Exotech Advances SOC AI for Autonomous and Sovereign Security Operations in Saudi Arabia

SOC AI combines AI-driven investigation, human-approved response, Arabic workflows and flexible deployment for modern Saudi security operations.



SOC AI

RIYADH, SAUDI ARABIA, September 26, 2026 /EINPresswire.com/ -- Exotech, a Saudi technology company specializing in artificial intelligence, data and digital transformation, is advancing SOC AI, its autonomous security operations platform designed to help organizations detect, investigate and respond to cyber threats while maintaining control over sensitive data and critical security decisions.

As Security Operations Centers face increasing alert volumes, fragmented security tools and pressure to respond faster, organizations are looking for ways to introduce artificial intelligence without creating new operational, governance or data-sovereignty risks.

SOC AI is designed around that challenge.

The platform connects with existing security technologies, including SIEM, Endpoint Detection and Response and other enterprise security tools, allowing alerts to flow into a unified investigation and response workflow.

Artificial intelligence can enrich security events with threat intelligence, assist with classification and support response actions, while human analysts retain oversight of consequential decisions.

“Artificial intelligence should increase the capability of the security team without removing

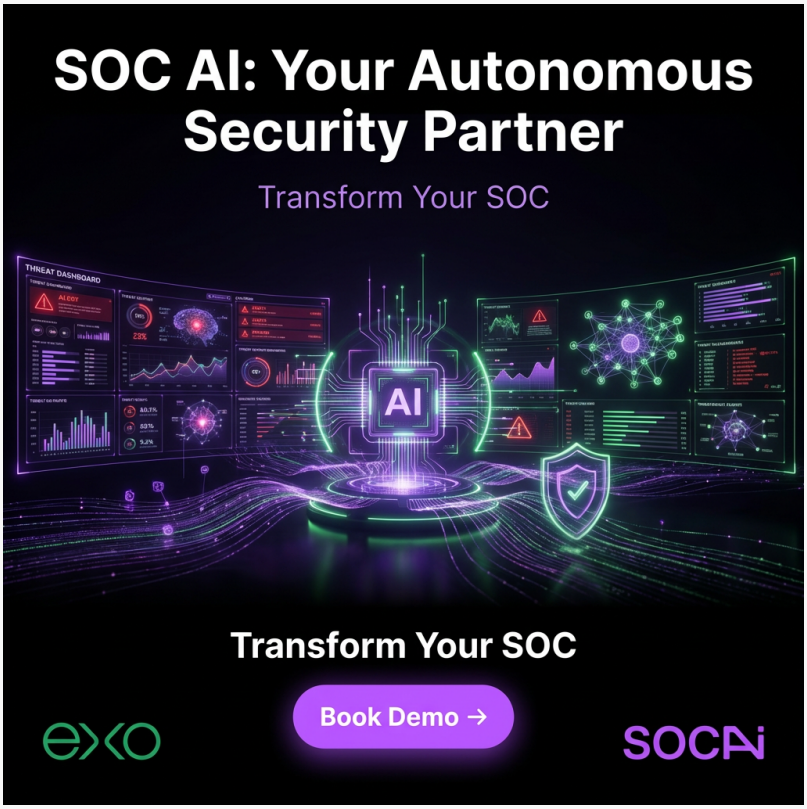
accountability from the people responsible for protecting the organization," said Ghannam Al Ghannam, CEO of Exotech. "SOC AI is designed to combine automation, visibility and local control so organizations can move faster while maintaining trust in the security process."

From Alert to Action

Traditional Security Operations Centers often require analysts to move between multiple tools before they can determine whether an event represents a genuine security threat.

SOC AI is designed to simplify that workflow through four connected stages: ingest, analyze, respond and report.

Security alerts can be collected automatically from connected systems and enriched with additional threat context.



SOC AI

Exotech Logo

The platform then uses AI-assisted analysis to help determine whether activity requires further investigation and can support the preparation of response actions.

Following investigation and response, the platform maintains an audit trail and provides reporting and dashboard capabilities for security teams and management.

> AI should increase the capability of the security team without removing accountability, data control or human oversight."
>
> *Ghannam Al Ghannam, CEO of Exotech*

This approach is intended to reduce repetitive manual triage and allow security professionals to spend more time on threat hunting, complex investigations and higher-value security decisions.

Human Oversight at the Center

As AI becomes more deeply integrated into cybersecurity operations, organizations increasingly need transparency around how automated decisions are made and executed.

SOC AI is built around a human-in-the-loop model.

Artificial intelligence can recommend actions and accelerate security workflows, while analysts can retain approval authority over critical response activities.

The platform also records investigation activity, security decisions and response actions to provide traceability for operational review, governance and compliance reporting.

This gives organizations a path toward greater automation without turning critical security decisions into an invisible process.

Designed for Data Sovereignty

Cybersecurity platforms process some of an organization's most sensitive operational information.

For Saudi organizations, particularly those operating in regulated or critical sectors, control over where that information is processed can be an important part of cybersecurity architecture.

SOC AI supports cloud, on-premises, hybrid and air-gapped deployment models.

Organizations can therefore select a deployment architecture according to their infrastructure, security and data-residency requirements.

On-premises deployment enables organizations to operate SOC AI within their own infrastructure, while hybrid deployment can combine local processing with cloud-based capabilities.

For environments where internet connectivity is restricted or prohibited, SOC AI can also operate in an air-gapped architecture using local AI models.

AI for Isolated and Critical Environments

Many modern AI platforms depend on permanent connectivity to external cloud services.

That model is not suitable for every cybersecurity environment.

SOC AI's air-gapped deployment model is designed for organizations that require isolated processing, including certain government, defense, utilities, energy and critical-infrastructure environments.

Local AI support allows security operations to use AI-assisted investigation capabilities without requiring continuous access to an external AI service.

This gives organizations greater flexibility in deciding where AI processing takes place and how closely the platform is integrated into sensitive networks.

Arabic-Native Security Operations

SOC AI has also been developed for Arabic-speaking security teams.

The platform supports Arabic-language interfaces and right-to-left workflows alongside English, helping organizations operate security processes in the language most appropriate for their teams.

For Saudi and GCC organizations, this localization can reduce the need to adapt international security platforms to local-language operational requirements.

Supporting Saudi Cybersecurity Requirements

Exotech has designed SOC AI with Saudi cybersecurity and data-protection requirements in mind.

The platform includes audit trails, security logging, reporting, data-residency options and control-mapping capabilities intended to support organizations working with frameworks such as the National Cybersecurity Authority Essential Cybersecurity Controls and other applicable Saudi cybersecurity requirements.

SOC AI also includes reporting capabilities that can help organizations organize security evidence and prepare for internal governance and regulatory reviews.

One Platform Across the SOC Workflow

SOC AI brings together alert management, investigation workflows, automated actions, threat intelligence, analytics and administrative controls within a unified platform.

The objective is to reduce the operational complexity created when security teams depend on multiple disconnected tools for investigation, workflow management and response.

For organizations with growing security environments, this approach can help create a more consistent workflow from detection through investigation, action and reporting.

“Security operations are moving toward a model where AI assists analysts continuously rather

than functioning as a separate tool," Al Ghannam added. "Our focus is to make that transition practical for Saudi organizations while preserving human oversight, data control and operational transparency."

A Saudi Approach to AI-Driven Security Operations

The increasing use of artificial intelligence is changing how Security Operations Centers operate.

Exotech believes that this transformation in Saudi Arabia must address more than automation alone.

Language, local deployment, data sovereignty, auditability and regulatory requirements all need to be considered as organizations introduce AI into cybersecurity operations.

SOC AI brings these capabilities together within a platform designed for enterprise, regulated and security-sensitive environments.

Organizations can request a personalized demonstration of SOC AI based on their own threat scenarios, security environment and preferred deployment model.

About Exotech

Exotech is a Saudi technology company headquartered in Riyadh, providing solutions across artificial intelligence, machine learning,

Ghannam Al Ghannam
Exotech
email us here
Visit us on social media:
LinkedIn
Facebook
X

This press release can be viewed online at: https://www.einpresswire.com/article/945438908

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.