BLACK BOX

FLYER
MANAGED SOC



Managed Security Operations and AI-led Orchestration

Security operations and services delivered at the pace of innovation

Cyber threats are accelerating, targeting critical infrastructure, enterprises, and government entities across the UAE. With increasing regulatory oversight and rising cyber risks, organizations must adopt proactive, intelligence-driven Security Operations Center (SOC) to protect their digital assets.

The UAE has emerged as a hub for digital innovation, smart cities, and cloud transformation, increasing demand for localized, sovereign cybersecurity capabilities that ensure data residency, regulatory compliance, and rapid incident response.

Black Box SOC-as-a-Service delivers a fully managed, UAE-based sovereign SOC, enabling organizations to monitor, detect, investigate, and respond to threats in real time, while ensuring compliance with UAE data protection and cybersecurity regulations.

Need for SOC Operations in the UAE

Organizations operating in the UAE face growing pressures to:

- Comply with UAE cybersecurity regulations and data sovereignty mandates
- Protect critical infrastructure and sensitive data from advanced cyber threats
- Maintain 24/7 visibility across hybrid IT and OT environments
- Address increasing risks from cloud adoption, remote work, and digital transformation
- Reduce incident response time and minimize impact

A locally hosted, sovereign SOC is critical for ensuring that security operations align with national regulatory requirements while delivering faster response and stronger threat visibility.

Business Challenges

Organizations generally encounter challenges, which include:

- A lack of centralized visibility across IT, OT, cloud, and endpoint environments
- Shortage of skilled cybersecurity professionals to manage SOC operations
- Increasing complexity of tools and security technologies
- Delayed detection and response to advanced persistent threats
- Difficulty in meeting regulatory compliance and audit requirements
- High costs associated with building and managing in-house SOCs
- Limited capabilities in threat intelligence, threat hunting, and proactive defense

Black Box Solution: Sovereign SOC-as-a-Service

- Black Box offers a locally operated SOC service in the UAE, delivering end-to-end security operations tailored to your organization
- Effective security is adaptive and locally compliant
- Our solution integrates security technologies, expert analysts, and automation to deliver real-time, actionable intelligence and rapid incident response

Black Box Global SOC Strength

- Five global SOC centers providing follow-the-sun operations
- Expertise across eight different SIEM platforms
- Multi-industry experience with enterprise and government clients
- Vendor-agnostic approach ensuring best-fit solutions
- Certified and experienced cybersecurity analysts

Core Capabilities

Security Monitoring & Analytics

- 24/7 monitoring from UAE-based SOC
- Real-time detection of threats across networks, endpoints, and cloud
- Advanced correlation using multi-SIEM architecture (8+ SIEM platforms globally)

EDR & XDR

- Endpoint Detection & Response (EDR) for endpoint-level protection
- Extended Detection & Response (XDR) for unified visibility across:
  - Endpoints
  - Networks
  - Cloud workloads
  - Applications

SIEM (Security Information & Event Management)

- Centralized log collection and analysis
- Real-time incident correlation and alerting
- Compliance reporting aligned with UAE regulations

SOAR (Security Orchestration, Automation & Response)

- Automation of repetitive SOC tasks
- Faster incident triage and response
- Reduced Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)

Threat Intelligence Platform (TIP)

- Integration of global and regional threat intelligence feeds
- Contextual threat analysis for proactive defense
- Continuous updates on emerging cyber threats

Threat Hunting

- Proactive detection of hidden and emerging threats
- Behavioral and anomaly-based analysis
- Continuous improvement of detection mechanisms

Brand Monitoring & Digital Risk Protection

- Monitoring of brand misuse, phishing, and impersonation attempts
- Early detection of dark web exposure
- Protection of organizational reputation and customer trust

Why Partner with Black Box

Organizations benefit from:

- Sovereign Security Operations with UAE data residency
- 24/7 Managed SOC without infrastructure investment
- Faster detection and response to cyber threats
- Stronger compliance with regional cybersecurity regulations
- Reduced operational complexity through integrated security stack
- Access to global expertise and security technologies
- Improved ROI on security investments
- Proactive risk mitigation through threat intelligence and hunting

Technology Partnerships

CROWDSTRIKE · SentinelOne · securonix · seceon · RAPID7 · IBM Radar · exabeam · FORTINET · Microsoft Sentinel · D3 SECURITY · AIRRIVED

CONTACT@BLACKBOX.COM