MDR-AS-A-SERVICE

"Uncover threats & protect your IT infrastructure with MDR"

Managed Detection and Response-as-a-Service (MDR-as-a-Service) offers a comprehensive security solution that utilizes industry-leading Enterprise-Grade ActiveEDR technology. This technology combines AI-powered prevention, detection, response, and threat-hunting capabilities to protect user endpoints, containers, cloud workloads, and IoT devices. With MDR, you can access turnkey security cost-effectively, as it is more affordable than hiring a single security analyst.
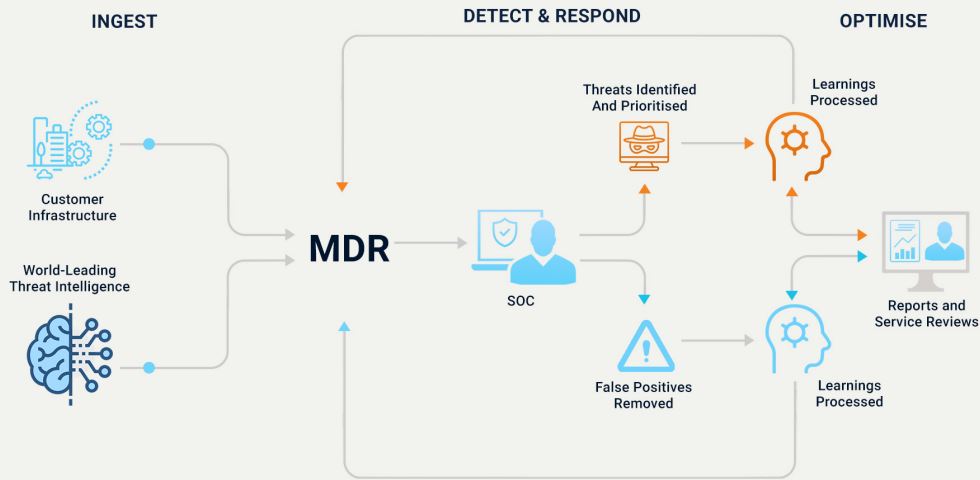
CHALLENGES OF MANAGING EDR IN-HOUSE

Managing Enterprise-Grade Endpoint Detection and Response (EDR) in-house can present several challenges, including:

- **Lack of expertise:** EDR requires specialized knowledge and skills to set up, configure, and maintain. Without an in-house team of experts, it cannot be easy to leverage an EDR solution's capabilities fully.
- **Limited resources:** Managing EDR in-house can be resource -intensive, requiring significant time and effort to keep systems updated and configured properly.
- **Keeping up with the threat landscape:** EDR requires monitoring and analyzing large amounts of data from various sources, including endpoints, network traffic, and other security tools. Keeping up with the ever-changing threat landscape can be a daunting task.

- **Scalability:** EDR solutions can be complex and difficult to scale, which can be a challenge for growing organizations or having many endpoints to protect.
- **Integration and Automation:** EDR should ideally integrate with other security tools and systems, such as SIEM, IDS, and firewalls, to provide a more comprehensive security posture. Automation is also important for handling large data sets and reducing human effort.
- **Cost:** Implementing, configuring, and maintaining EDR solutions in-house can be costly due to the need for hardware, software, and personnel.

WHY US

- **A SOC 2 Type II and ISO 27K Certified SOC**
- **Industry Beating Priced Premium Quality MDR Service**
- **300+ customers across 10+ countries**
- **Global MDR SOC Locations**
- **EDR Solution Agnostic Service**
- **Fixed Fee (No Nickel-&-Dime!)**
- **Fully-Managed Turnkey/Co-Managed Options**
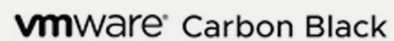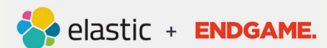- **15-Min Gold SLA**
- **GDPR and Local Privacy Laws Compliant**

HOW DOES MDR-AS-A-SERVICE WORK?

INGEST   DETECT & RESPOND   OPTIMISE

Customer Infrastructure

World-Leading Threat Intelligence

MDR

SOC

Threats Identified And Prioritised

Learnings Processed

False Positives Removed

Learnings Processed

Reports and Service Reviews

24X7 MDR SERVICE - BENEFITS

- Enterprise-Grade ActiveEDR
- Next-Gen AV & Behavioral AI
- Ransomware
- Advanced Persistent Threats (APTs)
- Proactive Threat Hunting
- Hunting via MITRE ATT&CK® Technique
- Lateral Movement Attacks
- Zero-day Attacks
- Customizable Network Isolation

- Script Misuse & Hacking-Tools
- Macros & Memory Exploits
- Trojans & Rootkits
- Triage via various IOC Repositories
- Deep Visibility Storyline Pivot
- Digital Forensics Investigations (DFI)
- Network Control Policies
- Device Firewall Policies
- USB/Bluetooth Device Control

SUPPORTED MDR VENDORS

SentinelOne   Microsoft Defender   Bitdefender   SOPHOS

CROWDSTRIKE   TREND MICRO   CHECK POINT   elastic + ENDGAME.

kaspersky   eset   vmware Carbon Black

CONTACT US

CONTACT US NOW!

📞 +1.612.532.5539   ✉ mohammed@archlightsolutions.com   🌐 www.archlightsolutions.com