SAMI ADVANCED ELECTRONICS
شركة الإلكترونيات المتقدمة

Gain Absolute Control Over Your Cybersecurity Landscape with

SAMI-AEC Managed Detection and Response (MDR)

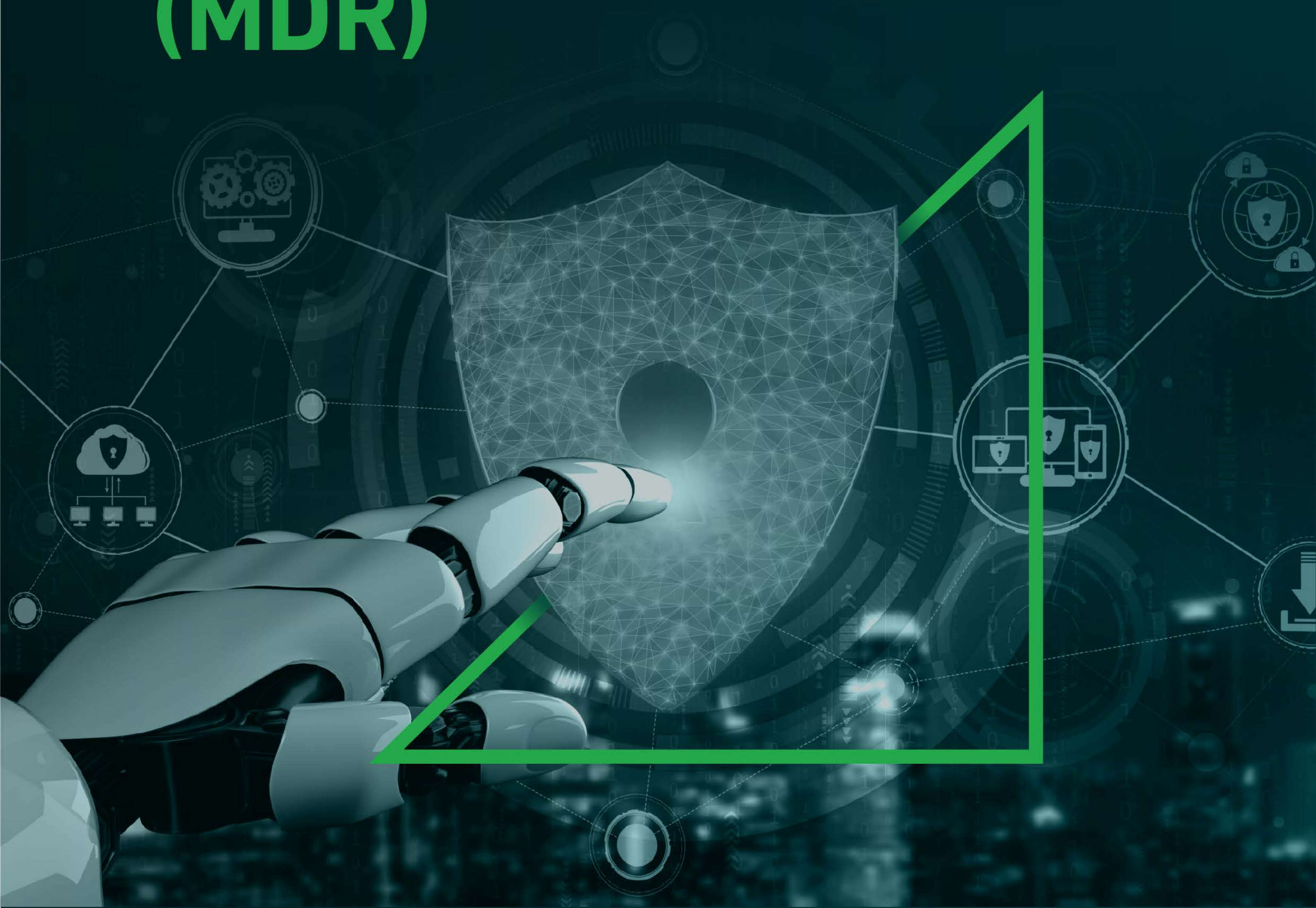


Table of Contents

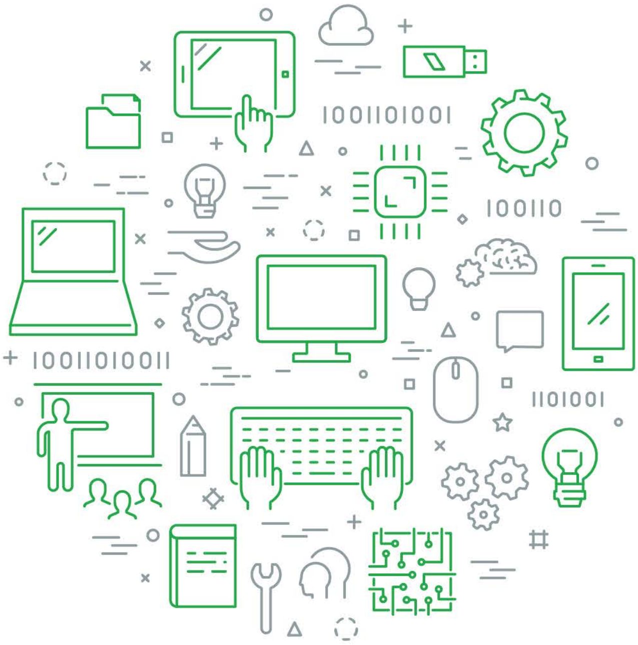
Executive Summary

The recent years have reiterated the importance of cyber resilience for modern businesses. The shift to remote work coupled with proliferation of the Internet of Things (IoT) has made the cybersecurity landscape more complex. As a result, the occurrence and severity of cyber attacks have increased. This necessitates organizations to focus on creating and employing comprehensive cybersecurity strategies.

Cybersecurity has also become a national priority in Saudi Arabia owing to the heightened modernization efforts across the Kingdom. Taking charge, the Kingdom is heavily investing in cybersecurity research and development, facilitating collaboration between public and private sectors, and promoting cybersecurity education and training programs. Such efforts strive towards building a resilient cyber ecosystem capable of thwarting emerging threats.

Both at global and national levels, Managed Security Services (MSS) have proved instrumental in improving cybersecurity across organizations of all sizes. Along with strengthening cybersecurity, MSS providers help organizations comply with industry standards by maintaining logs, conducting audits, and managing security protocols.

Across Saudi Arabia, SAMI-AEC Managed Detection and Response (MDR) services are creating a resilient cybersecurity infrastructure. The organization leverages deep local expertise and latest technologies to offer a comprehensive solution that combines advanced threat detection, incident response, and continuous monitoring. Thus contributing to KSA's digital transformation journey, safeguarding critical assets and fostering a secure and prosperous future.



Exploring the Present Global Cybersecurity Scenario

In the contemporary business landscape, cybersecurity has become a strategic imperative with much at stake – brand's reputation, business continuity, and financial losses. The work-from-home model across corporations and the widespread adoption of IoT devices have expanded the cyber attack surface. [4,12] Cybercriminals are exploiting these newly exposed loopholes, necessitating the need for a proactive cybersecurity strategy.

Understanding the Modern Cyber Threat Landscape

Key Threat Vectors

Ransomware 66%

of organizations were hit by ransomware in 2023 [1]

Malware 56%

of non-insider data breaches were triggered by malware in 2023 [2]

Insider Risks $4.90M

Average cost of breaches from insider threats [3]

Phishing $4.76M

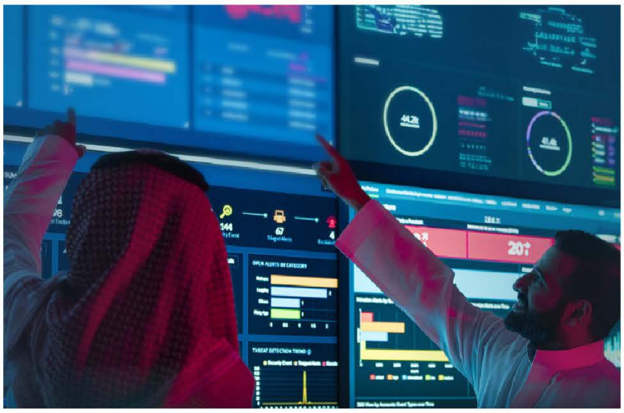
Cost of phishing attacks, the most common vector [3]

Cloud 82%

of breaches involve cloud-stored data in 2023 [3]

Cyberattack Costs Soaring [5]

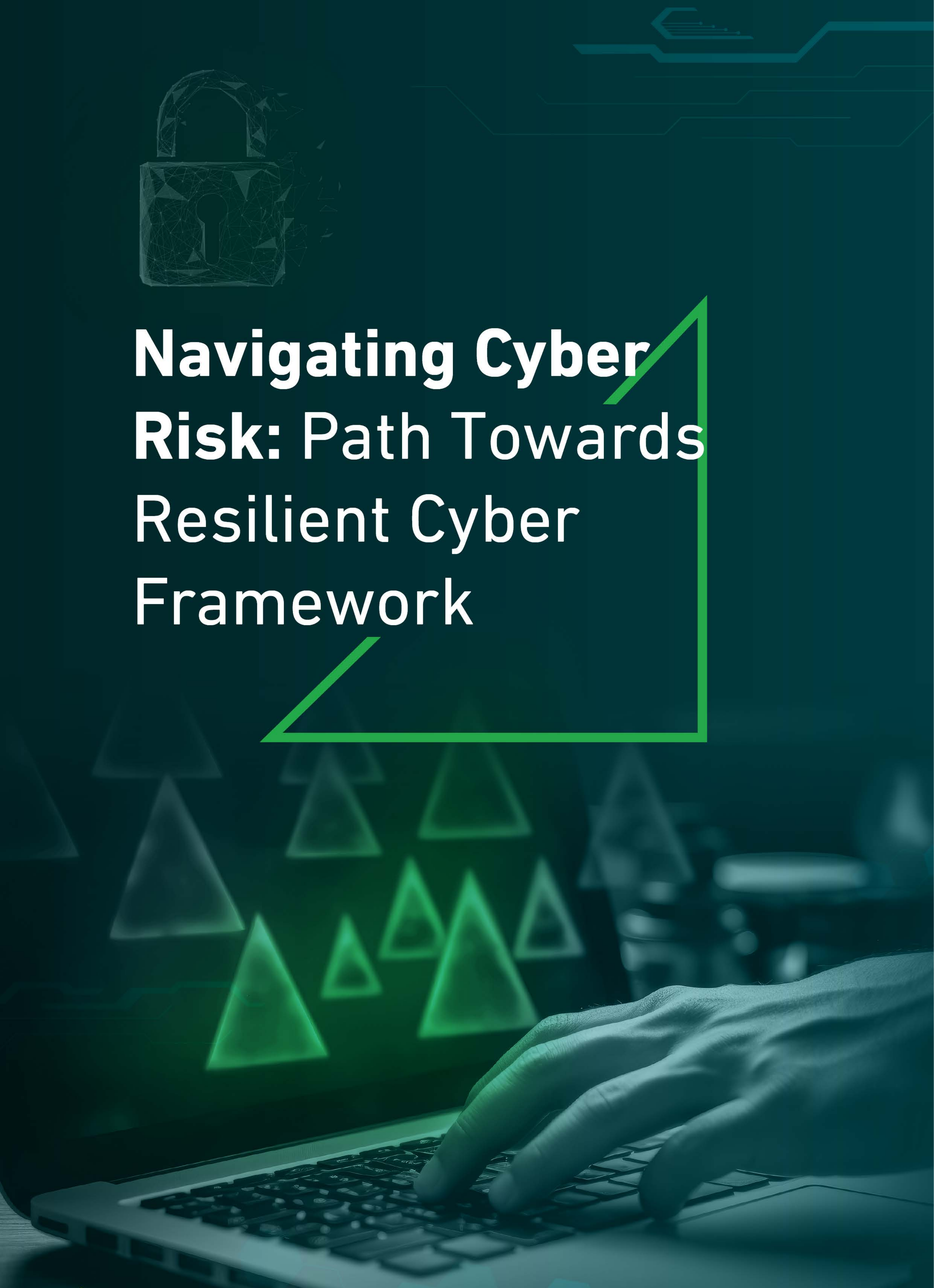
$10.5 Trillion in annual damage from cyberattacks anticipated by 2025



Increased Cybersecurity Spending

99% of organizations plan to increase their cyber budgets in the next 12 months [6]

51% of organizations increasing security investments after a breach [3]



Navigating Cyber Risk: Path Towards Resilient Cyber Framework

To combat rising cyber risk, organizations need to employ a dynamic, forward-looking strategy that will enable them to mitigate evolving threats. However, almost half of organizations (49%) are not armed to address cybersecurity challenges. Meanwhile, others (54%) are wasting their valuable time in combating low-level alerts, de-accelerating incident response processes. Besides this, there are substantial internal hurdles that are preventing security leaders from dealing with heightened external risks. [7]

Organizations Reveal Major Obstacles Impeding Security [8]

Absence of Required Expertise

38% Report current security tools necessitate a high level of specialized expertise

Scarcity of Sufficient Staffing

81% Agree that SecOps are hindered by the shortage of cybersecurity professionals

Lack of Adequate Tools

51% Reveal current tools struggle to detect and investigate advance threats

Key Focus Areas For a Cyber-Resilient Organization [7]

Secure Foundation

Deploy robust controls and multi-factor authentication to mitigate human risks

Best Practices

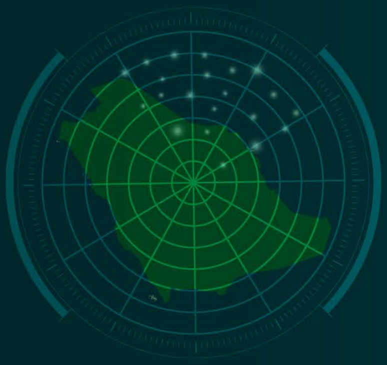
Adopt structured security practices for measurable and effective protection

Incident Response

Test, update, and refine processes to handle alerts with precision

Third-Party Support

Enhance response with managed detection services for faster containment and expertise



Securing the Kingdom: A Look at Saudi Arabia's Cybersecurity Landscape

Saudi Arabia's national development plans, as part of Vision 2030, and economy diversification initiatives have acknowledged emerging technologies as the facilitator of the key industry transformation. Inadvertently, the utilization of these technologies has made both the public and private sector susceptible to the evolving threats in the cyber landscape. To this end, 40% of business leaders in the Kingdom are anticipating moderate exposure and 20% are preparing for high exposure in the upcoming months. [9]

Taking a proactive approach to mitigate these risks, the Kingdom is developing capabilities and capacity to safeguard the technologies enabling growth initiatives. National Information Security Strategy (NISS) and National Cybersecurity Authority (NCA), cybersecurity programs by the Saudi government, are playing a key role in making KSA' enterprises cyber-resilient. [10]

Growing awareness among KSA's organizations to fortify their defenses and transform threats into opportunities [11]

62% Emphasize the importance of maintaining an optimal level of cybersecurity technology solutions

73% Give precedence to digital and technology-related risks, which are a top concern for over 51% of organizations worldwide

33% Expect an increase of 6-10% in their organization's cyber budget

'%' represents the percentage of business and tech executives

Bolstering Cybersecurity: The Role of Managed Security Services

In the last few years, global security teams have taken cognizance of growing cyber risk and employed proactive measures. However, the looming threat and the pressure to remain cyber resilient makes organizations overwhelmed, pushing them to take immediate action to fortify their cyber defenses. Partnering with managed security providers can significantly enhance incident response capabilities. A Managed Security Service Provider augments an organizations' existing staff, providing the in-depth knowledge and advanced tools needed to combat evolving threats. [7]

40% of breaches were discovered by external third parties or outsiders, while 33% were detected by internal teams and tools. [3]

42% of CISOs reveal that they outsource more than 25% of their organization's cybersecurity budget. [13]

Security Leaders State Key Benefits of Leveraging Managed Security Services [7]

55%	Rapid threat containment and response
53%	Augmenting in-house security expertise
50%	Enhanced automation of processes
48%	Faster threat detection
39%	More robust event logging
39%	Increased budget efficiency

SAMI-AEC Managed Detection and Response (MDR): Facilitating a Secured Cybersecurity Ecosystem Across KSA

SAMI-AEC Managed Detection and Response (MDR) provides Saudi organizations with 24/7 threat protection and expert guidance. Our local team, backed by global best practices, secures your hybrid cloud environment and simplifies regulatory compliance. Leveraging industry-leading software and expertise of certified professionals, SAMI-AEC MDR maximizes your security posture.

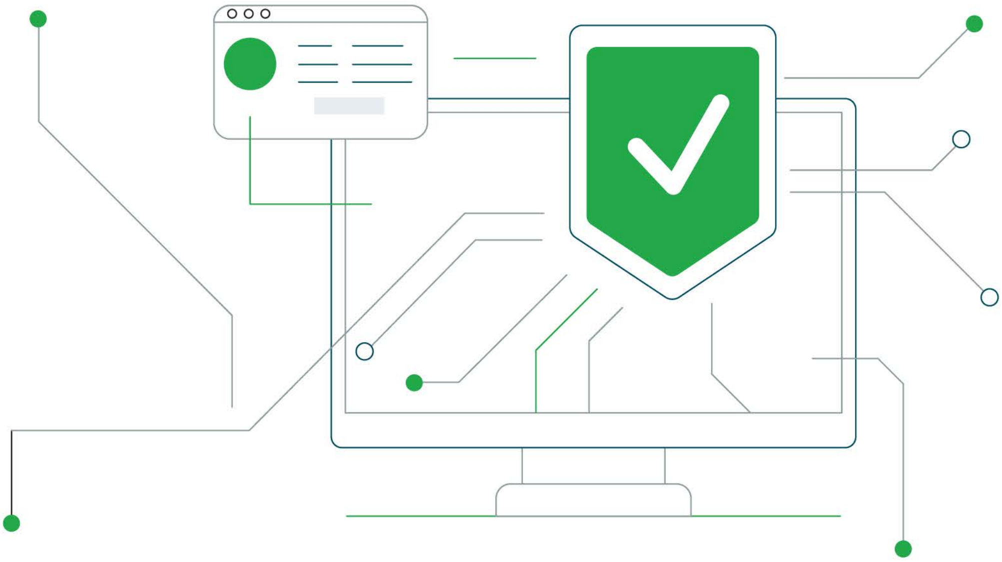
Essential Services for Holistic Protection

Threat Detection and Analysis

- Prioritizing threats
- Analyzing data for threats
- Continuous threat hunting

Log Analysis and Monitoring

- 24/7 monitoring
- Log and vulnerability management
- Incident ticketing and workflow



Digital Forensics and Incident Response

- Incident root cause analysis
- Data analysis and recovery
- Malware examination
- SIEM Management

Security Reporting and Governance

- KPIs and KRAs for security
- User-friendly search and alerts
- Configurable reports and dashboards
- Creation and review of SOC playbooks
- Security assessments and remediation

Conclusion

The technological advancement in Saudi Arabia is accompanied by a heightened cyber risk. This has led to an increased emphasis on improving the Kingdom's overall security and resilience to ensure a secure foundation for the envisioned knowledge-based economy. Pertaining to this, the Saudi government is undertaking various initiatives to centralize security efforts. Such endeavors have created cybersecurity awareness among Saudi enterprises, prompting them to take strategic cybersecurity measures.

Managed Security Service Providers (MSSP) can play a vital role in realizing the Kingdom's cybersecurity objectives. MSSPs offer a cost-effective way to deploy advanced security technologies. Offering access to a team of highly skilled and experienced security professionals, MSSPs empowers businesses of all kinds to achieve a robust cybersecurity posture.

SAMI-AEC MDR has emerged as the leader in Saudi Arabia. By deploying state-of-the-art tools, SAMI-AEC MDR enables organizations to navigate cyber threats with ease, reduce costs, improve efficiency, and address challenges such as lack of adequate talent. Hence, by fortifying the digital infrastructure essential for economic growth and innovation, SAMI-AEC MDR is advancing the nation's Vision 2030 objectives to create a secure and prosperous digital economy.

References

01 Deloitte (2024). Deloitte Cybersecurity Threat Trends Report 2024. Available at: https://www2.deloitte.com/us/en/pages/noindex/cyber/cybersecurity-threat-trends-report-2024-download.html.

02 Ponemon Institute (2024). Cost of Insider Risks. Available at: https://www2.dtexsystems.com/l/464342/2023-09-15/3w7l7k/464342/1694800570ZwvyrzsD/2023_Cost_of_Insider_Risks_Global_Report___Ponemon_and_DTEX___Dgtl.pdf.

03 IBM (2023). Cost of a Data Breach Report 2023. Available at: https://www.ibm.com/downloads/cas/E3G5JMBP.

04 Institute for Defense and Business (2024). COVID-19 and working from home: balancing cyber security and productivity. Available at: https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-home-office-cyber-security.html.

05 McKinsey (2023). What is cybersecurity? | Available at: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-cybersecurity.

06 PricewaterhouseCoopers (2023). 99% of organisations will increase their cyber budgets, out of which 50% envisaged an increase between 6% and 15% in the next 12 months: PwC's 2024 Digital Trust Insights. Available at: https://www.pwc.in/press-releases/2023/99-of-organisations-will-increase-their-cyber-budgets-out-of-which-50-envisaged-an-increase-between-6-and-15-in-the-next-12-months-pwcs-2024-digital-trust-insights.html.

07 VMware, Inc (2021). The state of incident response 2021: It's time for a confidence boost 2 THE STATE OF INCIDENTRESPONSE 2021. Available at: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-the-state-of-incident-response-2021.pdf.

08 Enterprise Strategy Group (2022). SOC Modernization and the Role of XDR 1 SOC Modernization and the Role of XDR june 2022. Available at: https://www.cisco.com/c/dam/global/en_uk/products/se/2022/6/collateral/soc-modernization-xdr.pdf.

09 PricewaterhouseCoopers (2024). 27th Annual CEO Survey: Saudi Arabia findings. Available at: https://www.pwc.com/m1/en/publications/27th-annual-ceo-survey-ksa-findings.html

10 IDC Saudi Arabia (2020). Cybersecurity and its impact on digital Saudi. Available at: https://resources.trendmicro.com/rs/945-CXD-062/images/Cybersecurity-and-its-Impact-on-Digital-Saudi.pdf.

11 PricewaterhouseCoopers (2024). Digital Trust Insights 2024 - The KSA perspective. Available at: https://www.pwc.com/m1/en/publications/middle-east-digital-trust-insights-2024/the-ksa-perspective.html.

12 Deloitte (2021). COVID-19 and working from home: balancing cyber security and productivity. Available at: https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-home-office-cyber-security.html.

13 Deloitte (2023). Cybersecurity insights 2023: Budgets and benchmarks for financial services institutions. Available at:https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-cybersecurity-insights-23-budgets-and-benchmarks.pdf.

SAMI
ADVANCED
ELECTRONICS
شركة الإلكترونيات المتقدمة

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

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

/AECSaudiArabia