BLACK BOX

Cyber Resilience at Scale

A Black Box point of view for securing AI-ready, cloud-first and distributed enterprises across the Middle East and Africa



Building Confidence in Digital Growth

Across the Middle East and Africa, digital ambition is reshaping economies and enterprises. Every investment in new capabilities carries a promise: that the services customers, partners and communities depend on will remain secure, reliable and worthy of their trust.

In my 15 years in cybersecurity, including eight in the UAE, I have seen security become central to conversations about growth, investment confidence and leadership accountability.

Building security practices across the region has reinforced one conviction: **resilience begins with decisions made long before disruption.** It depends on clear ownership, skilled people and the judgment to embed security into business priorities.

MEA's diverse markets, regulatory environments and levels of digital maturity demand an approach grounded in local context. The shared ambition is to give organizations the confidence to innovate while safeguarding what their stakeholders value.

This point of view invites leaders to reflect on whether their cybersecurity approach is keeping pace with their business ambitions, and the commitments needed to make digital growth sustainable.



Atul Gupta

Practice Leader, Cyber Security
Middle East and Africa | Black Box

Atul.Gupta@BlackBox.com

About Atul Gupta

Atul has built and scaled four regional practices: Managed SOC, Identity and Access Management, Infrastructure Security, and Governance, Risk and Compliance. He advises C-level leaders across education, government and enterprise organizations.

He holds CISA, CISM, CCSP, CEH and ISO 27001 Lead Auditor credentials and is pursuing an Executive PCDM in AI and Data Science at the Indian Institute of Technology Bombay.

Table of Contents

01 **MARKET SIGNALS** **04–06**

Rising Cyber Risk Demands Managed SOC 4
Cyber cost and investment pressure 5
Digital Growth Is Multiplying Cyber Risk 6

02 **ENTERPRISE EXPOSURE** **07–09**

Cybersecurity Has Entered the Growth Agenda 7
When Geopolitics Rewrites Cyber Risk 8
Can Your SOC Adapt Fast Enough? 9

03 **THE OPERATING GAP** **10–11**

Why More Tools Still Miss Risk 10
Where Does Your SOC Lose Time? 11

04 **THE MODERN MODEL** **12–14**

From Alert-Led Operations to Continuous Cyber Resilience 12
What Turns a Signal Into Action? 13
What Keeps a Managed SOC Effective? 14

05 **THE MODERNIZATION ROADMAP** **15–16**

Four Moves to Modernize Security Operations 15
Build SOC Maturity in Deliberate Increments 16

06 **THE EXECUTIVE MEASURE** **17–18**

Are You Measuring What Matters? 17
Three Outcomes That Prove SOC Value 18

07 **SHOWING BY DOING** **19–21**

Cyber Operations Connected to the Infrastructure They Protect 19
From Fragmented Tools to Faster Response 20
When Banking Growth Outpaces Security Operations 21

08 **THE EXECUTIVE DECISION | MEA** **22**

The Next Crisis Will Expose Today's Decisions 22

09 **RESEARCH FOUNDATION** **23**

References 23

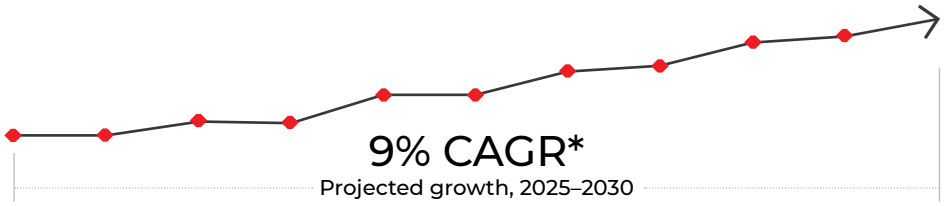
Rising Cyber Risk Demands Managed SOC

AI-enabled attacks, supply-chain exposure and rising breach costs are making continuous detection and coordinated response a business priority.

The SOC Market Is Scaling

$543M*

MEA SOC-as-a-Service market, 2024



$878M*

Projected market, 2030

Risk Pressure

26%**	Malicious breaches were AI-enabled
18%**	Phishing, including voice and SMS phishing
16%**	Supply-chain compromise
16%**	Social engineering

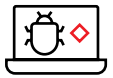
Cost Amplifiers



Mismanaged secrets and encryption keys



Excessive privileges and poor role management



Inability to prioritize threats

Sources: **Grand View Research, MEA SOC-as-a-Service Market Outlook, updated July 2025, ** IBM, Cost of a Data Breach Report 2026 – Middle East Findings, August 2026*

Cyber cost and investment pressure

Security-services spending is accelerating as breach costs push continuous visibility and coordinated response higher on the executive agenda.

Security Investment Is Accelerating

$1.52B*

MENA security-services spending forecast for 2026

+10.6%*

Fastest-growing information-security segment

The Cost of a Breach

$8M**

Average cost of a Middle East data breach in 2026

Executive Takeaway

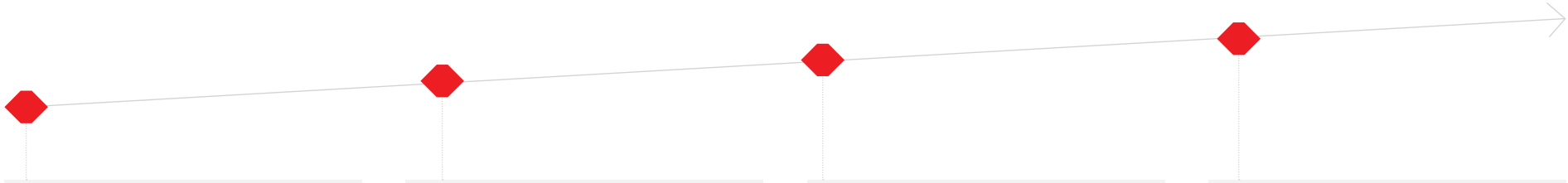
Managed SOC is moving from a monitoring option to a resilience imperative, providing continuous visibility, specialized expertise and coordinated response at scale.

Sources: *Gartner, MENA Information Security Spending Forecast, October 2025; ** Source: IBM, Cost of a Data Breach Report 2026 – Middle East Findings, August 2026

Digital Growth Is Multiplying Cyber Risk

As MEA enterprises scale cloud, AI, connected operations and third-party ecosystems, every new dependency increases exposure and the potential for business disruption.

Four Shifts Reshaping Enterprise Exposure



01

Cloud, SaaS and Identity

Critical workloads and identities increasingly sit beyond the traditional enterprise perimeter.

02

AI and Agentic Workflows

Machine-speed activity accelerates legitimate change while amplifying the speed and scale of malicious action.

03

OT, IoT and Connected Operations

Cyber incidents can now disrupt physical operations, safety and critical-service continuity.

04

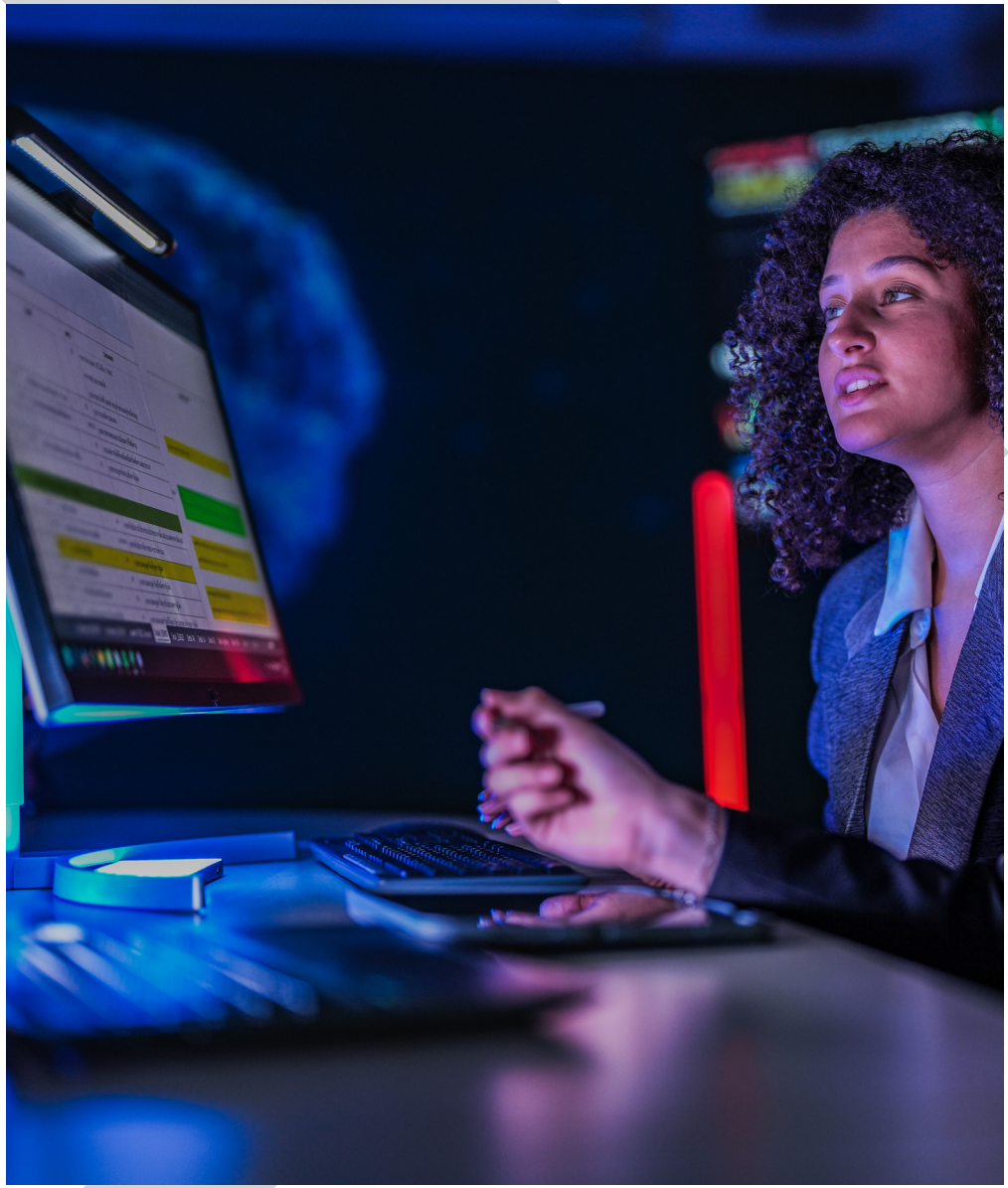
Third-Party Ecosystems

Supplier and platform incidents can cascade across interconnected business services.

Cybersecurity Has Entered the Growth Agenda

73%*

of Middle East organizations view cybersecurity as a strategic asset.



The Executive Question

Can security operations keep pace with the speed, scale and interdependence of enterprise growth?

The Operating Imperative

Move from isolated monitoring to continuous, business-aligned resilience.

Sources: *PwC, 2025 Global Digital Trust Insights: Middle East Findings.

When Geopolitics Rewrites Cyber Risk

Regional developments can rapidly intensify opportunistic attacks, espionage and disruption across critical infrastructure and supply chains.

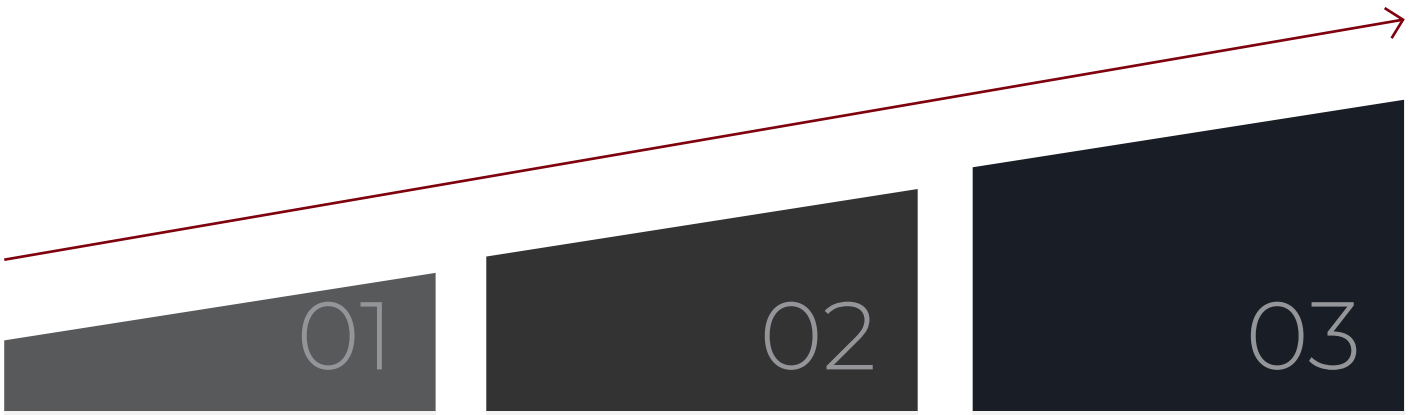
60%*

of Middle East business and technology leaders are increasing cyber-risk investments in response to geopolitical volatility.

Sources: *PwC, 2026 Global Digital Trust Insights: Middle East Findings.

Can Your SOC Adapt Fast Enough?

Three operating shifts can convert regional volatility into timely intelligence, sharper protection priorities and coordinated action.



Sense Shifts Early

Turn region-aware threat intelligence into event-driven detection updates.

Reprioritize Protection

Focus on critical services, OT, cloud control planes and privileged identities.

Coordinate at Speed

Activate predefined paths across SOC, incident response, business continuity, legal and executive leadership.

Sources: *PwC, 2026 Global Digital Trust Insights: Middle East Findings; Forrester, Predictions 2026: Cybersecurity and Risk.

Why More Tools Still Miss Risk

Traditional SOCs are constrained less by tool availability than by the operating model connecting telemetry, expertise, and governance.

Three Structural Causes

01

Technology Without Context

Telemetry remains separated across cloud, identity, endpoints, networks, OT and vulnerability tools, obscuring business-critical risk.

02

Expertise That Cannot Scale

Analysts spend time enriching and routing alerts while specialist coverage remains difficult to sustain around the clock.

03

Governance Without Business Relevance

Dashboards emphasize alert volumes and ticket counts rather than exposure, control effectiveness and resilience.

Sources: *PwC, 2026 Global Digital Trust Insights: Middle East Findings.

Where Does Your SOC Lose Time?

Delay accumulates at three critical handoffs, weakening the connection between technical signals and business response.

01

Signal to Priority

Disconnected telemetry creates incomplete context, forcing critical threats to compete with low-value noise.

Blind spots and missed priorities

02

Decision to Response

Manual enrichment and fragmented ownership delay investigation, containment and recovery.

Slower decisions and greater impact

03

Response to Assurance

Activity-led reporting obscures exposure, control effectiveness and resilience.

Limited executive confidence



Sources: *PwC, 2026 Global Digital Trust Insights: Middle East Findings; Forrester, Predictions 2026: Cybersecurity and Risk.

From Alert-Led Operations to Continuous Cyber Resilience

A modern Managed SOC connects telemetry, threat intelligence, automation, expert judgment and governance in one operating model.

Designed for distributed, cloud-first and AI-enabled enterprises.

24/7 Operating Mandate

Detect | Prioritize | Respond | Recover



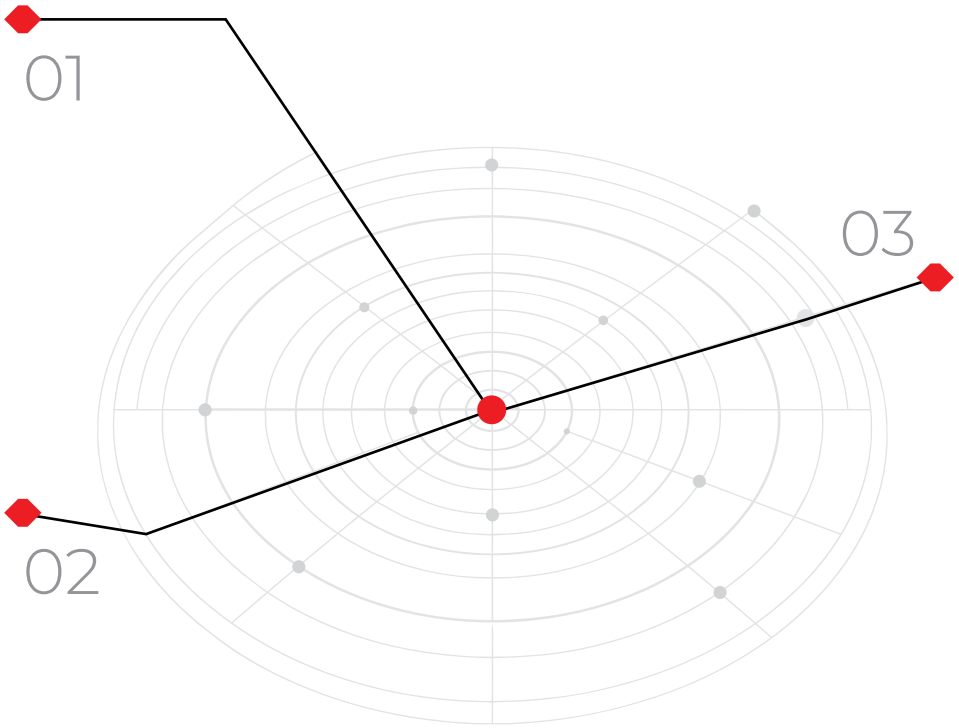
What Turns a Signal Into Action?

An unusual privileged-identity event is detected across cloud and endpoint environments. What happens next determines whether it causes disruption.

Detect and Connect

01

Extended Detection and Response (XDR) identifies unusual endpoint and identity behavior. Security Information and Event Management (SIEM) correlates asset criticality, identity, cloud and threat-intelligence data.



Decide and Contain

02

AI-assisted triage and expert validation determine business impact. Security Orchestration, Automation and Response (SOAR) isolates the endpoint, revokes access and activates incident response.

03

Recover and Learn

Teams validate recovery, update detections and provide evidence-ready reporting, reducing operational disruption and strengthening executive confidence.

What Keeps a Managed SOC Effective?

Scale depends on the foundations that keep expertise, technology and improvement operating as one system.

01

Accountable Expertise

Tiered analysts, hunters, detection engineers and incident responders operate with named service leadership and clear customer-provider decision rights.

02

Connected Operating Platform

SIEM, XDR, SOAR, threat intelligence and case management combine asset, identity, vulnerability and business-service context with controlled automation.

03

Governed Improvement

Use cases and response workflows evolve through post-incident learning, continuous evidence and risk-linked service reviews.

Four Moves to Modernize Security Operations

A Managed SOC can provide scale, specialist expertise and always-on execution, but modernization must begin with business risk and critical services.

01

Prioritize Business Risk

Define critical services, material exposures, regulatory obligations and resilience outcomes.

02

Integrate the Operating Picture

Connect SIEM, XDR, cloud, identity, network, OT, vulnerability and threat-intelligence signals around asset and business context.

03

Orchestrate Response

Use AI-assisted triage and SOAR playbooks to standardize investigation, escalation and containment, with expert validation for high-impact actions.

04

Measure and Improve

Track detection quality, containment, recovery, coverage and control effectiveness, then continuously tune detections and playbooks.

Modernization Principle

Modernize the operating model before expanding the toolset.

Build SOC Maturity in Deliberate Increments

A Managed SOC should expand only when foundational coverage, response discipline and governance are working reliably.

01

Establish the Foundation

Focus

Secure the basics and create operating discipline.

- Map critical services and telemetry coverage.
- Define severity, escalation and core response playbooks.
- Establish service ownership and compliance-ready reporting.

Evidence to advance

Critical assets are visible and priority incidents are consistently escalated.

02

Integrate and Automate

Focus

Improve context, speed and repeatability.

- Connect SIEM/XDR with identity, cloud, vulnerability and asset context.
- Automate enrichment, routing and approved containment actions.
- Tune detections against critical use cases and measure response performance.

Evidence to advance

Workflows are repeatable, coverage is measurable and triage friction is falling.

03

Optimize for Resilience

Focus

Anticipate threats and improve business outcomes.

- Expand threat hunting and exposure-led detection engineering.
- Apply AI with expert validation across investigation and prioritization.
- Link dashboards to business services, recovery and control effectiveness.

Outcome

Faster containment, stronger recovery and executive risk visibility.

Modernization Principle

Prove value through high-risk use cases, then expand coverage, automation and assurance.

Are You Measuring What Matters?

Managed SOC value is demonstrated through reduced exposure, faster containment, reliable recovery and credible evidence, not activity counts.

88%*

of surveyed Middle East organizations measure the potential financial impact of cyber risks to at least some extent.



The Executive Question

Can leaders see whether security operations are reducing business exposure or simply processing more activity?

Measurement Principle

Operational metrics matter only when they demonstrate earlier detection, faster containment, stronger recovery or lower business impact.

Sources: *PwC, 2026 Global Digital Trust Insights: Middle East Findings.

Three Outcomes That Prove SOC Value

Translate operational performance into outcomes that executives, boards and regulators can act on.

01

Protect

Detection quality and response performance

Measure

MTTD, critical-service coverage, containment time and escalation quality.

Ask

Are priority threats visible early enough to contain their impact?

02

Recover

Resilience and recovery readiness

Measure

Dwell time, recovery readiness, repeat incidents and lessons implemented.

Ask

Can critical services sustain operations and recover predictably?

03

Prove

Governance, assurance and operating sustainability

Measure

Evidence availability, control exceptions, analyst productivity and cost predictability.

Ask

Can leaders verify control effectiveness and sustain the operating model?

Cyber Operations Connected to the Infrastructure They Protect

Black Box combines Managed SOC expertise with deep knowledge of enterprise infrastructure, creating one coordinated operating model across networks, cloud, data centers, digital workplaces and connected environments.

Digital Infrastructure Context

Network · Cloud · Identity · Endpoint · Data center · Digital workplace · Connected environments

Managed SOC Operating Layer

Monitor · Detect · Hunt · Investigate · Respond · Govern · Improve

Flexible Delivery

Fully managed · Co-managed · Dedicated or hybrid

Open by Design

Integrates with existing SIEM, EDR/XDR, SOAR, cloud and threat-intelligence investments.

Black Box Scale

5	35+	8+	40+
Global SOC Centers	Countries	SIEM Platforms	Experienced Analysts

From Fragmented Tools to Faster Response

How a UAE automotive enterprise transformed disconnected security monitoring into an always-on resilience capability.

The Operating Challenge

Independent tools, manual monitoring and limited 24/7 coverage constrained visibility and slowed response.

The Managed SOC Response

A centralized security platform and UAE-based 24/7 Managed SOC unified monitoring, analytics, investigation, response, and governance.

Results

66+	13M	80%	60%
security log sources	security events daily	reduction in MTTD	reduction in MTTR



Executive Takeaway

Centralization turned fragmented security activity into faster detection, coordinated response and a scalable foundation for growth.

Read the Case Study →

When Banking Growth Outpaces Security Operations

How a leading Mongolian bank unified threat visibility and accelerated response across critical digital services.

The Operating Challenge

Distributed logs, reactive monitoring and rising alert volumes weakened correlation, increased investigation effort and added compliance pressure.

The Managed SOC Response

Securonix SIEM and UEBA, supported by a 24/7 Managed SOC, unified monitoring, threat hunting, investigation, response and reporting.

Results

90% reduction in manual investigation effort

100% visibility across onboarded systems

80% reduction in MTTD

75% reduction in MTTR

At scale: 42 security log sources | 8.62M security events daily

Executive Takeaway

Continuous visibility converted reactive monitoring into faster response and stronger service continuity.

Read the Case Study →



The Next Crisis Will Expose Today's Decisions

Resilience is built before disruption through clear priorities, decision rights, and tested recovery.

Three Decisions to Make Now

01

Protect What Cannot Fail

Identify critical services and align telemetry, detection, and recovery priorities to business impact.

02

Authorize Action Before Delay

Set containment thresholds, escalation paths and decision rights before an incident.

03

Prove Resilience Before Disruption

Rehearse cross-functional response and measure exposure, containment, recovery, and control effectiveness.

The Leadership Mandate

Build a Managed SOC that helps the enterprise see sooner, act faster and recover with confidence.

A Managed SOC creates value when it converts leadership decisions into continuous, measurable resilience.

References

External research consulted in developing this POV, with an emphasis on 2025 and 2026 Middle East findings.

Market and Security Spending

1. **MENA IT Spending Forecast to Reach USD 169 Billion in 2026**
   Gartner | 4 August 2025 | ***Official source →***

2. **MENA End-User Spending on Information Security Forecast to Reach USD 4 Billion in 2026**
   Gartner | 6 October 2025 | ***Official source →***

3. **Information Security Spending in MENA Forecast to Grow 14% in 2025**
   Gartner | 8 April 2025 | ***Official source →***

Cyber Risk and Threat Outlook

4. **Predictions 2026: Cybersecurity and Risk Leaders Grapple With New Technology and Geopolitical Threats**
   Forrester | 1 October 2025 | ***Official source →***

5. **Announcing Forrester's Top Cybersecurity Threats for 2026**
   Forrester | 10 June 2026 | ***Official source →***

Cyber Resilience and Executive Priorities

6. **AI and Quantum Readiness Reshape Cyber Resilience in the Middle East**
   PwC Middle East | 2026 Global Digital Trust Insights | ***Official source →***

7. **2025 Global Digital Trust Insights: Middle East Findings**
   PwC Middle East | 2025 | ***Official source →***

8. **28th CEO Survey: Middle East Findings**
   PwC Middle East | 2025 | ***Official source →***

Source Note

An asterisk throughout the POV identifies externally sourced data. Additional page-level sources include Grand View Research, IBM's Cost of a Data Breach Report 2026 and the two Black Box customer case studies. Third-party references provide context and do not imply endorsement.

Ready to Advance Your Cyber Resilience?

Visit **blackbox.com** or email **contact@blackbox.com**
to connect with a **Black Box** cybersecurity expert.

BLACK BOX®