Ontinue

ONTINUE IOT SECURITY
SERVICE DESCRIPTION

Ontinue IoT Security provides 24x7 threat monitoring, detection and response services specifically designed for IoT/OT environments. To activate and benefit from this service, in addition to the Ontinue ION service technology prerequisites (detailed earlier in this Service Description), you are required to license and deploy the Microsoft Defender for IoT system, ensure the Defender for IoT sensors are cloud enabled, and provide Ontinue access to the Defender for IoT Portal, so that alerts can be properly triaged. The Microsoft Defender for IoT system includes the following components, which must be deployed prior to commencement of service:

- The Defender for IoT Azure Portal
- Network Sensors – deployed on either a VM or physical appliance and cloud connected
- An embedded security agent (optional)

Following an onboarding phase where Cyber Defenders ensure appropriate configuration and baselining of the service, Ontinue monitors your IoT/OT environment using this solution and follows the "AAA" methodology described in this document to ensure the highest fidelity alerting possible. The Microsoft solution produces alerts in 5 categories and detection coverage is as follows:

Alert Category	Description	Ontinue Coverage
Malware	Triggered when the Malware engine detects malicious network activity. For example, the engine detects a known attack such as Conficker.	Covered including ticket generation, requires baselining and subject to AAA methodology.
Anomaly	Triggered when the Anomaly engine detects a deviation. For example, a device is performing network scans but isn't defined as a scanning device.	Covered including ticket generation, requires baselining and subject to AAA methodology.
Protocol violation	Triggered when the Protocol Violation engine detects packet structures or field values that don't comply with the protocol specification.	The alerting is used for correlation and context during investigations only.
Policy violation	Triggered when the Policy Violation engine detects a deviation from traffic previously learned.	Not included.
Operational	Triggered when the Operational engine detects network operational incidents or a device malfunctioning.	Not included.

Ontinue investigation and response capabilities are limited to information provided in Microsoft Sentinel. Microsoft Defender for IoT is deployed in a passive network sensor by design to ensure no interference with sensitive and critical OT system components. Ontinue will provide containment recommendations based on other preventive technologies owned by the customer where possible.