DATASHEET

CRITICAL**START**® MDR for Operational Technology

Gain end-to-end visibility and threat detection across your IT and OT environments.

KEY BENEFITS

- ✓ **Comprehensive protection**
  End-to-end visibility and threat detection across IT/OT environments
- ✓ **Scalable monitoring**
  Manage and monitor large and complex operations with location-specific alert segmentation
- ✓ **24x7x365 security**
  Round-the-clock monitoring by experienced security professionals
- ✓ **Mobile responsiveness**
  Address threats anywhere, at any time, with the Critical Start MOBILE**SOC**® app
- ✓ **Tailored IT/OT separation**
  Maintain operational integrity with read-only visibility and customized engagement rules
- ✓ **Enhanced tool integration**
  Maximize existing OT-specific security tool investments
- ✓ **Predictable costs**
  Simplify budgeting with flat-rate pricing
- ✓ **Operational alignment**
  Customize alerting and response workflows to match specific operational needs
- ✓ **Improved reliability**
  Deliver timely, actionable alerts to appropriate personnel

Monitor and protect industrial operations from cyber threats and internal incidents.

As Internet Technology (**IT**) and Operational Technology (**OT**) systems converge, the cyber threat landscape expands. **Critical Start Managed Detection and Response (MDR) for OT** provides 24x7x365 visibility and protection across your IT/OT environments, safeguarding critical industrial processes.

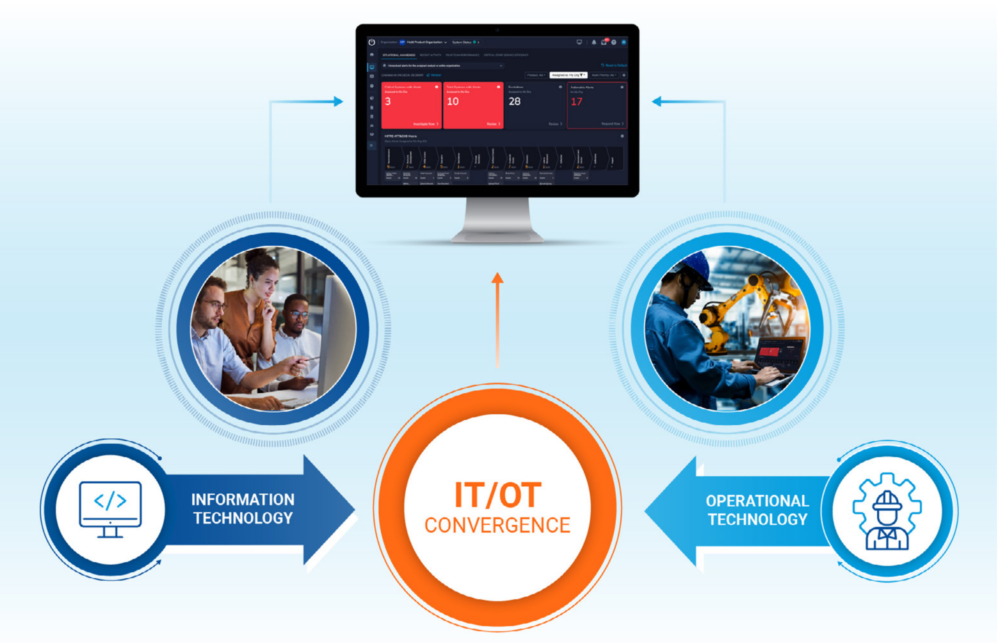
MDR for OT can be configured across multiple physical locations, separating IT and OT alerts for differentiated IT/OT threat detection and response handling. By delivering end-to-end visibility and monitoring, risk management and reduction through OT-specific threat analytics, and strict Rules of Engagement (**ROE**) guaranteeing read-only visibility, organizations can make informed decisions and continuously optimize defenses against human error and cyber threats.

Build defensible and cyber-resilient Industrial Controls System (ICS) networks.

Use Critical Start MDR for OT to be alerted to threats, including:

- OT segmentation violations (Boundary Traversal)
- OT systems accessed from the Internet
- Vulnerable OT device network compensating control monitoring
- Secure remote access usage violation
- Malware on OT servers/workstations
- Unapproved OT configuration changes
- OT configuration changes linked to IT systems accessing OT

Critical Start MDR Services for Operational Technology



How it works.

MDR for OT provides out-of-the-box value by collecting, aggregating, and analyzing log data from your OT environment (including Windows hosts, firewalls, switches, EDR/EPP solutions, and dedicated OT security tools). The data is ingested into our **Cyber Operations Risk & Response™** (**CORR**) **platform** and a purpose-built **Trusted Behavior Registry®** where it is normalized and monitored for potential security incidents using Critical Start-developed threat detections. This approach allows for fine-tuned control and reduces false positives by accounting for your unique OT environment.

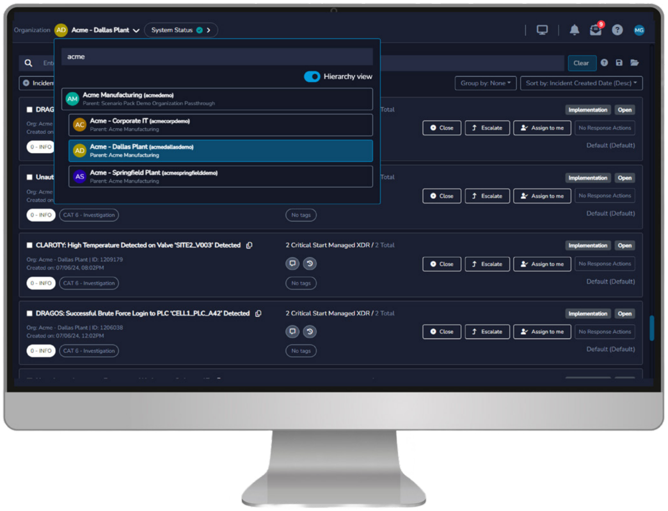
Flexible service tiers to support your OT security journey.

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

- **Base:** Utilizes existing infrastructure and IT security tools (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.

Both tiers offer 24x7x365 monitoring, threat detection, and alert routing, all backed by contractual SLAs and our trained security professionals.



acme

AM Acme Manufacturing (acmedemo)
Parent: Scenario Pack Demo Organization Passthrough

AC Acme - Corporate IT (acmecorpdemo)
Parent: Acme Manufacturing

AD Acme - Dallas Plant (acmedallasdemo)
Parent: Acme Manufacturing

AS Acme - Springfield Plant (acmespringfielddemo)
Parent: Acme Manufacturing

CLAROTY: High Temperature Detected on Valve 'SITE2_V003' Detected
Org: Acme - Dallas Plant | ID: 1209179
Created on: 07/06/24, 08:02PM
2 Critical Start Managed XDR / 2 Total

DRAGOS: Successful Brute Force Login to PLC 'CELL1_PLC_A42' Detected
Org: Acme - Dallas Plant | ID: 1206038
Created on: 07/06/24, 12:02PM
2 Critical Start Managed XDR / 2 Total

Key Features

Critical Start MDR for OT supports an organization's approach to building defensible and cyber-resilient ICS networks following the **Purdue Model** and the **SANS ICS Five Cybersecurity Critical Controls** through key features including:

- End-to-end visibility across IT/OT systems
- Hierarchical organizational views for individual location and global oversight
- Multi-site configuration with separate IT/OT alert handling
- Critical Start-developed threat detections for high-priority use cases
- OT-specific threat analytics for enhanced risk management
- Strict Rules of Engagement (**ROE**) ensuring read-only visibility
- Support for leading OT security tools (Dragos, Claroty, Nozomi, Otorio, Armis, Microsoft Defender for IoT, etc.)
- Customizable alerting and response workflows
- Flat-rate pricing

Why Critical Start MDR for OT?

Critical Start MDR for OT addresses the growing complexity and unique challenges of managing and securing converged IT/OT environments. Flexible deployment options scale as you grow, reducing the burden on internal teams and empowering you to protect your critical operations from both known and unknown cyber threats with the latest threat intelligence for 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/