CALIAN®

Confidence. Engineered.

# Calian MXDR Services

calian.com/itcs/cybersecurity

# Overview of Calian

## Company Background

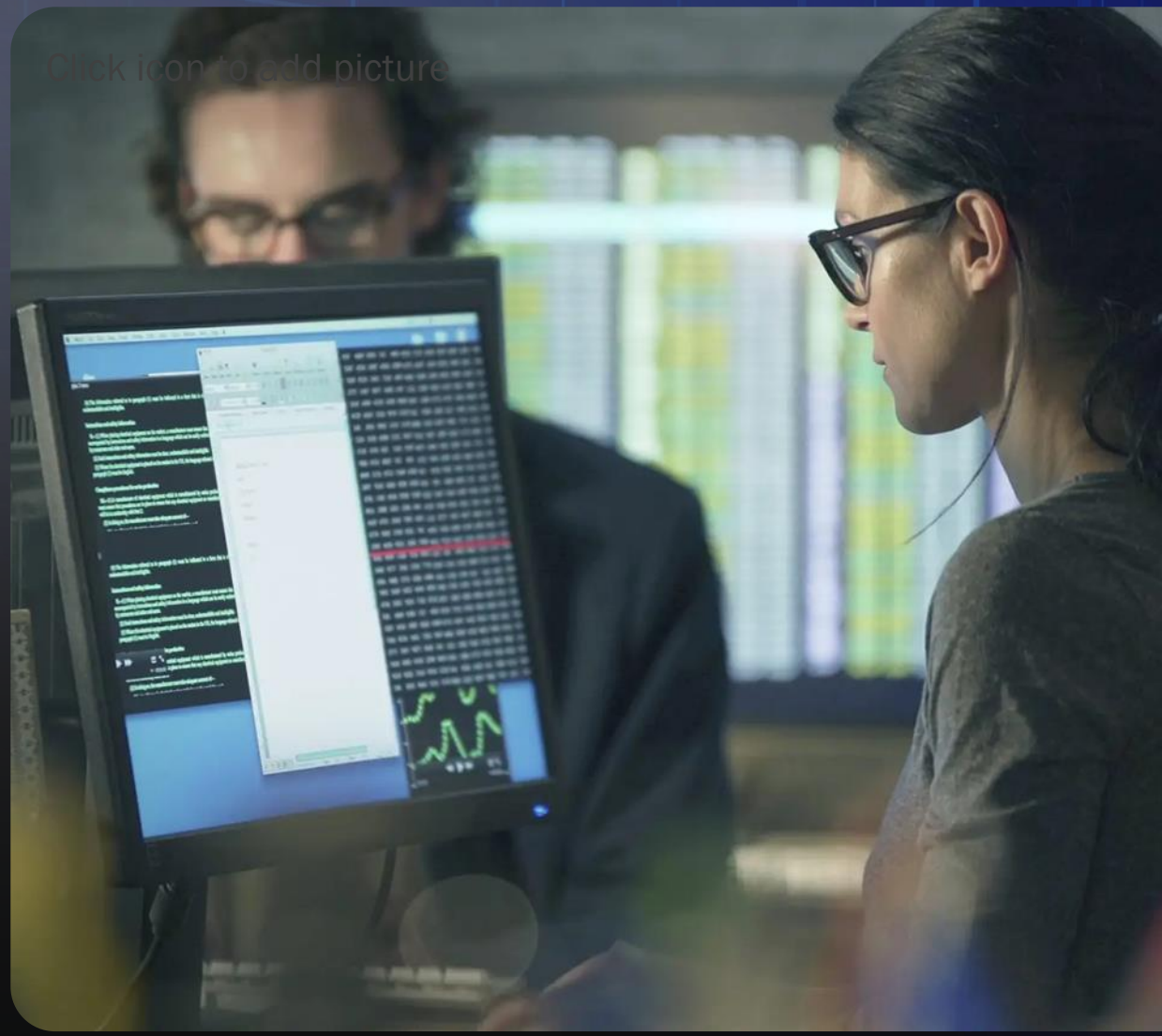
Calian Group Ltd. is a diversified Canadian company founded in 1982. Over the years, Calian has evolved into a global provider of innovative solutions across various sectors, including healthcare, technology, defense, manufacturing and engineering. Traded on the Toronto Stock Exchange under the symbol CGY, Calian has built a reputation for excellence and reliability.

## Commitment to Innovation

Innovation is at the heart of Calian's operations. Calian's innovative approach is evident in its diverse service offerings, which include advanced engineering solutions, cybersecurity, cloud services and AI-driven analytics. By leveraging the latest technologies, Calian ensures that its clients benefit from state-of-the-art solutions that drive efficiency, security and growth.

## Customer-Centric Solutions

Calian's customer-centric approach is a cornerstone of its business philosophy. The company is dedicated to understanding and addressing the needs of each client. This commitment is reflected in the tailored solutions Calian provides, which are designed to align with the goals and objectives of their clients.





# Calian Group: At a Glance

## Healthcare

Healthcare on demand

Virtual care solutions

Resource management

Patient support

Contract research organizations

## Advanced Technologies

Nuclear & environmental

Satcom

Electronics design & manufacturing

Agriculture technology

## Learning & Defence

Training-as-a-service

Emergency management solutions

Defence manufacturing

Communications & connectivity

Cyber defense

## IT & Cyber Solutions

Cybersecurity

Application modernization

Data and AI services

Enterprise solutions

Managed IT

Cloud services

CALIAN
Confidence. Engineered.

# Calian MXDR Offer

CALIAN
Confidence. Engineered.

# Transform Your Security Landscape with Calian MXDR Services

**Calian's cybersecurity team** provides 24/7 enhanced security operations, detection and response managed services, allowing you to focus on your business. Our security operations centre (SOC) and managed extended detection and response (Managed XDR) services offer a comprehensive view of your security landscape, surpassing traditional data and event correlation. Utilizing advanced analytics, artificial intelligence and automated response mechanisms, we effectively detect, prevent and respond to security events.

**Calian MXDR** integrates real-time monitoring with predictive analytics to proactively identify potential security incidents before they occur. This Sentinel-based offer is tailored for mid-sized organizations, combining top-tier Microsoft security with Calian's technical expertise to significantly enhance your security posture.

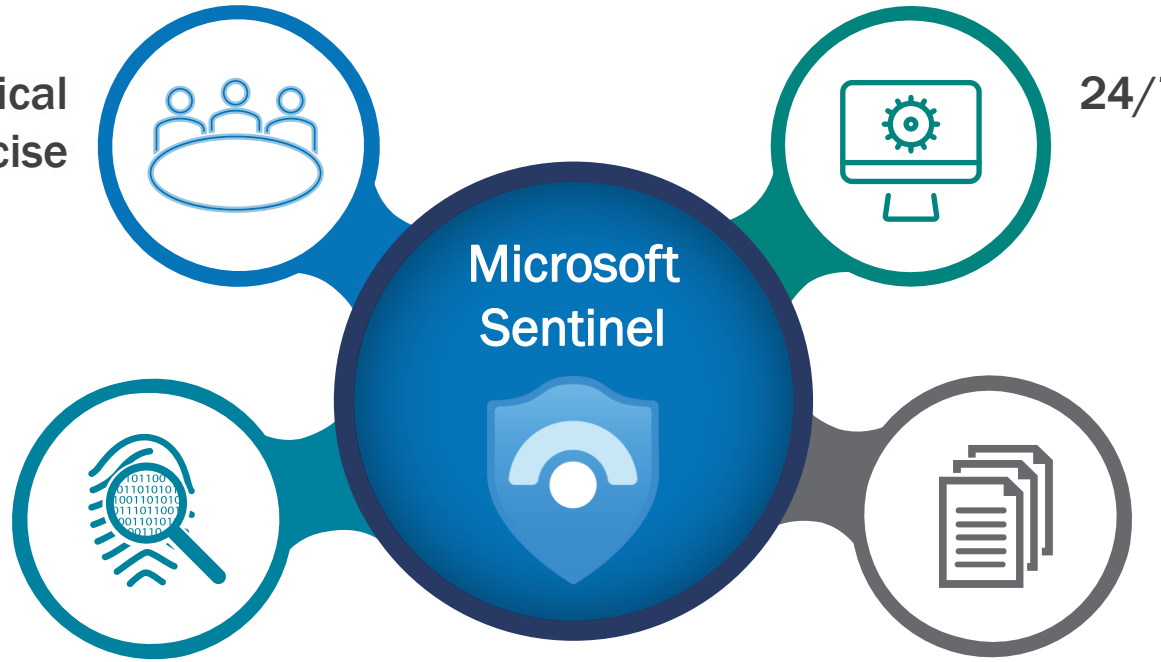


# Calian MXDR

Leadership/Technical
Tabletop Exercise

24/7 SOC & MXDR




Incident Response &
Digital Forensics

Incident response
plans and playbooks

CALIAN
Confidence. Engineered.

# Transform Your Security Landscape with Calian MXDR Offer

## Offer Details

- Migrate to Microsoft Sentinel at no cost (Calian investment)
- 24/7 SOC, 24/7 MXDR

## Sign-Up Incentives

- 1 Year of SOC + MXDR*: Select 1 value-added service at no cost
- 2 Years of SOC+ MXDR*: Select 2 value-added services at no cost
- 3 Years of SOC + MXDR*: Receive 3 value-added services OR 20 hours of incident response retainer**

## Value-Added Services (at no cost, according to the sign-up incentive tier)

- Incident response planning
- Incident response playbook
- Tabletop exercise
- 20 hours of incident response retainer* (only for 3+ years), expires in 12 months, and can be utilized for consulting services.

## Terms and Conditions

* Upon sizing and evaluating your environment, we will provide you with comprehensive budget for 1, 2 and 3 years of SOC+MXDR services.

** Customers are only eligible to select incident response retainer hours as value-added services with 3-year options and they cannot be combined with any other value services.

All value-added services are to be utilized in the first 12 months of signing the contract. Any services not utilized or requested by the customer within twelve (12) months from the date of contract execution shall be deemed expired and forfeited.

CALIAN
Confidence. Engineered.

# Calian MXDR Services Explained

CALIAN
Confidence. Engineered.

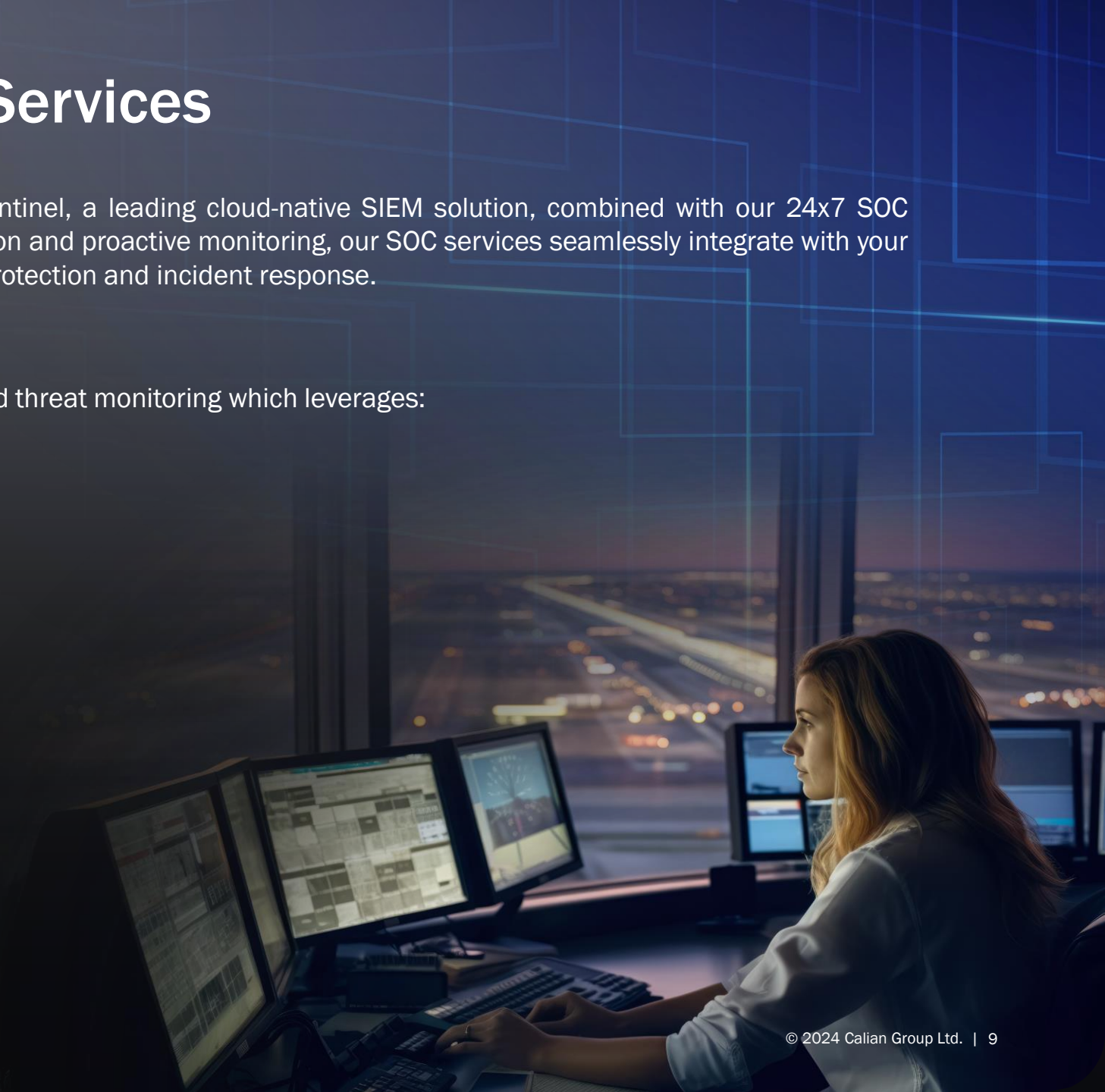
# 24/7 Security Operations Services

Calian enhances your security operations with Microsoft Sentinel, a leading cloud-native SIEM solution, combined with our 24x7 SOC services. Utilizing advanced analytics, AI-driven threat detection and proactive monitoring, our SOC services seamlessly integrate with your existing infrastructure and data sources to deliver real-time protection and incident response.

## SOC Features

24x7x365 on-prem or cloud-based (SaaS) managed advanced threat monitoring which leverages:

- Unmatched incident response speed and consistency
- Proactive threat hunting with advanced intelligence
- Mature and standardized investigation protocols
- Ai-driven threat detection for superior accuracy
- Streamlined and efficient incident management
- Comprehensive end-to-end visibility
- Custom SOAR playbooks for optimized response
- Real-time integrated threat intelligence
- AI-powered data analysis for rapid threat neutralization
- Collaborative incident response tools
- Certified and experienced SOC team



CALIAN
Confidence. Engineered.

# 24/7 Managed Extended Detection and Response Services

Calian's Managed XDR services combine threat hunting, AI and 24x7 security monitoring to detect both known and unknown cybersecurity threats.  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. Our preferred technology partner is Microsoft.

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. 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** - Assist the client in deploying and configuring EDR solution across all servers and endpoints.
- **Custom Security Policies Implementation** - Implement tailored security prevention policies for optimal threat detection and response.
- **Threat Modelling and Custom Use Cases** - Develop customized alerts based on client threat modelling and reports aligned with the client's environment.
- **24x7 Monitoring** - Provide around-the-clock monitoring and rapid response to security detections.
- **Access to CCS Portal** - Grant access to the CCS portal for efficient ticket management and real-time visibility.
- **Enhanced Cybersecurity Posture** - Strengthen the client's overall security framework through proactive detection and remediation efforts.

# Our Methodology & Approach

## Setup & Configuration

- Assess and optimize the current Microsoft Sentinel setup
- Manage data ingestion, log health and update data connectors

## Threat Detection & Incident Response

- Use advanced analytics and AI for proactive threat detection
- Prioritize and escalate incidents for fast containment and resolution

## Dashboard & Reporting

- Real-time dashboards for visibility into security operations
- Customized reports to meet specific customer requirements

## Maintenance & Updates

- Regular system updates and tuning to ensure optimal performance
- Align configurations with compliance standards (e.g., GDPR, PCI-DSS)

## Continuous Improvement

- Refine detection rules, incident response, and add new threat intelligence as needed

# Onboarding Process

**Initial Setup:** Conduct a thorough review of customer's systems and data sources

**Integration:** Ensure smooth integration of Microsoft Sentinel with all log sources and security tools

**Validation:** Validate data ingestion and detection rules prior to onboarding



# Dashboards and Reporting

## Real-Time Monitoring:

Get visibility into key security metrics through **customizable dashboards**

## Monthly Reports:

Delivered reports that highlight **incidents, trends and threat intelligence insights.**

## KPI Tracking:

Work with customers to identify key performance indicators (KPIs) that matter most.



# Security Monitoring & Threat Detection (Use Cases)

01

## 24/7 Threat Detection:

Calian SOC leverages Microsoft Sentinel's AI-driven capabilities to monitor and detect threats in real time.

02

## Behavioral Analytics:

We use machine learning to identify anomalous activity, enhancing detection of advanced threats.

03

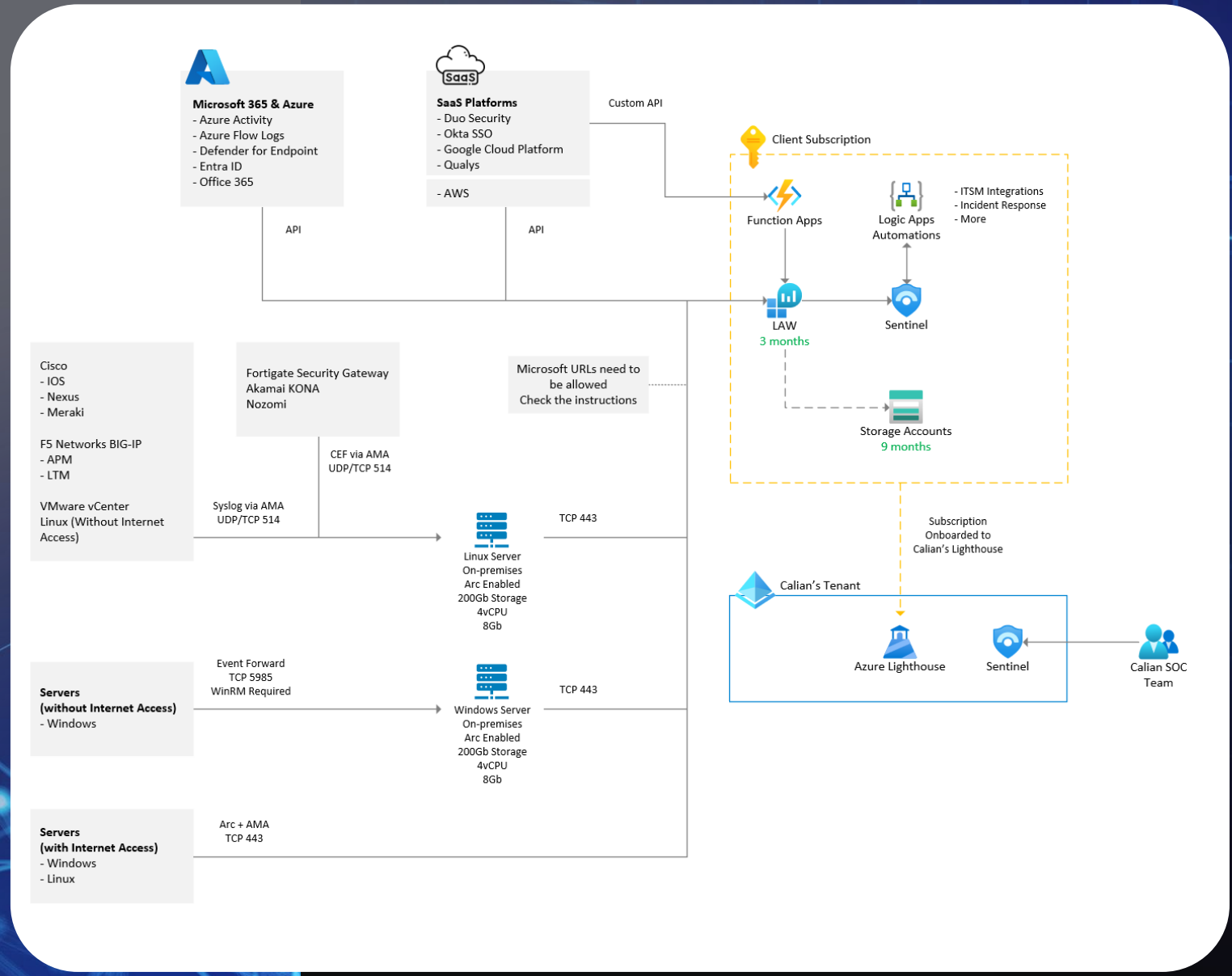
## Case Study:

A healthcare client saw a **35% reduction in detection times** after deploying our monitoring services.

CALIAN
Confidence. Engineered.

# Sentinel Integrations Architecture Diagram




CALIAN
Confidence. Engineered.

# Why Calian SOC & MXDR Services Powered by Microsoft Sentinel

## Unmatched Incident Response Speed

Rapid, Reliable Incident Handling: Minimize downtime and risk with our industry-leading response times.

## Proactive Threat Hunting

Advanced Threat Intelligence: Stay ahead of threats with our cutting-edge, proactive approach.

## Standardized Investigation Protocols

Refined Playbooks: Ensure thorough and efficient investigations with our mature, standardized processes.

## AI-Driven Threat Detection

Superior Accuracy: Leverage AI and machine learning for faster, more precise threat detection.

## Efficient Incident Management

Streamlined Operations: Maximize efficiency with our seamless, automated and manual incident management.

## 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 our highly experienced, certified SOC team for best-in-class security.

# Value-Added Services

CALIAN
Confidence. Engineered.

# Incident Response Retainer – 20 hours value added service**

Calian has conducted numerous digital forensics investigations and assessments for clients across Canada and the United States, including reviews of endpoints, web servers and firewall log file correlation. Over the past year, Calian has conducted over 25 incident response engagements.

We offer a yearly retainer-based incident response and digital forensics service to complement Microsoft security solutions. This includes 24/7 availability for incident investigation, analysis, containment and remediation support. Our team collaborates with the client's IT and operations teams to manage the entire security incident lifecycle. Certified Calian consultants will conduct thorough incident response activities, including digital forensics analysis, under this retainer.

## The specific scope includes:

- Conducting a network mapping (threat modelling) to understand the network.
- Establishing a 24/7 hotline for immediate incident response engagement.
- Running digital forensics and traffic analysis tools to uncover insights into attacker methods.
- Preserving evidence and providing a comprehensive digital forensics and incident response report with an executive summary for senior management.
- This retainer ensures the client has continuous, expert-level support for security incidents throughout the year.

**Customers are only eligible To select incident response retainer hours as value-added services with 3-year options only and cannot be combined with any other value services.

All value-added services are to be utilized in the first 12 months of signing the contract. Any services not utilized or requested by the customer within twelve (12) months from the date of contract execution shall be deemed expired and forfeited.

CALIAN
Confidence. Engineered.

# Incident Response Playbooks

Calian's incident response (IR) playbooks are comprehensive guides that outline step-by-step instructions on what an organization should do when responding to a specific cybersecurity incident. They serve as a blueprint for security teams to follow, ensuring a coordinated and effective response. Our playbooks are industry aligned and based primarily on the NIST SP800-61 r2 (Computer Security Incident Handling Guide) and NIST SP800-184 (Guide for Cybersecurity Event Recovery), and take into consideration alignment with NIST Cybersecurity Framework, ISO 27001, PIPEDA, and PHIPA. This model is extensible, and it supports cyber-breaches in sizes of 10s to 1,000,000s of records, and fits with any type of industry.

## Some examples of the threats that playbooks can be designed for include:

- Ransomware
- Data exfiltration and data breach
- Malware infections
- Denial of services including DDoS
- Phishing attacks
- Supply chain attacks
- Data loss/leakage
- Insider threats and attacks

CALIAN
Confidence. Engineered.

# Incident Response Planning

An incident response plan is a guide that an organization follows during their response to a cybersecurity incident. It is a more strategic document that contains a high-level overview of the entire incident response process.

The incident response plan covers the following areas:

- **Preparation:** Establishing and training an incident response team and setting up necessary tools and resources.
- **Detection and Analysis:** Identifying and analyzing potential security incidents to determine their scope and impact.
- **Containment:** Implementing measures to limit the spread and impact of the incident.
- **Eradication:** Removing the cause of the incident and ensuring that affected systems are clean.
- **Recovery:** Restoring and validating system functionality to return to normal operations.
- **Post-Incident Activities:** Conducting a thorough review to understand the incident, improve future responses and update the playbook as needed.


CALIAN
Confidence. Engineered.

# Difference Between IR Plan and IR Playbook

## IR Plan

- **Broad Framework:** An IR plan provides a high-level overview of the entire incident response process.
- **Strategic Focus:** It outlines the overall strategy, goals and objectives for handling incidents.
- **Roles and Responsibilities:** Defines the roles and responsibilities of the incident response team and other stakeholders.
- **Phases:** Covers all phases of incident response, from preparation to post-incident review.
- **Guidelines:** Offers general guidelines and principles for managing incidents.

## IR Playbook

- **Detailed Procedures:** An IR playbook contains specific, step-by-step procedures for responding to types of incidents.
- **Tactical Focus:** It focuses on the tactical execution of the IR plan during specific scenarios.
- **Scenario-Specific:** Tailored to address specific incident types, such as malware infections, data breaches or phishing attacks.
- **Actionable Steps:** Provides detailed actions, checklists and workflows for the incident response team to follow.
- **Operational:** More operational in nature, ensuring that the response is consistent and efficient.

# Tabletop Exercise

Calian provides two types of tabletop exercises.

- Senior Leadership Team IR Tabletop – This type of tabletop focuses on the activities related to the executive leaders, and provides awareness of their roles and responsibilities and key decisions that they will need to make during an incident.
- IT/Technical Team Incident Response Tabletop – This tabletop focuses on the IT/IS and technical teams. It provides awareness of their roles, responsibilities and their activities during the incident response.

## Benefits:

- **Improved Preparedness:** Ensures all team members understand their roles and responsibilities during an incident.
- **Enhanced Communication:** Tests and improves internal and external communication protocols.
- **Identifies Gaps:** Reveals weaknesses in the incident response plan and areas for improvement.
- **Builds Confidence:** Provides a safe environment for practicing responses to incidents without real-world pressure.
- **Realistic Training:** Delivers scenarios based on existing operational plans, ensuring practical and relevant responses.
- **Collaborative Thinking:** Encourages teamwork and improves both technical and soft skills necessary for resolution.
- **Security Awareness:** Enhances security awareness for executives, senior managers and operational staff.

## Format:

- Moderator-led session
- In-person or remote

CALIAN
Confidence. Engineered.

# Calian: Your Trusted Technology

Partner for Robust and Reliable IT and Cybersecurity Solutions

| | |
|---|---|
| **Trusted Partner** | Proven track record in North America for cybersecurity services |
| **Industry Expertise** | Trusted by public sector, NATO and healthcare organizations to secure their complex and critical infrastructures |
| **Competitive Pricing** | Enterprise grade services at competitive Pricing |
| **Customized Cybersecurity Solutions** | Tailored Microsoft security solutions for comprehensive protection |
| **Robust Services Portfolio** | End-to-end solutions across data, AI and infrastructure with a secured foundation |
| **Technical Delivery Expertise** | Americas-based technical experts and engineers to support your organization |