Privia SECURITY

Managed Detection and Response (MDR) Service

Professional Defensive Security Services

"Professional Services for Global Threats!"

The information contained in this document pertains to the Forensic Services performed by Privia Security Information Technology and Consultancy Services Inc. and is of a **general** nature. All information in this document is publicly available.

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

"With advanced threat intelligence and continuous monitoring processes, we meet organizations' cybersecurity needs in today's global threat landscape. Our professional solutions against global threats elevate organizations' security strategies to the highest level."

MDR (Managed Detection and Response) Service is a comprehensive security offering that continuously (24/7) monitors, analyzes and neutralizes threats to an organization's cybersecurity operations. As cyber threats become increasingly complex and widespread, security needs evolve rapidly. MDR Service strengthens organizations' defensive infrastructure against sophisticated threats. Supported by cybersecurity experts and threat-detection systems, this service ensures that vulnerabilities are identified immediately. Rapid threat analysis accelerates incident response processes, thereby raising organizations' security maturity. By integrating with technologies such as SIEM, EDR and NDR, MDR Service optimizes the processes of threat detection and response.

Cyberattacks attempt to exploit an organization's security weaknesses through various techniques. This reality requires security teams to remain continuously prepared. MDR Service enables organizations to detect threats in advance by continuously monitoring security systems. With advanced threat detection algorithms and AI-supported analysis processes, MDR Service provides real-time intelligence and management capabilities to security teams.

MDR Service not only identifies threats but also neutralizes them. When vulnerabilities or suspicious activities are detected, rapid response mechanisms are triggered. These quick-response measures are designed to close security gaps and protect digital assets before threats can escalate. By alleviating the workload of in-house security teams, MDR Service makes security operations more efficient.

Service Components

Tenable MDR Service and Product Management

Tenable MDR Service encompasses the management and operation of the Tenable product family, which monitors and detects security vulnerabilities. By continuously scanning system and network weaknesses, organizations can take proactive measures against current global threats. Tenable's detailed reports guide security teams on which vulnerabilities should be prioritized for remediation. Our MDR team configures and optimizes Tenable products to actively operate within the environment and minimize security gaps.

Picus MDR Service and Product Management

Picus MDR Service uses continuous cyberattack simulations to test the effectiveness of security systems. These simulations evaluate how well implemented security controls and policies perform. Our MDR team analyzes the current state of firewalls, IDS/IPS and other security solutions. Organizations gain early insights into where security systems fall short and can take corrective actions. Regular tests with Picus simulations measure and improve the effectiveness of security measures.

ThreatMon MDR Service and Product Management

ThreatMon MDR Service protects organizations through real-time threat detection and monitoring. Our MDR team leverages the ThreatMon platform to provide cyber threat intelligence. By continuously monitoring malicious networks, the service delivers timely intelligence relevant to the organization. ThreatMon's analytics enable early identification of threat sources and threat actors.

Trellix (McAfee and FireEye) MDR Service and Product Management

Trellix MDR Service accelerates threat detection and response by integrating McAfee and FireEye solutions. Our MDR team operates the full Trellix product suite, including endpoint security, network security and threat hunting. By combining FireEye's advanced threat intelligence with McAfee (Trellix)'s endpoint protection features, comprehensive coverage is achieved. Organizations using Trellix MDR solutions gain the ability to manage all security operations across their environment.

Wazuh MDR Service and Product Management

Wazuh MDR Service includes open-source security monitoring and threat-detection solutions. Our MDR team utilizes Wazuh's SIEM and HIDS capabilities to analyze security events. Wazuh provides detailed visibility into network activities and security incidents. Vulnerabilities are detected in real time and immediate response measures are applied. With Wazuh's data analytics and reporting features, security policies are continuously refined.

DarkTrace MDR Service and Product Management

DarkTrace MDR Service employs AI-powered cybersecurity solutions to detect network-based anomalies. Our MDR team uses DarkTrace's advanced anomaly detection capabilities to analyze security weaknesses. As a machine-learning–supported solution, DarkTrace learns an organization's normal network behavior and identifies unusual activity. The MDR team monitors these anomalies and responds to threats instantly. DarkTrace's sophisticated analytics help quickly determine the source and impact of threats.

Netsparker MDR Service and Product Management

Netsparker MDR Service enables the analysis of web applications through web security scanning solutions. Our MDR team uses Netsparker's scanning tools to perform vulnerability assessments on web applications. When security flaws are identified, detailed reports are provided to security teams for remediation. By regularly testing for vulnerabilities, the MDR team ensures the ongoing protection of web applications.

Acunetix MDR Service and Product Management

Acunetix MDR Service manages solutions that detect web security vulnerabilities. Our MDR team conducts regular application security tests using Acunetix to close identified weaknesses. By preventing common web application vulnerabilities, the organization's overall security posture is strengthened. Acunetix's detailed reports enable security teams to prioritize and address risks effectively.

Cloudflare MDR Service and Product Management

Cloudflare MDR Service protects organizations' digital infrastructure by managing security and network protection solutions. Our MDR team operates Cloudflare's DDoS protection, Web Application Firewall (WAF) and Content Delivery Network (CDN) features. By inspecting web traffic, Cloudflare blocks malicious activities in real time and secures websites. While protecting online assets, the service also enhances performance and speed. Our MDR team aligns all Cloudflare security features with the organization's overall security strategy.

Rapid7 MDR Service and Product Management

Rapid7 MDR Service manages and operates Rapid7 solutions that monitor security vulnerabilities and attack threats. Our MDR team optimizes Rapid7 products—such as InsightVM—for instant vulnerability detection. By strengthening threat detection processes with InsightIDR, security teams can respond rapidly. Rapid7's intelligence-driven analysis prioritizes risks and helps eliminate weaknesses. Our MDR service continuously monitors vulnerability management and threat-detection processes to address emerging security gaps.

Elasticsearch MDR Service and Product Management

Elasticsearch MDR Service encompasses the operation of data analytics and event-monitoring solutions. Our MDR team uses components like Elasticsearch, Logstash and Kibana to analyze security events. By transforming large volumes of data into meaningful insights, the service enables quick identification of vulnerabilities and threats. Elasticsearch's data visualization tools help security teams understand the origins of incidents. The MDR team configures Elasticsearch solutions to meet the organization's specific security needs. Detailed analyses of security events provide regular reporting to minimize threats.

Qualys MDR Service and Product Management

Qualys MDR Service supports vulnerability management and compliance processes. Our MDR team operates Qualys solutions that scan and analyze security vulnerabilities. By promptly identifying and remediating weaknesses, Qualys products streamline the work of security teams. Regular reports and alerts from Qualys enhance the effectiveness of security operations. The MDR service meets security and compliance requirements, ensuring organizations remain prepared against threats.

Fortify MDR Service and Product Management

Fortify MDR Service manages and operates application security solutions. Our MDR team configures Fortify's solutions to analyze code for security vulnerabilities, allowing security measures to be integrated into the software development lifecycle. Fortify scans source code to identify and remediate vulnerabilities at the coding level. Our MDR service ensures that software development processes proceed securely.

SentinelOne MDR Service and Product Management

SentinelOne MDR Service manages endpoint security solutions (EDR) to protect against cyber threats. Our MDR team uses SentinelOne's advanced threat detection and response features to analyze security events. SentinelOne monitors endpoints in real time, detecting threats as they occur. The MDR team tracks and analyzes detected threats on endpoints to initiate response processes immediately.

Checkmarx MDR Service and Product Management

Checkmarx MDR Service manages code security solutions to enhance security in software development. Our MDR team operates Checkmarx's static code analysis solution to identify security vulnerabilities. By conducting regular source-code scans, potential risks are detected and remediated early. Checkmarx also provides developers with guidance on writing secure code. The MDR service ensures regular code-scanning processes to maintain a secure software infrastructure.

Thales MDR Service and Product Management

Thales MDR Service manages data protection and encryption solutions to ensure the security of sensitive information. Our MDR team operates Thales product sets to enforce data security and manage encryption processes. By encrypting sensitive data, Thales prevents unauthorized access and protects against data breaches.

Swimlane MDR Service and Product Management

Swimlane MDR Service manages security orchestration and automation solutions to accelerate security operations. Our MDR team implements Swimlane solutions to enable automated incident response processes. Swimlane automates the analysis and response to security events. The MDR team uses automated response workflows to accelerate operations and reduce human error, making security operations more efficient.

Cobalt Strike MDR Service and Product Management

Cobalt Strike MDR Service manages penetration testing and security assessments to analyze an organization’s security posture. Our MDR team conducts regular penetration tests using Cobalt Strike to identify vulnerabilities early. Cobalt Strike provides security teams with insights into the root causes and priorities of vulnerabilities. By performing regular tests, MDR Service helps organizations remain prepared against global threats.

FAQ

What is MDR service and how does it benefit organizations?

MDR (Managed Detection and Response) is a managed cybersecurity service that enables organizations to detect, monitor and respond to cyber threats. MDR Service combines advanced cybersecurity technologies with specialized teams of experts to create a robust defense against cyberattacks. By continuously operating security operations, MDR identifies and neutralizes potential threats in real time. This approach aims to minimize vulnerabilities and ensure business continuity. Additionally, MDR Service evaluates an organization's existing security infrastructure, recommends necessary improvements and implements them. Throughout the process, tailored cybersecurity solutions are provided to meet each organization's specific needs, with security strategies continuously refined.

How does MDR service differ from traditional security services?

Traditional security services typically rely on passive defense mechanisms—such as firewalls, antivirus software and IDS/IPS. While they protect against known threats, these solutions can fall short when facing advanced and emerging attack techniques. MDR Service, on the other hand, includes continuous monitoring, threat intelligence and rapid incident response to strengthen cybersecurity defenses. Furthermore, MDR Service is managed by expert security analysts who operate around the clock, detecting and responding to anomalous activities. By going beyond traditional security approaches, MDR adapts to dynamic and ever-evolving threat environments.

What should be considered when procuring an MDR service?

When selecting an MDR service, the provider's experience and expertise should be the top considerations. It is crucial that the provider can offer solutions tailored to the organization's industry and needs. Additionally, the use of up-to-date and advanced technologies is essential for effective threat detection and response. A provider's 24/7 monitoring and rapid response capabilities are necessary to defend against cyberattacks effectively. Reporting and transparency ensure that organizations stay informed about their security posture. Finally, a balance between cost and service coverage should be evaluated.

Which industries are suitable for MDR service?

MDR Service is suitable for any industry exposed to cybersecurity threats—such as finance, healthcare, energy, manufacturing, retail and government. It is particularly critical in sectors that process and store sensitive data. In finance, MDR Service protects customer information and financial assets. In healthcare, it safeguards patient records and medical data. In the energy sector, MDR Service ensures infrastructure security and operational continuity.

What is the cost of MDR service and how should budgeting be approached?

The cost of MDR Service varies based on an organization's size, needs, service scope and chosen technologies. Generally, as service scope expands, costs increase. When budgeting, consider the organization's current security posture, risk profile and the value of assets requiring protection. Compare the benefits of MDR Service against the potential costs of cyberattacks. In addition to cost, evaluate the quality and effectiveness of the service.

How does MDR service differ from a SOC (Security Operations Center)?

A SOC (Security Operations Center) is an in-house unit responsible for managing and monitoring an organization's cybersecurity operations. It can be operated internally or by external partners. MDR Service, however, is an outsourced offering that focuses on operating security technologies. While MDR can fulfill the functions of a SOC, it also includes threat intelligence, advanced analytics and automated response capabilities. By providing external support for incident response and management, MDR Service reduces operational burdens. MDR offers flexible, externally supported solutions and its automated response and threat-monitoring capabilities strengthen SOC functions. MDR can be viewed as a complementary and supportive solution to a SOC.

Which security threats does MDR service protect against?

MDR Service defends against a wide range of threats—including malware, backdoors, ransomware, phishing attacks, advanced persistent threats (APT), DDoS attacks and data breaches. By monitoring security technologies 24/7, it detects suspicious activities and anomalous behaviors early. MDR Service pinpoints threat sources and triggers immediate response processes. With threat intelligence, organizations are prepared for the latest threat vectors. Automated response workflows quickly neutralize malicious activities. MDR Service fortifies an organization's security infrastructure against both internal and external threats.

Your Trusted Partner in Cybersecurity

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

Global and Local Cybersecurity Solutions

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East and the Americas. Our specialized teams in Offensive, Defensive and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions and military organizations, it bridges the gap between training and real-world readiness.

A Secure Future Through Advanced Technology

With R&D centers located in Istanbul, Ankara, London and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "**Privacy For You**" we bring a fresh, innovative perspective to security and privacy—ensuring that our clients' digital futures are secure.

Privia
SECURITY