OBRELA

MDR

MANAGED DETECTION AND RESPONSE

OBRELA | SECURITY OVER EVERYTHING

MDR

MANAGED DETECTION AND RESPONSE

INTERNATIONALLY RECOGNIZED TURNKEY THREAT DETECTION AND RESPONSE SERVICE THAT HELPS ORGANIZATIONS TO MANAGE OPERATIONAL RISK

and significantly reduce the mean time to detect and respond to cyberattacks. At Obrela, we identify, predict and prevent cyber threats in real-time. As a Service. Personalized. On-Demand.

Obrela's MDR solution combines technology, expertise, and proactive monitoring to provide organizations with a comprehensive suite of capabilities to detect, respond to, and mitigate cyber threats. By leveraging this solution, organizations can bolster their cybersecurity defenses and effectively combat sophisticated and evolving threats.

Utilizing a cloud-native PAAS technology stack, our purpose-built Global and Regional Cyber Resilience Operation Centers (ROCs) provide continuous visibility, and situational awareness to ensure availability of business operations.

When cyber threats are detected, rapid response services ensure operational resilience is restored and maintained with minimal client impact.

With engagements that range from financial institutions, stock exchanges, telecommunications, critical infrastructure to on-line service providers, Obrela collects and analyses structured and unstructured data, generating valuable intelligence for new, emerging, and advanced security threats, giving its clients a unique advantage in predictability, preparation, and response.

At Obrela, we build more than a better cyber defense, we build resilience into businesses so you are ready for what comes next, no matter what comes next. We enable you to scale with real-time, risk-aligned cybersecurity that covers every aspect of your business, no matter how far it reaches or how complex it grows.

1.6M+
TRIAGED ALERTS

500K+
DEVICES MONITORED

99.9%
AVAILABILITY SLA

12.3'
RESPONSE TIME

2023 FIGURES

MDR PRODUCTS

Obrela protects clients throught a combination of MDR products and service capabilities based on their size, technology stack and security profile.

MDR CORE

Designed to provide organizations with continuous monitoring, detection, and response capabilities for potential threats and security incidents at the endpoint level. Enables early breach detection and adaptive response against endpoint compromise-related threats.

MDR INFRA

Combines human expertise with artificial intelligence to provide 24x7 monitoring of the entire IT stack, detecting, investigating, and responding to potential threats. A turnkey experience, using a scalable technology stack that collects relevant logs, data and contextual information.

MDR CLOUD

Combines collective intelligence practices and methods with leading edge security analytics and sophisticated risk management technology to identify, analyze, predict and prevent cyber-security threats targeting multi-cloud infrastructures. Leverages a comprehensive cloud native MDR Stack and supports AWS and GCP, as well as other modern cloud platforms.

MDR FOR OT

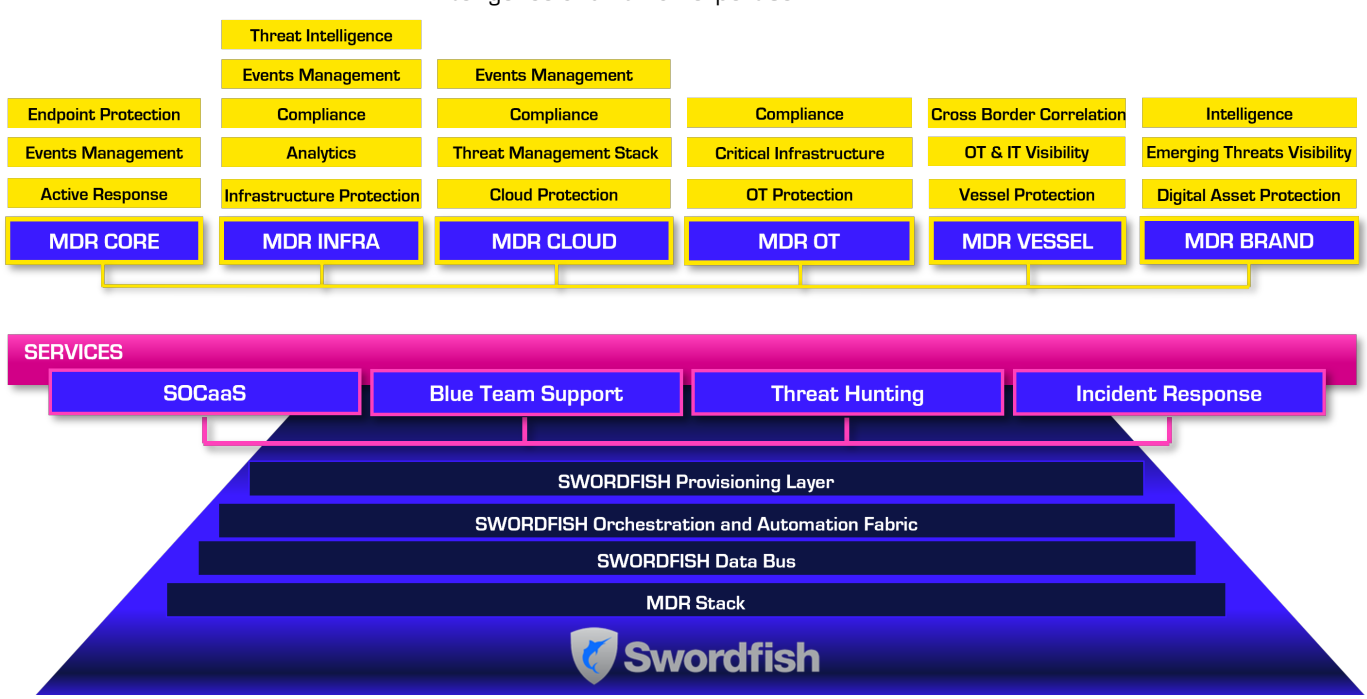
Designed specifically for industrial control systems (ICS) and other OT environments that are typically used in critical infrastructure such as energy, transportation, and manufacturing. Empowers organizations with extended detection and response (XDR) that is rapidly deployed and works with diverse endpoints, IoT, OT, and industrial control system (ICS) devices.

MDR FOR VESSELS

A specialized approach that ensures the safety and security of vessels, crew, and cargo. Purpose-built to address industry-specific challenges by providing a comprehensive cybersecurity solution that covers both Vessel IT and OT systems.

MDR FOR BRAND

Provides protection for all client external digital risks. Empowers organizations with comprehensive visibility and protection across the surface, deep and dark web. Proactively identifies and mitigates online threats to an organization's brand and intellectual property by leveraging a combination of advanced technologies, threat intelligence and human expertise.



MDR SERVICE CAPABILITIES

At Obrela we provide an umbrella of cybersecurity expertise to complement your team. We help you put an end to the unpredictable complexity of the security tools and orchestrate and streamline security operational activities across your organization.

SOCAAS

Ensures continuous security monitoring and provision of all necessary information and provides insights around a humanly verified incident, as well as guidelines and recommendations on its handling. Empowers clients with clients with top-tier cyber threat defense and allows the operations team to remain functional and productive without exposing the essential details of incidents to the wider world.

BLUE TEAM SUPPORT

Assures that incidents can be adequately comprehended escalated and mitigated until responsibility can be handed over to them to continue their threat monitoring and incident response procedures autonomously. Senior analysts assist by searching for attackers in logs and network traffic and by identifying threats to a specific IT, Cloud, OT environment or on the endpoints.

THREAT HUNTING

Combines knowledge, intuition, and automation to proactively search for covert signs of an active or attempted compromise. Leverages advanced analytics and threat intelligence to investigate and mitigate malicious activities within an organization's digital universe, delivering comprehensive security coverage, enhanced threat detection, and rapid incident response.

PROACTIVE INCIDENT RESPONSE

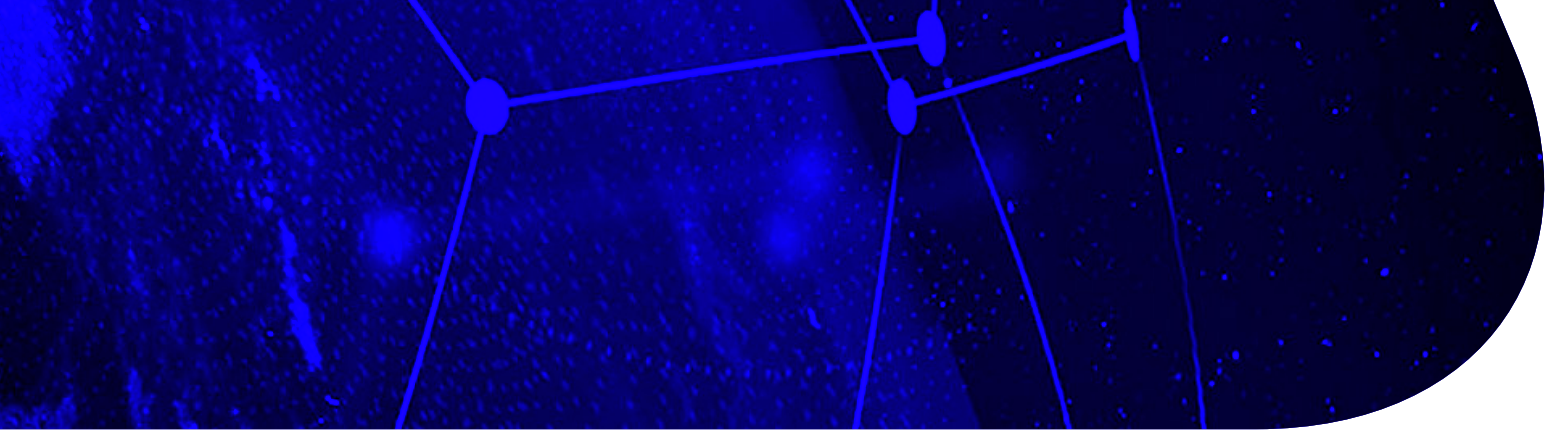
Ensures fast response, investigation, containment, and mitigation to cyber threats. Leverages extensive experience and expertise gained from conducting a wide variety of incident response and data breach investigations ranging in size and complexity. We have also worked with regulatory and law enforcement authorities.

PLATFORM ENGINEERING AND SUPPORT

The platform engineering and support team encompasses all preventive maintenance and operations-driven technical tasks related to the SaaS platform and the customers' CPE and integrations with their systems via SWORDFISH® SRM for technical requests.

ADVANCED COMPUTER SECURITY INCIDENT RESPONSE

Provides investigation and response to any organization-wide intrusions, breaches or events which cannot be safely managed by the existing security team. Enables system response to an incident, taking corrective actions against malicious actors but also helping with legal issues that may arise during incidents.



WHY OBRELA MDR

Obrela MDR provides a cost effective, on-demand solution that collects and analyzes structured and unstructured data generating valuable intelligence for new, emerging, and advanced security threats empowering organizations with a unique advantage in predictability preparation, and response.

CUSTOMER-BASED

- Risk-Based Approach. Manage and mitigate threat based on the business risk. With a centralized view, we prioritize the most important issues in real-time, to help you quickly adapt to changing circumstances.
- Real-Time Visibility Over Your Digital Universe. A single pane of glass that offers extended detection and response (XDR) across complex digital infrastructures and diverse endpoints, IoT, OT, and industrial control system (ICS) devices.
- Adaptive. Easy adaptation to the client's security requirements adjusting the risk tolerance, reporting needs, notification requirements, etc.
- 24x7 Protection. Fully staffed and skillful global and regional Resilience Operation Centers (ROCs) that engage with customer data daily and ensure continuous and uninterrupted monitoring (24x7x365) and response.
- Proactive Approach. The MDR Services encompass both reactive activities and proactive measures, with the latter enhancing real-time threat detection.
- Service Governance. Customer Security Success Manager serves as the point of contact providing guidance to ensure customer success.

TECHNOLOGY-BASED

- Cyber Security As-A-Service Model. Our SaaS based MDR model removes the barriers to entry offering our clients a service experience based on outcomes with predictable pricing and no hidden costs.
- Artificial and Human Intelligence Combined. Leverages AI-powered risk management and automation technology along with human-led analysis and threat hunting to deliver a comprehensive solution. It provides a turnkey experience and fast threat response in hybrid multi-cloud environments.
- Unified Operations and Service Provisioning Fabric. As the single point of service for our MDR solutions, SWORDFISH® provides a unified and technology-agnostic SOAR and service provisioning fabric for our clients' operations.
- Continuous Algorithmic Development. With Embedded Obrela proprietary HardCore™ Content that embodies 10+ years of continuous research, ongoing algorithmic development and experience in operational security, we serve multiple clients and many industries across the globe.
- Detection of Emerging and Unknown Threats. We constantly develop and improve our algorithms to ensure accurate and timely identification of evolving, emerging, and zero-day threats.
- Digital Surface Exposure Management. Exposure management capabilities help with the prevention of attacks by reducing the digital surface exposure in the customer environment.
- Alert Context Associated with MITRE ATT&CK Framework. Our alert context is aligned with the MITRE ATT&CK framework, which enhances threat detection, provides situational awareness, and promotes continuous improvement in cybersecurity.

WHY OBRELA

WHAT WE DO

Make businesses resilient by deploying a real-time cybersecurity system over an ever-expanding digital universe.

WHY WE DO IT

With full-stack threat detection, aligned to business risk, powered by the SWORDFISH® platform, and driven by expertise more relentless than any threat.

HOW WE DO IT

No matter the threats that may loom over our customers, we provide an umbrella of security that protects every person, every thing, and every goal their business has.

Obrela delivers real-time, risk-aligned cybersecurity that provides an umbrella of defense over every aspect of your business. We focus on risk over threats to bring business perspective to cyber defense to make security scalable, no matter how much your business grows.

With SWORDFISH®, an Integrated Cyber Risk Management in Real Time Platform, we deliver predictability over uncertainty, allowing you to orchestrate and control all aspects of cybersecurity. By centralizing security data, we deliver visibility over your entire digital universe.

At Obrela, we do more than create better cybersecurity. We create cyber resilience to defend every person, asset and goal your business has.

ACKNOWLEDGED AND ACCREDITED BY

ABOUT OBRELA

Obrela is a global provider of cyber security services. We provide security analytics and risk management services to identify, analyze, predict and prevent highly sophisticated security threats in real time. Founded in 2010, Obrela delivers real-time cyber risk management combining Threat Detection and Response (Managed Detection and Response, MDR) with Managed Risk and Controls (MRC) services to resolve technology fragmentation and process disconnects, while aligning technology to business objectives leading to better decision-making.

Our mission is to 'Keep Your Business in Business' at all times.

“BECAUSE UNPREDICTABLE DOESN’T HAVE TO MEAN UNCERTAIN.

OBRELA

OBRELA.COM

LONDON | ATHENS | FRANKFURT | DUBAI | RIYADH