

Enhance Enterprise-Wide

Cyber Resilience with
Effective SOCaaS

TABLE OF CONTENTS

- 01 Executive Summary
- 02 Today's Advanced Persistent Threats Intensify Cyber Insecurity
- 03 The Need of Modern Businesses: Building Resilience into Security Architecture
- 04 Security Teams Consistently Strengthen Security Operations, but Challenges Persist
- 05 What Makes a Security Operations Center Effective?
- 06 Building the Case for an Effective SOC Through Next-Gen MSSPs
- 07 Key Recommendations for Choosing a Reliable and Efficient MSSP
- 08 Maximize SOC Effectiveness Through SAMI-AEC SOCaaS
- 09 Conclusion
- 10 References

EXECUTIVE SUMMARY

The growing sophistication and frequency of today's cyberattacks have necessitated the need for highly advanced cyber defense strategies across all types and sizes of organizations. As cybercriminals continue to experiment with new tactics, techniques, and procedures, enterprises continue to be at a heightened risk of falling prey to extortion attempts, novel phishing schemes, and unusual malware attacks. [5] Owing to this exceptionally advanced and collaborative cyberattack environment, enterprises across the globe are recognizing the business value of a modern security operations center (SOC).

Future-facing SOCs can empower security-conscious organizations to robustly counter cyber threats, implement proactive incident response (IR) strategies, and identify indicators of compromise (IoCs) in near real time. However, owing to the overwhelming burden of security alerts and shortage of analyst talent, internal security operations teams perform better with the assistance and skilled support of managed security service providers (MSSPs). [9]

Internal security operations teams can perform better with the skilled assistance of managed security service providers (MSSPs).

The business case for security operations center-as-a-service (SOCaaS) is well-acknowledged by leading enterprises. But what stands crucial is understanding the meaning of building a resilient and effective SOCaaS. This whitepaper will shed light on the contemporary cybersecurity scenario, SOC maturity opportunities for next-gen companies, and outline suggestions to build a robust security posture with the support of a security operations center as a service.



Today's Advanced Persistent Threats Intensify Cyber Insecurity

In an age of highly distributed and fragmented company networks, operations, and applications, corporate security teams face complex challenges in securing their enterprise's ecosystems. The rampant rise in collaboration among cybercriminals and emergence of new types of vulnerabilities has severely burdened security professionals and organizations alike. In this context, the need for an effective and competent security operations center (SOC) is more pronounced than ever before. [5]

31,000

New vulnerabilities discovered by organizations over 2020-21 [1]

11,047

Daily average of security alerts faced by IT security teams [4]

107%

Year-over-year increase in ransomware and extortion operations in 2021 [5]

The challenge of responding to an exceedingly uncertain and innovative threat landscape is further intensified by shortage in security skills talent and misalignment between business goals and security needs. Globally, organizations consistently raise concerns over their inability to retain or hire skilled security talent. Adding to this, almost two-thirds of IT security teams still rely on legacy endpoint security solutions – a major barrier in realizing robust cyber resilience. [4]

42%

of companies cite risk, compliance, security & privacy skills as the most vital to hire or develop. [1]

Organizations in Saudi Arabia Respond to the Need for Next-Level Cybersecurity

Saudi Arabia's prominence in the Middle East, and the world, has made it imperative for its enterprises to build an impenetrable cybersecurity net. Developing a strong cyber defense can enable the Kingdom to preserve its national sovereignty, promote economic stability, and accelerate digital transformation. This can create a secure environment that supports regional and international business collaboration, while positively contributing to the global cybersecurity landscape. Consequently, companies across KSA are directing their business goals and resources to create a resilient cybersecurity environment, with many opting to manage their SOC via third-party security vendors. [9]

Cybersecurity Spending Forecast in KSA's Organizations (in SAR Millions) [7]

604

Security services

259

Network security equipment

195

Infrastructure protection

176

Identity access management

*Forecast for 2023

The Need of Modern Businesses: Building Resilience into Security Architecture


Rise in the ingenuity of cyberattacks has magnified the need for running next-gen SOC's. Companies are now rapidly adopting emerging cybersecurity technologies to strengthen their security posture for built-in resilience. But as enterprises turn to advanced technologies, it is equally crucial to adopt a proactive security strategy, while recognizing that MSSPs are indispensable to attain enterprise-wide cyber resilience. [3]

Essentials to Enhance Organizational Cyber Resilience

1. Align security maturity with business goals

Security risks should be shared across the executive team to build security advocates in the business. Risk-based business review promotes more informed, meaningful, and security-first actions.


Only **21%** of SOC leaders feel that their SOC is fully aligned with their business needs. [3]



3. Actively pursue Zero Trust principles

Zero Trust helps to constantly monitor the perimeters, processes, users, and services across an organization's security posture. Its strong emphasis on verification and authentication increases the possibility of identifying potential threats.


43% of firms cited that a Zero Trust strategy helped to improve their SOC's efficiency. [2]



2. Integrate security operations and products

Multiple security solutions that are poorly integrated prevent security teams from focusing on higher-value security tasks. Companies can improve their overall security operations with fewer, better integrated solutions [6] – a benefit offered by MSSPs.


80% of firms are executing/interested in a vendor consolidation strategy for more efficient security. [6]



4. Access analyst and security skills via MSSPs

The security skills gap in companies can be readily bridged by an MSSP's extensive suite of security analysts and specialists. Further, their round-the-clock support can aid continuous threat monitoring, enabling near real-time incident response.

41% of firms buy managed security services to secure their cloud environments. [1]



Security Teams Consistently Strengthen Security Operations, but Challenges Persist

The business case for proactive cybersecurity is well-recognized by companies across the globe. To bolster security operations, incident response, and recovery, internal security personnel and senior management are geared toward building more multifaceted and pervasive defenses. However, the following problems related to people, processes, and technology continue to persist, weakening the practical execution of security strategies.

Tool Complexity

78%



of CISOs have over 16 tools in their cybersecurity vendor portfolio. [6]

Manual Processes

74%



of firms stated that their alert triage efforts are slowed by manual processes. [4]

Talent Shortage

50%

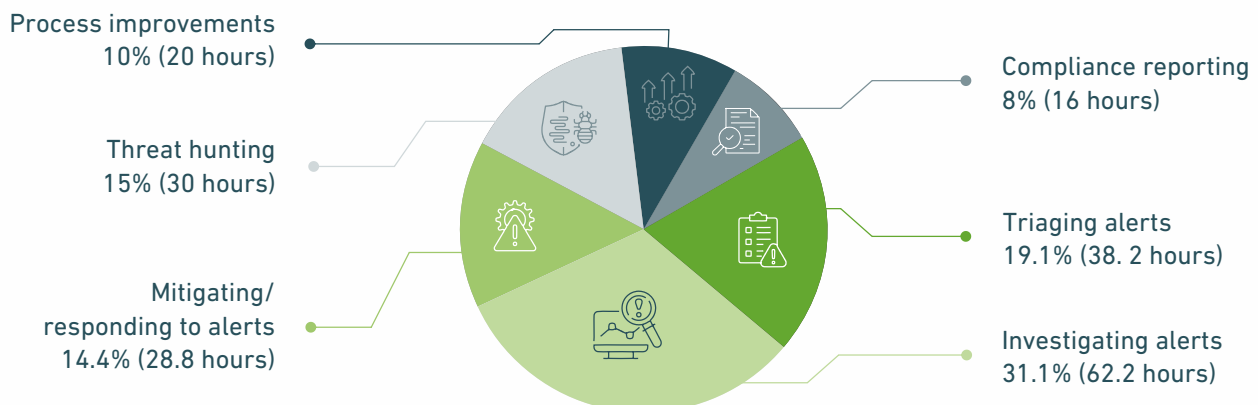


of firms believe that the lack of skilled personnel makes their SOC ineffective. [3]

To achieve SOC-readiness, organizations must prioritize automation and the people factor of security operations.

Internal security operations suffer due to fragmented and multiple security solutions, high reliance on manual processes and outdated technologies, and understaffed and under trained analyst teams. [4] As a result, essential tasks such as proactive threat hunting, risk detection, and triaging alerts could fail to receive the right response at the right time.

Time Spent by Internal SecOps Resources to Perform Key Security Tasks [4]



* Percentage of hours spent in an average week
 ** Percentage values do not sum up to 100

Most efforts of organizations' security teams go towards investigating alerts, with many cases of false positives. These barriers to SOC-readiness can be readily overcome by accessing the experience, technology, and skills of a managed security service provider. With an MSSP, companies can implement a layered cybersecurity approach using cutting-edge technologies, eradicating threats present in their security environment more quickly.

What Makes a Security Operations Center Effective?

To gain a clear understanding of an “effective” security operations center (SOC), organizations should acknowledge that it can have different implications for different parties. From senior executives, security leaders, customers, to the organizational staff, the KPIs used by these audiences to assess an SOC’s effectiveness can vary greatly. The essence of embracing an effective security operations program is to approach it with the aim to cater to one’s business goals as well as the concerns of the entire organization. ^[10]

How can Enterprises Build an Effective SOC?

Understand business & customer goals and risks



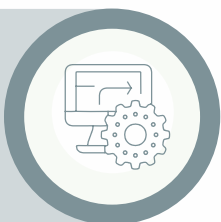
Concrete understanding of one’s business goals and risks facilitates the development of a business-aligned security operations center. At the same time, knowing the customer’s goals and risks is vital to learn what is important to clients and what is the best route to meet customers’ security needs and expectations. SOCs should assess these aspects before finalizing any metrics or best practices. ^[11]

Value both qualitative & quantitative metrics



Moving beyond numbers is imperative to assess SOC effectiveness. Traditional security indicators are useful, however, they should be realistic, clearly defined, and well-aligned to corporate goals. Qualitative metrics should also be measured; these can include the workforce’s ability to implement cybersecurity training, how security teams prioritize security operations, and how people interact with security threats and tools. ^[10]

Embrace automation & integration



The pace of today’s threats builds the case for robust automation across the SOC. Effective SOCs automate the most time-consuming manual tasks of the investigation and response cycle which can reduce MTTR, prevent analyst burnout, and enable teams to focus on strategic initiatives. Moreover, integrating security tools, a service offered by leading MSSPs, into a unified platform is essential to effectively expedite threat correlation and orchestrated response processes. ^[4]

Building the Case for an Effective SOC Through Next-Gen MSSPs

At the core of an effective SOC lies the power of skilled people, agile processes, and suitably-integrated technology [12]. Using the 'people, processes, technology' framework, companies strive to develop future-ready security operations centers. However, given the external threat environment and internal barriers in achieving SOC-readiness, organizations can better reach security maturity with the assistance of managed security service providers (MSSPs).

60% of enterprises in the GCC either manage their SOC via third-parties or have a hybrid SOC. [9]

Managed security services (MSS) offer extensive coverage of the IT security landscape, facilitating advanced threat detection, faster remediation, and resilient recovery. With MSSPs like SAMI-AEC, corporate security leaders can collaborate on a global level and holistically secure their organizations. Leveraging security operations center as a service (SOCaaS), enterprises can effectively combine commercial SIEM native capabilities with advanced analytics, threat intelligence, and 24x7 analyst support to detect and act on cyber threats in near real time. [13]

Benefits of Security Operations Center as a Service [11, 14]

Simplified and Cost-Efficient Operations

- Reduction in operational cost
- Decrease in operational complexity
- Highly-integrated processes and solutions



Actionable Threat Intelligence

- Reduction in false positives
- Real-time event analysis and correlation
- Understand preliminary incident response

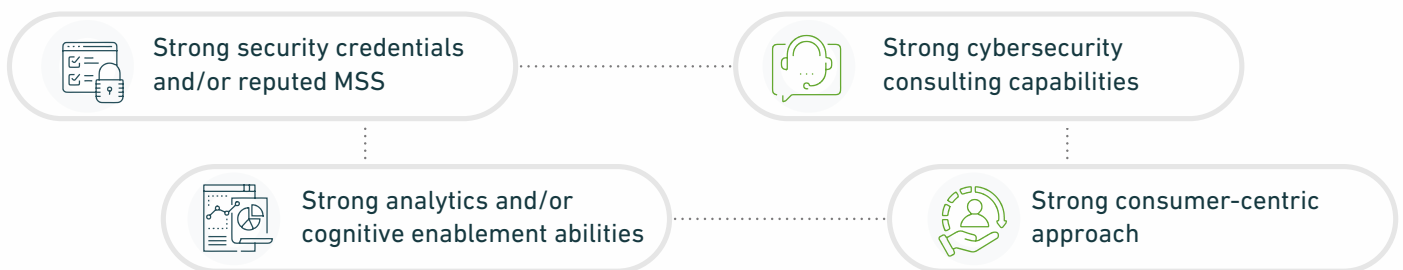
Empowered Internal Security Teams

- 24x7x365 access to expert SOC analysts
- Maintenance of case reviews and custom IR playbooks
- In-depth monitoring of security posture (on-site, cloud, IoT, OT)

Key Recommendations for Choosing a Reliable and Efficient MSSP

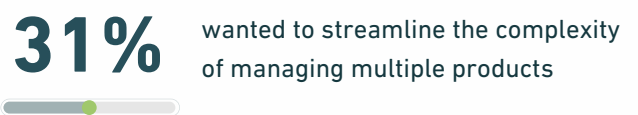
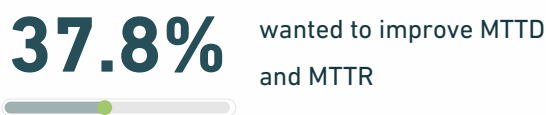
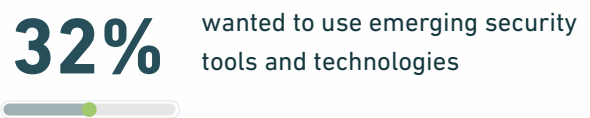
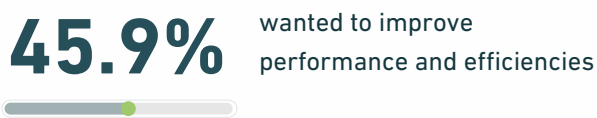
As organizations recognize the business value and necessity of utilizing MSS, it is important to understand the factors that should be considered to select the most suitable MSSP. The truly efficient managed security service vendor focuses on providing access to advanced security capabilities, and excels in offering on-demand expert support. Further, they take time to understand a company's specific business objectives, needs, and expectations to tailor security solutions best suited to their requirements.

Future-Thinking MSSPs Should have ^[8]



In line with the defining factors of future-ready managed security service vendors, organizations are driven towards high-end technologies and overall business efficiency when selecting an MSSP.

Top Reasons for MSS Customers to Use Security Services Provider ^[8]



Consider the Following Before Selecting an MSSP ^[8, 4]

- Range and breadth of the MSS portfolio; maturity of cloud security strategy
- Ability to evaluate an organization's people, process, and technology
- Current level of advanced security capabilities and approach towards innovation
- Extent of integration of automation and orchestration into core delivery platforms
- Multi-regional or global capabilities that provide SOCaaS capabilities
- Customer engagement programs, security expertise, and portal reporting abilities

Maximize SOC Effectiveness Through SAMI-AEC SOCaaS

SAMI Advanced Electronics Company has established itself as a leader in offering comprehensive managed security services across the GCC. By utilizing SAMI-AEC SOCaaS, organizations can expedite their SOC maturity journeys, while running agile and seamless business operations. Our team of skilled cybersecurity experts and SOC analysts can enhance your defense against APTs, new TTPs, and opportunistic cybercriminals in today's threat environment.

SAMI-AEC's Approach to Build an Effective SOCaaS



Understand your business agenda



Tailor SecOps as per your digital road map



Offer scalable systems well-suited to your business needs

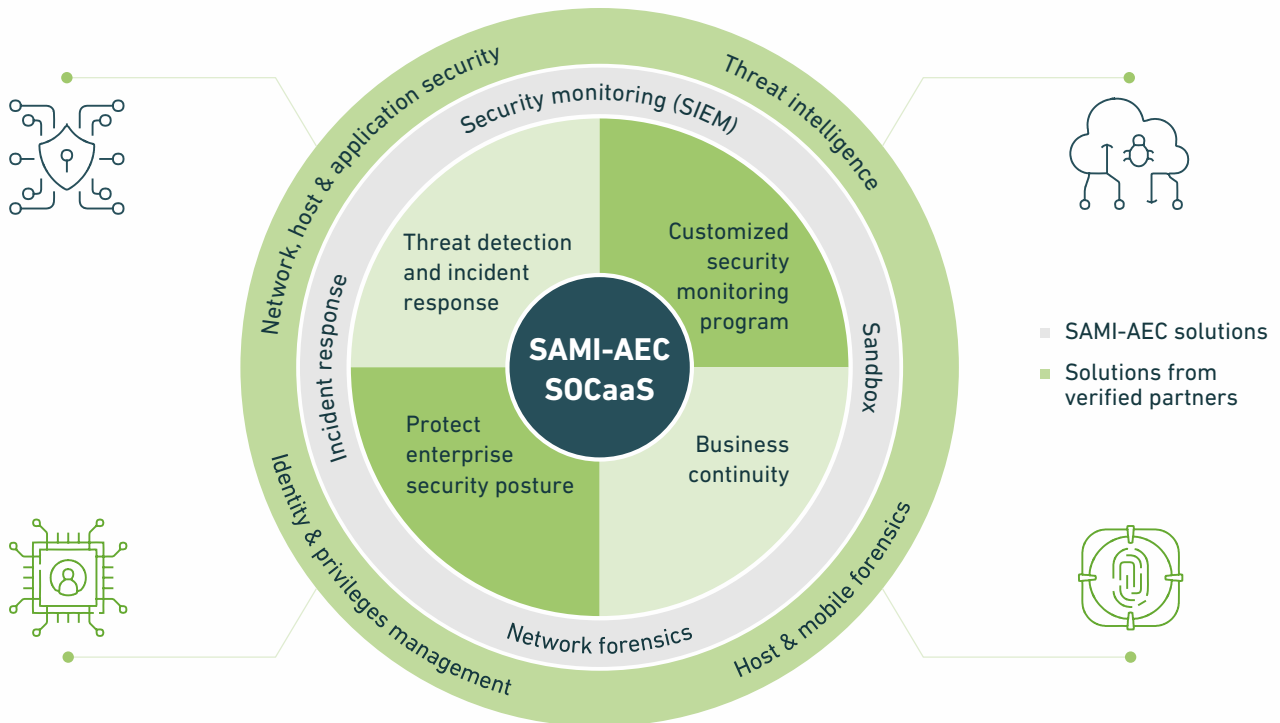


Provide 24x7 expert assistance to internal security teams



Obtain insights into your current and future technology environment

Level-Up SOC Maturity with SAMI-AEC



The extensive suite of SAMI-AEC's managed security services can help reduce company's personal costs associated in managing in-house SOC's, thus increasing the ROI on security services. Moreover, SAMI-AEC SOCaaS ensures compliance to global cybersecurity regulatory guidelines and can also conduct independent cybersecurity assessments. Thus, with SAMI-AEC's effective SOCaaS, enterprises are well-positioned to realize robust enterprise-wide cyber resilience.

CONCLUSION

The outcomes of outsourcing the SOC to managed security service providers is steadily gaining traction across the global turf. From detection to recovery, the SOCaaS model readily supports internal security teams at every stage of their security monitoring and response cycles. With leading MSSPs, enterprises are, no doubt, efficiently-positioned to unlock and unleash the power of their security operations. The extensive suite of emerging security tools, solutions, and services offered by managed security services facilitate an organization's journey to develop next-level cyber defense while focusing on their core business operations.

At all levels, SAMI-AEC is ever-prepared to help you reach the best level of enterprise-wide cybersecurity.

SAMI-AEC is a well-known provider of trustworthy, business value-oriented, and advanced security solutions to organizations belonging to different verticals and industries across the GCC. Moreover, the vast experience and knowledge of SAMI-AEC's cybersecurity personnel can enable companies to tackle varied forms of cyberattacks and new vulnerabilities, accelerating remediation and recovery. Security-first organizations can rely on SAMI-AEC to uphold its promise to technological excellence and customer-centric services.

What's Next?

Connect with us to learn how SAMI-AEC SOCaaS can help organizations to enhance cyber-readiness. With our sophisticated cybersecurity services and exceptional technical support, you can upgrade the performance and existing level of your security operations program. At SAMI-AEC, our team of cyber experts is well-prepared and well-equipped with the latest security technology to offer outstanding assistance towards building a future-ready and highly effective security operations center.



REFERENCES

1. Brown, D., Richmond, C., Maslennikov, D. and Stahnke, C. (2021). Building Resilience into Modern Security Architectures. [online] IDC. Available at: <https://www.avanade.com/-/media/asset/solutions/avanade-security-architecture-idc-white-paper.pdf?la=en&ver=1&hash=507D978B34A90596950F21783A4E3365>.
2. ZScaler (2021). The State of Zero-trust Security Strategies. [online] Available at: <https://info.zscaler.com/resources-industry-report-the-state-of-zero-trust-security-strategies>.
3. Devo (2021). 2021 Devo SOC Performance Report: SOC Leaders and Staff Not Aligned. [online] Available at: <https://www.devo.com/wp-content/uploads/sites/1/2021/12/2021-Devo-SOC-Performance-Report.pdf>.
4. Forrester (2021). State Of SecOps In 2021: Rise Of The SOC's Autonomy. [online] Available at: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/forrester-2021-soc-automation.pdf?utm_source=marketo&utm_medium=email&utm_campaign=Global-DA-EN-21-06-28-7014u000000eXmmAAE-P3-Cortex-2021-state-of-secops-forrester.
5. Accenture (2022). Threats Unmasked: Cyber Threat Intelligence Report Volume 2 -2021. [online] Available at: https://www.accenture.com/_acnmedia/PDF-158/Accenture-2021-Cyber-Threat-Intelligence-Report.pdf#zoom=40.
6. Gartner (2021). Gartner Top Security and Risk Trends for 2021. [online] Gartner. Available at: <https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021>.
7. Alwazir, A. and Dichter, J. (2020). USSABC Economic Brief: Saudi Arabia's Emergence in Cyber Technology. [online] Available at: <http://ussaudi.org/wp-content/uploads/2020/01/Economic-Brief-Saudi-Cybersecurity-Leadership.pdf>.
8. Vazquez, M. (2020). IDC MarketScape IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment. [online] IDC. Available at: https://www.btireland.com/docs/default-source/analyst-reports/idc_marketescape_report_2020.pdf
9. Rychkov, K. and Ozturk, Y.A. (2020). Battle for the Modern Security Operations Center. [online] IDC. Available at: https://www.intelligentcio.com/wp-content/uploads/sites/12/2020/11/IDC-Spotlight-SOC-META_v1.pdf.
10. Deepwatch. Maximizing SOC Effectiveness with MDR. [online] Available at: <https://www.deepwatch.com/wp-content/uploads/deepwatch-Maximizing-SOC-Effectiveness-with-MDR-Whitepaper.pdf>.
11. EY (2021). How to Transform Your Security Operations Center (SOC), Powered by Microsoft Azure Sentinel and Microsoft 365 Defender. [online] Available at: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/consulting/ey-how-to-transform-your-soc-powered-by-microsoft-eyg-no-001828-21-gbl.pdf.
12. Kaliyaperumal, L.N. (2021). The Evolution of Security Operations and Strategies for Building an Effective SOC. [online] ISACA Journal. Available at: <https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc>.
13. NTTT (n.d.). Security Operations Center-as-a-Service. [online] Available at: <https://hello.global.ntt/-/media/ntt/global/products-and-services/managed-services/managed-security-services/security-operation-center-as-a-service/mss-v3-datasheet-socaas.pdf?rev=56528ac858e34da6a18f33077c4812ad>.
14. Fortinet (2021). FortiCloud SOC-as-a-Service. [online] Available at: <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/forticloud-socaas.pdf>.

SAMI Advanced Electronics Company

King Khalid International Airport Industrial Estate
P.O. Box 90916,
Riyadh 11623, Saudi Arabia

 **+966112201350** **Email** - info@aecl.com

 **in**  **/AECSaudiArabia**