Ontinue

ION FOR DIGITAL FORENSICS & INCIDENT RESPONSE **SERVICE DESCRIPTION**

Table of Contents

1. ABOUT THIS DOCUMENT

This service description of Ontinue ION for Digital Forensics & Incident Response (DFIR) Service provides an overview of how the service extends the ION Managed Extended Detection and Response (MXDR) Service by providing enhanced incident response and digital forensic capabilities that extend beyond the MXDR service scope. **Ontinue ION for DFIR is available exclusively as an add-on to the Ontinue ION MXDR Service**. Subject to ordering and payment of applicable fees, this Ontinue ION for DFIR Service description is incorporated into the Master Services Agreement available at www.ontinue.com/msa for ION MXDR Services ("MSA"). The services delivered by Ontinue's DFIR alliance partner are governed by the agreement established directly between Customer and partner, available via link or included as an attachment in Customer's order with Ontinue.

Notwithstanding anything to the contrary, Customer acknowledges and agrees that Ontinue may modify or update the ION for DFIR Service over time, provided that any such modifications or updates do not materially degrade the security or function of the ION for DFIR Service.

This document covers the following:

Section	Description
ION for DFIR Service	A high-level explanation of the ION for DFIR service.
ION for DFIR Technology	The technology deployments and licenses that are either prerequisites or recommendations for using the service.
ION for DFIR Service Launch	The details of how the service is configured and deployed for Customers, designed to deliver value from the start.
ION for DFIR Service Operations	How ION for DFIR operates, including the responsibilities on both the Ontinue, Partner and Customer side.

2. ION FOR DFIR SERVICE

ION for DFIR is an add-on service to the ION MXDR service that enables enhanced capabilities to handle high-impact security incidents. With ION MXDR, Customer receives detection, investigation, and response for security incidents generated by Ontinue's and Microsoft's advanced threat detection. **The ION for DFIR service extends the 24/7 response capabilities to enhanced incident response and digital forensics used for rare high-impact security incidents, alleviating the need for Customer's security teams to engage multiple service providers during these events.** For the vast majority of security incidents, the containment actions delivered through Ontinue's ION MXDR service are fully sufficient to effectively remediate always evolving security incidents and prevent any further impact. For rare, high-impact security incidents that require a deeper level of forensics and response, Ontinue offers the ION for DFIR service delivered in collaboration with hand-picked specialist partners. This approach brings together Ontinue's ION MXDR service - delivering continuous, real-time detection, investigation, and proactive threat containment - with the advanced forensic expertise of Ontinue's DFIR alliance partners. Through hands-on experience, state-of-the-art forensic laboratories, evidence preservation, and close collaboration with law enforcement, Ontinue's DFIR alliance partners ensure that even the most complex and high-impact security incidents are managed with effectiveness and confidence.

A rare, high-impact security incident refers to an exceptional event that has the potential to significantly disrupt business operations, compromise sensitive data, or otherwise extend beyond the scope of routine MXDR response. Such confirmed true-positive incidents may include, for example, lateral movement, compromise of multiple privileged identities or directory services, or ransomware activity.

Ontinue's ION for DFIR service covers all IT systems that are operated directly by Customer, by an outsourcing partner on behalf of Customer, or by a service provider for Customer. This includes SaaS, PaaS, and IaaS solutions, provided the security incident in question impacts IT systems in use and under Customer's direction or control. Please note that the service does not extend to providing DFIR support for incidents that occur entirely within an outsourcing partner's or service provider's own environment.

3. ION FOR DFIR TECHNOLOGY

The ION FOR DFIR service uses a variety of technologies to precisely and swiftly handle high-impact security incidents in cooperation with Ontinue's DFIR alliance partner and Customer. **In addition to technologies required for the ION MXDR service and depending on which Ontinue DFIR alliance partner is providing Customer with the DFIR services, there may be specific deployments or licenses required.** Such deployments and licenses are defined in Ontinue's DFIR alliance partners service description.

4. ION FOR DFIR SERVICE LAUNCH

The ION for DFIR service add-on service leverages the Microsoft Teams-based collaboration interfaces, and delivery teams of Ontinue's ION MXDR service and is enhanced by Ontinue's DFIR alliance partners specialists.

The same service launch roles and responsibilities as the ION MXDR core service (detailed in the ION MXDR Service Description) hold true for the ION for DFIR service add-on, with the addition of the responsibilities specified below:

Key Party	Contact / Entity	Launch Responsibilities
Ontinue ION	Customer Operations	Ensure that the ION for DFIR service launch advances swiftly, with key milestones successfully completed.
	Cyber Advisors	Ensure the correct update of Teams channel configuration as well as Escalation Matrix and Rules of Engagement. Participate in workshops to provide ION MXDR service insights.
Ontinue's DFIR Alliance Partner	DFIR Specialist	Serve as the contact for all technical DFIR requests. Lead the initial kickoff, one-day DFIR workshop and half-day tabletop exercise. Responsible for initial kickoff, one-day DFIR workshop and half-day tabletop exercise outcomes and documentation.
Customer	CISO or Head of Security or equivalent	Provides details of who is authorized to invoke the DFIR service.
	IT Security Operations	Participate in workshops to provide Customer environment insights.

Service Launch Phases

Service launch typically takes 15 business days from the Initial Kickoff to enter the fully operational phase of the service, from which it takes on average 5 business days to execute the final tabletop exercise. ION for DFIR launch milestones are as follows:

Step	Launch Responsibilities
The following steps are completed during the onboarding phase.	
Initial Kickoff	Initial workshop with Ontinue's Cyber Advisor and Customer Operations Manager, Ontinue's DFIR alliance partner specialists and Customer. It begins with team introductions and alignment, followed by a detailed overview of the agreed service scope.
One-Day DFIR Workshop	The session provides an initial assessment of the Customer's DFIR readiness, reviews incident response and escalation procedures, outlines key communication channels and operational workflows, and concludes with a summary of key findings and outcomes.
ION Teams Configuration Update	A dedicated Microsoft Teams channel is established for delivering the ION for DFIR service. The channel is accessible to Customer, Ontinue, and Ontinue's DFIR alliance partner to ensure seamless collaboration and communication.
Engagement and Escalation Update	Operational procedures for ION MXDR are extended to include Ontinue's DFIR alliance partner in the Escalation Matrix, enabling direct and timely escalation of high-impact security incidents to DFIR specialists.
End-to-End Test	The Cyber Advisor validates that ION for DFIR is operating across the entire end-to-end process.
Half-Day Tabletop Exercise	A technical tabletop exercise is conducted designed to train cross-functional teams in coordinated incident response.

5. ION FOR DFIR SERVICE OPERATIONS

The same ongoing operational roles and responsibilities as the ION MXDR core service (detailed in the ION MXDR Service Description) hold true for the ION for DFIR service, with the addition of the responsibilities specified below.

Key Party	Contact / Entity	Ongoing Operational Responsibilities
Ontinue ION	Cyber Defenders	Escalate high-impact security incidents, as needed, to Ontinue's DFIR alliance partner. Work with Ontinue's DFIR alliance partner to provide further investigation details as required. Execute response actions based on Ontinue's DFIR alliance partner recommendations as required.
	Threat Hunters	Execute threat hunting for high-impact security incidents based on recommendations provided by Ontinue's DFIR alliance partner.
	Detection Engineers	Maintain and enhance detection use cases in alignment with Ontinue's holistic detection coverage model, incorporating recommendations from Ontinue's DFIR alliance partners.
	Customer Operations	Ensure close collaboration between Ontinue, Ontinue's DFIR alliance partner, and Customer.
Ontinue's DFIR Alliance Partner	DFIR Specialist	Lead the annual half-day DFIR review workshop. Responsible for annual half-day DFIR review workshop outcomes and documentation. Provide and coordinate in-depth DFIR investigations, including timeline, determination of the attack path, indications of other affected objects, identification of IoCs and indications of data exfiltration.

		Provide status updates for management of Customer. Coordination and support of analysis tool installation. Responsible for in-depth DFIR investigations outcomes and documentation.
Customer	CISO or Head of Security or equivalent	Decide if advanced digital forensics & incident response services are invoked after Initial Security Incident Assessment.
	IT Security Operations	Notify Ontinue of any IT environment changes that may affect the execution of the ION for DFIR service. Participate in workshops to provide Customer environment insights.
	IT Team or designated MSP/CSP	Acts as the primary contact for the technical deployment of required IT forensics and incident response tools during high-impact security incidents.

Digital Forensics & Incident Response Standards and Methods

The service is based on proven standards and checklists, complemented by proprietary methodologies developed by Ontinue's DFIR alliance partner.

Depending on the nature of the high-impact security incident and specific Customer requirements, recognized standards and frameworks such as ISO, BSI, NIST, the ISECOM OSSTMM, and vendor-specific hardening guidelines (e.g., from Microsoft) are applied. To ensure the highest quality standards, team members from Ontinue's DFIR alliance partner hold relevant academic degrees and industry-recognized certifications in digital forensics and incident response.

Scope of Digital Forensics & Incident Response Operations

Step	Service Responsibilities
Initial Security Incident Assessment	Ontinue's Cyber Defense Center escalates and engages Ontinue's DFIR alliance partner and Customer in case of high-impact security incidents as defined in the Escalation Matrix. To enable swift collaboration, a Microsoft Teams meeting is used, which is joined by

	the responsible Cyber Defenders from Ontinue's Cyber Defense Center, the DFIR specialists of Ontinue's DFIR alliance partner within one (1) hour. Additionally, the dedicated shared Microsoft Teams channel can be used for communication. If Ontinue escalated the incident on behalf of Customer, Customer receives 60 complimentary minutes per case for an initial assessment provided by Ontinue's DFIR alliance partner, free of charge. Ontinue's Cyber Defense Center provides required information to Ontinue's DIFR alliance partner to allow an initial but detailed assessment. After the initial 60-minute assessment, Customer decides whether further digital forensics & incident response services are required.
Full Security Incident Assessment	Once a Full Security Incident Assessment is approved by Customer, further remote support is provided by the alliance partner. Depending on which Ontinue DFIR alliance partner is providing Customer with the DFIR services, there may be specific deployments or licenses for further digital forensics and incident response required. When an on-site engagement is requested, the DFIR alliance partner will be dispatched to a mutually agreed Customer location, established in advance.
Annual Half-Day DFIR Review Workshop	The annual half-day DFIR review workshop includes a review of interfaces and readiness, as well as a tabletop exercise to ensure that training is ongoing and interface definitions are up to date. Note: An annual half-day DFIR review workshop is conducted starting in the second year of service.

6. ION FOR DFIR FEES

The fees charged for ION for DFIR are independent of the number of Ontinue Units that Customer has procured for their subscription of the ION MXDR service. Excluding any initial 60-minute complimentary assessment to which Customer is entitled, any DFIR services performed by the DFIR alliance partner will be charged on a time and materials basis, per 15-minute increment. All fees are payable to Ontinue for the DFIR services.