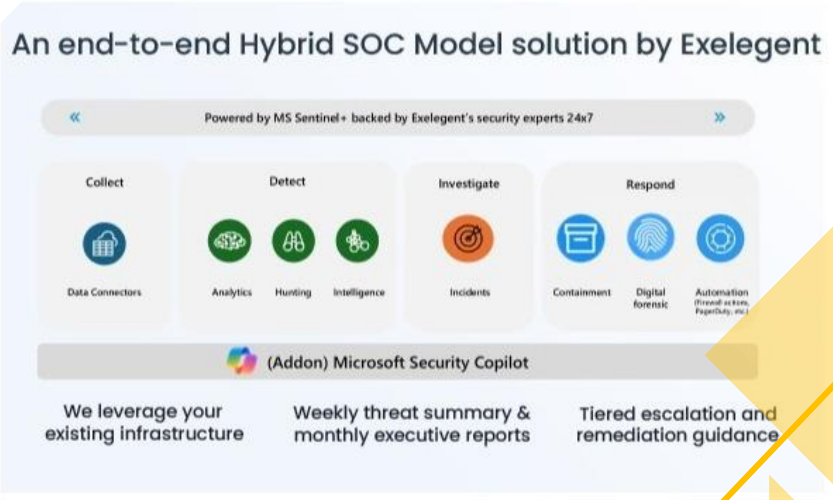
Exelegent | Microsoft Solutions Partner

Security



An end-to-end Hybrid SOC Model solution by Exelegent

Powered by MS Sentinel+ backed by Exelegent's security experts 24x7

Collect: Data Connectors

Detect: Analytics, Hunting, Intelligence

Investigate: Incidents

Respond: Containment, Digital forensic, Automation (Firewall actions, PagerDuty, etc.)

(Addon) Microsoft Security Copilot

We leverage your existing infrastructure

Weekly threat summary & monthly executive reports

Tiered escalation and remediation guidance

24/7 SOC service powered by Microsoft Azure Sentinel to detect the threats.

About Exelegent /Managed SOC and XDR Services:

Exelegent's Security Operations Center (SOC) service delivers 24/7 threat monitoring, detection, and incident response, powered by Microsoft Azure Sentinel, Microsoft's cloud-native SIEM and SOAR platform. By leveraging advanced analytics, AI, and threat intelligence, we provide real-time visibility into your environment, proactively identify suspicious activity, and respond swiftly to security incidents.

What we offer

Exelegent delivers managed Security Operations Center (SOC) services, powered by Microsoft Azure Sentinel, a cloud-native SIEM and SOAR platform, that enables 24x7 monitoring, advanced threat detection, and comprehensive incident response.

The SOC team continuously analyzes security events, triages alerts, and escalates confirmed incidents, ensuring rapid and effective responses. Azure Sentinel's AI-driven analytics and seamless integration with Microsoft's broader security portfolio, including Defender for Endpoint, Defender for Identity, and Microsoft 365 Defender, provide robust visibility and protection across cloud, hybrid, and on-premises assets

With a focus on proactive threat hunting and actionable intelligence, Exelegent's SOC service empowers organizations to strengthen their security posture and maintain compliance, leveraging the full power of Microsoft's enterprise security ecosystem.

Why Exelegent Team?

Our team of security analysts ensures continuous protection, helping you reduce risk, meet compliance requirements, and strengthen your overall cybersecurity posture.

Exelegent

https://exelegent.com | sales@exelegent.com | 973-732-5230

Why Exelegent Managed SOC and XDR Services?

The SOC team continuously analyzes security events, triages alerts, and escalates confirmed incidents, ensuring rapid and effective responses. Azure Sentinel's AI-driven analytics and seamless integration with Microsoft's broader security portfolio, including Defender for Endpoint, Defender for Identity, and Microsoft 365 Defender, provide robust visibility and protection across cloud, hybrid, and on-premises assets

With a focus on proactive threat hunting and actionable intelligence, Exelegent's SOC service empowers organizations to strengthen their security posture and maintain compliance, leveraging the full power of Microsoft's enterprise security ecosystem

Scope of Services:

24/7 Security Event Monitoring: Proactive 24/7 monitoring of log data and security events is performed via the Microsoft Sentinel SIEM platform. Exelegent's SOC analysts continuously review alerts from Sentinel's detection rules, hunting queries, and integrated security tools, ensuring persistent threat detection and rapid incident response.

Alert Triage and Analysis: When an alert or potential incident is generated, Exelegent performs immediate triage and analysis. This process includes validating whether the alert represents a genuine security threat or a false positive. SOC analysts enrich alert data with relevant context, such as threat intelligence or asset information, to accurately determine severity and urgency. Alerts are categorized as Critical, High, Medium, or Low based on predefined criteria, including impact, threat likelihood, and asset criticality, ensuring a structured and prioritized incident response.

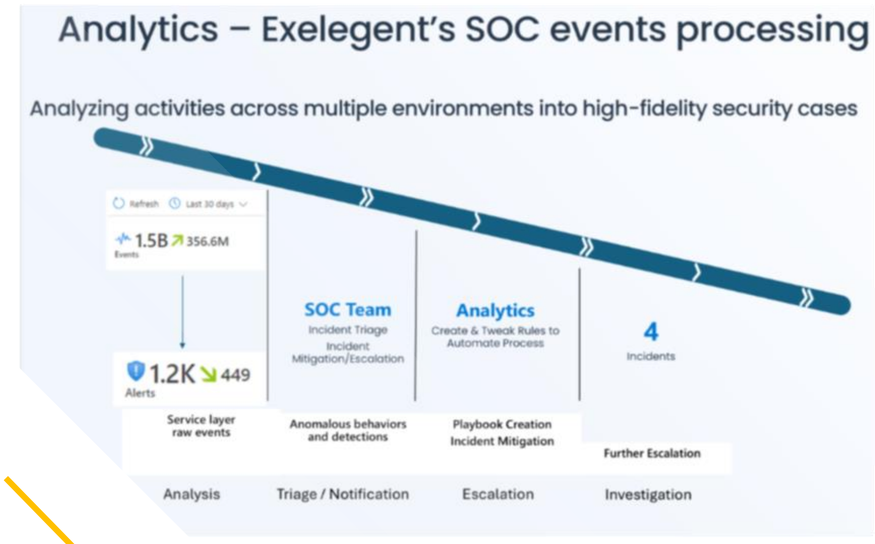
Incident Confirmation and Investigation: For alerts that indicate a likely security incident (e.g., a confirmed malware infection, unauthorized access, or data exfiltration attempt), Exelegent will escalate to incident handling. Exelegent will assign an incident identifier and analyst, who will perform an in-depth investigation such as root cause analysis, extent of compromise assessment, and recommended containment steps. Advanced tools, including Microsoft Sentinel playbooks and integrations, may be utilized to gather additional evidence and support a thorough incident investigation.

Threat Containment Support: Exelegent is available to support containment efforts by providing recommendations and guidance for immediate threat mitigation, such as discussing remediation strategies and best practices. In addition, Exelegent can facilitate and execute remote response actions to help organizations swiftly address security incidents and minimize operational impact.

Incident Escalation & Notification: Exelegent ensures prompt incident notification once a security event is confirmed, in strict accordance with established SLAs and escalation procedures. Critical incidents trigger immediate outreach to designated contacts via priority channels, while lower severity events are communicated through agreed-upon methods. Each notification includes essential incident details, severity, and recommended actions to support rapid response.

Periodic Threat Hunting: Exelegent conducts proactive threat hunting exercises on a monthly basis, seeking out indicators of hidden or emerging threats that may not be detected by standard alerts. All findings are thoroughly documented and reported in accordance with established procedures, supporting ongoing security awareness and risk management.

Exelegent
https://exelegent.com | sales@exelegent.com |973-732-5230



Analytics – Exelegent's SOC events processing

Analyzing activities across multiple environments into high-fidelity security cases

Microsoft
Solutions Partner
Security
Specialist
Threat Protection

Why Microsoft Sentinel

Microsoft Sentinel is a cloud-native SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) solution that provides a comprehensive view of an organization's security posture. It leverages AI and machine learning to detect, investigate, and respond to threats across an organization's entire digital estate. Sentinel helps organizations modernize their security operations by offering a unified platform for threat detection, investigation, response, and proactive hunting.