DATASHEET

CRITICAL**START**® MDR for Operational Technology

Gain comprehensive visibility and threat detection across your IT and OT environments.

KEY BENEFITS

- ✓ Gain broad visibility and threat detection across IT and OT environments
- ✓ Reduce financial and operational risks associated with cyber threats targeting critical processes
- ✓ Scale your OT security with a cost-effective solution that grows with your needs
- ✓ Benefit from 24x7x365 monitoring, threat detection, and response backed by experienced security professionals
- ✓ Respond to threats anywhere, at any time, with the Critical Start MOBILE**SOC**® app
- ✓ Ensure the operational integrity of your OT environment with tailored Rules of Engagement that keep IT and OT responses separate

The need for increased visibility in the era of IT/OT convergence.

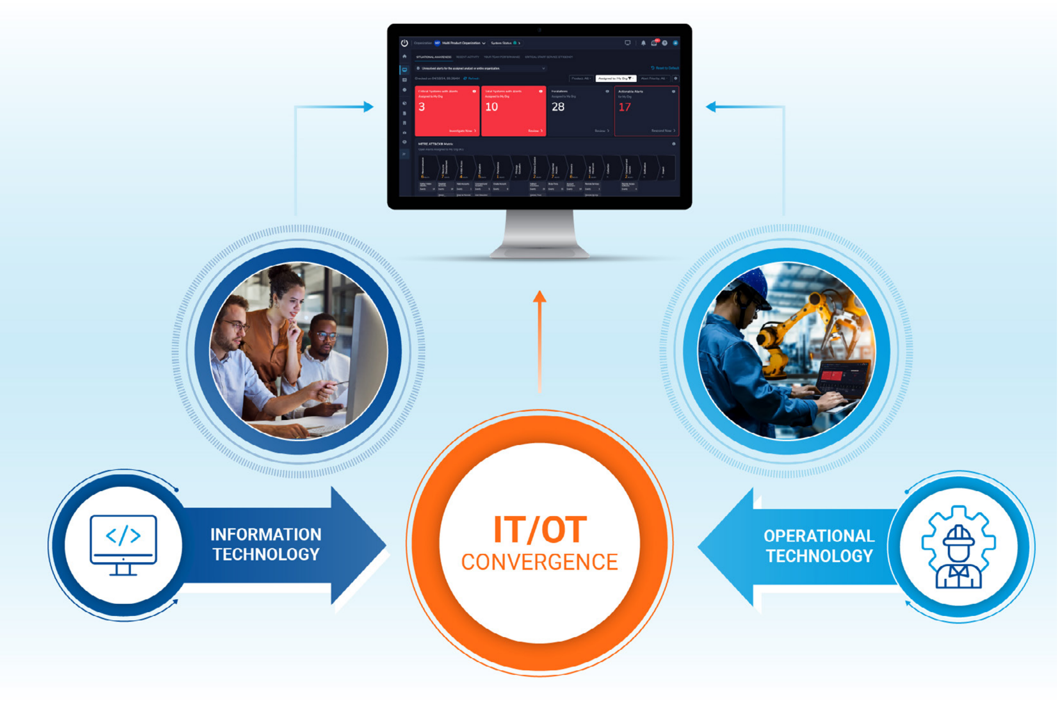
As Internet Technology (**IT**) and Operational Technology (**OT**) systems become increasingly interconnected, the attack surface for cyber threats expands, putting critical industrial processes at risk. Organizations need a solution that provides end-to-end visibility, 24x7x365 monitoring, and expert threat detection and response across both IT and OT environments.

We monitor and help you protect your industrial operations from cyber threats.

Critical Start Managed Detection and Response (MDR) for OT is a comprehensive solution tailored specifically for industrial organizations with Operational Technology and Industrial Control Systems (**ICS**). Backed by a team of experienced security professionals, our MDR for OT solution enhances your security posture by providing the holistic visibility you need for more effective threat detection and response across your IT and OT environments.

Critical Start MDR for OT leverages existing data sources across the Purdue model and offers flexible service tiers to accommodate different levels of OT security maturity This enables industrial organizations to reduce financial and operational risks associated with cyber threats targeting their critical processes.

Critical Start MDR Services for Operational Technology



How it works.

Critical Start MDR for OT collects, aggregates, and analyzes log data from various sources within your OT environment, such as Windows hosts, firewalls, switches, and EDR/EPP solutions, as well as dedicated OT security tools like Dragos, Claroty, and Nozomi. Our **Cyber Operations Risk & Response™** (**CORR**) **platform** normalizes this data and correlates it with threat intelligence to identify potential security incidents.

Flexible service tiers to support your OT security journey.

Built as part of CORR, Critical Start MDR for OT offers two service tiers designed to support organizations at different stages of their OT security maturity:

- **Base:** Monitor your OT environment using existing infrastructure (Windows hosts, firewalls, switches, etc.) as data sources, along with any IT security tools (EDR/EPP) deployed in the OT environment.
- **Extended:** Adds support for dedicated OT security tools (Dragos, Claroty, Nozomi, Otorio, Armis, Microsoft Defender for IOT, etc.) to provide even greater visibility and threat detection capabilities.

Our holistic approach allows you to address challenges related to OT security monitoring, threat detection and response, and compliance, all backed by industry-leading SLAs and the expertise of our security professionals.

Key Features

- 24x7x365 continuous monitoring of IT and OT environments by experienced security professionals
- Customizable alerting and escalation workflows to ensure timely notification and response
- Seamless integration with leading OT security tools for enhanced visibility
- Custom detections for high-priority use cases (IT/OT boundary traversal, network segmentation violations, etc.)
- Aggregated reporting and real-time dashboard visibility across all industrial operations
- Consolidated reporting for a holistic view of your OT security posture
- Multi-tenancy and role-based access control for segmented security views
- Hierarchical organizational views for individual plants, facilities, and geographies, plus roll-up unified views at the global level

Why Critical Start MDR for OT?

Critical Start MDR for OT is designed to address the unique security challenges faced by industrial organizations in the era of IT/OT convergence. By combining 24x7x365 monitoring, threat detection, and response capabilities with flexible deployment options, our service empowers you to protect your critical operations from both known and unknown cyber threats.

Our team of experienced security professionals continuously monitors the latest threat intelligence and adapts our detection and response strategies to keep your organization one step ahead of potential attackers. With Critical Start MDR for OT, you can focus on driving your business forward, confident that your industrial operations are protected by a leading security solution that delivers the greatest cyber risk reduction per dollar invested.

Contact us to learn more about protecting your industrial operations

From gaining visibility into your OT environment to detecting and responding to threats, we're here to support you at every stage of your OT security journey. Benefit from a leading MDR service, customized integrations, and unwavering commitment to your success as you navigate the complexities of securing your converged IT/OT infrastructure.

Schedule a customized demo to see how Critical Start MDR for OT can help you protect your industrial operations from cyber threats.
www.criticalstart.com/contact/request-a-demo/

CRITICALSTART®