IDC Link
Real-Time IDC Research® Opinion on Industry News, Trends, and Events

Ontinue Raises the Bar for SOC Automation

June 12, 2025

By: Cathy Huang, David Clemente, Craig Robinson

IDC'S QUICK TAKE

Ontinue's use of deterministic and agentic AI for incident investigation represents a leap forward in MDR capabilities. This innovation not only improves the speed and consistency of threat detection and incident investigation but also empowers security teams to focus on strategic initiatives, ultimately driving better business outcomes.

PRODUCT ANNOUNCEMENT HIGHLIGHTS

From day 1, Ontinue has architected its ION SecOps platform to ensure that AI and automation are central to every aspect of its security operations center (SOC) activities. This includes capturing every action taken by its defenders, such as mouse clicks during investigations and triage processes. This meticulous data and context collection allows Ontinue to continuously refine and enhance its own AI — ION IQ, ensuring that its SOC operates at peak efficiency.

The recent production announcement — regarding autonomous investigation — is the result of using deterministic automation and agentic AI to handle complex tier 2 and tier 3 SOC investigative tasks. This reduces the time and effort required by human analysts to process incidents. Ontinue's ION SecOps platform was designed to help mitigate what Ontinue sees as two main areas that the security industry has struggled to automate:

- Incident escalation and response — largely due to nuances in the way that each organization wants (or needs) to respond, plus their tolerance for allowing vendors into their environment
- Novel, multi-phased incident investigation — where deterministic automation tends to be less effective

Ontinue's Smart Response system further enhances its response capabilities by providing a highly customizable and automated escalation matrix. This ensures that incidents are routed to the right personnel at the right time, based on predefined criteria, and that responses are tailored to each customer's operational model.

To aid with the prevention of future threats, the ION IQ Assistant, integrated into Microsoft Teams, offers real-time insights and recommendations for posture hardening, acting as an automated cyberadvisor.

IDC #lcUS53574125

IDC'S POINT OF VIEW

Recognized in *IDC MarketScape: Worldwide Emerging Managed Detection and Response Services 2024 Vendor Assessment,* Ontinue has distinguished itself through innovation and strategic market segmentation. Spun out in 2023 from its parent company Open Systems, the company has experienced remarkable growth and expanded its customer base and its team across three continents.

Strategic Market Segmentation

Ontinue targets customers that have chosen to standardize on Microsoft's XDR, Defender, and Sentinel offerings, especially those that cannot afford to have a big in-house cybersecurity team. This decision is rooted in its mission to reimagine security operations (SecOps) and address fundamental challenges that many organizations face, including too many products and portals, incompatible tools, and understaffed and/or overworked analysts.

This strategic focus allows Ontinue to maximize client ROI on existing Microsoft investments, reduce tool sprawl, and provide a more consistent and efficient security solution for its clients. It is worth noting that the way its customers interact with its services — including with Ontinue's cyberadvisors and defenders — is primarily through Microsoft Teams (for organizations that do not use Microsoft Teams, Ontinue provides a web-based interface to engage with the service).

Differentiations

Every Ontinue customer is assigned a dedicated cyberadvisor upon onboarding. This cyberadvisor takes the time to thoroughly understand the client's environment, including their business operations, risk posture, and stakeholders. The cyberadvisor is responsible for helping curate prevention tactics and posture recommendations for each client. IDC recognizes that the targeted customer size segment that Ontinue focuses on desires to work with cybersecurity providers that understand their organizations' IT and cybersecurity capabilities. Having a trusted partner that can help them meet the ever-changing threat environment is a desired outcome.

On the detection and response front, Ontinue employs a team of cyberdefenders — highly trained security analysts — who operate 24 x 7 around the clock.

Ontinue's agentic AI and automation is a cornerstone of its incident escalation and response strategy. It enables a level of automation for context gathering that was previously highly laborious or unattainable. Unlike other vendors, Ontinue is taking a more generalist approach, rather than use case specific. Its AI autonomously investigates incidents, providing enriched data and insights before human analysts even begin their work. This not only speeds up the investigative process but also ensures that analysts

have a comprehensive understanding of each incident, leading to more informed decision-making.

In addition to the technical requirements of SecOps, Ontinue has also given thought to reporting, and offers a suite of persona-based dashboards integrated into Microsoft Teams. On its near-term road map, Ontinue is building a template for exporting data into a management-friendly board reporting document or creating custom reporting templates.

Subscriptions Covered:

Cybersecurity Consulting and Professional Security Services, European Security Services, MDR and Managed Security Services