	The Cyber Advisor enables alert-based incident handling in the Cyber Defense Center. Final validations of the end-to-end components of ION are performed. **Outcome:** Customer understands how to interact with the ION service. The Cyber Defense Center monitors and responds to alerts 24/7. SLAs now apply to the Ontinue ION service.
Special Detection Optimization & Localization **Part 2 of 2**	During an additional 10 business days, the ION service is further localized to the customer's environment (note service localization continues throughout the engagement on a recurring basis; this is a special effort to kickstart customers with a solid base localization). The Cyber Advisor coordinates localization efforts with the customer in weekly 1-hour calls. The customer provides feedback to questions on their environment to this end.

	Outcome: Curated set of use cases deployed and baselined. The customer's environment is stable and ready for the SLA (Service Level Agreement) start.

Microsoft Sentinel Access

ION gains authorized access to the customer's Microsoft Sentinel instance through Azure Lighthouse, which is based on Azure delegated resource management. With Azure delegated resource management, authorized Ontinue users can work directly in the context of customer subscriptions without having an account in, or being a co-owner, of the customer tenant. Data in transit as well as data at rest is encrypted. To onboard customer tenants, an active Azure subscription is required.

5. ION SERVICE OPERATIONS

Security Operations Key Parties and Responsibilities

Key Party	Contact / Entity	Responsibilities
Ontinue ION	ION Automation	Executes initial incident triage, investigation, and mitigation. Works on the continual reduction of benign positives. Executes mitigation and approved containment actions, and escalates incidents, as needed, to Cyber Defenders and customers.
	Detection Engineers	Design and maintain the coverage model designed to ensure customer environments are comprehensively protected. Curates the security controls and log sources that ION leverages for threat detection, to maximize coverage while minimizing noise and costs. Develop, deploy, and maintain detection use cases. Evaluate customer requests for new use cases.
	Cyber Defenders	Perform in-depth investigations. Execute mitigation and approved containment actions, and escalates incidents, as needed, to customers. Serve as the strategic contact on responding to identified incidents.
	Threat Hunters	Execute proactive threat hunting. Execute Requests for Hunts (RFHs).
	Cyber Advisors	Provide ongoing strategic recommendations to improve posture, based on observations in delivering the service. Lead Quarterly Security Improvement Reviews. Serve as the customer interface for the service in general. Ensure ongoing, correct technical implementation of ION.
Customer	CISO or Head of Security	Serves as the security strategy and IR policy owner. Provides approvals, serves as a key point of escalation. Onboards third-party providers, e.g. legal advisors. Serves as the link to a Steering Committee, if needed.
	IT Security Operations	Serve as the incident peer for Cyber Defenders. Take emergency decisions and provides verifications.

		Notify Ontinue of any environmental changes that may affect the execution of the ION service.
	IT Team or designated MSP/CSP	Perform updating and uninstallation of software components. Execute scanning of endpoints, in cases where it's been agreed that Ontinue does not handle the scanning. Perform end-user follow up and verification. Perform endpoint re-imaging, domain policy adjustments. Execute backup and restoration of data and systems.
Third Parties	Law Enforcement	Perform filing of global digital criminal complaints, as needed. Ensure prompt transmission to international parties and liaises with relevant authorities (e.g. INTERPOL).
	Forensics	Serve as an on-demand emergency contact. Perform analysis and recovery of hard drives and files. Gather evidence, ensures collaboration with law enforcement.
	Incident Response on Demand	Serve as an on-demand emergency contact. Deliver IR capabilities – e.g. large, on-site investigations.

Note: Ontinue is not a provider of Incident Response (IR) and forensics services. As detailed above, in the case that incident response and/or forensics is needed, that would be the responsibility of a third-party. Ontinue can recommend an IR provider in the customer's region if needed.

Threat Intelligence

Threat intelligence is the systematic gathering of information on current and potential cyber threats. To ensure Ontinue keeps on top of the latest threats to ION customers, the Ontinue Threat Intelligence team invests in and curates a range of intelligence feeds and tools. These may include the Recorded Future Intelligence Cloud, VirusTotal Enterprise, and more. The intelligence gathered by the team is leveraged throughout the ION service, including in informing threat hunts, detection use cases, and more.

Threat Advisories

One key output of Threat Intelligence is regular Threat Advisories. Threat Advisories are focused on new, high-impact, high-velocity, remotely executable threats. The intent of these advisories is to help customers proactively mitigate vulnerabilities that may impact their environments in cases where there is high likelihood of exploitation before regular patching cycles will address the vulnerabilities may apply. Advisories are also issued in the case where software or services used to deliver the ION service are found to be vulnerable, such as Defender for Endpoint vulnerabilities (where mitigation or patches can be applied). Where possible - Ontinue seeks to analyze the applicability of a particular advisory to a customer and identify impacted assets where that telemetry is available.

In case of a significant industry incident, the aim is to issue an initial Threat Advisory within 1 day. The Threat Advisory will be updated as and when there are additional security relevant developments.

Threat Detection

Holistic Coverage Model

The ION Holistic Coverage model focuses on the coverage of breach detection close to impact and actual damage, on extrusion as opposed to intrusion, all while building scalable and efficient threat detection. A guiding principle is achieving solid signal-to-noise ratio when expanding the coverage, while taking into consideration critical business assets, evolving TTPs, and the most common threats, such as phishing, ransomware, insider threat or zero-day exploits.

AAA Framework – Use Cases

To help ensure that signal-to-noise ratio is not compromised when expanding detection coverage, the AAA framework is used for all ION detection logic. Any use case included for monitoring in the ION service is assessed for:

Applicability: is it applicable to a given threat to a relevant asset?

Actionability: does it have clearly defined desired outcomes in runbooks/automation workflows?

Accuracy: is it of high fidelity in detecting malicious behavior?

The inclusion of use cases into ION is subject to the AAA requirements and to prioritization in the Detection Engineering roadmap.

Requesting New Use Cases

Customers can request new detection use cases via their Cyber Advisor. The Cyber Advisor will relay the details of the request, in a structured format, to the Threat Detection team for evaluation and potential implementation. New detection use case requests will fall into one of two categories:

- Based on an existing log source: use case will be evaluated against the AAA framework.
- Based on a new log source: log source will first be evaluated against the AAA framework. If the log source meets the standard, then work on log source ingestion follows. Thereafter, the use case will be evaluated against the AAA framework.

Scope Of Use Cases

Custom use cases are not part of the ION Service. ION supports detections released by Microsoft (for more details see the Adaptive Coverage section) and those developed, deployed, and managed by the Ontinue Threat Detection team.

Custom analytic rules and policies that are in the customer's Microsoft products are not applicable to the ION service, as these are beyond the control of ION.

ION Use Case Library

A comprehensive library of detection use cases is available upon request to customers upon request to their Cyber Advisor.

Adaptive Coverage

Adaptive Coverage delivers broader detection coverage, faster, by operationalizing new detection logic from Microsoft Defender products in near real-time. This enables customers to better leverage existing Microsoft security controls, as well as conveniently expand into new Microsoft security controls. Adaptive Coverage currently operationalizes signals from the following Microsoft Security products:

- Microsoft Defender XDR
    - Defender for Endpoint
    - Defender for Identity
    - Defender for Office 365
    - Defender for Cloud Apps
    - Microsoft Defender for Cloud
    - Microsoft Entra ID Protection

The architecture of Adaptive Coverage drives efficiency by operating largely within the customer tenant. Ontinue works to ensure new, potentially noisy detections don't disrupt operations by baselining new detections in a learning phase. This enables the Ontinue Threat Detection team to quickly validate the effectiveness of the new logic in actual customer environments, augmenting the logic as necessary. Once the accuracy threshold for use in SecOps is achieved, Adaptive Coverage takes the new logic live and it can be further enhanced with automated actions. The Ontinue Threat Detection team continues to monitor performance, with additional tuning executed as necessary.

Threat Detection Scenarios

By leveraging the Holistic Coverage model, ION covers a wide range of scenarios. This includes, but is not limited to:

Asset Category	Detection Scenarios
Endpoint	Detection of malicious software, ransomware activities and unusual or suspicious activities on the endpoints.
Identity	Identifying phishing attempts to obtain sensitive information, anomalous login activities, and unauthorized attempts to escalate user privileges.
Network	Anomaly detection for unusual network traffic patterns, detecting threats like network scanning, port scanning, C2 connections and data exfiltration.
Cloud	Monitoring of unauthorized access, exposure of sensitive data, security misconfigurations and anomalous activities in the cloud environment.

Threat Hunting

Threat hunting is the proactive effort of searching for signs of malicious activity in IT infrastructure that evaded existing security measures. It complements security operations in uncovering attacker techniques. Threat hunting is based on the logs ingested to Microsoft Sentinel. Thus, the scope of threat hunting is one factor to keep in mind when considering which logs to ingest into Microsoft Sentinel. For the best threat hunting results, our best practice is to use the set of "highly recommended" log sources detailed in the following table. Please note that threat hunting can only be done when the team has access to the minimum required set of logs.

There are two forms of threat hunting activity executed as part of the ION service:

Type of Hunting	Description
Structured	Performed at a minimum weekly, the threat hunting team designs a new threat hunt that targets notable exploits. The threat hunt looks for specific threat actor TTPs and the parameters of the hunt are determined using the latest threat intelligence. A report is then produced, that details the result of the threat hunt. The report is delivered either through the ION Dashboards or via the ION Advice Teams channel.
Continuous	Ontinue ION maintains a library of past threat hunts and performs these hunts on a regular schedule looking for signs of compromise. If malicious activity is detected, a report is provided and/or an incident is raised.

Incident Severity

Incident severity measures the impact a given incident might have on the business. The levels are as follows:

Incident Severity	Typical Example
Critical	Triggered using automation, customers can reach out to ION for situations that are critical and business impacting. A Critical Severity incident is defined as an incident that would render customer business operations non-operative and both the Customer and Ontinue are willing to commit resources 24x7 to resolve. (In Microsoft Sentinel, these are created and categorized as High severity).
High	Suspected lateral movement based on compromised account.
Medium	Malicious file execution on standard workstation, but no other suspicious activity.
Low	Potentially unwanted application detected.
Requests/ Informational	Questions about a specific incident or requests for additional information as well as any Microsoft Sentinel Incidents that triggered as Informational.

Determining Incident Severity

Incidents are initially classified using the severities established by Microsoft Sentinel. These are standard definitions that cannot be altered by either the customer or Ontinue. The SLA of all incidents is measured against the original Microsoft Sentinel categorization.

The severity of any incident may be promoted or demoted by either the customer (via the ION platform) or Ontinue, based on triage findings and/or other information.

Ontinue reserves the right to determine the final severity of any incident after analysis of the situation and discussion with the customer.

ION Automate

ION Automate is the proprietary automation engine built into ION to improve the speed and accuracy of security operations. It automates tier 1 activities by picking up incoming alerts, assessing the context surrounding the alert, then enriching the alert by checking a variety of data sources. These checks could be done using customer data sources (such as checking whether the device is managed or unmanaged through Microsoft Entra ID) or 3rd party data sources (such as checking if an IP or filehash is known to be malicious).

Capabilities of ION Automate

The following is a high-level list of actions ION Automate can either presently take:

Action
Running searches
Adding comments
Adding worknotes
Updating severities
Closing incidents
Running active response, including: • Defender for Endpoint's Automated investigation and response (AIR) • Isolating a host • Blocking an IoC • Restricting app execution • Running Antivirus

To the extent possible, ION Automate aims to fully resolve incidents, through to auto close. In cases where it's not possible to auto close an incident, ION Automate escalates the now enriched incident to the ION Cyber Defense Center for a Cyber Defender to work on.

In the case of a benign or false positive, ION Automate will add comments and close the incident, with the associated verdict and supporting evidence. In the case of a true positive, ION Automate will act and/or escalate the incident to the Cyber Defender.

Continuous improvement of ION Automate

The Ontinue Automation team works to continuously improve ION Automate, both by improving existing automations, as well as adding new automations.

Customers are informed when there are significant new improvements and/or additions to ION Automate. Additionally, customers can also request more information on ION Automate at any time from their Cyber Advisor.

Incident Escalation and Escalation Matrix

ION aims to minimize the number of security incidents escalated to the customer. When an incident does need to be escalated, ION follows the protocol jointly defined with the customer in the Escalation Matrix.

The Escalation Matrix defines the escalation contact(s) for the 4 incident severity levels: low, medium, high, and critical. Each contact has an associated email address and phone number, as well as their preferred medium of communication. The Escalation Matrix also captures the trigger for escalating notification to the next level. Typically, this will be following no response after a certain number of attempts to communicate with the contact.

The customer is responsible for ensuring the ongoing accuracy of the Escalation Matrix, including notifying their Cyber Advisor if changes need to be made.

Supported notification mediums are Microsoft Teams, phone, and email.

Incident Collaboration

ION improves effectiveness in SecOps by using Microsoft Teams to enable better collaboration between customers and Ontinue's Cyber Defenders. The rich set of capabilities provided by Teams, including chat, channels, video calls, notifications, screenshare and more, reduce the friction of working together. There's minimal adoption effort, given the wide range of platforms supported and existing familiarity with Microsoft Teams.

In addition to the direct messages and Teams channel that enable real-time and asynchronous collaboration, customers can also use ION ENGAGE.

ION ENGAGE serves as the go-to method for customers to escalate an issue, in case of an emergency, attack, or breach. Based on the information provided, ION ENGAGE creates a Teams meeting (including sending out the link to appropriate recipients) and creates an incident with the appropriate severity level.

Note: ENGAGE is only intended to be used for emergencies, attacks, or breaches.

Supported collaboration mediums are Microsoft Teams, phone, and email.

Incident Reporting and Tracking

The status and details of incidents are available to customers via the ION Platform. Beyond the ION Platform, customers can also consume incident reporting and tracking by having incidents synchronized to their internal ticketing systems.

ION Dashboards

The ION service includes situational awareness dashboards that summarize operational performance and provide visibility into security incidents. Several key areas are covered, including prevention, security posture changes, incidents, and cost. Dashboards are updated hourly.

For details on the ION Dashboards please see the ION User Guide.

ION Cyber Advisory

Cyber Advisor Role

Customers are assigned a **designated Cyber Advisor** from the start of their engagement with Ontinue. Cyber Advisors serve as a customer's trusted security advisor, guiding customers on security posture improvements and maximizing the value of security products and services. The ION Cyber Advisor role fully encompasses the common MSSP roles of Technical Account Manager (TAM) and Service Manager.

Interacting with Cyber Advisors

Cyber Advisors are reachable via ION for Microsoft Teams. On site visits to customers are charged on a time and material basis, and subject to availability.

As part of their role, Cyber Advisors adhere to the following Service Level Objectives (SLOs):

- One [1] business day for acknowledgement of a request.
- Two [2] business days to respond to requests with a detailed update and next steps.

In case of a cybersecurity incident, Cyber Advisors can provide a maximum of up to 3 days of support, working in conjunction with the customer's Incident Response provider. As part of this the Cyber Advisor can join daily customer incident war rooms and will serve as the liaison between all Ontinue teams in the Ontinue Cyber Defense Center and the customer.

Note: The Cyber Advisor support detailed above is only in case of a cybersecurity incident and cannot be used for other purposes.

The following table provides information on who to contact in different situations:

Situation category	Who to contact?	Example situations
Security incident / emergency	ION Cyber Defense Center	Suspected compromise
General security matters	Cyber Advisor	Questions on enabling Attack Surface Reduction (ASR) rules, updates to Escalation Matrix, questions on recent Threat Advisory
Non-security, ION service related	Account Manager	Questions on ION pricing and renewals, questions on Ontinue certifications

Cyber Advisor Responsibilities

The responsibilities of Cyber Advisor are defined in the Service Onboarding and Service Operations sections of this document.

Cyber Advisory Service Components

A quarterly Service Improvement Review focused on ways to improve security posture, including:

- A review of the improvements implemented in the previous quarter.
- Improvements planned for the upcoming quarter.
- The list of improvements that could not be implemented due to any blockers, and the corresponding list of mitigations.

A quarterly Operational Report that provides an overview of operational statistics, including:

- A prioritized list of security improvement recommendations, as agreed at the most recent Security Improvement Review.
- The threat landscape for the customer's sector.
- A threat hunting lookback and outcomes.
- Insights from Threat Intel.
- Key incidents and operational service metrics review.
- A detection coverage summary.

An automated monthly Action Report that tracks the recommendations customers need to act, decide, and communicate, with regards to their security program. Action reports include the following sections:

- Security Posture Recommendations.
- Threat Intelligence Insights.
- Threat Hunting Outcomes.

Ad-hoc Posture Improvement Tracking meetings that customers can request to discuss the implementation of recommendations made by their Cyber Advisor and/or any customer escalations to the Cyber Advisor.

6. ION UNIT METRIC COUNT

ION MXDR is licensed per unit. A unit is calculated as follows:

- 1 unit = 1 Authorized User (up to 5 devices per individual user licensed for Microsoft Defender for Endpoint).
- 1 unit = 1 server protected by Defender for Cloud / Servers.