

Exotech Advances SOC AI with 7 HARES™ to Bring AI-Powered Security Investigations to Saudi Enterprises

Exotech Advances SOC AI with 7 HARES™

RIYADH, SAUDI ARABIA, September 1, 2026 /EINPresswire.com/ -- [Exotech](#), a Saudi emerging technology company specializing in artificial intelligence, data and digital transformation, is advancing its [SOC AI](#) platform with [7 HARES™](#), an AI-powered investigation

layer designed to help Security Operations Center teams investigate threats, understand attack context and accelerate response.



“

Organizations need speed, but they also need trust. SOC AI is designed to give security teams both while keeping critical security decisions in human hands.”

*Ghannam Al Ghannam, CEO
of Exotech*

Security teams today operate across increasingly complex environments, with alerts distributed across SIEM platforms, endpoint security tools, identity systems, network infrastructure and threat intelligence sources. Investigating a single incident can require analysts to move between multiple systems, manually correlate events and reconstruct the sequence of an attack.

Exotech's SOC AI is designed to reduce that burden.

Through 7 HARES™, analysts can interact with security investigations using natural language in Arabic or English. The platform can gather relevant evidence from connected security systems, correlate related events and help construct an evidence-backed picture of an incident.

Instead of simply presenting another alert, SOC AI is designed to help answer the questions behind it: what happened, which assets or users are affected, how the activity is connected and what action should be considered next.

“The future of the SOC is not simply about adding more automation. It is about helping security

teams understand what is happening, make better decisions and respond faster without giving up control,” said Ghannam Al Ghannam, CEO of Exotech. “With SOC AI and 7 HARES™, artificial intelligence works alongside the analyst — connecting the evidence, explaining the situation and preparing the response while keeping critical decisions in human hands.”

From Alerts to Evidence-Driven Investigations

Traditional SOC workflows often require security analysts to manually examine multiple sources before determining whether activity represents a genuine threat.

7 HARES™ introduces a conversational investigation model.

Security analysts can ask questions about suspicious activity, affected systems, indicators of compromise or relationships between different security events. SOC AI can then use available information from connected security technologies to build investigation context and support analyst decision-making.

The objective is to reduce repetitive investigation work while allowing security professionals to focus more heavily on threat assessment, risk and response.

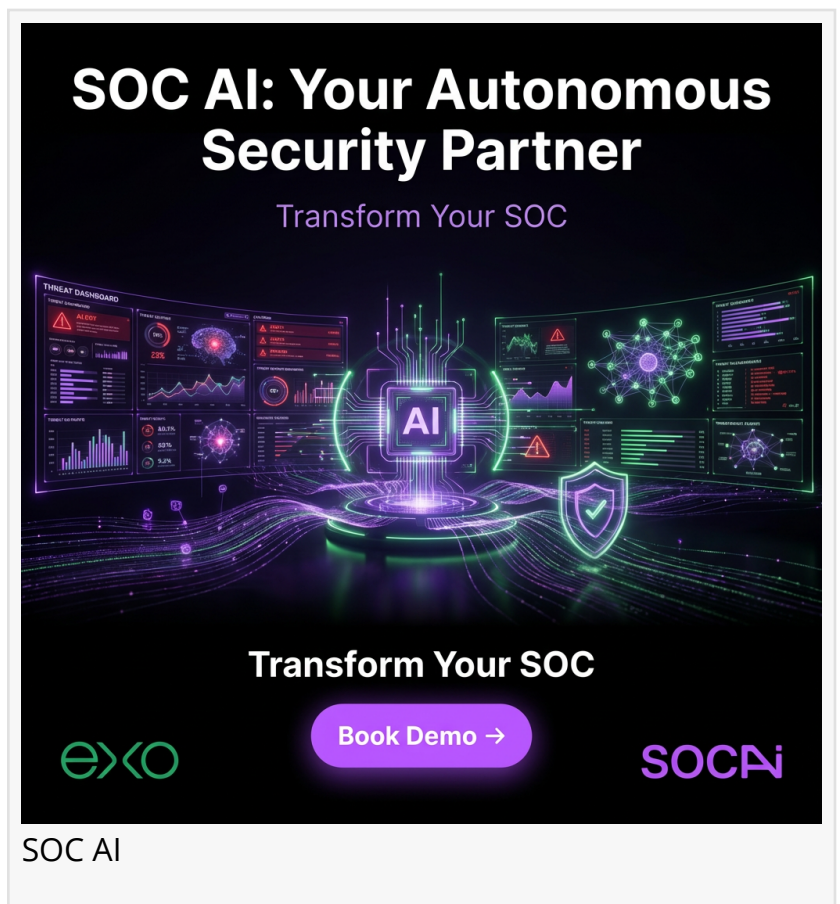
Human Oversight Remains Central

As artificial intelligence becomes more involved in cybersecurity operations, organizations increasingly need to balance automation with governance and accountability.

Exotech designed SOC AI around a human-in-the-loop operating model.

When the platform recommends consequential actions, analysts retain the ability to review, modify, approve or reject those actions before execution.

This approach allows organizations to benefit from AI-assisted investigation without removing human judgment from critical security decisions.

The advertisement features a dark background with glowing green and blue digital elements. At the top, the text "SOC AI: Your Autonomous Security Partner" is displayed in large, bold, white font, with "Transform Your SOC" in a smaller, purple font below it. The central graphic shows a futuristic interface with multiple panels displaying charts, graphs, and data. A prominent "AI" logo is surrounded by glowing lines and a shield icon with a checkmark. At the bottom, the text "Transform Your SOC" is repeated in white, followed by a purple button labeled "Book Demo →". The Exotech logo (eXO) is on the left and the SOC AI logo is on the right. Below the advertisement, the text "SOC AI" is written in a simple, white font.

SOC AI: Your Autonomous Security Partner

Transform Your SOC

Transform Your SOC

[Book Demo →](#)

eXO SOC AI

SOC AI

Investigation evidence, recommendations, approvals and actions can also remain traceable, providing organizations with greater visibility into how artificial intelligence is being used within their security operations.

Built for Saudi and GCC Environments

SOC AI and 7 HARES™ have been developed with the operational needs of organizations in Saudi Arabia and the wider GCC in mind.

The platform supports Arabic and English investigation workflows, allowing security teams to interact with the system in the language most appropriate for their operations.

Deployment models can include on-premises, hybrid and isolated environments, providing greater flexibility for organizations with strict requirements around infrastructure, sensitive security information and data control.

This approach is particularly relevant for organizations operating critical infrastructure, government environments and other security-sensitive sectors.

Working With the Existing Security Stack

SOC AI is designed to work alongside existing cybersecurity investments rather than requiring organizations to replace their current security architecture.

The platform can support investigation workflows involving technologies such as SIEM, Endpoint Detection and Response, identity systems, network security platforms and threat intelligence sources.

By connecting information from multiple security systems, SOC AI aims to help turn fragmented security alerts into coherent investigations that analysts can understand and act upon.

Toward an AI-Assisted SOC

The growing role of AI in cybersecurity is beginning to change how SOC teams operate.

Rather than spending significant amounts of time collecting evidence, switching between tools and conducting repetitive investigation steps, AI can increasingly assist with information gathering, correlation and investigation preparation.

Security professionals can then concentrate on the areas where human expertise remains most important: judgment, threat hunting, risk analysis and response decisions.

“Autonomous security should not mean invisible security,” Al Ghannam added. “Organizations need speed, but they also need trust. Our objective is to give security teams both.”

Organizations interested in SOC AI and 7 HARES™ can learn more or request a demonstration at Exotech's SOC AI website.

About Exotech

Exotech is a Saudi emerging technology company headquartered in Riyadh, providing 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, scalable technology solutions designed for the requirements of Saudi Arabia and the wider region.

For more information, visit exotech.com.sa.

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/938611400>

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.