CALIAN®
Confidence. Engineered.

Managed Extended Detection & Response (MXDR)

Calian's Managed XDR services combine threat hunting, AI and 24×7 security monitoring to detect cybersecurity threats. The MXDR service aims to strengthen the client's cybersecurity posture, ensuring a proactive approach to detecting, investigating and responding to potential threats within your network and infrastructure. Our technology-agnostic MXDR solution monitors endpoints, on-premises networks and cloud environments. Automation plays a critical role in alerting customers to vulnerabilities, while Calian's analysts provide active threat hunting.

Calian's managed extended detection and response (MXDR) services provide comprehensive cybersecurity solutions tailored to the client's needs, including:

- **Continuous Threat Monitoring:** Continuous monitoring, triage and investigation of detections and incidents
- **EDR Deployment:** Assisting the client in deploying and configuring EDR solution across all servers and endpoints
- **Custom Security Policies Implementation:** Implementing tailored security prevention policies for optimal threat detection and response
- **Threat Modelling and Custom Use Cases:** Developing customized alerts based on client threat modelling and reports aligned with the client's environment
- **24×7 Monitoring:** Providing around-the-clock monitoring and rapid response to security detections
- **Access to CCS Portal:** Granting access to the CCS portal for efficient ticket management and real-time visibility.
- **Enhanced Cybersecurity Posture:** Strengthening the client's overall security framework through proactive detection and remediation efforts

Objectives

1. **Proactive Threat Detection:** Continuously monitor the environment to detect and mitigate threats in real-time
2. **Rapid Incident Response:** Implement response strategies and playbooks to handle security incidents quickly and effectively, minimizing potential impact
3. **Improved Security Posture:** A higher level of protection against sophisticated attacks, including advanced persistent threats (APT) and ransomware
4. **Actionable Insights:** Real-time alerts and reporting that provides insights into security incidents, vulnerabilities and mitigation strategies
5. **Regulatory Compliance:** MDR services enable organizations to remain compliant with industry standards by identifying and addressing regulatory gaps

Scope of Service

1. **Threat Hunting and Monitoring:** Proactive identification of potential threats through 24/7 monitoring of systems and endpoints
2. **Incident Detection and Containment:** Real-time detection of security events and quick containment to prevent escalation
3. **Endpoint Protection:** Monitoring and securing endpoints through EDR solutions, ensuring a rapid response to endpoint-based attacks
4. **Reporting and Analysis:** Detailed reports on security incidents, investigations and recommendations for improving security posture
5. **EDR Solution Management:** Tuning prevention policies, creating exclusion, allowlisting to reduce false positives and adding IoCs to the blocklist
6. **Deployment Support:** Assisting client to roll out EDR solutions

Out of scope

1. **Physical Security:** On-site hardware installation, physical access controls and security camera systems
2. **Custom Development:** Developing custom security tools or scripts beyond standard MDR toolsets
3. **Legacy System Support:** Providing support for legacy or unsupported software and hardware beyond initial identification of issues

Requirements

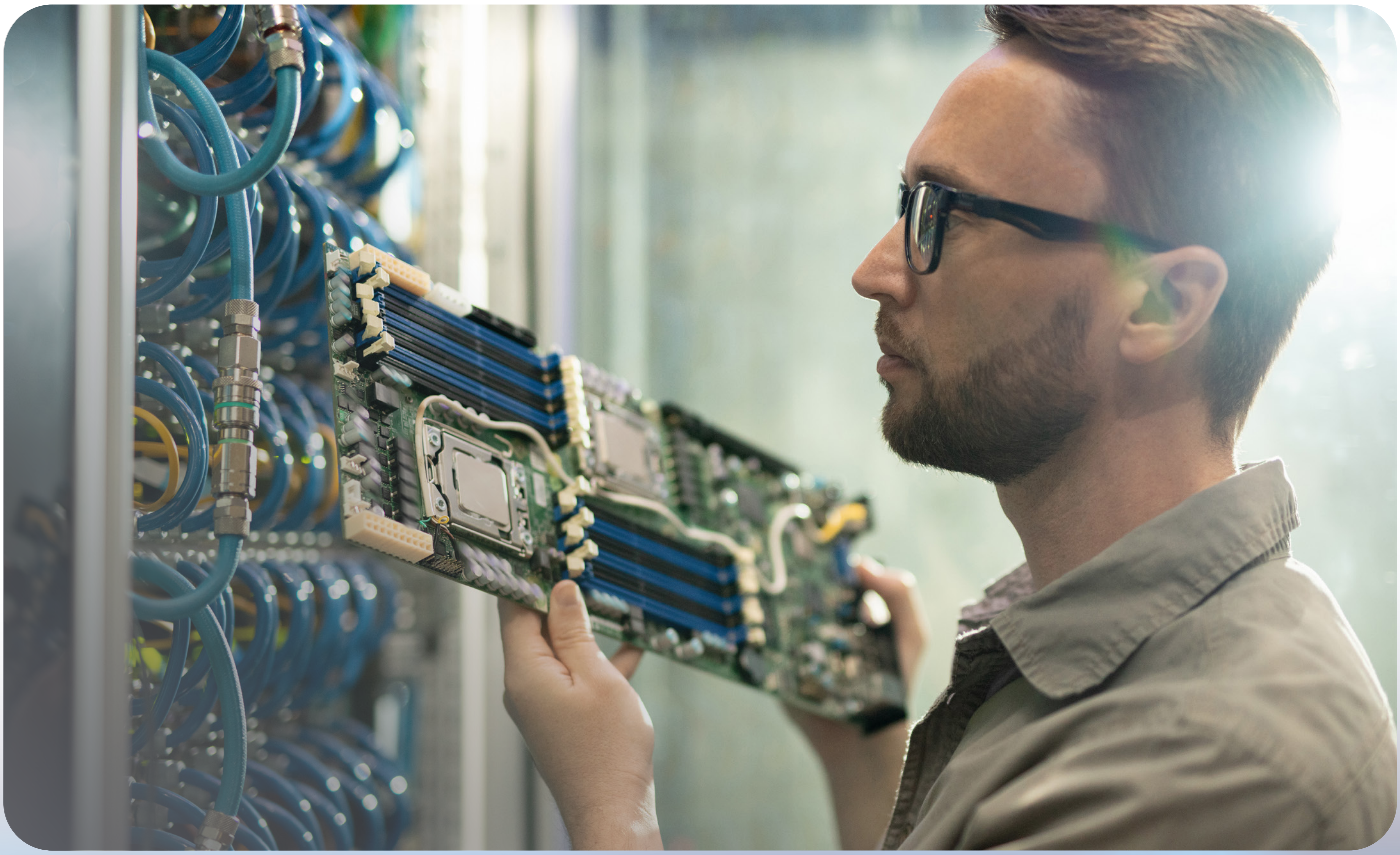
1. **Pre-Onboarding:** Initial discovery and scoping of the client's environment, including understanding the architecture, security posture and existing tools
2. **Environment Setup:** Deploy EDR solution and logging agents across the client's environment and partner with client to ensure full coverage
3. **Knowledge Transfer:** Provide necessary documentation and knowledge transfer to the client's IT and security teams to ensure seamless collaboration

SLA (Service Level Agreement)

Priority /Type	Definition	Examples	CCS SLA	Client Response Expectation
P1 – Critical Severity Alerts	**Critical Severity (P1) Alerts** are triggered when a security incident is detected **or when internal/ external malicious actors are active in the environment.**	Detected command and control to known malicious IP addresses. Administrative access to Active Directory domain controller detected from unauthorized workstations. Critical security vulnerability execution (e.g. remote code execution) detected on the internal network.	**P1 – Escalation workflow:** • Notify the Client by established Escalation Procedure within 30 minutes after receiving and confirming a P1 Alert has occurred. Alternatively, resolve false positives within **30 minutes** of receiving automated P1 alerts. • A Summary report can be made available upon request. • This includes using telephone or pager system within 30 minutes after confirming a P1 alert has occurred. Included in the weekly SOC reports.	Respond within **30 minutes after receiving the alert.**

Priority /Type	Definition	Examples	CCS SLA	Client Response Expectation
P2 – High Severity Alerts	**High Severity (P2) Alerts** are triggered when: • The detected event(s) indicates a significant probability that that a security incident is ongoing or that attacker's actions will lead to a security incident. • High risk of attempts becoming successful and turning into an incident. **A Security Incident** – is defined as unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources.	• Reconnaissance activities such as internal unauthorized network scanning. Exposed services such as SFTP receiving brute force authentication attempts from a known malicious IP address.	**P2 – Escalation workflow:** • **Notify the Client** by established escalation procedure within **4 hours after receiving** and confirming a P2 Alert has occurred. Alternatively, resolve false positives within 4 hours of receiving automated P2 alerts. • A Summary report can be made available upon request. Included in the weekly SOC reports.	**Respond within 4 hours** after receiving the alert.
P3 – Medium Severity Alerts	**Medium Severity (P3) Alerts** are triggered when: • Medium-risk malicious activity that requires mitigation action to prevent it from escalating. • Confirmation from the client is required to ascertain risk level. • The initial CCS assessment is a non-urgent matter, however still of significance to make client aware, confirm and add context/clarification. • Any event that warrants escalation of priority after business hours alerts will be classified as a P1 or P2. Client may escalate the ticket to a P1 or P2 at their discretion or after consultations with CCS.	• Targeted reconnaissance or persistent attempts to exploit sensitive applications (e.g. excessive attempts at SQL injection). • Suspicious Authentication failures. • Suspicious objects (e.g. malware) blocked in email or by security device. • Impossible travel detected by Office365 Changes in firewall or another monitored critical device.	**P2 – Escalation workflow:** • Notify the client by established escalation procedure **within 24 hours.** Included in the weekly SOC reports.	Respond **within one business day** with resolution or target date for resolution, if not feasible to address within one business

Priority /Type	Definition	Examples	CCS SLA	Client Response Expectation
P4 – Low	**Low / Informational Requests** initiated by CCS SOC or Client to improve service and other non-service impacting work for the purpose of threat hunting and discovery.	SOC asking clarification for potential false positives, improvements. Client requesting root cause analysis, or other clarification.	**P2 – Escalation workflow:** • Notify the client by established escalation procedure **within 24 hours.** Included in the weekly SOC reports.	**Respond within a week** with a resolution or target date for resolution, if not feasible to address within a week.
P5 – Informational Requests	Whitelisting and false positive approval process.	SOC team needing clarification for non-malicious events that require whitelisting to minimize noise	**P2 – Escalation workflow:** • Notify the client by established escalation procedure **within 24 hours.** Included in the weekly SOC reports.	**Respond within a week** with a resolution or target date for resolution, if not feasible to address within a week.



calian.com/**itcs**
For more information, contact: itcs@calian.com

calian.com | info@calian.com | 1.877.225.4264 |

Service:
Managed Extended Detection and Response services

Duration:
Annual Contract
Service Level: 24/7 service
Technical Level: Sr. MXDR Analysts