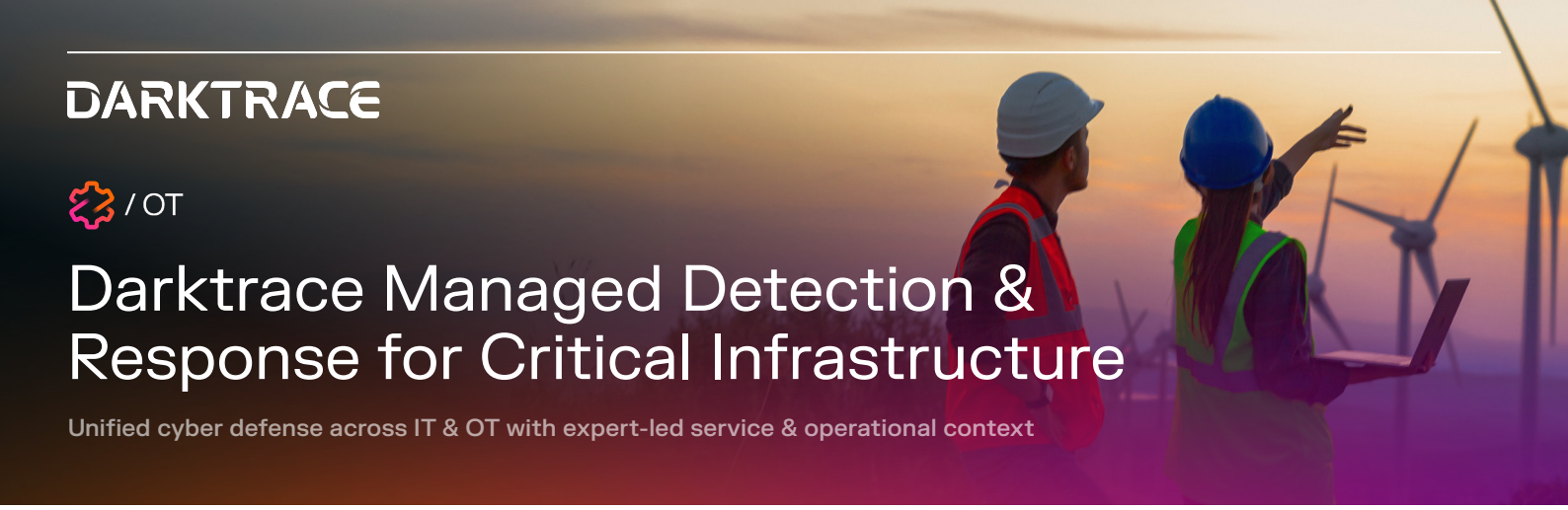
DARKTRACE

/ OT

Darktrace Managed Detection & Response for Critical Infrastructure

Unified cyber defense across IT & OT with expert-led service & operational context



Key benefits

- **24/7 managed detection & response** across network, cloud, OT, endpoints, & SaaS
- **OT-specific visibility & behavioral monitoring** across industrial environments
- **AI-led investigations with Cyber AI Analyst** to accelerate triage & incident understanding
- **Expert support that helps teams act faster** & strengthen resilience over time

Why Darktrace?

AI that learns your environment

Darktrace's Self-Learning AI understands the normal pattern of life across your organization, helping detect threats that static rules & signatures may miss.

Expert-led 24/7 support

Darktrace analysts continuously monitor, investigate, & escalate high-priority incidents so internal teams can focus on remediation & operational decision-making.

Built for converged environments

Darktrace combines enterprise-wide monitoring with OT-specific visibility & contextual risk understanding, helping teams investigate threats across IT & OT in one workflow.

Customer challenges

24/7 threat monitoring & response gaps
Many organizations lack the staff to maintain round-the-clock threat detection & response, especially across complex & globally spanning IT/OT environments.

Visibility & coordination across IT, IoT, IOMT & OT/ICS
Traditional tools fail to provide unified visibility, leaving gaps in communication & security posture between IT & OT security teams & increasing risk.

OT security skill shortages
Security teams may lack some of the specialized knowledge to investigate & respond to OT-specific threats.

Patch management limitations
OT environments often cannot be patched quickly, leaving vulnerabilities exposed for extended periods where network monitoring of those assets becomes the predominant & imperative compensating control.

Maximize your cyber defenses across IT & OT

Critical infrastructure organizations need more than tools alone. They need a managed security service that can extend detection & response across converged environments while accounting for operational realities such as uptime requirements, limited specialist capacity, & the complexity of industrial systems.

Darktrace Managed Detection & Response (MDR) help organizations strengthen coverage with 24/7 SOC monitoring, investigation, & escalation across network, cloud, OT, endpoints, & SaaS. Darktrace / OT adds the industrial visibility & contextual understanding needed to investigate threats in relation to assets, behaviors, & operational risk across the environment. Together, they help security & operational teams respond faster, reduce investigation burden, & make better-informed decisions when incidents span both enterprise & industrial systems.

The Darktrace advantage

24/7 Expert-led threat detection & response pillar

Darktrace MDR provides continuous monitoring, investigation, & containment of threats by a global SOC team. This helps organizations:

- Respond faster to high-priority & fast-moving threats
- Respond faster to high-priority & fast-moving threats

Unified IT/OT visibility & protection

Darktrace / OT bridges the gap between IT & OT by providing:

- Full asset discovery & behavior profiling across IT, OT, IoMT & IoT
- AI-driven anomaly detection that identifies novel & zero-day threats across all Purdue levels
- A single pane of glass correlating alerting & aligning to MITRE ATT&CK frameworks

Autonomous threat containment without disruption

Darktrace supports precise threat response in OT environments through configurable actions designed to help reduce risk while supporting operational continuity. This helps organizations:

- Limit intrusion impact & blast radius
- Contain rogue or suspicious devices
- Reduce the risk of ransomware spreading deeper into industrial environments

Operational efficiency & strategic insights

With regular reporting & analyst reviews, organizations benefit from:

- Biannual operational efficiency reports
- Monthly SOC performance summaries
- Tailored recommendations to optimize deployment & ROI at the SOC & site level

Key use cases

- **Living-off-the-land attacks in OT environments** - Detect suspicious use of trusted tools, native protocols, & normal-looking activity that can mask malicious behavior in industrial environments.
- **Prevent ransomware spillover into OT** - Identify & contain ransomware activity before it disrupts industrial operations or spreads deeper into critical systems.
- **Zero-day exploits & insider threats** - Detect novel & pre-CVE activity, including suspicious behavior that may not yet be tied to known indicators or public disclosures.
- **Supply chain & remote access compromise** - Strengthen visibility into rogue devices, third-party access, & suspicious external pathways that can introduce risk into OT environments.
- **Sophisticated APT activity** - Investigate advanced, multi-stage intrusions that target critical infrastructure & blend across enterprise & operational environments.

About Darktrace

Darktrace is a global leader in cybersecurity AI, protecting over 10,000 organizations worldwide. Its Self-Learning AI continuously adapts to your unique environment, helping detect & respond to threats that static rules & signatures may miss.

Darktrace also brings OT-focused expertise through analysts with certifications including GIAC GRID, GIAC GICSP, & ISA/IEC 62443, helping critical infrastructure organizations respond with greater conf-idence across converged IT & OT environments.

Business benefits

- **Accelerated threat response:** AI-led investigations reduce triage time by up to 92%.
- **Improved IT/OT collaboration:** Plain-English reporting & shared visibility help align IT & OT teams.
- **Operational continuity:** OT-aware response helps contain threats without unnecessary disruption.

Conclusion

Darktrace MDR & Darktrace / OT combine 24/7 expert-led service with OT-specific visibility & context to help critical infrastructure organizations detect, investigate, & respond to threats across converged environments with greater speed & confidence.