CALIAN
Confidence. Engineered.

Security Operations Centre (SOC)

Calian enhances enterprise security operations with 24×7 SOC services. Using advanced analytics, AI-driven threat detection and proactive monitoring, Calian's SOC services seamlessly integrate with existing infrastructure and data sources to deliver real-time protection, detection, investigation and containment.

- **Unmatched Event and Alert Investigation Speed**
  Rapid, Reliable Investigation Handling: Minimize downtime and risk with industry-leading response times. Maximize efficiency with seamless, automated and manual incident management.
- **Proactive Threat Hunting**
  Advanced Threat Intelligence: Stay ahead of threats with Calian's cutting-edge, proactive approach.
- **Standardized Investigation Protocols**
  Refined Playbooks: Ensure thorough and efficient investigations with mature, standardized processes.
- **AI-Driven Threat Detection**
  Superior Accuracy: Leverage AI and machine learning for faster, more precise threat detection.
- **Comprehensive Visibility**
  Holistic Monitoring: Gain unparalleled end-to-end visibility across all environments.
- **Custom SOAR Playbooks**
  Optimized Response: Automate routine tasks for faster, error-free incident response workflows.
- **Real-Time Threat Intelligence**
  Up-to-Date Defences: Enhance detection and mitigation with real-time integrated threat intelligence.
- **AI-Powered Data Analysis**
  Rapid Neutralization: Quickly detect and neutralize threats with AI-driven data analysis.
- **Collaborative Response Tools**
  Real-Time Coordination: Foster faster, more coordinated responses with integrated collaboration platforms.
- **Certified SOC Team**
  Expert Protection: Benefit from Calian's highly experienced, certified SOC team for best-in-class security.

Calian SOC and IR Teams' Certifications

- Certified Threat Intelligence Analyst (CTIA)
- Certified Digital Forensics Examiner (CDFE)
- Certified Incident Handler (GCIH)
- Certified Incident Handler (GCIH)
- Certified Information Systems Security Professional (CISSP)

Microsoft Certifications

- Microsoft Security, Compliance and Identity Fundamentals (SC-900)
- Microsoft Azure Fundamentals (AZ900)
- Microsoft Security Architects Expert (SC100)
- Microsoft Security Operations Analyst (SC200)
- Microsoft Identity and Access Administrator (SC300)
- Microsoft Information Protection Administrator (SC400)
- Microsoft Azure Security Engineer Associate (AZ500)

Objectives

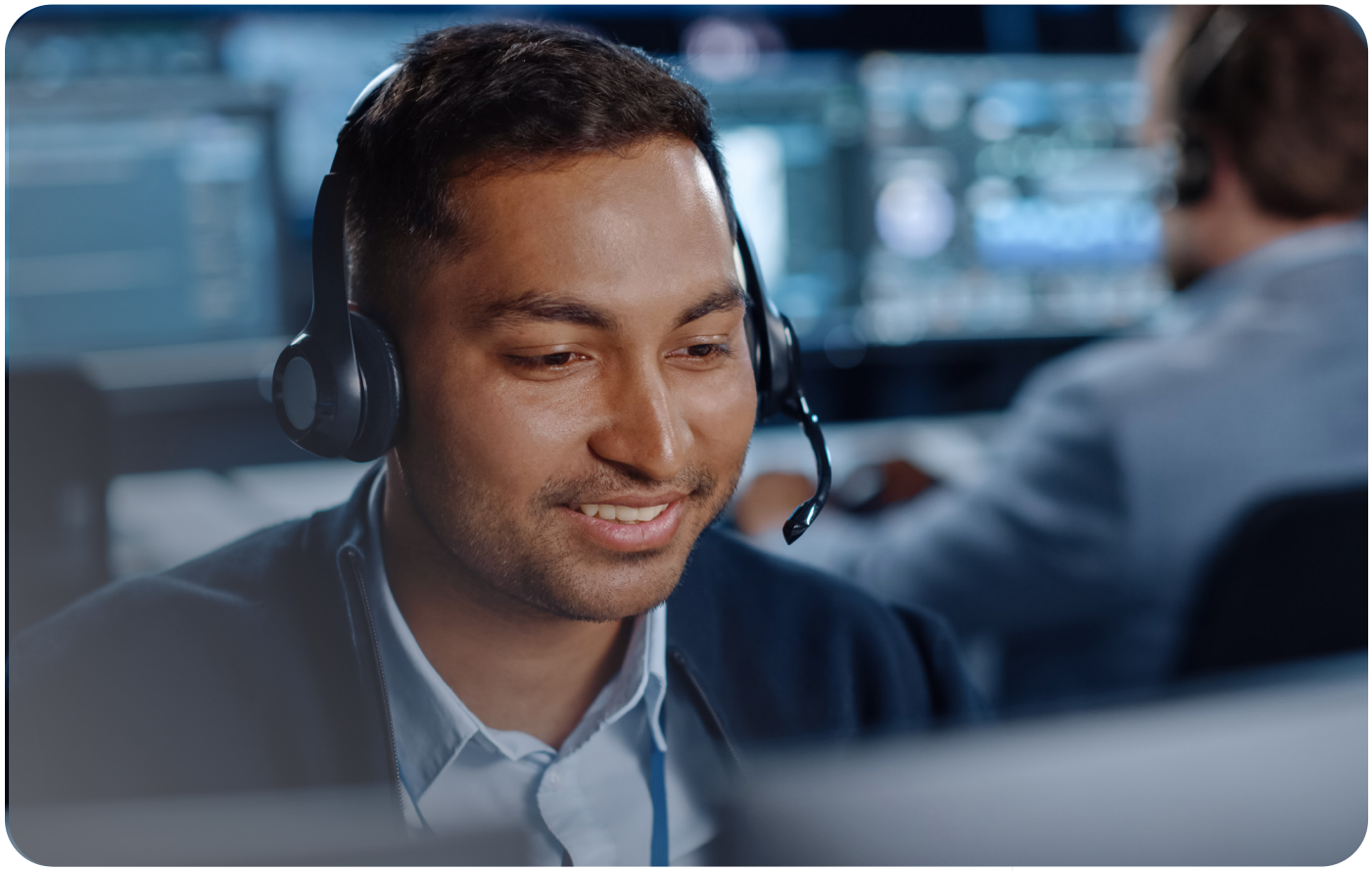
1. On-board log sources for threat detection
2. Maintain and regularly update list of analytical rules to detect evolving threats
3. Develop and maintain intuitive workbooks
4. Report bi-weekly on critical trends and important data
5. Acknowledge and investigate detections generated by SIEM tenant
6. Timely escalate to CTI team, IR team and customer, if needed
7. Conduct monthly governance sessions with customers through designated technical account managers
8. Ensure availability of a phone hotline and ticketing portal
9. Monitor billing and log patterns to control costs
10. Proactive log optimization recommendations

Scope of service

1. Alert acknowledgement and escalation as per the defined procedure
2. Proactive log pruning and rationalization for cost optimization
3. Analytic rules creation and maintenance
4. Custom workbooks creation and maintenance
5. Use case creation and maintenance
6. Threat intelligence feeds integration

Out of scope

Investigation on any platform other than the supported SIEM



Capabilities

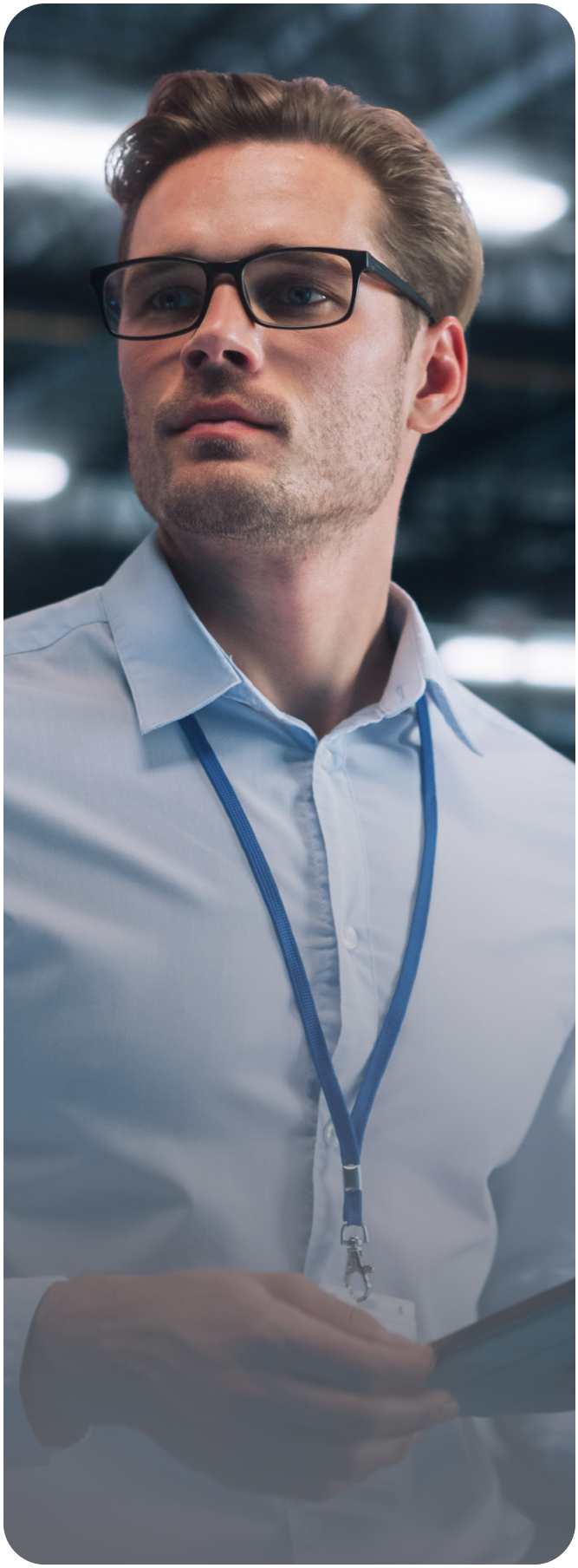
1. Monitoring of security controls
2. Monitoring of security alerts
3. User and entity behaviour analytics (UEBA)
4. AI assisted investigation
5. Automated playbooks for response

Pre-Onboarding

One hour customer session with security team to review environment scope and log sources

Onboarding

1. Assign project manager and project lead
2. Define onboarding phases
3. Environment set up for MS Sentinel
4. Connection to MSSP tenant via Azure Lighthouse
5. Integration of Microsoft services
6. Integration of critical SaaS services
7. Integration of on-prem data sources
8. Log sources custom integration development
9. Integration of telemetry/flow sources
10. Enable analytical rules and reports
11. Perform Q/A testing
12. Ticketing portal access provisioning
13. Customer training on ticketing and support



SLA

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

Priority /Type	Definition	Examples	CCS SLA	Client Response Expectation
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 his 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.	**P3 – 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 Day.

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 requesting clarification for potential false positives, improvements. Client requesting root cause analysis, or other clarification.	**P4 – 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	**P5 – Escalation workflow:** • Notify the client by established escalation procedure **within 48 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