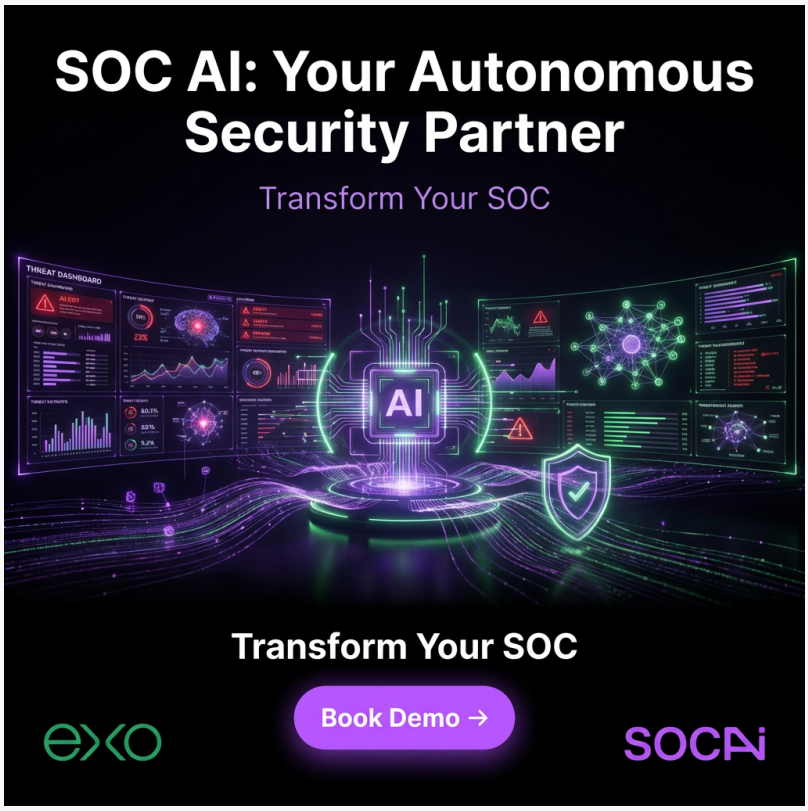
Exotech Expands SOC AI for Sovereign and Air-Gapped Security Operations in Saudi Arabia

Arabic-native AI, local deployment and human-controlled response bring autonomous security operations to regulated and critical environments.



SOC AI

RIYADH, SAUDI ARABIA, September 20, 2026 /EINPresswire.com/ -- Exotech, a Saudi technology company specializing in artificial intelligence, data and digital transformation, is advancing its SOC AI platform to address one of the most important challenges facing organizations adopting artificial intelligence in cybersecurity: how to gain the speed and automation benefits of AI without giving up control of sensitive security data, critical decisions or operational visibility.

SOC AI combines AI-assisted threat investigation, automated security workflows and human oversight with deployment options that include cloud, on-premises, hybrid and fully air-gapped environments.

> Saudi organizations need AI that moves at machine speed without sacrificing sovereignty, control or human oversight."
>
> *Ghannam Al Ghannam, CEO of Exotech*

For organizations operating critical or highly sensitive infrastructure, SOC AI can run using local AI models without dependence on external internet connectivity, helping security operations remain within controlled environments.

"Artificial intelligence in cybersecurity cannot come at the expense of sovereignty or control," said Ghannam Al Ghannam, CEO of Exotech. "Saudi organizations need technology that can move at machine speed while

respecting where data is processed, who approves critical actions and how every decision is recorded. That is the principle behind SOC AI."

Security Automation Without Giving Up Control

SOC AI is designed to integrate with existing security technologies including SIEM platforms, Endpoint Detection and Response systems and other enterprise security tools.

Security alerts can be ingested, enriched with contextual information and analyzed using AI to help determine whether activity may represent a genuine threat.

The platform can then prepare or coordinate response actions while maintaining human oversight over consequential security decisions.



SOC AI

Exotech Logo

Rather than operating as an invisible automation layer, SOC AI follows a human-in-the-loop model in which analysts can review and control critical actions.

Security events, AI verdicts, approvals and response actions can also be retained within an audit trail to improve accountability, investigation and reporting.

Designed for Data Sovereignty

For regulated and security-sensitive organizations, the location and handling of cybersecurity data are becoming increasingly important.

SOC AI supports multiple deployment models, allowing organizations to select an architecture that aligns with their operational and security requirements.

The platform can be deployed through cloud infrastructure, within an organization's own environment, in hybrid architectures or in fully isolated air-gapped networks.

Local and isolated deployment models are intended to help organizations retain control over sensitive cybersecurity information and reduce dependence on external infrastructure.

This approach is particularly relevant for government, energy, utilities, financial services, healthcare and other sectors where cybersecurity operations can involve sensitive operational or regulated information.

AI for Air-Gapped and Critical Environments

Many modern AI platforms depend on continuous connectivity to external cloud environments.

That model is not suitable for every organization.

SOC AI can support local AI models and isolated deployments, enabling AI-assisted security investigations and workflows in environments where external connectivity is restricted or prohibited.

This creates an opportunity for organizations operating critical infrastructure or isolated networks to introduce AI into their security operations without creating a continuous dependency on external AI services.

Arabic-Native Security Operations

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

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

Exotech's conversational investigation capabilities also allow analysts to investigate security activity using natural-language interaction in Arabic and English.

This approach is designed to make AI-assisted security operations more accessible to organizations in Saudi Arabia and the wider GCC while reducing the need to adapt global security technologies to local language requirements.

Supporting Saudi Cybersecurity Requirements

SOC AI has been developed with Saudi cybersecurity and data-protection requirements in mind.

Capabilities such as security logging, audit trails, controlled data processing and reporting can support organizations working within Saudi regulatory and cybersecurity frameworks.

The objective is to help organizations introduce AI-driven security operations while maintaining the visibility and governance expected in regulated environments.

From Alert Management to AI-Assisted Operations

Traditional Security Operations Centers often require analysts to spend significant amounts of time manually reviewing and prioritizing alerts before investigations can begin.

SOC AI is designed to automate more of these repetitive first-line activities.

The platform can ingest security alerts, enrich them with additional information, assist with classification and coordinate investigation workflows so security teams can focus more heavily on complex investigations, threat hunting and response decisions.

Exotech structures this workflow around four stages: ingest, analyze, respond and report.

The result is intended to move security operations from alert-heavy manual processes toward a more coordinated AI-assisted operating model.

“AI should expand what the security team can accomplish, not remove accountability from the security team,” Al Ghannam added. “Our focus is to combine automation with visibility, local control and a clear audit trail.”

A Saudi Approach to Autonomous Security

The growth of artificial intelligence is beginning to change how organizations design and operate their Security Operations Centers.

For Saudi organizations, Exotech believes that transformation must address not only automation and response speed, but also language, local deployment, governance and data sovereignty.

SOC AI brings those considerations together within one security operations platform designed for enterprise and security-sensitive environments.

Organizations can evaluate SOC AI through a personalized demonstration using their own security scenarios, deployment requirements and investigation workflows.

About Exotech

Exotech is a Saudi technology company headquartered in Riyadh, delivering solutions across artificial intelligence, machine learning, agentic AI, data strategy and governance, analytics, automation and digital transformation.

The company works with government organizations and enterprises to develop secure and scalable technology solutions designed for the requirements of Saudi Arabia and the wider region.

For more information, visit exotech.com.sa/soc-ai.

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/943724708

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.