OVERWATCH MANAGED ENDPOINT DETECTION AND RESPONSE (MEDR) SERVICE DESCRIPTION

1. OVERVIEW

Our innovative Managed Endpoint Detection and Response (MEDR) service leverages the capabilities of Endpoint Detection and Response (EDR) and Security Orchestration, Automation, and Response (SOAR) technologies to protect desktop computers, laptops, and servers from cyber threat actors. It provides your organization with robust security monitoring, threat detection, incident response, and management solutions to keep your endpoints fully monitored for security events with the ability to take direct, powerful mitigations through centralized management and via automated SOAR runbooks.

2. SERVICE DEPLOYMENT

Our MEDR service deployment includes:

2.1 SERVICE FEATURES

2.1.1 24/7 ALERT MONITORING, NOTIFICATIONS, TICKET CREATION, AND MITIGATION RESPONSE:

Our service offers round-the-clock security alert monitoring. Any anomalous behavior or potential threats are promptly identified, and immediate alerts are sent. Following the detection, a ticket is created in our Overwatch Ticketing Portal to effectively track the response and mitigation process.

2.1.2 DEDICATED SERVICE DELIVERY DEPLOYMENT TEAM

Our dedicated team will work hand-in-hand with your organization to ensure a smooth and secure deployment. We provide a dedicated project manager to assist in even the most complex deployments, ensuring that your business continues to operate without interruption.

2.1.3 MANUAL AND AUTOMATED THREAT HUNTING, ROOT CAUSE ANALYSIS, INCIDENT ANALYSIS, AND CORRELATION

Our experts manually hunt for threats, while automated processes bolster the identification of potential vulnerabilities. Additionally, we conduct a thorough root cause analysis, correlating events to find hidden patterns and trends that could indicate more significant, systemic issues.

2.1.4 MANUAL AND AUTOMATED MITIGATION RESPONSE AND REMEDIATION FOR ENDPOINT THREATS

Our service quickly identifies, isolates, and mitigates threats on your endpoints. Remediation processes are initiated manually by our team of experts and augmented by automated responses to ensure immediate and efficient threat containment and eradication.

2.1.5 100% US-BASED SECURITY OPERATIONS CENTER (SOC) AND ANALYSTS

Our SOC is entirely US-based and operates round-the-clock, ensuring local expertise and timely response. We employ all our analysts and development resources in-house, which gives us better control and agility to adapt to evolving security needs.

2.1.6 FULL TENANT MANAGEMENT AND ADMINISTRATION OF THE EDR PLATFORM

We offer complete administration and management services for your EDR platform, allowing you to focus on your core business functions while we take care of your cybersecurity.

2.1.7 DEDICATED CLIENT-SPECIFIC RUNBOOKS

We create personalized runbooks detailing the client's engagement rules, which our SOC follows when communicating and responding to incidents. This ensures a consistent and aligned response strategy.

2.1.8 TROUBLESHOOTING AGENT HEALTH (LEVEL 1 & 2 TECHNICAL SUPPORT)

Our technical support team is on standby to assist with troubleshooting any issues with your EDR agents, ensuring minimal disruption to your operations.

2.2 SOAR INTEGRATION FOR AUTOMATED VALIDATION OF SECURITY ALERTS

A critical element of our MEDR service is the automated validation of security alerts via SOAR. Our system rapidly processes alerts, filtering out false positives and prioritizing genuine threats. This reduces manual workload and response time, ensuring that our security team can focus on the most significant risks in your environment.

2.3.1 AUTOMATED RESPONSE PLAYBOOKS DEVELOPED BY IN-HOUSE SECDEVOPS EXPERTS

The heart of our SOAR solution is the automated response playbooks, meticulously developed by our in-house security experts. These playbooks codify our team's knowledge and experience, defining a series of automated actions to respond to various types of threats. Each playbook is tailored to address specific threat scenarios, ensuring a rapid, effective response that minimizes the potential impact of any security event.

By deploying our MEDR service, you will significantly enhance your cybersecurity capabilities. The combination of automation and expert-driven playbooks ensures a swift, efficient response to threats, minimizing potential damage, and enhancing your security posture. Stay ahead of evolving cyber threats and protect your digital assets with our advanced SOAR service.

3. SERVICE MANAGEMENT

Our MEDR service management includes:

3.1 24/7/365 US-BASED MONITORING AND RESPONSE

Our MEDR service offers round-the-clock monitoring by our 100% US-Based SOC Analysts to ensure consistent protection of your integrated security solutions. We identify and neutralize threats before they can cause significant damage, mitigating the risk of downtime and data loss.

3.2 REAL-TIME ALERTS

With MEDR integration into the SOC, you will receive real-time alerts of varying levels for any unusual activity or threats. Real-time alerts enable immediate identification and response to potential threats, minimizing potential damage and disruption. We guarantee a less than 15-minute notification Service Level Objective (SLO) for critical incidents.

This classification system allows us to prioritize threats and respond appropriately, immediately addressing the most critical issues. It also enables you to understand the severity of each alert and take appropriate action. It enhances the visibility and control you have over your security point-solution applications, thereby reinforcing the overall security posture.

3.3 THREAT HUNTING & INCIDENT RESPONSE

Our cybersecurity professionals actively hunt for signs of potential threats to your network and swiftly respond to any alerts. By integrating multiple industry-leading threat intelligence feeds, the MDR platform allows our experts to investigate incidents, respond to threats, and minimize the impact on your organization.

3.4 REGULAR REPORTING

We provide regular reports on the security status of your organization, including detailed analyses of detected threats, responses, and recommended improvements. Our service includes predefined compliance reports, baselining for statistical anomaly detection, and basic security reporting.

3.5 CONTINUOUS UPDATES & MAINTENANCE

Our MEDR service and integrations are continuously updated to respond to the latest threat trends and vulnerabilities. New detection rules and SOAR response pathways are added in as emerging threats become known. Regular maintenance ensures the efficiency and effectiveness of the service, minimizing your cybersecurity risks.

4. BENEFITS

With our integrated MEDR service, we aim to provide a robust and proactive cybersecurity solution that aligns with your business needs. We are committed to delivering a top-tier service that helps you maintain a strong security posture and resilience against cyber threats.