OVERWATCH MANAGED EXTENDED DETECTION AND RESPONSE (MXDR) SERVICE DESCRIPTION

1. OVERVIEW

The Overwatch Managed eXtended (or Everything) Detection and Response (MXDR) service is a comprehensive cybersecurity solution that integrates multiple security technologies across your attack surface into a cohesive, automated detection and response service. We provide unparalleled detection and response times, leveraging streaming data analytics to continuously monitor events, threats, and anomalies across your entire enterprise. This enables immediate alerts and instant responses to potential attacks, allowing your business to act proactively rather than reactively to new and evolving threats.

2. SERVICE DEPLOYMENT

2.1 NETWORK & SECURITY INFRASTRUCTURE ANALYSIS

The deployment process begins in pre-sales, and continues into service delivery, starting with a thorough analysis of your existing network and security infrastructure. Depending on complexity, our team of cybersecurity experts will assess the current systems, types of data crossing the network, and the threats your customer is facing. This step is crucial in understanding the specific security needs of your organization and creating a tailored XDR strategy.

2.2 MXDR INTEGRATION

At the start of the Service Delivery phase, our team will integrate the MXDR service with your existing security stack, utilizing a plethora of available integrations. The MXDR solution leverages machine learning to identify malicious behavior, anomalies, and potential threats across the entire attack surface, integrating endpoint detection and response (EDR), firewalls, identity and access management, cloud, and collaboration suites with security information and event management (SIEM) capabilities.

See all current integrations below (Section 6.0).

2.2.1 NORMALIZATION AND CORRELATION OF SECURITY TELEMETRY

Our MXDR service stands out in its ability to normalize and correlate disparate telemetry data to identify malicious behavior across your attack surface. By collecting and integrating data from a broad array of sources across your digital environment, it delivers a unified view of your security landscape and risk posture. This comprehensive perspective enables the system to identify complex threats that could be missed by less sophisticated solutions. Our service leverages NextGen SIEM with machine learning for incident correlation and a dedicated Security Orchestration Automation and Response (SOAR) platform for orchestrated and automated responses at machine speeds.

2.2.2 NETWORK DETECTION AND RESPONSE WITH INTERNAL IDS ANALYSIS

With an addon to the main service (or appropriate ingestion allotment), we can provide real-time network detection and response via an on-premises Suricata engine running in our local log collector appliance or Virtual Machine. Our system employs AI and machine learning analytics alongside high-level human analysis for timely detection of anomalies and potential threats from east and west traffic inside your local area network. This information is integrated with the rest of the analytical data from the environment and further enriched and triaged via SOAR.

2.2.3 FIREWALL SYSLOG INGESTION WITH API RESPONSES FOR IP ADDRESS BLOCKING AND MITIGATIONS

Firewall logs are continually ingested into the SIEM (Via direct TLS-delivered syslog to an open endpoint we manage, or local collection via appliance/VM) and analyzed with additional enrichment and triage provided via SOAR. Suspicious activities trigger automated IP blocking and other mitigation responses, including remote modification of traffic routing and security policies on your associated firewall.

2.2.4 SERVER LOG INGESTION FROM WINDOWS OR LINUX SERVERS AND WORKSTATIONS

We can monitor and analyze server and workstation logs from both Windows and Linux machines for enhanced threat detection across your infrastructure. Our service also includes killing suspicious server processes or applications and isolating to halt identified infiltration where the interdiction capabilities exist (such as having Overwatch managed EDR deployed alongside the MXDR/SIEM service, or other comparable fully integrated point-solution).

2.2.5 EDR/NGAV MONITORING AND RESPONSE INTEGRATION WITH CURRENTLY DEPLOYED SOLUTION

Our service integrates with your existing EDR/NGAV solution (where currently feasible, additional integration available given technical viability and development pipeline), enhancing detection capabilities and coordinating response actions.

2.2.6 PAAS / IAAS MONITORING

We can extend protection to your Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) deployments, offering both agent-based and agentless advanced log and NetFlow transport. API integrations to services such as AWS GuardDuty and Azure EventHub (When properly configured by the Partner MSP) are preferential and provide very quick deployment.

2.2.7 IDP/IAM MONITORING AND RESPONSE

We monitor your Identity Provider (IdP) and Identity and Access Management (IAM) systems to detect and respond to unauthorized access attempts, including suspending suspicious Active Directory accounts and escalating privileges.

2.2.8 EMAIL SECURITY SOLUTION MONITORING AND RESPONSE

Our solution monitors your currently deployed email security systems for phishing attack alerts, malware alerts, and other email-borne threat alerts, providing a rapid response to potential incidents and a constant vigil over the alert monitoring of those point solutions.

2.2.9 WEB SECURITY SOLUTION MONITORING AND RESPONSE

We provide continuous monitoring and swift response actions for web security threats, including malicious websites, attacks, and unauthorized access, as identified by the client's Firewall or other prevention defense orientated integration in the SIEM. Our response capabilities include blocking suspicious network traffic and blacklisting malware domains, and other API-based responses tied to the integrated point-solution (where available and feasible).

2.3 SOAR INTEGRATION FOR AUTOMATED TRIAGE AND POTENTIAL RESPONSE OF SECURITY ALERTS

A critical element of our MXDR service is the automated validation of security alerts via SOAR (Security Orchestration and Automated Response). 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. This is provided as a function of the MXDR service and is not an additional service-fee.

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 MXDR w/ SOAR 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.

2.4 USER AND ENTITY BEHAVIOR ANALYTICS

Our service incorporates User and Entity Behavior Analytics (UEBA), leveraging stateful data processing, machine learning, and deep learning to model the behavior of users and devices on corporate networks. Overwatch MXDR generates deep insights about abnormal activity by using more than 2000 stateful behavioral models that correlate events over time, running in the hot memory of the compute unit to ensure dramatic reduction in MTTD (Mean-time-to-Detect).

3. SERVICE MANAGEMENT

24/7/365 US-BASED MONITORING AND RESPONSE

Our MXDR service offers round-the-clock monitoring by our 100% US-Based and W2'd SOC Analysts to ensure consistent protection of your integrated security solutions. We help to identify and neutralize threats before they can cause significant damage, mitigating the risk of downtime and data loss, and we do so with a team that is in the contiguous 48-states, with analysts we have vetted, hired, trained, and developed. We employ multiple tiers of analysts with Tiers 1, 2, 3 and the SOC management all available to authorized users when the need presents itself via 24 x 7 phone, chat, ticket or E-mail options all available.

3.2 NEAR REAL-TIME ALERTS

With our MXDR security stack, you will receive near real-time (generally less than 1 minute from the alert data flowing into the SIEM to the completion of various SOAR runbooks in relation to the triggering data), alerts of varying levels for any unusual activity or threats we have been able to identify or corollate within your environment. Near real-time alerts (powered by observability pipelines) help to enable expedient identification and response to potential threats, mitigating damage and disruption. We guarantee a 15-minute notification Service Level Objective (SLO) for critical incidents. This classification system allows us to prioritize threats and respond appropriately, quickly addressing the most critical issues. It also enables you to understand the severity of each alert and take appropriate action, enhancing the visibility and control you have over your security point-solution applications and reinforcing the overall security posture of the client environment.

3.3 MANUAL AND AUTOMATED 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 MXDR platform allows our experts to investigate incidents, respond to threats, and minimize the impact on your organization. If a threat is identified proactively by our team, we will immediately contact the authorized personnel to establish a gameplan for moving forward.

3.4 REGULAR REPORTING & REVIEW

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. Regular reviews are conducted to ensure the MXDR service evolves with your organization and continues to provide the most effective protection. As always, customization to the reporting paradigm can be adjusted by our team upon request.

3.5 CONTINUOUS UPDATES & MAINTENANCE

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

3.6 POST-DEPLOYMENT SUPPORT

Post-deployment, we provide ongoing support to ensure the MXDR service and SOAR platform integration are functioning optimally. Our support team is available 24/7 to answer any queries or concerns you may have. We operate as your tier 1 and 2 tech support for all deployed services with dedicated SMEs on staff. It is highly recommended that your team engages their CAM to coordinate SOC reviews and technology reviews to ensure you are getting the most out of your service investment. We stand ready to hear your feedback and work diligently to implement the needed changes to affect the delivery of the MXDR service to your specifications.

4. BENEFITS

Overwatch MXDR is developed and delivered by our U.S.-based SOC team to provide unprecedented security and cost benefits:

Security Benefits	**Cost Benefits**
1. Protects your entire attack surface 2. Deploys across your network, cloud and endpoint infrastructure 3. Enhances your existing cybersecurity infrastructure with superpowered AI 4. Uses stateful behavioral models to detect, analyze and respond to security threats based on historical and ongoing behavior patterns 5. Provides best-in-class intelligence regardless of your existing security products and services **6.** Generates exponential improvements in mean time to detection (MTTD) and response (MTTR)	• Leverages existing infrastructure • Reduces the number of incidents to manage and recover from • Speeds recovery time with SOAR integration • Expands and extends in a vendor-agnostic fashion • Streamlines sourcing and operations

5.0 FEATURE SET

Overwatch Solution	**XDR**
Pricing (varies based on scope)	$$
Overwatch Managed Services	
24/7 U.S. based SOC Monitoring	yes
24/7 U.S. based SOC Detection	yes
24/7 U.S. based SOC Response	yes
SOAR Playbook Integration	yes
Automated Alert Triage and Response	yes
U.S. Security Analysts Support Upon Request	yes
SOC Ticketing	yes
Available for Businesses of All Sizes	yes
Onboarding and Training	yes

Technical Features	
Real time Detection	yes (MTTD=0)
Real Time, Automatic Response	yes (+SOAR)
SOAR Integration/Fast, Customized Responses	yes
100% Alert Triage	yes
Multiple 3rd Party Intelligence Feeds	yes
Full Data Flow, Management, Alerting –Observability Pipeline	yes
Base Log Retention in AWS S3	yes 365 days
Live Streaming Analytics (Extract, Transform, Load)	yes
End-to-End Alert Resolution Support	yes
Unique Query Language (Fluency Programming Language)	yes
Proprietary High Speed Database	yes LavaDB
Full UEBA Correlation w/ Alert Clustering	yes (user and entity behavior)
Custom Dashboards	yes
Custom Reporting	yes
Live Streaming Metrics	yes
Multi-Tool API Data Joining and Reporting	yes
Full Open-Source Sigma Rule Native Ingress	yes
Fully Segmented Storage for Enterprise Clients	yes
Ad hoc Querying	yes
Strong / Flexible Role Based Access Controls	yes
Entire Attack Surface Visibility	yes
Syslog Collection and Retention (firewalls, servers, workstations)	yes 365 days (see full list)
Network Traffic Analysis Built-In (NetFlow Capture)	yes
AWS Infrastructure Monitoring & Alerting	yes
SaaS Apps Integrations (Google Cloud Platform, M365, etc)	yes
Risk Scoring	yes
IAM Alerts (login activity, IP restrictions)	yes
Alert Tuning/Noise Responses	yes
Forensic Searching	yes
Stateful Behavioral Models	yes (2,000+)
Native Multitenancy	yes
Full HEC Connections Supported	yes (parsing dev may be required)
Integration With Other Tools/Open APIs	yes (see full list)
Strong Ease of Use	yes
Hot Searchable Logs	365-days
Agentless	yes
Parsing New Products Included	yes
Single Pane of Glass Ingress Other Tools/Configs	yes
Unified Module-Maps RMM to SaaS Console	no (does correlation mapping)

6.0 CURRENT INTEGRATIONS

It is important to note that new integrations are added regularly, and this list may not be exhaustive. Also, new integrations can be requested for point solutions that are currently not supported provided they can supply the appropriate information / integration potential. HEC compliant APIs and syslog parsers are by far the easiest and can be accommodated quickly.

6.1 API INTEGRATIONS

6.1.1 SAAS APPLICATIONS

- Microsoft 365
- Google Workspace
- Duo

6.1.2 CLOUD INFRASTRUCTURE

- AWS GuardDuty
- AWS EC2 Audit
- AWS Kinesis
- AWS Firehose
- AWS Lamda
- AWS S3 Bucket
- AWS S3 w/ SQS
- Azure EventHub

6.1.3 EDR

- SentinelOne
- CrowdStrike Falcon
- BitDefender

6.1.4 E-MAIL SECURITY

- Mimecast
- Proofpoint

6.1.5 COMMS

- Slack
- PagerDuty
- ServiceNow

6.1.6 ON-PREM IAM / AD

- Active Directory
- LDAP

6.1.7 CRM

- SalesForce

6.2 CUSTOM PARSERS

6.2.1 AGENTS AND SYSLOG PARSING

- Checkpoint FW Syslog
- Cisco Meraki FW Syslog
- Citrix NetScaler Syslog
- CrowdStrike Falcon Console Syslog
- Fastly Web Server
- FortiGate FW Syslog
- Linux Agent-gathered Syslog (NXLog)
- Palo Alto FW Syslog
- Ruckus AP Syslog
- SentinelOne Console Syslog
- SonicWall FW Syslog
- Windows Agent-gathered Syslog (NXLog)