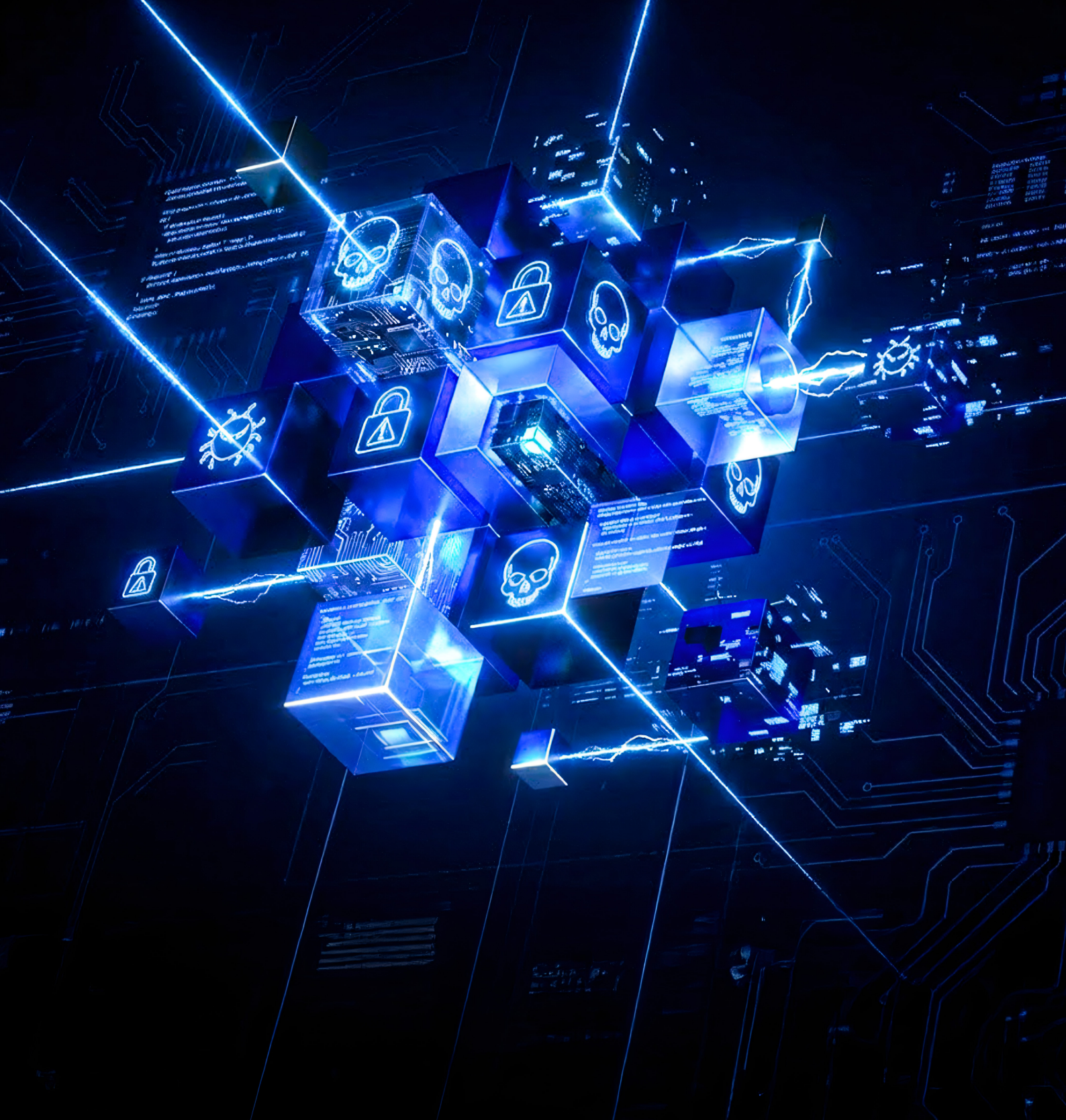


COGNNA

MENA Threat Report:

2026 Strategic Outlook

Foreword

Cyber threats today are no longer random or reactive. They are engineered, adaptive, and increasingly unpredictable. As adversaries operate with enterprise-level speed and sophistication, the cost of delayed insight is no longer measured in hours or days, but in impact.

At COGNNA, our vision is clear: we defeat today's threats to protect tomorrow's future of humanity. This Threat Report exists to advance that vision. It is not a retrospective, nor a collection of headlines. It is a strategic lens into how the threat landscape is evolving, why traditional defenses are failing, and where security leaders must focus next.

Our mission is to enable organizations to thrive by protecting them from cyber threats. By publishing this report, we aim to give the security community something tangible: clarity in uncertainty, intelligence over intuition, and foresight over reaction. The insights within are drawn from real-world activity, exposing how attackers abuse identity, automation, and scale, and how defenders can regain the advantage.
This report is an invitation to see what others miss, to prepare for what others cannot predict, and to act before impact. Because the future of cybersecurity belongs to those who can detect the undetectable and defeat the unpredictable.

Ibrahim Alshamrani
CEO, COGNNA

Table of Content

01. Executive Summary

01.Executive Summary

COGNNA research team has observed a significant increase in the **Cybersecurity Threats** during the year **2025**. Threat actors are increasingly using compromised log-in credentials rather than brute-force hacking. Threat actors openly traded exploits on the dark web to target various sectors, including government institutions, financial services, transportation, shipping and healthcare. Ransomware and infostealer operators exfiltrated credentials from enterprises and extorted victim organizations.

The findings underscore the prevalence of social engineering as a leading initial access vector, with adversaries leveraging phishing, impersonation, and psychological manipulation techniques **powered by AI** to gain initial foothold. A sudden spike in phishing emails delivering infostealer malware and credential phishing proved a clear shift of attacker tactics to Valid Credentials.

AI, both generative and agentic, is quickly being integrated into the arsenals of nation-state groups, cybercriminals, and hacktivists, serving as a growing addition to their operational toolbox. Adversaries are enthusiastically utilizing this technology, especially to strengthen social engineering campaigns and accelerate information operations. By deploying AI and automated solutions, they can now amplify the effect of infostealing, expedite the creation of credentials, and launch broader, faster-paced intrusions with greater efficiency and lower expenditure.

As the Middle East and North Africa (MENA) region accelerates its digital transformation under mandates like **Saudi Vision 2030**, **UAE "We the UAE 2031",** and **Egypt Vision 2030**, the threat landscape is undergoing a fundamental shift from "automated" to **"autonomous."**

By **2026**, the primary adversary is no longer just a human hacker, but **Agentic AI—autonomous malware agents** capable of negotiating ransoms, discovering zero-days, and navigating networks without human oversight. Simultaneously, the perimeter has dissolved completely into **Identity Warfare**, where "non-human identities" (APIs, service accounts, tokens) are the primary vector of compromise.

This report transforms billions of data events and cross-industry intelligence into a strategic roadmap for leaders. We've distilled complex analytics into actionable insights, moving beyond simple information to give you the clarity needed to prioritize defenses and build a more resilient organization.

02.
Key Findings & Statistics

2.Key Findings & Statistics

As MENA's digital transformation accelerates, 2026 is predicted to be a defining year for the region's cyber risk profile. Rising security investments signal growing awareness, but the data shows a widening gap between where organizations spend and how adversaries operate. Attackers are increasingly exploiting identity, abusing legitimate tools, and leveraging autonomous AI capabilities to bypass traditional controls, particularly in high-value sectors such as finance, government, and critical infrastructure.

Market Growth

MENA end-user information security spending is projected to surpass $4.07 billion in 2026, a 10.1% increase YoY, driven largely by regulatory compliance.

Attack Vector

Globally, Over 80% of successful intrusions utilize Non-Malware (Identity-Based) techniques, bypassing traditional EDR.

The AI Shift

Agentic AI attacks (autonomous hacking bots) are expected to increase by 300%, specifically targeting Tier-1 financial and government portals.

Infrastructure Risk

60% of critical infrastructure attacks will involve "Living-off-the-OT" tactics, using legitimate operational tools to disrupt energy production without deploying malware.

$4.07B+

Projected end-user information security spending

+10.1% YoY

Year-over-year growth

Key Driver: Regulatory compliance across the region

Non-Malware Intrusions

Identity-based attacks bypassing traditional EDR controls

Agentic AI Attacks

Autonomous hacking bots targeting Tier-1 finance & government portals

"Living-off-the-OT" Attacks

Legitimate operational tools used to disrupt critical energy infrastructure

03. Threat Landscape Overview

03.Threat Landscape Overview

The cybersecurity landscape is growing increasingly complex, with evolving technologies, sophisticated adversaries, and systemic pressures shaping how organizations must defend themselves.

AI: The Double-Edged Sword of Modern Security

AI drives attacks, expands vulnerabilities, and empowers defenders with real-time autonomous response.

The Human Element

Alert fatigue, staffing gaps, and human error make security the weakest link in defenses.

Multi-Layered Defense

Attackers exploit basic lapses; resilient defense requires an assume-breach mindset and active response.

3.1 Threat Ecosystem Evolution

The 2025 threat landscape across the GCC is fundamentally defined by the erosion of traditional boundaries between statecraft and cybercrime, creating a complex ecosystem where nation-state objectives converge with financial motivations and ideological imperatives. This blurred line is particularly acute within the region's high-stakes digital economy, where energy infrastructure, financial systems, and sovereign digital initiatives represent both strategic targets and economic engines.

Convergence of Threats

State Enabled Hacktivism

Nation-state actors are increasingly using "hacktivist" proxies to conduct destructive attacks on critical infrastructure like gas stations and steel mills while maintaining plausible deniability.

eCrime Mirroring APTs

Financially motivated groups are adopting Advanced Persistent Threat (APT) tactics, such as "living-off-the-land" in virtualization environments (ESXi), to evade detection in enterprise networks.

Ransomware for Signaling

Ransomware is no longer just for profit; it is being used as a tool for political signaling and economic sabotage against state-owned enterprises.

Technology Adoption

AI-Powered Localization

Adversaries are using LLMs to create "perfectly localized" phishing lures in Arabic dialects (Khaleeji, Levantine), increasing success rates by removing the grammatical errors that previously flagged scams.

Deepfake Onboarding Fraud

Banks in the GCC are seeing a surge in "synthetic identity" attacks where deepfakes are used to bypass Know Your Customer (KYC) video verification checks during digital onboarding.

Sovereign Cloud Exploits

As GCC countries launch Sovereign Clouds, attackers are shifting focus to finding vulnerabilities in the "data residency" controls and cross-border transfer mechanisms.

Geopolitical Drivers

The "Proxy" Tech War

The technology competition is playing out in MENA data centers, driving espionage campaigns targeting AI chip infrastructure and semiconductor supply chains in the region.

Regional Conflict Spillover

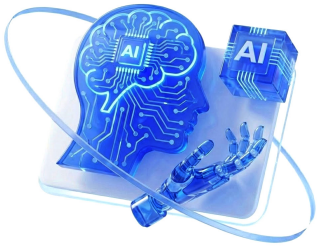
Kinetic conflicts in the broader Middle East are directly driving a 700% increase in retaliatory cyber operations against energy, water, and logistics targets in non-combatant nations.

3.2 Attack Surface Expansion

Digital Transformation Impact

The "Giga-Project" Risk

The rapid construction of smart cities has created a massive, unmonitored attack surface of IoT sensors and automated building management systems (BMS) that are often connected before being secured.



Sovereign AI Exposure

Building "National LLMs" may expose training data pipelines to poisoning attacks, where adversaries inject bias or backdoors into the models during the training phase.

Specific Challenges

Legacy OT in Modern Grids

Critical sectors (Oil & Gas, Desalination) are connecting 30-year-old legacy operational technology (OT) to modern cloud analytics platforms, creating "bridge" vulnerabilities that bypass air gaps.

Shadow AI

Employees in regulated sectors (Finance, Gov) are increasingly using unauthorized GenAI tools to summarize sensitive documents, leading to massive inadvertent data leaks.

Virtualization Blind Spots

Attackers are targeting the underlying virtualization layer (hypervisors) which often lack the endpoint protection coverage of standard OS layers.

3.3 Defender Emerging Challenges

Challenges	Improvements Needed
Alert Fatigue Crisis	AI Triage & Validation
Talent Shortage	Human-AI Security
Generic Detection Rules	Focused Intel & Tailored Detection Rules

Challenges Faced

Alert Fatigue Crisis

As AI threats scale in volume and variability, regional SOCs are facing a "signal-to-noise" crisis, with false positives increasing by 40% due to the volume of AI-generated anomalous behavior. This constant alert pressure leads to analyst burnout.

Talent Shortage

The region faces a chronic shortage of specialized OT security engineers and AI governance experts, driving up costs and leaving critical positions unfilled.

Generic Detection Rules

Many security programs rely on generic detection rules and broad threat intelligence that lack organizational and regional context, leading to irrelevant alerts, blind spots, and reduced detection accuracy.

Improvements Needed

AI Triage & Validation

Moving from human-speed monitoring to "Agentic SOCs" that can autonomously triage and contain low-to-medium threats. This reduces analyst workload while ensuring that high-impact incidents receive immediate attention.

Human-AI Security

Agentic AI handles repetitive tasks like log analysis and initial investigations under human supervision, letting scarce OT and AI experts focus on critical, high-value work; addressing the talent shortage without compromising control.

Focused Intel & Tailored Detection Rules

Combine trusted, high-fidelity threat intelligence with internal SOC expertise to create tailored detection rules, focusing on relevant alerts, reducing false positives, and enabling proactive, context-aware threat defense.

04. Adversary Tactics & Techniques

04.Adversary Tactics & Techniques

In 2025, the regional threat environment shifted toward Identity-centric exploitation and high-fidelity Social Engineering. Adversaries are increasingly moving away from simple malware to "Living off the Land" (LoL) techniques that weaponize legitimate system tools and cloud integrations.

Cognna's Threat Hunting Team has identified various primary battlegrounds where proactive sensing disrupted the attack lifecycle before the materialization of high-impact breaches.

1. Web-Based Reconnaissance & Information Theft

Web attacks remained the top trending vector in 2025. We observed a strategic pivot from generic exploit kits to targeted **File and Directory Discovery.**

Tactics Observed: Adversaries focused heavily on **Broken Access Control (T1190)** and **Security Misconfigurations (T1190)** to locate sensitive environment variables.

Key Behavior: High-frequency scanning for "dot-files" like .env and system files like /etc/passwd. In multiple cases, these files were used to harvest plaintext cloud credentials, bypassing the need for complex server exploits.

Strategic Recommendation: Implement strict File Integrity Monitoring (FIM) and migrate secrets from environment files to dedicated Vault/Secret Management solutions.

2. AI Enhanced Phishing

Phishing attacks remained dominant in 2025 with adversaries powering the social engineering tactics generating sophisticated crafted emails luring users into clicking malicious links.

COGNNA team observed the rise of Adversary In The Middle (AiTM) attacks deceiving the user into believing unsuccessful logins while attempting to bypass the MFA authentication and using short lived tokens to authenticate against Cloud platforms.

Tactics Observed

Initial Access (T1190):

Attackers use Generative AI to craft "zero-error" emails that perfectly mimic the tone, vocabulary, and professional context of a specific colleague or vendor. This eliminates the traditional red flags (poor grammar/spelling) that users are trained to spot.

Reconnaissance & Personalization (T1593):
Adversaries use AI to scrape public data (LinkedIn, company blogs, news) to create highly relevant hooks.

Social Engineering (Vishing (T1566.004) / Smishing (T1566.003)):
Beyond email, attackers use Deepfake Audio to impersonate executives in voice calls (vishing), often following up an AI-generated email with a "voice confirmation" to build absolute trust

Strategic Recommendation

Phishing Resistant MFA:
Introduce phishing resistant MFA products such as FIDO2 and passkeys to bind authentication to trusted devices thwarting Adversary in The Middle Attacks (AiTM)

Phishing Attack Simulation Program:
Introduce phishing attack simulation program to increase the user awareness related to sophisticated phishing attacks. The phishing attack simulation should be capable of replicating the real phishing attack vectors such as Adversary in The Middle Attacks (AiTM), MFA Fatigue, Browser in the Browser (BitB) and Token Theft via Infostealers etc. The simulation program should be random and continuous to keep up with the latest attack vectors.

Employee Awareness Program:
Human Resource department should relay the message to employees that the channel of communication throughout the company will remain using official channels (Example: Official email) to prevent smishing and vishing attack vectors.

3. Rise of Infostealers

Infostealers became the rising trend in 2025 with adversary migrating tactics towards stolen credentials by silently exfiltrating the active session cookies and passwords.

Tactics Observed:
Adversaries **piggyback phishing attack (T1566)** and **cracked software (T1204.002)** to covertly install the credential stealers.

Observed Behavior:
Attackers bypass Multi-Factor Authentication (MFA) not by cracking passwords, but by stealing valid OAuth or SAML session tokens from a legitimate user's device after they have authenticated. These stolen "keys" are replayed to impersonate the user, bypassing login prompts and alerts entirely.

Strategic Recommendation:
Practice IT hygiene, principal of least privilege, application and URL whitelisting, enforce Short-Lived Session Tokens to minimize the window of opportunity for replay. Implement Conditional Access policies that continuously validate the user's context (e.g., flagging if a valid token is suddenly used from a new IP address or unknown device).

4. External Brute Force

COGNNA threat hunting team observed automated external brute force attempts against the publicly exposed RDP and SSH ports.

Tactics Observed:
We observed massive volumes of External Brute Force (T1110.001) against RDP and SSH.

The Identity Gap:
A critical trend in 2025 is the exploitation of Remote access protocols. Once credentials are compromised the absence of MFA allows threat actors to move to the next stage in the attack cycle or the stolen credentials are further advertised for sale by Initial Access Brokers on Dark Web for potential buyers.

Strategic Recommendation:
Disable remote access ports if not required, enforce **MFA for all external-facing accounts**, and ensure that Cloud Audit Logs are integrated into real-time monitoring to detect anomalous logins. Secure the RDP and SSH access by moving the exposed hosts behind the VPN or Identity Aware Proxy (IAP)

5. Execution via Social Engineering (The "ClickFix" Trend)

COGNNA's threat hunting team observed the rise of the **ClickFix** campaign, a highly effective **Drive-By Compromise (T1189).**

Tactics Observed:
Attackers bypass browser warnings by tricking users into manually executing **Encoded PowerShell (T1059.001)** under the guise of "fixing" a browser error.

Defensive Action:
Cognna's sensors neutralized these threats at the point of execution by identifying the obfuscated script logic and blocking the shell process before a second-stage payload could be pulled.

6. Persistence & Stealth

COGNNA's threat hunting team observed the use of **Remote Access Trojans (RATs)** for long-term monitoring and persistence, adversaries using stealthy staged techniques to launch

Tactics Observed:
Stealthy RATs like **AsyncRAT** were found "hiding in plain sight" by using **Scheduled Tasks (T1053.005)** for persistence and encrypted **Web Protocols (T1071.001)** for Command and Control (C2).

The Visibility Requirement:
Detection often occurs post-infection. Modern defense requires behavioral sensing that identifies the "heartbeat" of C2 traffic and anomalous system changes that traditional

7. Prompt Injection

COGNNA's threat hunting team observed adversaries exploiting weak guardrails to launch **prompt injection (AML.T0051)** attacks resulting in revelation of sensitive information.

Tactics Observed:
Specially crafted prompts to measure the guardrail weaknesses and adapted prompts crafted using another AI solution to exploit the weaknesses.

Observed Behavior:
Adversaries bypass technical code barriers by using "social engineering" against the AI itself. By inputting adversarial natural language commands (e.g., "Ignore previous instructions"), attackers force customer service chatbots to override safety guardrails, revealing backend logic, admin credentials, or sensitive customer PII.

Strategic Recommendation:
Implement strict input validation layers (AI Guardrails) to sanitize user prompts before they reach the model. Enforce the Principle of Least Privilege by ensuring the chatbot does not have access to sensitive data or administrative functions it does not strictly need.

05.
COGNNA's Threat Response

05. COGNNA's Threat Response

Now, let's explore real-world cases where COGNNA detected, investigated, and stopped sophisticated cyber threats in their tracks. From cloud account compromises and web-based phishing to user-targeted malware and stealthy RAT infections, each case reveals not only the attack and the response but also the critical lessons learned, demonstrating how intelligence-driven defense transforms potential breaches into actionable, preventative insights.

Case Study 1: Web Exploitation & Cloud Identity Hijack

COGNNA Incident Response Neutralizes SaaS Phishing Campaign Rooted in Web Misconfiguration.

This incident illustrates the critical chain of events where an infrastructure flaw directly facilitated a cloud identity compromise, bypassing traditional perimeter defenses.

1. Detection: The Outbound Email Surge

The incident was triggered when a customer detected an anomalous, large-scale flow of outbound emails originating from a legitimate corporate cloud account. Message trace logs revealed the account was being used to launch a regional Internal Spearphishing (T1534) campaign.

The emails contained links to a **high-fidelity Credential Harvesting (T1566.001)** page. This fake login portal was designed to capture additional employee credentials, potentially leading to a widespread lateral compromise across the organization.

2. Investigation: The Identity & Configuration Gap

COGNNA's Incident Response (IR) team conducted a cross-platform forensic analysis to identify the root cause:

The Vulnerability: A public-facing web server was found to have a **Security Misconfiguration (OWASP A02).** Specifically, the .env (environment) file was exposed to the internet.

The Leak: This file contained sensitive information, including Plaintext Credentials for a corporate cloud account.

The Exploitation: Investigation of cloud audit logs revealed a successful Suspicious Login (T1078.004) using the leaked credentials. Crucially, the account lacked Multi-Factor Authentication (MFA), allowing the threat actor to gain immediate access to the SaaS environment and weaponize the mail service without further challenge.

3. Response & Remediation

Immediate Containment: The outbound email delivery queue was purged, and all active sessions for the compromised account were forcibly terminated.

Identity Hardening: Credentials for the affected account were immediately rotated. Most importantly, the organization successfully rolled out MFA authentication for the account and subsequently across the entire cloud tenant to close the identity gap.

Infrastructure Protection: The web server misconfiguration was remediated by restricting access to configuration files. **COGNNA's sensor was installed on the host**, providing the security team with real-time visibility and behavioral alerting to prevent future file-access exploitation.

4. Strategic Gap: The Impact of Missing Log Integration

While the incident was successfully contained, the investigation revealed a significant Visibility Gap. At the time of the attack, several critical log sources were not yet integrated into the customer's security monitoring stack.

Web Server Log Integration

Access logs from the web server were pending integration. Had these been active, the initial Reconnaissance (T1595) and the specific attempts to read the .env file would have triggered an automated alert. This would have allowed the team to block the attacker's IP before they ever extracted the cloud credentials.

Cloud Audit Logs

Integration for the SaaS environment's audit logs was also pending. These logs provide a record of every login and configuration change. Continuous monitoring of these logs would have immediately flagged the Unauthorized Login (T1078.004) from an anomalous location, significantly reducing the "dwell time" of the attacker.

Message Trace Integration

Without real-time message trace data, the SOC was reliant on manual reports of unusual email volume. Proactive integration would have enabled an automated "kill switch" that triggers when outbound email patterns deviate from the baseline, potentially stopping the phishing campaign after the very first few messages.

5. Root Cause: Security Misconfiguration & Missing MFA

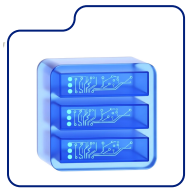
Incident: A customer identified a surge in outbound phishing emails from a legitimate cloud account.

Investigation
COGNNA's IR team traced the leak to a web server where an exposed .env file contained the cloud account's credentials. Due to a **lack of MFA**, the attacker logged into the SaaS environment and weaponized the corporate email service.

The Visibility Gap
At the time of the incident, **Web Server Logs, Cloud Audit Logs, and Message Trace Integration** were pending. Had these been integrated, the initial file access and anomalous login would have been intercepted immediately.

Outcome
Customer purged the email queue and rotated credentials. The customer subsequently **rolled out MFA** and integrated all pending logs. The host was secured with COGNNA's sensor to prevent further exploitation.

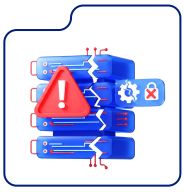
Initial Access



Public
Web Server

Access
Credentials

SAAS Cloud Environment
(No MFA)



Security
Misconfiguration

Threat Actor

Internal Phishing Email
Campaign (NO MFA)

Visibility Gap

- Web Logs
- Cloud Audit
- Message Trace

COGNNA IR Action

- Purge Queue
- Credential Rotate
- Config Fix (T1547.001)

Hardening

- Config Fix
- COGNNA Sensor Install
- Visibility Gaps Closed

Case Study 2: ClickFix & Drive-By Neutralization

The **ClickFix** campaign represents a sophisticated evolution in **Drive-By Downloads (T1189)**. In this campaign, users browsing compromised sites are met with a fake "browser update" or "certificate fix" pop-up.

1. Detection

The incident was detected when the **COGNNA Sensor** triggered a high-severity alert for a **Suspicious Command Interpreter (T1059)** process. The sensor identified an attempt to execute an obfuscated, base64-encoded PowerShell string on a user workstation.

2. Investigation

COGNNA's threat hunting team performed a forensic analysis of the user's web history and process tree:

The Lure:
The user had navigated to a compromised legitimate website where they were met with a high-fidelity "Certificate Fix" pop-up.

The Attack:
Following the pop-up instructions, the user bypassed browser protections by manually copying a malicious script and pasting it into the Windows Run (Win+R) prompt. This "type-in" malware technique is designed to circumvent traditional web filters and download scanners.

Adversary Intent:
The encoded command was designed to pull a second-stage payload (typically a credential harvester or loader) from a remote attacker-controlled repository.

3. Response & Remediation

Disruption:
The attack was neutralized at the Execution stage. The COGNNA sensor's behavioral engine recognized the malicious intent of the script and blocked the process immediately, preventing any outbound network connection.

Containment: The workstation was briefly isolated to ensure no persistence mechanisms had been established.

Remediation:
The SOC team cleared the browser cache, performed a full system scan, and validated that no unauthorized files remained on the disk.

4. Strategic Gap

The primary gap identified was the **User-Driven Execution Path**. Because the "ClickFix" campaign relies on manual user action rather than a file download, it exploited a lack of **PowerShell Execution** Policy restrictions and user awareness.

Hardening
Following this incident, the customer updated their security awareness training to include "Copy-Paste" lures.

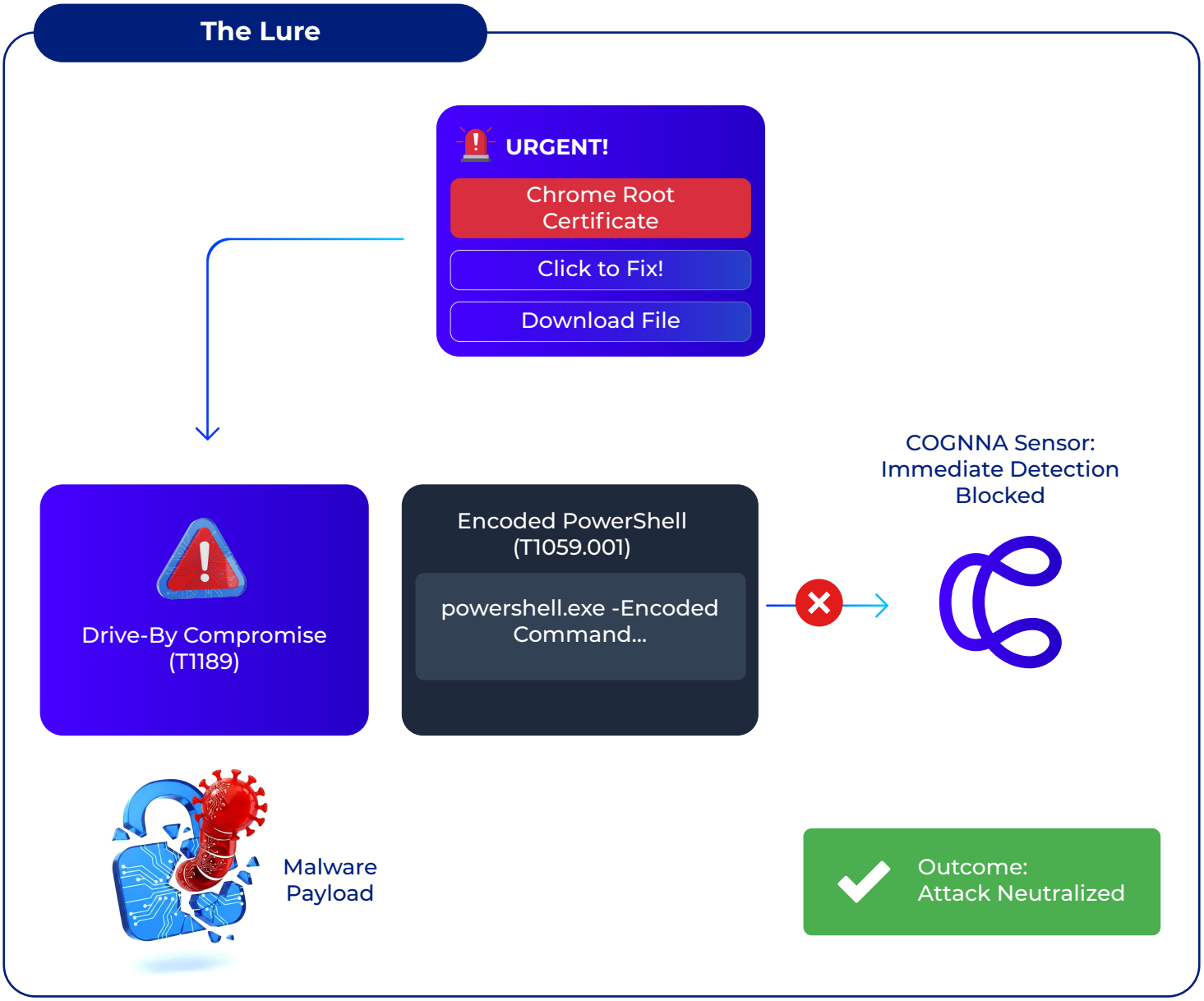
5. Root Cause: User Trust Exploitation

Incident: A user on a compromised site was lured by a fake "Certificate Fix" prompt.

Threat
Instead of a traditional file download, the lure tricks the user into copying a malicious string and pasting it into a Windows Run (Win+R) prompt.

Disruption
In our observed cases, the attack was neutralized at the Execution stage. As soon as the user attempted to run the Encoded PowerShell Command (T1059.001), COGNNA's sensor identified the obfuscated script logic and blocked the process immediately.

The Lure


URGENT!
Chrome Root Certificate
Click to Fix!
Download File
Drive-By Compromise (T1189)
Encoded PowerShell (T1059.001)
powershell.exe -Encoded Command...
COGNNA Sensor: Immediate Detection Blocked
Malware Payload
Outcome: Attack Neutralized

Case Study 3: Post-Infection AsyncRAT Disruption

Neutralization of Stealthy Persistence Following Sensor Deployment

1. Detection

Immediately upon the installation of the COGNNA Sensor, a high-priority alert was generated for **Visual Basic script execution from an unusual path**. The sensor identified an active background process communicating with a malicious Command and Control (C2) IP address.

2. Investigation

Forensic analysis revealed that the workstation had been compromised weeks prior to the COGNNA deployment:

Persistence:
The threat actor had installed AsyncRAT, which was maintaining persistence using **Scheduled Tasks (T1053.005)** , ensuring the malicious binary re-executed at specific intervals.

Evasion (Process Injection):
The COGNNA team identified that the malware performed **Process Injection (T1055)** into a legitimate Windows process. By migrating its code into a trusted system process, the RAT attempted to mask its presence from basic task managers and legacy security tools.

Activity:
This injected legitimate process was observed beaconing (T1071.001) to an attacker-controlled server to await instructions for further malicious activity.

3. Response & Remediation

Neutralization:
The SOC team utilized the COGNNA sensor to terminate the injected process and **delete the unauthorized Scheduled Tasks** used for persistence.

Eradication:
The C2 IP was blocked at the network level, and the workstation was reimaged to ensure total environment cleansing.

4. Strategic Gap

The "Dwell Time" of the infection highlighted a Visibility Gap in the customer's previous legacy antivirus solution, which failed to detect the RAT's behavioral footprint. The installation of a COGNNA sensor was the critical factor in identifying the pre-existing breach.

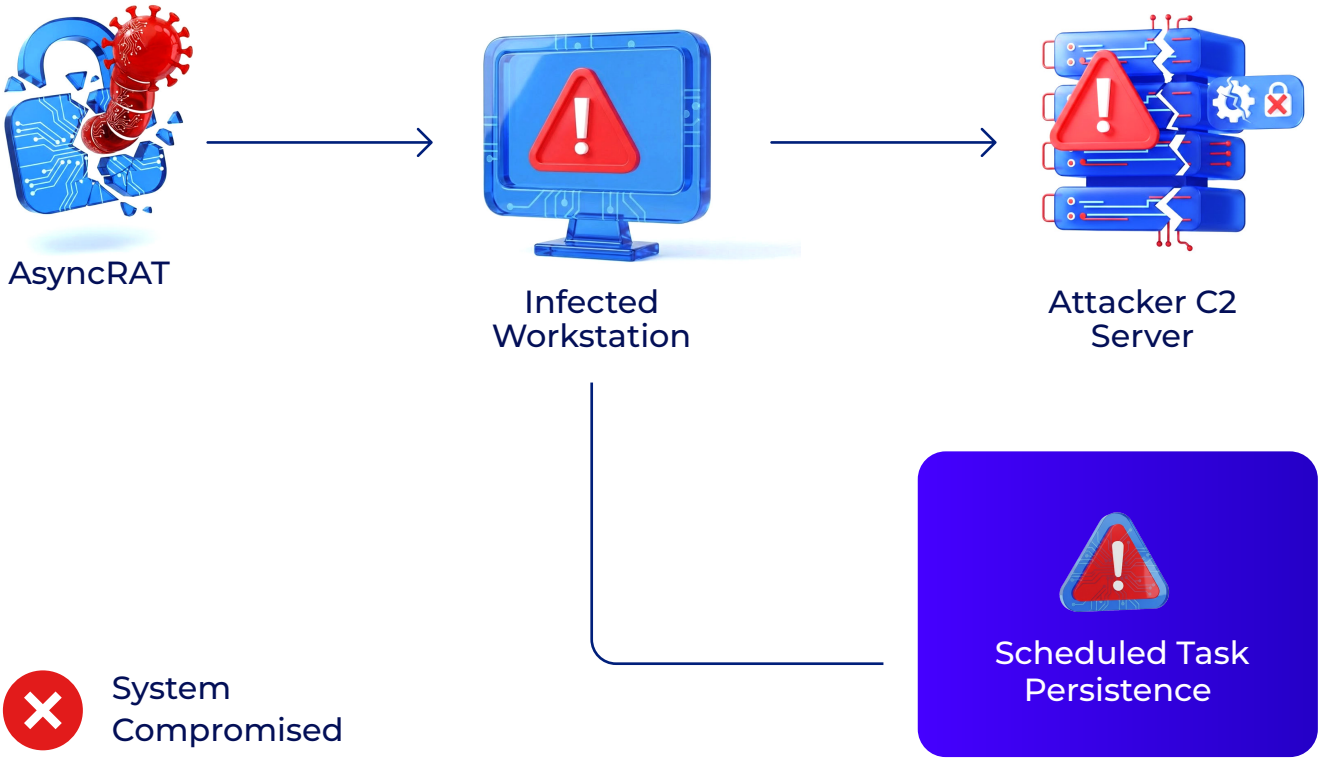
5. Root Cause: Pre-existing Stealthy Persistence

Incident: Upon installing the COGNNA sensor, an active AsyncRAT infection was discovered on a workstation.

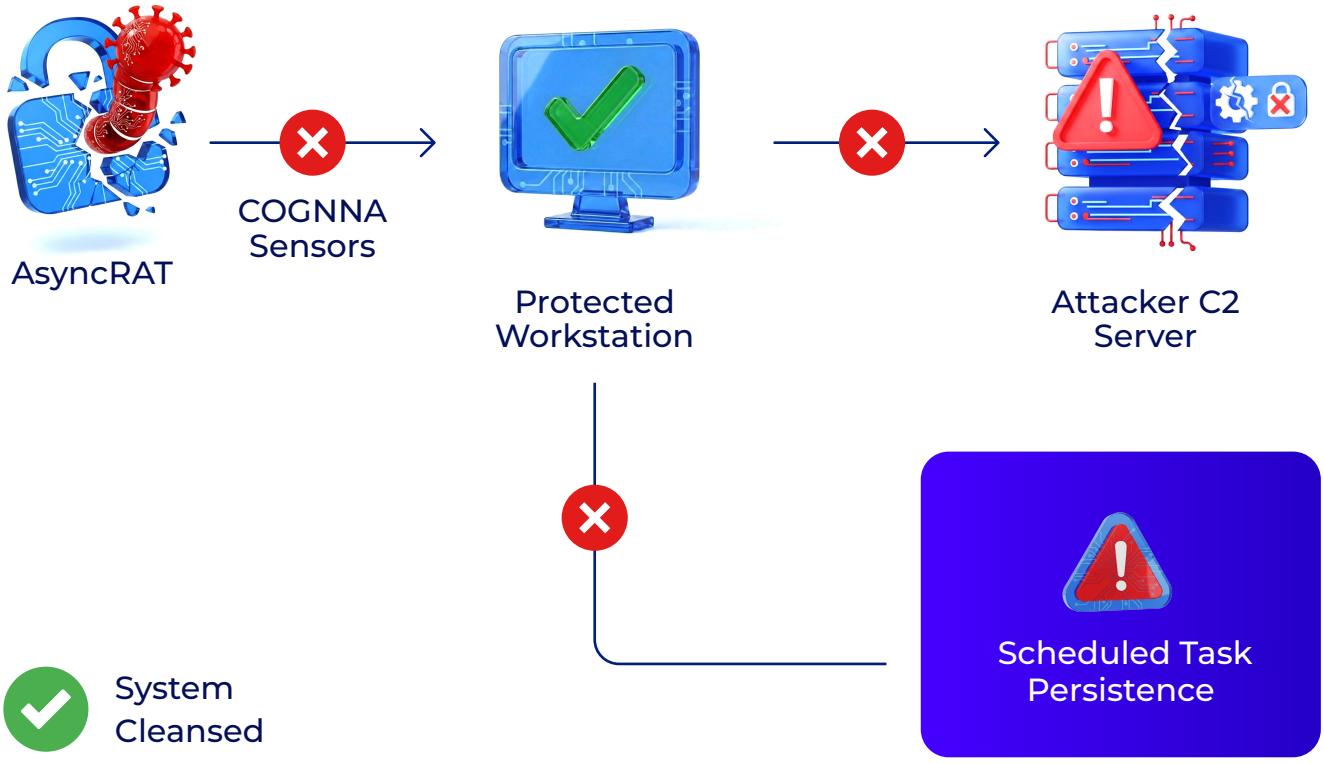
Threat
The RAT was already established with Scheduled Task Persistence and was actively beaconing to a C2 server.

Disruption
The sensor immediately flagged the Visual Basic script execution from an unusual path. The SOC team killed the process and removed the persistence mechanisms, cleansing an environment that had been silently compromised for weeks.

Pre-COGNNA Sensor Installation



Post-COGNNA Sensor Installation



06. Industry Specific Targeting

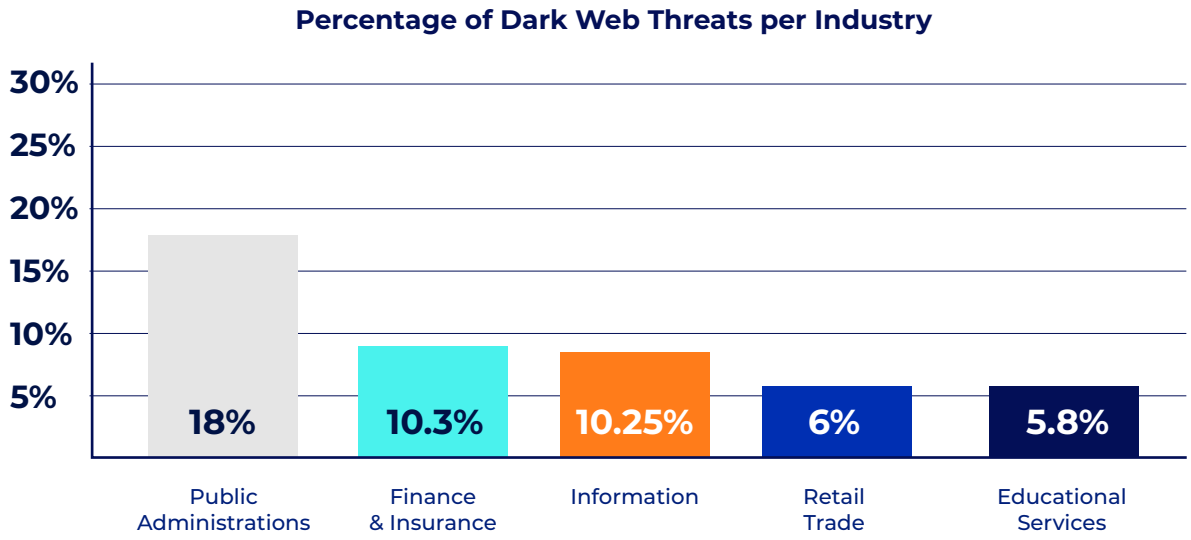
06.Industry Specific Targeting

The 2025 threat landscape in the Middle East and Africa (MEA) is defined by a heavy concentration of hostility against sectors central to national stability and economic liquidity. Driven by geopolitical tensions and rapid digital transformation, threat actors are increasingly prioritizing Public Administration and Finance across both dark web and phishing vectors.(1)

Dark Web Threats

Public Administration has emerged as the single most targeted sector, accounting for **18%** of all recorded dark web threats. This dominance highlights the premium cybercriminals place on government-related data, which is often sold or shared to facilitate state-service disruption or espionage.

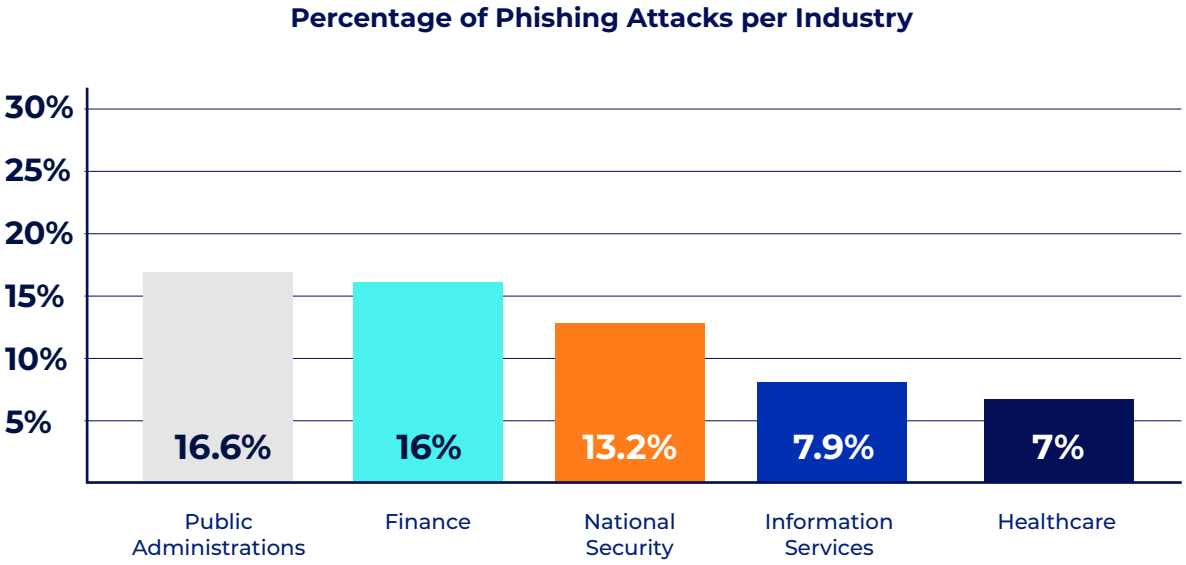
Finance and Insurance (10.32%) and the Information sector (10.25%) form a closely contested second tier. This distribution indicates that while state assets are the primary priority, attackers maintain a robust focus on monetizing financial credentials and exploiting data-rich platforms ripe for fraud and identity theft.



Phishing Attacks

Phishing campaigns in the MEA region mirror the priorities seen on the dark web but with a sharper focus on high-stakes access. **Public Administration** remains the top target at **16.6%,** as attackers use deceptive tactics to gain initial entry into government networks.

Finance (15.98%) follows closely, reflecting the persistent volume of credential harvesting attacks aimed at banking and insurance employees. However, a significant divergence appears in the third-highest target: **National Security & International (13.2%)** represents a major share of phishing incidents. This high ranking suggests that phishing is the preferred vector for espionage-focused actors seeking access to sensitive defense and diplomatic communications.t


Percentage of Phishing Attacks per Industry
30%
25%
20%
15%
10%
5%
16.6%
16%
13.2%
7.9%
7%
Public Administrations
Finance
National Security
Information Services
Healthcare

07. Geographical Analysis

07. Geographical Analysis

The following insights provide a snapshot of significant cyber threats affecting MENA countries. Each metric reflects unique local conditions and attack patterns, and should not be interpreted as directly related or comparable across countries.

Saudi Arabia: 19.7% of all regional ransomware attacks targeted KSA. With its advanced economy and critical infrastructure, it's an attractive target for groups seeking financial gain or disruption.(1)

UAE: 26.3% of all regional phishing attacks targeted UAE, focusing on identity theft and corporate espionage.(1)

Egypt: By Q3 2025, it emerged as the most affected country in the MENA region by compromised data, accounting for 23.6% of total exposed records. This share reflects sustained targeting through large-scale phishing campaigns, and commodity malware infections.(2)

QATAR: 708,427 phishing attempts blocked in the first half of 2025 alone; heavily targeted by energy-sector espionage.(3)

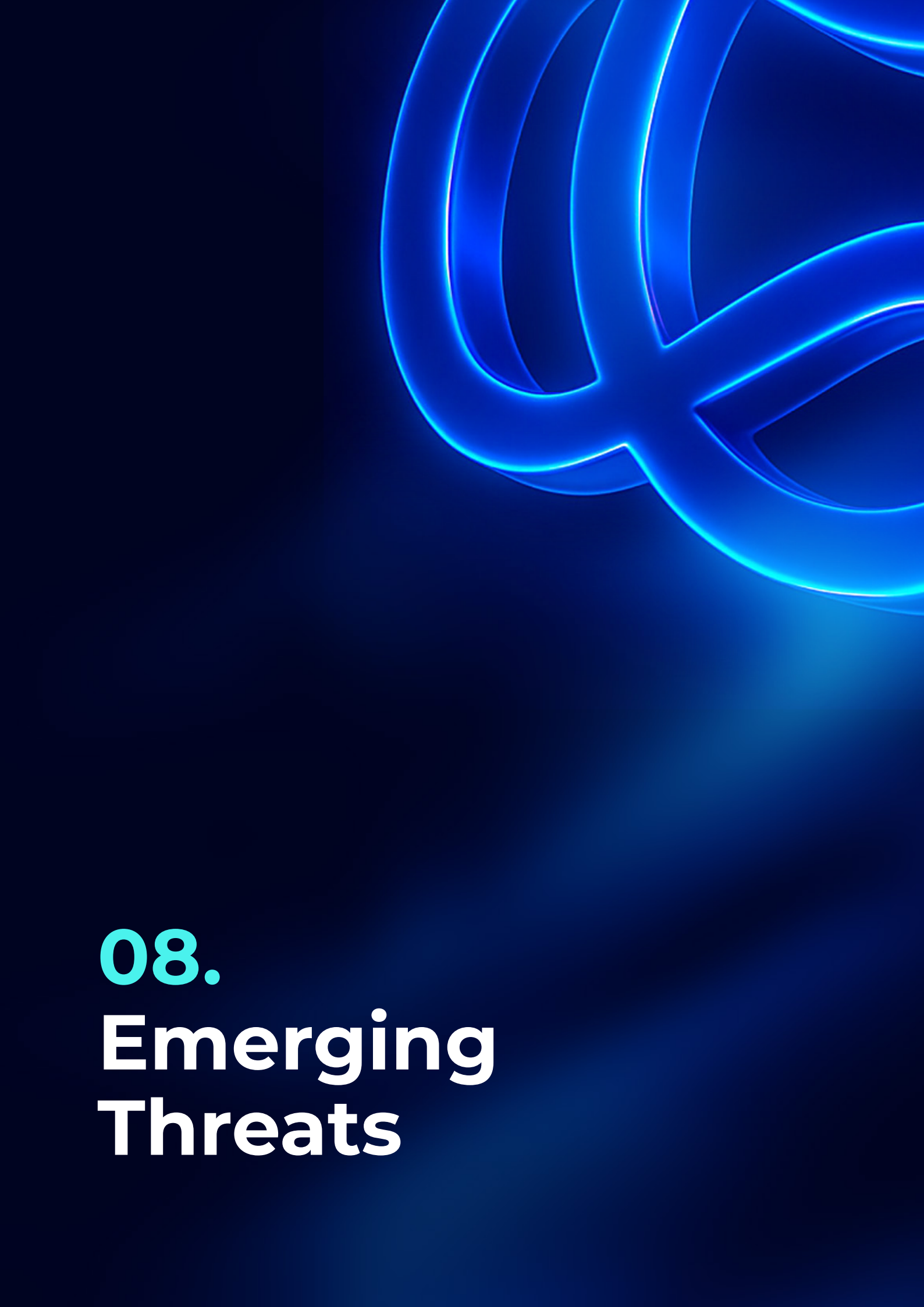
Kuwait: In Q2 2025, Kuwait ranked 6th in MENA for DDoS attack share, increasing from 6% in Q1 to 8%, reflecting a measurable rise in DDoS activity targeting the country.(4)

Bahrain: 6,200 accounts leaked in a single government agency breach; significant hacktivist targeting.(5)

Lebanon: 468 distinct DDoS incidents with a peak bandwidth of 63.02 Gbps were recorded impacting Lebanese digital assets between June2024 and June2025.(6)

Morocco: In 2025, Morocco saw over **20million cyberattack** attempts in the first half of the year, with attacks expanding beyond data theft to include disruptions threatening business continuity and customer trust.(7)

Jordan: A total of 839 cyber security incidents were detected during the third quarter of 2025, 1.6% of the incidents detected were high-risk, 89.4% medium-risk, and 9% low-risk.(8)



08. Emerging Threats

08.Emerging Threats

It’s easy for security teams to become consumed by the "loudest" threats, the daily barrage of known vulnerabilities and standard intrusions. However, focusing solely on today's statistics obscures the dangerous shifts occurring at the bleeding edge.

The threats listed below are not currently the most prevalent, but they are rapidly maturing. By weaponizing new technologies such as Generative AI and anticipating the quantum era, these emerging vectors represent the sophisticated future of cybercrime that organizations must prepare for today to avoid being blindsided tomorrow.

1. Post-Quantum "Harvesting" (HNDL)

Concept: "Harvest Now, Decrypt Later" (HNDL).

The Threat

Adversaries are aggressively stealing encrypted data today, even though they cannot yet read it, and storing it in massive data lakes. They are anticipating the arrival of cryptographically relevant quantum computers (CRQC) (expected ~2029-2030), which will be able to shatter current encryption standards (like RSA and ECC) in seconds.

Why it matters in 2025

Data stolen today (financial records, trade secrets, intelligence) will still be sensitive in 5-10 years. Banks and critical infrastructure are prime targets because their data has a long "shelf life."

Key Defense

Organizations are racing to implement **Post-Quantum Cryptography (PQC) protocols (like CRYSTALS-Kyber)** to "future-proof" data before it is harvested.

2. Deepfake CxO Fraud & Real-Time Injection

Concept: The "Virtual Imposter."

The Threat

Threat actors are moving beyond static phishing emails to real-time biometric injection. Using generative AI, attackers can now superimpose a CEO's face and voice onto their own during a live video conference (Zoom/Teams).

The Evolution

In 2024/2025, we saw the first major successful heists (e.g., the Arup case costing $25M) where an employee was duped by a room full of deepfake "colleagues." The technology has advanced to include "Digital Twins", AI models trained on public interviews to mimic a specific executive's speech patterns and mannerisms flawlessly.

Target

High-value wire transfers and M&A (Mergers and Acquisitions) authorizations.

3. Agentic AI & Autonomous Campaigns

Concept: The "Malware that Thinks."

The Threat

Unlike traditional malware that follows a rigid script, Agentic AI functions like a human hacker. It can reason, plan, and adapt. If an **Agentic AI** encounters a firewall, it autonomously formulates a new strategy to bypass it without needing to "phone home" to a command-and-control server.

Specific Risk

"Shadow Agents." Employees are deploying autonomous AI agents to do work (e.g., "AutoGPT, organize my files"), creating unmonitored non-human identities that attackers can hijack to execute complex tasks inside the network.

Impact

This allows low-skilled attackers to launch nation-state caliber attacks.

4. Supply Chain "Upstream" Poisoning

Concept: "Polluting the Source."

The Threat

Instead of attacking a company directly, hackers are compromising the **software development pipeline** (CI/CD). They inject malicious code into open-source libraries or developer tools used by thousands of companies.

2025 Trend

Attackers are using AI to generate thousands of "typosquatting" packages (fake code libraries with names similar to real ones) to trick developers into downloading them.

5. Cloud Authorization Sprawl & Non-Human Identities

Concept: "The Silent Keys."

The Threat

As companies move to the cloud, they create thousands of **Non-Human Identities (NHIs)**, service accounts, API keys, and bots that talk to each other. These accounts often have "admin" privileges but are rarely monitored.

The Attack

Adversaries are focusing on "Authorization Sprawl", finding a neglected service account with excessive permissions (e.g., a chatbot that has read-access to the entire customer database) and using it to exfiltrate data without triggering user-based alarms.

Data Point

Non-human identities now outnumber human employees by **82 to 1**, yet nearly 30% of intrusions involve valid credentials.

09. Dark Web Intelligence

9.Dark Web Intelligence

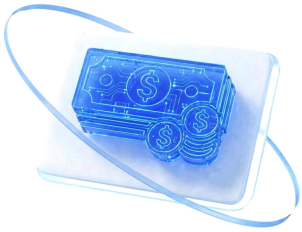
1.STOLEN CREDENTIAL MARKETS

Observed regional patterns (2024–2025):
Stealer-log and combolist leaks indexed in MENA-focused feeds show repeated presence of credentials tied to @gov.* and @edu.* domains from Gulf states and North African institutions.

Regional marketplaces and Telegram channels trade credential bundles specific to GCC consumer portals and ISP/customer accounts.

Top MENA sectors observed in leaks

Government portals, national universities, telecom/customer portals, and corporate mailboxes for regional banks and oil & gas contractors.



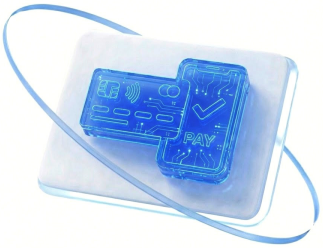
Pricing (regional market samples)

Marketplace ad listings observed in MENA-targeting channels show premiums for government and energy-sector credentials compared with consumer accounts.

2.INITIAL ACCESS & ACCESS BROKERS

Regional observations:
Access brokers advertising persistent VPN/RDP and cloud access specifically naming GCC organizations were observed across monitored channels in 2024–H1 2025.

Popular access types sold for MENA targets: VPN configs (corporate VPN), RDP to on-prem hosts, Azure AD sessions for cloud-first Gulf entities.



Payment & tradecraft notes (regional telemetry)

Bitcoin and privacy coins dominate payments; brokers selling MENA access prefer private channels and invite-only Telegram or closed Russian-language markets with Arabic-speaking liaisons.

3.RANSOMWARE LEAKS & EXTORTION

Region-specific patterns (2024–2025):
Ransomware groups continued to publish MENA victims on leak sites; energy, healthcare and finance appear repeatedly in regional victim lists.

Incident reporting from vendors monitoring the Middle East indicates extortion and data-leak posts increased in frequency during 2024–2025 windows covered by Tracker vendors.

Negotiation & impact notes for MENA victims

Initial demands vary widely; settlement behavior mirrors global patterns but is influenced by regulatory and disclosure regimes in Gulf states.

4.MALWARE-AS-A-SERVICE (MaaS)

Observed regional characteristics:
Stealer families and RATs (localized builds or Arabic-support variants) are actively marketed in region-focused channels and used to harvest credentials from Gulf consumer apps and enterprise VPN clients.

Subscription and one-time-purchase pricing models persist for MENA-targeting toolkits; customizations for Arabic-language social engineering are offered by some sellers.

5.VULNERABILITY TRADING

Regional priorities:
Mobile exploit buyers and surveillance-focused actors expressed interest in iOS/Android exploits due to high smartphone usage in Gulf countries; localized exploit code and weaponized PoCs for regional VPN appliances and routers surfaced in monitored exchanges.

Pricing for high-value zero-days targeting high-profile MENA targets follows global ranges but buyers specifically solicit telecom and critical-infrastructure vendor flaws.

6.DARKNET FORUMS, TELEGRAM & REGIONAL CHANNELS

Forum landscape (MENA):
Actors trade MENA-specific dumps in Arabic-enabled Telegram channels and invite-only forum threads; successors to legacy forums host regionally-relevant leak announcements.

Arabic-language tutorials and social-engineering guides facilitate localized phishing campaigns against Gulf institutions.

7.MONITORING & TAKEDOWN - MENA EFFORTS

Regional enforcement & vendor activity (2024–2025):
Regional public–private cooperation has increased: major vendors report more takedown coordination for MENA-targeted content, and national CERTs in Gulf states are engaging with international partners on specific high-profile takedowns.

Recommended mitigations for MENA organizations: continuous dark-web monitoring (brand + credential), targeted takedown requests via vendor partners, enforce strong MFA and conditional access for cloud/VPN, and pre-approved IR processes for extortion incidents.

10. Recommendations & Mitigations

10.Recommendations & Mitigations

Strategic defense measures based on the 2025 threat findings.
Based on the intelligence gathered regarding Agentic AI, Stealer Log proliferation, and Cloud Sprawl, organizations are advised to adopt the following mitigation strategies to preemptively neutralize these risks.

A. Closing the "Speed Gap" in Threat Response

The rise of Agentic AI allows attackers to automate network navigation and exploitation faster than human teams can react.

Recommendation:
Move beyond passive monitoring to Agentic Defense. Organizations should deploy AI-driven SOC capabilities that can autonomously triage Level 1 and Level 2 alerts.

Implementation Path:
Utilization of agentic SOC platforms allows for the automation of alert validation and false-positive reduction (up to 99%), freeing analysts to focus on the sophisticated "Shadow Agent" threats.

B. Immunizing Against Valid Credential Theft

With over **217,900+ compromised hosts** in the region providing valid credentials to dark web markets, traditional perimeter defenses are failing.

Recommendation:
Implement Context-Enriched Identity Detection. Security teams must correlate User Entity Behavior Analytics (UEBA) with threat intelligence to detect when a valid login is actually a stolen session.

Implementation Path:
Deploy detection engines that flag "impossible travel" or anomalous token usage patterns in real-time, a core capability of the Cognna platform, to neutralize the threat of stealer logs before data exfiltration occurs.

C. Ensuring Sovereign Data Resilience

The targeting of **"Sovereign AI"** and **Giga-projects** by global threat actors necessitates strict adherence to data residency laws.

Recommendation:
Adopt a **"Compliance-by-Design"** architecture. Security operations must be natively mapped to **NCA (Tier 2 MSOC) and SAMA** frameworks to ensure that sensitive national data is monitored and retained within the kingdom's borders.

Implementation Path:
Select security partners that are certified Tier 2 MSOC providers (like COGNNA) to ensure that all threat hunting and data retention practices automatically satisfy the rigorous audit requirements of Saudi regulators.

D. Unifying the Hybrid Attack Surface

The explosion of **Cloud Authorization Sprawl** and non-human identities **(82:1 ratio)** has created blind spots between on-premise IT and cloud environments.

Recommendation:
Establish **Unified Visibility.** Organizations must ingest and correlate logs from cloud-native sources (Kubernetes, APIs) alongside traditional on-premise logs to detect lateral movement across the hybrid environment.

Implementation Path:
Leverage multi-layered detection engines that bridge the IT/OT and Cloud gap, preventing the "Cloud Hopping" techniques currently being traded on dark web forums.

11. Threat Predictions For 2026

11.Threat Predictions For 2026

Rapid AI-enabled Attacks

The **MENA** region's fast adoption of **generative AI** and its integration into business processes is creating a larger, more dangerous cyber-attack surface. Adversaries are likely to exploit AI for predictive social engineering, highly personalized phishing campaigns, and automated reconnaissance.

Risk	Mitigation
Attackers using AI will scale their operations and evade traditional defenses	Organizations must build AI governance frameworks, enforce strict API access, and monitor for anomalous model behavior.

Convergence of IT and OT / Critical Infrastructure Risk

The region's large critical infrastructure, especially in energy, utilities, and transport, is increasingly digitized and converging IT and OT (operational technology).

Risk	Mitigation
As OT systems become more connected, threat actors could launch AI-driven cyberattacks that disrupt physical operations or cause cascading failure.	Strengthen segmentation, invest in OT-specific threat detection, and develop incident response playbooks that account for both IT and OT systems.

Ransomware & Extortion Amplified by Geopolitical Tension

Ransomware remains a high threat in MENA, with geopolitical conflict and third-party risk exacerbating the problem.

Risk	Mitigation
Attack groups may combine traditional ransomware with disruption to national-critical infrastructure, using extortion and geopolitical leverage.	Adopt a zero-trust approach, enforce just-in-time access, and ensure resilience (offline backups, crisis communications).

Supply-Chain Risk, Including Third-Party & AI Vendors

The MENA region is deeply engaged in global digital supply chains, third-party risk is a growing concern with weak zero-trust architecture in many organizations.

Risk	Mitigation
Attackers can compromise software dependencies (especially those involving AI or cloud-native components) and use them as stepping stones.	Attackers can compromise software dependencies (especially those involving AI or cloud-native components) and use them as stepping stones.

Identity & Access Threats

With digital transformation accelerating, the region is also seeing increased risk around identity and privileged access. Data shows a gap in robust identity access management (IAM) and zero-trust adoption.

Risk	Mitigation
Weak or over-privileged credentials can be exploited by both cybercriminals and state-backed actors.	Implement multi-factor authentication, just-in-time (JIT) access, and continuous monitoring for anomalous identity behavior.

Geopolitical / Hacktivist Risk Intensifies

The MENA region's geopolitical landscape is uniquely volatile. In April-May 2025 the MENA region saw a record 236% spike in DDoS attacks, driven by geopolitical tensions and hacktivism.

Risk	Mitigation
Nation-state actors, proxy groups, or hacktivists could launch cyber operations timed to political events, targeting governments, energy, or telecom sectors.	Encourage regional intelligence sharing, run red-team tabletop exercises, and establish cross-border cyber-resilience initiatives.

11. Conclusion

12.Conclusion

The 2026 MENA cyber landscape closes on a decisive inflection point: human-scale threats have been overtaken by machine-speed, Agentic AI–driven campaigns, and identity, not infrastructure, has become the true perimeter. The data throughout this report shows that while regional security spending is rising and expected to exceed $4.07 billion in 2026 (+10.1% YoY), adversaries are scaling faster, weaponizing autonomous agents, non-human identities, and OT-native techniques to systematically bypass traditional controls.

Strategic Closing Message

MENA defenders now operate in an environment where more than 80% of successful intrusions abuse valid identities and non-malware techniques, rendering legacy perimeter and signature-based controls increasingly obsolete. Financial extortion remains the most common outcome, but the strategic risk is shifting toward data poisoning of sovereign AI models, disruption of giga-project infrastructure, and long-horizon threats such as post-quantum “harvest now, decrypt later” campaigns. Organizations that continue to treat cybersecurity as a compliance project rather than an operational resilience function will find themselves consistently outpaced by adversaries automating every phase of the kill chain.

At the same time, the region’s unique geopolitical role and aggressive digital agendas (Vision 2030, sovereign clouds, national LLMs) mean MENA is now a primary theater for both state-aligned operations and high-end cybercrime. State actors are using the region as a proxy battleground for technology competition, while ransomware and extortion groups have shifted to pure data theft and multi-vector coercion, exploiting weak identity controls and over-privileged non-human accounts. Closing the “speed gap” with Agentic SOC capabilities, enforcing identity-centric zero trust, and building sovereign threat intelligence are no longer optional enhancements, they are prerequisites for defending national projects, financial stability, and public trust through 2026 and beyond.

About COGNNA

COGNNA is a Saudi-born, AI-led cybersecurity company purpose-built to close the “speed gap” between MENA defenders and increasingly autonomous, AI-driven adversaries. Founded in 2022, it delivers an Agentic SOC platform that combines autonomous AI agents with human expertise to turn noisy, high-volume telemetry into fast, explainable action, reducing alert fatigue, improving time-to-respond, and aligning security operations with regional regulatory frameworks such as NCA and SAMA.

Designed for enterprises and SMEs across finance, government, and critical infrastructure, COGNNA provides proactive, scalable, and cost-effective security operations as a service, including continuous asset discovery, threat hunting, incident response, and audit-ready compliance reporting. In 2025, COGNNA secured a $9.2 million Series A round led by Impact46 and co-led by BNVT Capital, with participation from Vision Ventures and Tali Ventures. The funding is being used to scale its Agentic SOC capabilities, expand across MENA and into global markets, and further invest in AI automation, engineering, and SOC operations; positioning COGNNA as a regional champion capable of competing on the global cybersecurity stage.

Learn More:
cognna.com

Follow Us:

Sign Up with COGNNA

References

- Gartner. (2025). Forecast: MENA End-User Spending on Information Security, 2026.
- CrowdStrike. (2025). Global Threat Report.
- Google Cloud Threat Intelligence. (2026). Cybersecurity Forecast 2026.
- PwC. (2025). AI and Quantum Readiness Reshaping Cyber Resilience in the Middle East.
- (1) SOCRadar. (2025). MEA Threat Landscape Report.
- (2) Mauritius CERT (CERT-MU). (2025). Cybersecurity Trends and Predictions.
- (3) Doha News. (2025). AI-Powered Phishing Surge in Qatar and the Middle East.
- (4) StormWall. (2025). Q2 2025 DDoS Attack Report: MENA.
- (5) Cyfirma. (2025). Rising Cyber Threats to Bahrain: Hacktivism and Data Breaches.
- (6) SOCRadar. (2025). Lebanon Threat Landscape Report.
- (7) 7News Morocco. (2025). Findings from Kaspersky KNext Event in Rabat.
- (8) National Cyber Security Centre Jordan. (2025). Cyber Security Situation Report: Q3 2025.
- Palo Alto Networks. (2024). Harvest Now, Decrypt Later (HNDL).
- SC Media. (2024). Deepfake Video Conference Fraud Case Study.
- Sumsub. (2025). Annual Fraud Report: Shift to Complex Multi-Step Schemes.
- Anthropic. (2024). Disrupting AI Espionage.
- Cybersecurity Ventures. (2025). Economic Impact of Software Supply Chain Attacks.
- Veracode. (2025). Software Supply Chain Attacks in 2025.
- SecurityBuzz. (2025). The Five Most Dangerous Cyber Threats Emerging.
- IBM. (2025). X-Force Threat Intelligence Report.
- CS4CA MENA. (2025). MENA Cyber Summit Annual Report.
- Cyberint. (2025). Intelligence & Brand Protection Report.
- Check Point Research. (2025). The State of Ransomware – Q3 2025.
- IBM Institute for Business Value. (2025). Threat Intelligence Index.
- Brandefense. (2025). Dark Web Breach Trends.
- CS4CA MENA. (2025). Annual Cybersecurity Report.
- Information Security Media Group (ISMG). (2025). AI Defense Blueprint from MENA Cyber
- Summit.