ADACOM
## SECURITY BUILT ON TRUST

AI-Driven Next-Generation Security Operations Center (SOC) Services

⭨ **ADACOM, a Byte subsidiary, is a leading cybersecurity provider,** delivering cutting-edge SOC services that integrate Artificial Intelligence (AI), automation, and advanced threat intelligence to protect organizations from sophisticated cyber threats. With extensive experience in cybersecurity operations, ADACOM enables enterprises to achieve real-time threat detection, rapid response, and continuous security improvement. Our SOC services are designed to provide holistic, AI-powered protection for businesses across industries, ensuring cyber resilience and compliance with regulatory frameworks such as NIS 2, GDPR, and ISO **27001.**
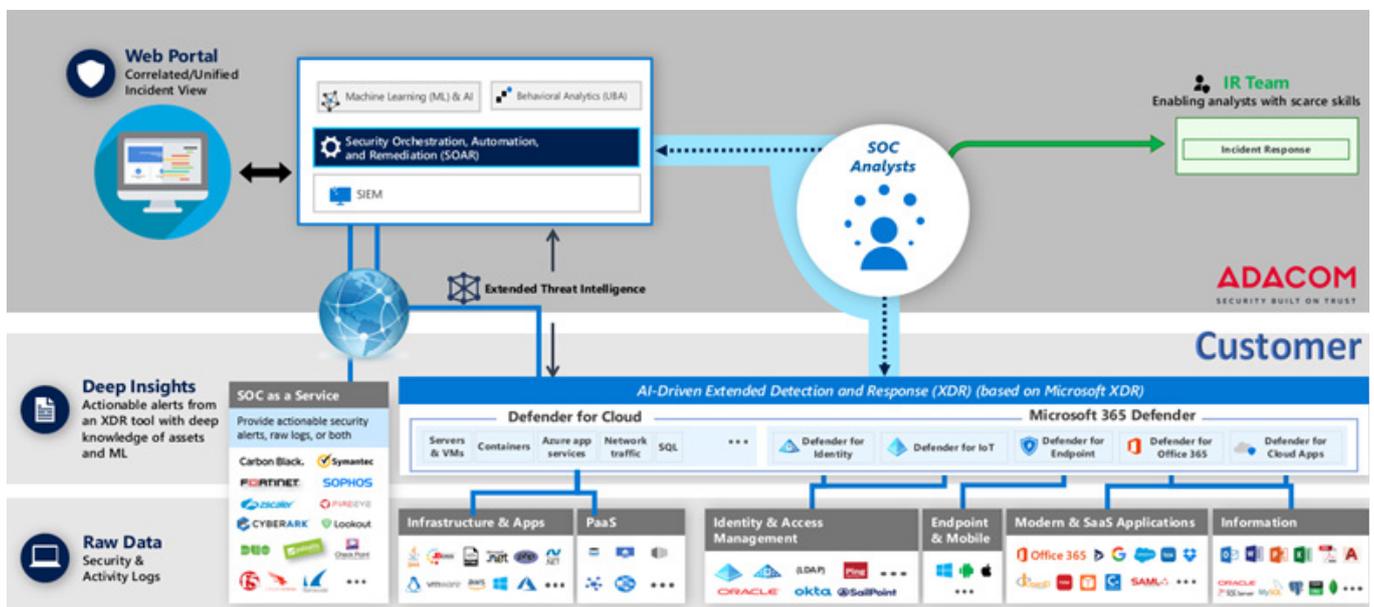
SOC as a Service (SOCaaS)

⭨ **The SOC as a Service (SIEM-based) solution,** powered by IBM QRadar and Microsoft Sentinel, ensures AI-enhanced threat detection by analyzing massive datasets, correlating security events, and identifying anomalies in real time. Advanced AI models enable faster triage, reducing false positives while prioritizing critical threats. The integration of automation streamlines incident response, allowing security teams to detect, investigate, and remediate threats faster than ever before.

Managed Detection and Response (MDR)

⭨ **Our Managed Detection and Response (MDR) service** leverages Microsoft Defender for Endpoint, Cisco Secure Endpoint, CrowdStrike, and FortiEDR, incorporating AI-driven behavioral analytics to identify malicious activities, lateral movement, and advanced persistent threats (APTs). The use of AI enhances adaptive defense strategies, learning from past attacks to improve threat detection accuracy and response speed, ensuring zero-trust security principles are upheld across the organization's infrastructure.

AI-Driven XDR

⭨ **With AI-Driven XDR powered by Microsoft XDR,** ADACOM correlates security signals across multiple attack vectors, including endpoints, identities, cloud workloads, and applications. AI-powered automation dynamically analyzes threat patterns, stopping attacks before they cause harm. The intelligent fusion of security telemetry enables faster root cause analysis, improving threat visibility across hybrid and multi-cloud environments.

Extended Threat Intelligence

↘ **Threat Intelligence is at the heart of ADACOM's SOC services,** providing organizations with real-time insights into emerging cyber threats. By leveraging open-source, commercial, and proprietary intelligence feeds, ADACOM delivers actionable threat intelligence that enhances detection capabilities and strengthens security defenses. Through continuous monitoring of TTPs (Tactics, Techniques, and Procedures) used by threat actors, our SOC proactively adapts security measures to counter evolving threats. The integration of MITRE ATT&CK, STIX/TAXII, and AI-driven analytics enables organizations to anticipate attacks, reduce risk exposure, and enhance decision-making in cybersecurity operations.

↘ **Attack Surface Management (ASM) uses AI-driven asset** discovery and continuous monitoring to map, assess, and secure the organization's external-facing infrastructure. By identifying exposed services, shadow IT, and potential vulnerabilities, ASM enables a proactive defense strategy, significantly reducing cyber risk.

↘ **Digital Risk Protection (DRP) enhances security beyond traditional SOC capabilities,** utilizing AI-based deep web and dark web monitoring to detect brand impersonation, credential leaks, phishing campaigns, and emerging cyber threats in real time. By delivering actionable insights and automated risk mitigation, organizations can effectively protect their brand reputation, employees, and sensitive data from external digital threats.

Proactive Threat Hunting

↘ **Our Proactive Threat Hunting service** integrates AI-assisted threat intelligence, leveraging frameworks like MITRE ATT&CK and machine-learning-driven anomaly detection. By continuously analyzing behavioral patterns, detecting advanced attack techniques, and proactively searching for hidden adversaries, ADACOM ensures organizations stay ahead of emerging cyber threats.

Incident Response

↘ **Incident Response is at the core of ADACOM's SOC services**, providing both proactive and reactive security measures to minimize the impact of cyber incidents. Our proactive approach includes threat anticipation, security posture assessments, and breach simulation exercises, ensuring organizations are prepared for emerging threats. In the event of a security breach, our reactive incident response team delivers rapid containment, forensic analysis, root cause investigation, and coordinated response actions to mitigate damage and restore operations efficiently.

↘ **By integrating Artificial Intelligence, automation, threat intelligence, and expert-driven cybersecurity strategies, ADACOM's SOC services deliver next-generation cyber resilience.** AI-powered analytics enhance threat prediction, real-time response, and security orchestration, enabling organizations to detect, respond, and recover from cyber threats with unparalleled efficiency. Our AI-Driven SOC ensures continuous adaptation to the ever-changing threat landscape, making security proactive, intelligent, and future-ready.

Contact Us

www.adacom.com

GREECE / HQ
25, Kreontos str., 104 42
Athens, Greece
+30 210 51 93 700
info@adacom.com

GREECE / Thessaloniki Office
10th km Thessalonikis - Thermis
570 01, Thermi, Thessaloniki
+30 2310 474 296
info@adacom.com

CYPRUS
10, Katsoni str., 1082
Nicosia, Cyprus
+357 22 444 071
infocy@adacom.com

KINGDOM OF BAHRAIN
Manama Center, Blog: 316
Road: 383, Building: 128 Flat/
Office: 2030
info@adacom.com