Managed Detection and Response (MDR) Buyer’s Toolkit

A Guide to Choosing Managed Detection and Response Services

MDR services should deliver outcome-based detection, investigation, and response. These services should help you manage risk; reduce alert fatigue; provide comprehensive visibility, fast investigation, and remediation; and reduce attacker dwell time.

MDR can help you acquire SOC capabilities or augment or accelerate your SOC maturity and get the most out of your XDR product, but how do you know if your MDR partner has the right tools, expertise, and processes to help meet your goals? The following checklist identifies key requirements to help you evaluate the capabilities of the services you're considering.

Use this checklist as a starting point, and tailor it to your company's needs to ensure you're able to identify partners and vendors that can best support your organization.

Download the spreadsheet version to start your RFP today.

1. Managed Service Requirements

- □ Provides 24/7/365 monitoring and threat hunting (including 24/7 geographic coverage of your location).
- □ Ability to deliver active response/guided remediation actions with expert analysis.
- □ Monitoring and detection by experts who will proactively respond to and stop attacks.
- □ Ability to leverage threat intelligence and knowledge obtained from working with many customers across multiple industries and geographies.
- □ Ability to utilize pre-existing or custom playbooks for response in customer environments.
- □ Access to MDR service provider specialists on staff via email, phone, or messaging system (e.g., Slack®).
- □ Customer has access to visibility, communication, and response portal or mobile or other application.
- □ Team of highly trained analysts on staff experienced with alert triage, forensics, investigation, and threat hunting.
- □ Ability to scale and expand services at the same rate your organization grows even if there is a step change (i.e., M&A, rapid response programs, business unit launches).

2. MDR Service Best Practices

Leading MDR service providers can include these capabilities:

- □ Experts available to help you properly tune and manage dedicated infrastructure. This expertise includes relevant vendor and industry certifications, such as:
  - □ XDR product certifications/authorizations:
    - □ SOC 2 Type II Plus certification
    - □ FedRAMP authorization
    - □ ISO 27001 certification
- □ Demonstrates experience within your industry or other relevant industries.
- □ Tuning tools/policies to individual customer environments, including custom rules and exceptions.
- □ Routine health checks, configuration checks and deployment checks.
- □ Managed agent and software updates.
- □ Customer access to tools.
- □ Ongoing sharing of best practices in alert management, incident investigation, incident response (IR) and threat hunting.
- □ Sharing of customer success stories to validate expertise, value provided and experience.
- □ Proprietary proactive threat hunting.
- □ Offers integration into customer ticketing systems for managing requests or support.
- □ Ability to integrate with a SOAR tool (within a service provider or customer environment).

3. Technology Stack Requirements

- □ Ability to ingest logs from **any data source**, including network, endpoint, cloud, identity, application, HR, and any other data source for threat hunting, correlation, and detection.
- □ Integrated threat intelligence from multiple sources.
- □ Integrated forensics tool(s) (optional) that helps investigate incidents swiftly with comprehensive forensics evidence.
- □ MDR services extend endpoint security hygiene via:
  - □ Host firewall
  - □ Disk encryption
  - □ USB device control
  - □ Customizable prevention rules
  - □ Application inventory
  - □ Vulnerability management
- □ MDR services offer **extended** data collection abilities, including:
  - □ Ability to ingest, prioritize, and triage alerts from multiple vendors.
  - □ Visibility into lateral movement across the network and other parts of the infrastructure.
  - □ Detection and response for threats involving managed and unmanaged endpoints.
  - □ Detection and response for threats involving remote users.
  - □ Detection and response for threats involving cloud servers.
- □ Ability to retroactively detect attacks via custom correlation rules or filters.
- □ Detection of attack techniques across the attack lifecycle, including discovery, lateral movement, command and control, and exfiltration.
- □ Demonstrated ability to detect attacker tactics and techniques through proven machine learning and AI technologies.
- □ Ability to gather and integrate forensics data from offline and air-gapped devices.
- □ Scalable, cloud-based management and agent deployment.
- □ Single, web-based management console for endpoint security as well as extended detection and response.
- □ Ability to use automation and orchestration to analyze, detect, triage, and respond to threats.

4. Visibility and Detection Requirements

- □ MDR services offer **comprehensive** visibility, including:
  - □ Comprehensive visibility across network, endpoint, cloud assets and data.
  - □ Visibility into data sources includes endpoint device, network packet/session, and cloud packet/session/config.
- □ Monitoring and detection of behavioral anomalies on unmanaged devices.
- □ Monitoring and detection of behavioral anomalies for users.
- □ Optimized and customizable detections and BIoCs.
- □ Identity analytics to detect user-based threats such as lateral movement.
- □ Behavioral analytics to profile behavior and detect anomalies indicative of attack by analyzing network traffic, endpoint events, and user events over time.

5. Deployment, Management and Security Requirements

- □ Offers role-based access control (RBAC) for granular permissions.
- □ Offers multi-factor authentication (MFA) for management.
- □ Customizable dashboards and reports for high-level status of security and operational information.

6. Threat Hunting and Threat Intelligence Requirements

□ Proven and established protocols for threat hunting. Defined threat hunting process and triggers for threat hunts and hunt success measurement.

□ Integration with threat intelligence feeds for the identification of IoCs.

□ Defined indicators that will trigger a proactive threat hunt.

□ Ability for MDR to create custom queries (BIoCs) on endpoint and network behavior (can run on demand or on schedule) for known threats and CVEs and on demand.

7. Investigation Requirements

MDR services built on industry-leading technology that enables:

□ Querying of online and offline hosts.

□ Querying log data from any source, including network, cloud, endpoint, identity, and forensics log data.

□ Granular filtering and sorting of query results.

□ MDR provides access for customers to run independent threat hunting exercises leveraging guided practices.

□ Automatic aggregation of relevant IP or hash information, including threat intelligence, events, and related incidents, in a single view to simplify investigations.

□ Identification of whether an event was blocked by an endpoint agent, firewall, or another prevention technology.

□ Continuous threat hunting across managed and unmanaged devices by analyzing network and endpoint data.

□ Both human-led and AI-led threat hunting (semi-automated and manual).

□ Intelligence sharing and impact reports via email, syslog, Slack® messages, and alerts in the product's management console.

□ Automated grouping of related alerts from various sources into a single incident (correlation) makes investigations easier, faster, and more efficient.

□ Automated stitching of security alerts and endpoint, network, cloud, and identity data.

□ Customizable incident scoring and indicators.

□ Automated root cause analysis of any alert, including network alerts, if endpoint data is available.

□ Visualization of the chains of execution leading up to an alert.

□ Timeline analysis view to see all actions and alerts on a timeline.

□ A 360-degree user view with customizable user risk scores.

□ A cloud investigation view with cloud-specific events and artifacts.

8. Incident Management and Response Requirements

Incident management and response can include the following options:

□ Intuitive incident view with MITRE ATT&CK® Framework TTP mappings.

□ Listing of notable artifacts from alerts and their threat intelligence information.

□ Listing of users and hosts involved in incidents to quickly determine the scope of an incident.

□ Ability to assign incidents to team members.

□ Automated notifications on incident assignment.

□ Ability to add comments to incidents.

□ End-to-end management of the incident lifecycle (new, investigation, closed, handled, etc.).

□ Ability to combine multiple alerts or incidents into one alert or incident (automatically or manually).

□ Ability to send incident data to third-party case management.

□ Remote isolation of a single endpoint or multiple endpoints.

□ Remote file deletion of a single endpoint or multiple endpoints.
□ Automatic and manual collection or retrieval of quarantined files and objects.
□ Remediation suggestions to restore hosts to their original state.
□ Ability for MDR provider to search for and destroy malicious files and swiftly sweep across endpoint and eradicate threats.
□ Integration with firewalls to block access to malicious IP addresses or domains.
□ Integration of XDR with a security orchestration, automation, and response (SOAR) solution for incident analysis.
□ Integration of XDR with security information and event management (SIEM) solutions.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com