Infratech Expands NCA-Licensed mSOC Services for Saudi Organizations

24/7 monitoring, threat intelligence and incident response help Saudi organizations strengthen security operations and cyber resilience.

mSOC

infratech

RIYADH, SAUDI ARABIA, September 1, 2026 /EINPresswire.com/ -- Infratech, a Saudi cybersecurity and technology services provider, is strengthening its Managed Security Operations Center services to help organizations across the Kingdom improve threat visibility, accelerate incident response and maintain continuous security monitoring.

Operating through an NCA-licensed Managed Security Operations Center, Infratech provides organizations with around-the-clock cybersecurity monitoring and access to experienced security professionals without requiring enterprises to build and maintain an entire Security Operations Center internally.

As Saudi organizations continue to expand cloud services, digital infrastructure, connected systems and critical operations, security teams face a growing challenge: detecting increasingly sophisticated threats while managing large volumes of security alerts across multiple technologies.

Infratech's mSOC is designed to help address this challenge through continuous monitoring, investigation and response capabilities tailored to Saudi organizations and regulatory environments.

> Cybersecurity requires continuous visibility, experienced people and rapid response. Our mSOC gives Saudi organizations access to those capabilities around the clock."
>
> *Eng. Ayman Alsuhaim, CEO of Infratech*

"Cybersecurity today requires continuous visibility, experienced people and the ability to respond quickly when something changes," said Eng. Ayman Alsuhaim, CEO of Infratech. "Our mSOC gives organizations access to those capabilities around the clock while allowing their internal teams to remain focused on their core business and strategic security priorities."

24/7 Managed Security Operations

Infratech's mSOC provides continuous security monitoring and analysis to help organizations identify potential threats and suspicious activity before they escalate into major incidents.

The managed service can support capabilities including real-time threat monitoring and alerting, incident investigation and response, SIEM management and log correlation, threat intelligence integration and security reporting.

By centralizing monitoring and investigation activities, organizations can gain greater visibility across their security environment while reducing the operational burden placed on internal IT and cybersecurity teams.

The service is designed for organizations that need enterprise-level security operations capabilities but may not want to build, staff and operate a complete SOC independently.

From Detection to Incident Response

Detecting a security alert is only the beginning of an effective cybersecurity operation.

Infratech's managed security services are designed to support organizations throughout the security lifecycle, from identifying suspicious activity through investigation, containment and response.

Security analysts continuously review security events and investigate activity across connected environments, helping organizations distinguish meaningful threats from routine alerts.

When potentially malicious activity is identified, incident response processes can be initiated to help organizations contain the threat, understand its impact and reduce potential disruption.

This approach helps reduce dwell time — the period during which a threat can remain undetected inside an environment — while giving organizations access to security specialists who monitor threats continuously.

Combining Managed and Offensive Security

A key element of Infratech's cybersecurity approach is the combination of managed defense with offensive security expertise.

While the mSOC focuses on continuous monitoring, detection and response, Infratech's Offensive Security team helps organizations proactively discover weaknesses before attackers can exploit them.

Offensive Security services include penetration testing, red teaming, vulnerability assessments, application and API security testing and other adversarial security exercises.

Together, these capabilities allow organizations to approach cybersecurity from both sides: continuously monitoring for active threats while actively testing whether existing defenses can withstand real-world attack techniques.

The result is a cybersecurity model built around identifying weaknesses, improving defenses and continuously monitoring the environment for signs of malicious activity.

Built for Saudi Organizations

Infratech's cybersecurity operations are based in Saudi Arabia and are designed around the operational and regulatory requirements organizations face within the Kingdom.

The company operates an NCA-licensed mSOC and provides cybersecurity services for both government and private-sector organizations.

Infratech's managed security portfolio can also support organizations working toward requirements and security frameworks relevant to Saudi Arabia, while providing local cybersecurity expertise and support.

For organizations operating in regulated sectors, government, financial services, critical infrastructure and other security-sensitive environments, access to local security operations can help simplify cybersecurity management while supporting requirements around visibility, governance and data control.

Extending Existing Cybersecurity Investments

Organizations frequently operate security environments containing multiple products across endpoint protection, network security, identity, cloud services, SIEM platforms and threat intelligence.

Infratech's managed security approach is designed to work with and optimize these existing cybersecurity investments rather than requiring organizations to replace their security architecture.

Security platform integration, SIEM monitoring, endpoint security, threat hunting and incident management can be incorporated into the managed service model according to each organization's environment.

This enables organizations to gain greater value from cybersecurity technologies they already operate while adding the continuous monitoring and expertise of a managed security team.

A More Sustainable SOC Model

Building an internal 24/7 Security Operations Center requires investment in technology, infrastructure, processes and — most importantly — skilled cybersecurity professionals.

For many organizations, maintaining sufficient staffing across continuous shifts while retaining specialized security expertise can become a significant operational challenge.

A managed SOC model gives organizations another option.

By extending internal teams with dedicated security monitoring, threat hunting, incident response and advisory capabilities, organizations can build a more sustainable approach to continuous security operations while maintaining visibility into their cybersecurity posture.

“Our objective is not simply to generate more alerts,” Alsuhaim added. “The objective is to give organizations the visibility, expertise and response capability they need to make better security decisions and protect their operations.”

Organizations interested in Infratech's Managed Security Operations Center and cybersecurity services can contact the company to discuss their security environment and managed-service requirements.

About Infratech

Infratech is a Saudi technology and cybersecurity services provider headquartered in Riyadh.

The company provides cybersecurity services across managed security, NCA-licensed mSOC operations, governance and compliance, cybersecurity technologies, incident response and forensics, offensive security, OT security, training and awareness.

Infratech serves government and private-sector organizations across Saudi Arabia with cybersecurity and technology services designed to strengthen resilience, improve visibility and

support secure digital operations.

For more information, visit www.infratech.com.sa.

Ayman Al Suhaim
Infratech
email us here
Visit us on social media:
LinkedIn
Facebook
X
