telelink
business
services

MANAGED EXTENDED DETECTION AND RESPOND

Challenge

Organizations nowadays face a sophisticated cybersecurity landscape. The persistent growth of advanced cyber crimes and the constantly changing nature of IT systems (including hybrid, multi-cloud environments, IoT devices, etc.) make it difficult to effectively build attach defense. Additionally, regulations and security standards are becoming stricter, adding another layer of complexity. The best way to address these challenges is to centralize the security efforts; yet, establishing an in-house Security Operations Center (SOC) is significantly difficult for most organizations since it requires an enormous amount of time, expertise, and money.

Our solution

Outsourcing these activities to a managed Extended Detection and Respond team provides continuous monitoring, rapid incident response, access to experienced cybersecurity professionals and advanced systems. It also offers cost-efficiency, scalability, compliance support, and allows organizations to focus on core business activities without compromising on cybersecurity. Telelink Business Services' managed Extended Detection and Respond fully reconciles with the increasingly sophisticated cyber threats and attacks. Our solution combines innovative technologies, skilled cybersecurity experts, and strategies to efficiently aggregate events from different sources such as endpoints and network flows, correlate them with user behavior analytics to detect security incidents. It's a proactive service where incorporated cyber threat intelligence feeds to enrich identified offenses understanding attacker behavior. Empowered by AI, our team can almost in real-time contain attacks and minimize cybersecurity risks within an organization's IT environment.

Key benefits

We provide predefined service plans that can easily be adapted and aligned with your organization's requirements and business needs. The Managed Extended Detection and Respond technology can be deployed on-premises, hosted by us, or in the cloud. Additionally, we offer supplementary services from our offering families such as **Security testing and validation, Managed security awareness and training, Digital Forensics** and **CISO as a Service** to enhance your overall cyber security resilience.

telelink business services

MANAGED EXTENDED DETECTION AND RESPOND

Why us?

EXPERTISE: Our managed Extended Detection and Respond team is composed of cybersecurity experts with both offensive and defensive skills. In addition, we hold a variety of certifications from leading and renowned institutes and training providers.

EXPERIENCE: Proven experience in different industries gives us a range of possibilities to adequately act in accordance with your industry. A proven track of projects is within - Public, energy, IT, Telco, Retail, etc.

We follow the industry standards – **NIS2, MITTRE, ENISA, CSA, ISO 27001, NIST, CREST.**

Longtime partnerships with **technology market leaders** to deliver cutting-edge security solutions.

Features

Telelink Business Services' Managed Extended Detection and Respond (MXDR) includes the following key features:

- **Advanced Threat Detection:** Detects sophisticated threats, anomalies, and suspicious activities in real time using advanced security tools such as SIEM (Security Information and Event Management), UEBA (User and Endpoint Behavior Analytics), NDR (Network Detection and Response), threat intelligence feeds and AI analytics.
- **Continuous Monitoring:** Provides 24/7 monitoring and analysis of security events, logs, network traffic, user behaviors, and system activities across endpoints, networks, multi-cloud environments, and other digital assets to identify potential security incidents and breaches promptly. A comprehensive reporting bulletin is delivered regularly.
- **Threat Hunting and Investigation:** Engages in proactive threat hunting activities to search for hidden threats, indicators of compromise (IoCs), and advanced persistent threats (APTs) within the organization's IT infrastructure. Conducts in-depth analysis and correlation of security data to uncover complex attack patterns and tactics.
- **Incident Response and Remediation:** Follows well-defined incident response processes, playbooks, and workflows to respond swiftly to security incidents, contain threats, and mitigate vulnerabilities. Orchestrates response actions with internal or external teams in an effective manner.
- **Forensic Investigation:** Execute forensic analysis and digital investigations to determine the root cause of security incidents, gather post-mortem evidence, and conduct lessons learned sessions. Documents findings for regulatory compliance, legal purposes, and continuous improvement of security measures.
- **Security Orchestration and Automation:** Implements security orchestration, automation, and response (SOAR) capabilities to streamline incident response workflows, automate routine tasks, and improve response times.
- **Vulnerability Assessment:** Conducts vulnerability assessments using different scanning tools to identify weaknesses and misconfigurations, assessing their severity and potential impact, and creating prioritized remediation plans.

Service Plans

Our MXDR service is flexible for organizations of all sizes and tech environments, including Microsoft ecosystems and others.

LITE

Suitable for small and mid-size organizations

PROFESSIONAL

Convenient for enterprise and public organization

MICROSOFT SECURITY

Developed for Microsoft cloud-native companies

**Tailor-made plans are subject to further discussion.*

tbs.tech | simplify the complex