Ontinue

ION FOR IOT SECURITY
SERVICE DESCRIPTION

Table of Contents

1. ABOUT THIS DOCUMENT

This service description of Ontinue ION for IoT Security provides an overview of how the service helps mitigate threats and reduce risk in Operational Technology (OT) environments. **ION for IoT Security is available exclusively as an add-on to customers of the ION Managed Extended Detection and Response (MXDR) service**. Upon ordering Ontinue ION for IoT Security, for the applicable term this service description is incorporated into the Master Services Agreement available at www.ontinue.com/msa, or if applicable the agreement executed by and between Ontinue and Customer for ION Services ("MSA"). Notwithstanding anything to the contrary, the Customer acknowledges and agrees that Ontinue may modify or update the ION for IoT Security service add-on 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: 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 for IoT Security Components	An explanation of the component parts of ION for IoT Security, covering both the platform and the human teams.
ION for IoT Security Technology	The technology deployments and licenses that are either prerequisites or recommendations for using the service.
ION for IoT Security Service Launch	The details of how the service is operationalized for customers, designed to deliver value from the start.
ION for IoT Security Service Operations	How ION for IoT Security runs security operations, including the roles and responsibilities on both the Ontinue and customer side.

2. ION FOR IOT SECURITY SERVICE

ION for IoT Security is **an add-on service to the ION MXDR service** and is centered on OT/IoT sensor telemetry. Together, the ION MXDR and ION for IoT Security services offer Ontinue customers unified protection of their IT, OT and IoT environments. ION for IoT Security customers also benefit from the Cyber Defense Center and Cyber Advisory services.

3. ION FOR IOT SECURITY SERVICE TECHNOLOGY

The ION for IoT Security service is based on telemetry from specialized OT/IoT sensors, which enables customers to discover, manage, and monitor OT devices across their organization. **It is the responsibility of the customer to procure the required technology licenses and deploy the required technologies**, as listed below.

Technology supported for ION for IoT Security

Vendor	Product	In-Scope Alerts
Microsoft	Defender for IoT	Alerts in the *Malware* and *Anomaly* categories. Alerts in the *Protocol Violation* category are also ingested to provide additional correlation and context during investigations. Alert types and categories are defined by Microsoft.
Claroty	xDome Continuous Threat Detection (CTD)	All alert types from the Claroty Threat Detection module which are part of the *Threat* category. Alerts from other modules and custom alerts are out of scope. The scope can be tailored per customer by excluding network types (Industrial, Corporate, Guest); all configured types are monitored by default. Alert types and categories are defined by Claroty.
Armis	Centrix for OT / IIoT Security	Alerts in the curated *ArmisAlerts* watchlist, maintained by the Ontinue Threat Detection team. Alerts from customer-defined custom policies are out of scope. Alert types and categories are defined by Armis.

4. ION FOR IOT SECURITY SERVICE LAUNCH

ION for IoT Security Service Launch Key Parties and Responsibilities

Key Party	Contact / Entity	Responsibilities
Ontinue	Cyber Advisors	Ensure the Escalation Matrix is updated to reflect any OT escalation contacts that might need to be included with the addition of the ION for IoT Security service.
Customer	CISO or Head of Security or equivalent	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. OT/IoT sensor deployment support partner. Ensures all required technology is licensed and deployed.
	IT Security Operations	Ensures accuracy of Critical Asset inventory. Ensures accuracy of Escalation Matrix, including the addition of OT escalation contacts. Ensures that the OT/IoT sensor configuration is based on Ontinue's and/or Ontinue's OT Alliance Partner best practices.
	OT Engineers	Provide detailed information of the customer OT environment for the ION for IoT Security service. Serve as an escalation contact when appropriate.
	IT Team or designated MSP/CSP	Serves as the Azure Global Admin for technical onboarding with Cyber Advisors and for access package approvals.

ION for IoT Security Service Launch Phases

ION for IoT Security customers benefit from a fast launch, as the service is built to leverage existing components from the ION MXDR service. For consistency, customers get the benefit of the same designated Cyber Advisor as the ION MXDR service and the same 24/7 Cyber Defense Center. The key launch milestones are:

Phase	Description	Supported by
Technology implementation	During this phase, the customer deploys the sensors at the relevant locations with support of Ontinue's Consulting Services team, Ontinue's OT Alliance Partner or a 3rd party deployment partner if required and for an additional cost.	Ontinue Consulting Services. Ontinue's OT Alliance Partner or 3rd party deployment partner
Service Setup	Service parameters, such as the Rules of Engagement and Escalation Matrix are configured. Ontinue will guide customers on which escalation criteria can be used to ensure the correct person is contacted in the event of a security incident in the OT environment. Relevant log connectors and playbooks are enabled. Additional configuration and installation occur in the backend without need for customer interaction. **Outcome**: Service Setup for ION for IoT Security is completed, and the customer's environment is ready for Operational Start.	Ontinue Cyber Advisory
Operational Start	The Cyber Advisor validates that ION for IoT Security is functioning. **Outcome**: The customer's OT environment is now under the protection of ION for IoT Security. In case of distress, the customer may raise critical incidents to the Ontinue Cyber Defense Center 24/7 through ION ENGAGE. The Ontinue Threat Detection team begins work on continuous detection optimization & localization. During this phase, the Cyber Defense Center responds to any incidents raised through ION ENGAGE.	Ontinue Cyber Defense Center
Calibrate and fine-tune	Alerts generated by the OT/IoT sensors are optimized with respect to their signal to noise ratio, to enable accurate and relevant detection of threats. **Outcome:** Curated set of use cases deployed and baselined. Escalation Matrix updated. The customer's environment is stable and ready for SLA (Service Level Agreement) start.	Ontinue Threat Detection team

SLA-start	The Cyber Advisor enables alert-based incident handling in the Cyber Defense Center. **Outcome:** The Cyber Defense Center monitors and responds to in-scope OT alerts 24/7. SLAs now apply to the Ontinue ION for IoT Security service.	Ontinue Cyber Defense Center

5. ION FOR IOT SECURITY SERVICE OPERATIONS

Key Party	Contact / Entity	Responsibilities
Ontinue	ION Automation	Executes incident enrichment and initial incident triage. Works on the continual reduction of benign positives. Escalates incidents, as needed, to Cyber Defenders and customers.
	Detection Engineers	Evaluate the OT/IoT sensor alert categories and alerts to be included in the scope of the ION for IoT Security service. This evaluation is done per sensor product.
	Cyber Defenders	Perform incident investigations. Escalate incidents, as needed, to customers. Serve as the strategic contact on responding to identified incidents. Provide containment recommendations, when possible, based on other preventive technologies that are in place.
	Cyber Advisors	Serve as the customer interface for the service in general. Ensure ongoing, correct technical implementation of all Ontinue services.
	Customer Operations Manager	Support Cyber Advisors with action tracking and non-technical activities in service delivery to the customer.
	Account Manager	Questions on pricing and renewals.
Customer	CISO or Head of Security or equivalent	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 provide verifications. Notify Ontinue of any IT environment changes that may affect the execution of the ION MXDR service.
	OT Engineers	Serve as the incident peer for Cyber Defenders, in the case of incidents affecting OT environments. Take emergency decisions and provide verifications, in the case of incidents affecting OT environments. Notify Ontinue of any OT environment changes that may affect the execution of the ION for IoT Security service.

Third Parties	Law Enforcement	Perform filing of global digital criminal complaints, as needed. Ensure prompt transmission to international parties and liaise 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 any of the services listed under "Third Parties". In case any such service is required, for example Incident Response, that would be the responsibility of a third party. Ontinue can recommend an Incident Response provider in the customer's region if needed.

Incident Escalation and Escalation Matrix

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

The Escalation Matrix defines the escalation contact(s) based on various criteria, including incident severity. Each escalation 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 and availability of contacts included in the Escalation Matrix, including notifying their Cyber Advisor/Customer Operations Manager if changes need to be made. **The ION for IoT Security service uses the same Escalation Matrix as the ION MXDR service. Thus, OT specific escalation contacts should be integrated into the Escalation Matrix, using the supported escalation criteria to ensure the correct person is reached.**

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

The process of incident collaboration, reporting, and tracking, as well as interaction with Cyber Advisors, is the same as the ION MXDR Service. The processes are described in detail in the ION MXDR Service Description, available at: https://www.ontinue.com/service-descriptions/

6. ION FOR IOT SECURITY LICENSING MODEL

Please refer to the ION License Guide for details: http://ontinue.com/ion-license