esentry

Threats knocked, We responded

esentry Q1 2025 report

Table of Content

CBO's Corner: When Threats Knock, We Don't Just Answer – We Act

Over the past few months, we've taken a step back, not to pause, but to evolve. What started under Cybervergent has now taken on a life of its own. **esentry** is officially standing solo — sharper in our focus, stronger in our purposeand more committed than ever to doing cybersecurity the way it should be done: with clarity, speed and care.

This new chapter isn't just about independence, it's about intention. Because the threats don't slow downand neither can we. Our mission is simple: Catch the threats before they become problems. Keep your business moving. Safeguard business sustainability, customer trust, and resilience.

This Q1 report marks the start of that renewed commitment. We're here. We're ready. And we're just getting started.

> **Threats knocked. We responded. And now, we're giving you the tools to respond too.**

Let's stay secure. Together.

Gbolabo Awelewa
CBO, esentry

Executive Summary

The cyber battlefield has fundamentally transformed. What we witnessed in Q1 2025 was not merely an uptick in attacks, but the emergence of a new adversarial paradigm, one that mirrors the sophistication and discipline of enterprise operations.

Threat actors have evolved beyond opportunistic exploits into coordinated entities with structured tooling pipelines and remarkable adaptability. They've shifted away from traditional phishing campaigns to leverage default credentials, living-off-the-land binariesand remote access tools, all carefully orchestrated to bypass conventional defenses and establish long-term network presence.

Our investigations exposed persistent service-based intrusions, encoded payloadsand targeted log evasion techniques, all signals of adversaries prioritizing stealth and sustained access over quick wins. These methodologies allow attackers to remain undetected for extended periods, expanding their foothold while evading traditional security measures.

Most concerning is the compression of response timelines: vulnerability exploitation now occurs within 48 to 72 hours of initial discovery. This acceleration leaves traditional security models dangerously exposed, particularly at the application layer where threats like zero-day remote code execution (RCE) exploits are actively leveraged before patching or detection measures are in place

The African market faces unique challenges as attackers craft region-specific tactics targeting mobile banking infrastructures, bypassing USSD implementationsand exploiting rapid cloud adoption without adequate security controls.

At **esentry**, we've responded with precision, implementing tailored security frameworks across financial, energy and telecommunications sectors. Our clients benefit from enhanced threat visibility, accelerated response capabilities and proactive defense engineering that anticipates rather than reacts.

The message is clear: yesterday's security posture cannot withstand today's threats. Organizations must elevate their defensive capabilities through improved identity management, enhanced monitoringand operational discipline, not as isolated initiatives but as an integrated security strategy.

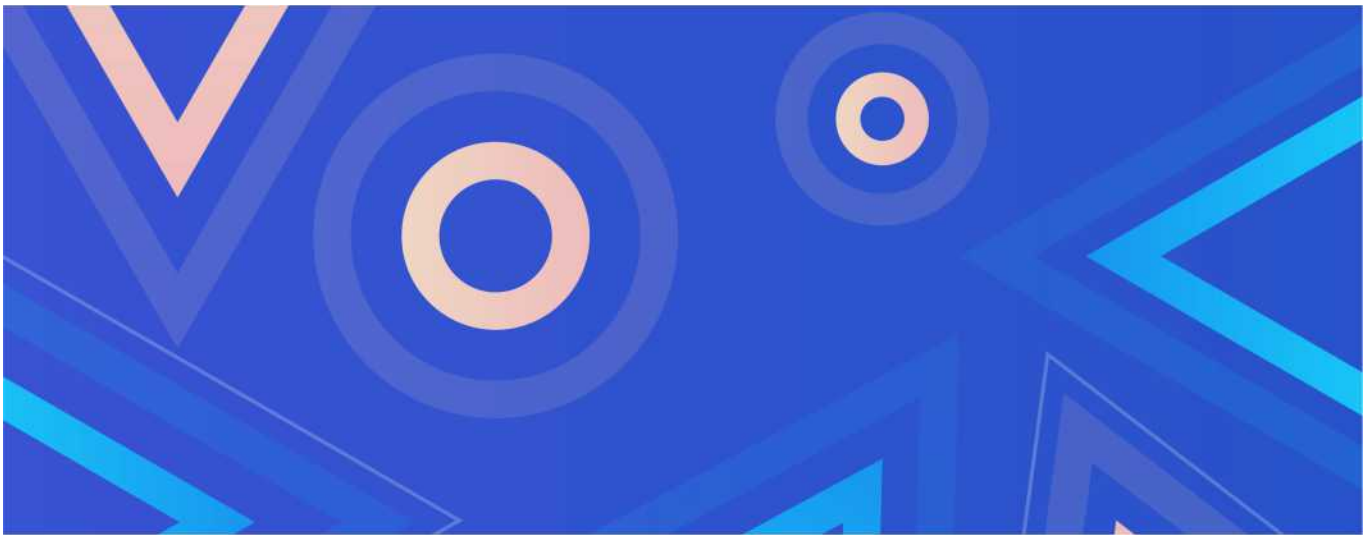
> **Adversaries have evolved their tactics, So must we.**

Facing the New Enterprise of Cyber Threats

In Q1 2025, the cyber threat landscape continued to evolve at an aggressive pace, marked by a significant rise in adversarial sophistication and coordination. Our investigations reveal that threat actors are no longer isolated entities relying on opportunistic exploits; instead, they now exhibit structured, enterprise-like behavior; complete with tooling pipelines, operational discipline and rapid adaptability.

For Q1 we highlight critical incidents involving the exploitation of default credentials, living-off-the-land binaries, and abused remote access tools all leveraged to bypass traditional defenses and persist within enterprise networks. Notably, techniques such as service-based persistence, encoded PowerShell payloads and log evasion were frequently observed, underscoring a strategic shift toward stealth and sustained access over smash-and-grab tactics.

We have further provided a technical deconstruction of notable tactics, techniques and procedures (TTPs) mapped to MITRE ATT&CK, supported by real-world artifacts, attack timelines and strategic recommendations to strengthen enterprise defenses.



revolutionising the African cybersecurity space.

www.esentry.io

Threats Came Knocking In Q1

Key Highlights Observed from Q1:

Widespread Credential Exposure Remains a Core Risk

Despite stronger enterprise identity controls, leaked credentials continue to undermine organizational defenses. Over 500 compromised user accounts were discovered on dark web marketplaces in Q1 alone. These credentials were frequently leveraged in initial access attempts, reinforcing that credential-based attacks remain a preferred and effective vector for both opportunistic and targeted threat actors.

Increased Abuse of Default and Misconfigured Accounts

Adversaries have shifted away from traditional phishing in favor of exploiting default system accounts. These accounts, often overlooked during deployment or misconfigured without proper restrictions, provided direct access to internal systems. This method bypasses user interaction entirely and significantly reduces detection likelihood during the initial compromise phase.

Continued Evolution of Stealer Malware Families

Threat actors do not always introduce novel malware but instead refine proven toolsets. Q1 saw a proliferation of upgraded variants of known malware, particularly Lumma Stealer featuring enhanced anti-analysis techniques, encrypted communications and improved stealth mechanisms. These adaptations reflect a focus on persistence, efficiency and evasive execution.

Expansion of Living-Off-the-Land Techniques

The use of native Windows binaries for malicious purposes continues to rise. Tools like rundll32.exe and mshta.exe, intended for legitimate administrative tasks, were abused to deploy payloads, establish persistence and execute commands while bypassing traditional security detections. This method complicates forensic research and places more pressure on behavioral analysis and telemetry correlation.

Persistent Activity from State-Aligned Advanced Threat Groups

Nation-state threat actors, particularly those associated with China, Russia and Iran, remained highly active throughout the quarter. Their operations demonstrated clear strategic intent favoring long-term access, credential harvesting and internal reconnaissance over disruptive attacks. These campaigns frequently exploited credential reuse and lateral movement through unmanaged assets.

Exploitation of Edge Device Vulnerabilities

A notable number of intrusions originated from the rapid exploitation of publicly disclosed vulnerabilities, especially those affecting internet-facing devices such as VPN gateways, firewalls and remote access appliances. In many cases, attackers acted within 48 to 72 hours of exploit release, leveraging misconfigured or outdated systems as entry points.

DDoS Activity Surges to Multi-Year High

Q1 experienced a 913% increase in Distributed Denial of Service (DDoS) attacks compared to the same period last year. These attacks ranged from volumetric disruptions to targeted smokescreens used to mask concurrent intrusions. The accessibility of DDoS-as-a-Service platform has further enabled less sophisticated actors to launch high-impact campaigns.

Methodology

Our Q1 analysis is built on a fusion of active threat hunting, incident response case studies, malware analysis, and proprietary research from client environments across critical sectors. The methodology employed reflects our operational philosophy: proactive defense, adversary disruption and business-aligned security outcomes.

Data Sources

Security Operations Telemetry:
Real-time logs, endpoint detections, behavioral anomalies and incident tickets collected across multiple client networks.

Threat Hunting Missions:
Proactive sweeps against MITRE ATT&CK techniques, targeting lateral movement, persistence, privilege escalation and initial access vectors.

Incident Response Analysis:
Deconstructed real-world intrusions blocked or contained by our detection systems, with forensic investigation revealing tactics, techniques and procedures (TTPs).

Global Threat Intelligence Feeds:
Correlation against curated intelligence on APT groups, criminal organizations, malware families and vulnerability exploitation trends.

Open-Source Intelligence (OSINT):
Monitoring of underground forums, leak sites and public vulnerability disclosures to identify early-stage threat actor operations.

Approach

Triage to Attribution:
All suspicious activity was triaged using a structured analysis pipeline; detection, validation, enrichment, behavioral correlation and, when possible, attribution to known or emerging threat clusters.

Adversary Emulation Labs:
Simulated attack sequences were developed based on observed adversary behavior to validate client defenses and test detection resilience against evolving threat models.

Human-Machine Collaboration:
Our security analysts leveraged machine learning-based anomaly detection augmented by manual review and expert threat actor profiling.

Business Impact Lens:
Beyond technical analysis, each incident was evaluated through a business risk lens, assessing operational disruption potential, data exposure likelihood and compliance ramifications.

This multi-pronged methodology ensures that our Q1 findings are not theoretical projections but grounded, evidence-backed insights into the adversarial landscape actively confronting our clients.

Top MITRE ATT&CK Technique Found in Q1 2025

The most prevalent ATT&CK techniques identified in Q1

Figure 1:
Shows the most prevalent ATT&CK techniques identified in Q1

TECHNIQUE ID	TECHNIQUE	CATEGORY
T1078	Valid Accounts	Initial Access
T1059	Command and Scripting Interpreter	Execution
T1053	Scheduled Task/Job	Execution
T1087	Account Discovery	Discovery
T1047	Windows Management Instrumentation	Execution
T1562	Impair Defenses	Defense Evasion
T1218	System Binary Proxy Execution	Defense Evasion
T1036	Masquerading	Defense Evasion
T1543	Create or Modify System Process	Persistence
T1112	Modify Registry	Defense Evasion

Technique Spotlight

Valid Accounts: Default Account Misuse

In Q1, an enterprise environment was affected by a coordinated activity involving the unauthorized use of default system accounts; a threat vector often deprioritized in security hardening cycles. These accounts, typically provisioned during initial setup phases, were leveraged by adversaries to establish authenticated access without triggering intrusion detection thresholds.

The campaign exploited institutional gaps in identity lifecycle management, exposing a broader issue: inadequate credential hygiene in legacy or mismanaged assets.

Incident Summary: Silent Authentication Abuse

The campaign began with the use of **unchanged local administrator and DefaultAccount credentials,** which remained active on several Windows endpoints. These credentials provided immediate interactive or remote access **(via RDP)** and enabled adversaries to bypass perimeter protections that rely on anomalous authentication or brute-force detection.

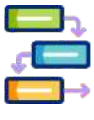
Post-authentication, threat actors established persistent services under **LocalSystem** context. Tools such as **RustDesk, SupremoRemoteDesktop and CloudRaService** were installed via Service Control Manager (Event ID 7045), granting long-term access with administrative privileges. The service names were obfuscated to resemble system-critical processes, a method that allowed them to evade routine service audits.

Data staging and reconnaissance were performed through **self-deleting batch files**, executing network enumeration (ipconfig, netstat, query user) and redirecting output to hidden shares (admin$). These scripts were dropped into %SYSTEMROOT% and %TEMP% directories and executed with minimal forensic traces.

Key Observables

Persistence via Services:

- Custom binaries such as RustDesk.exe and CloudRaService.exe are installed as services using nssm.exe.
- Service names mimicked system processes (e.g., svchostsv.exe).



Execution Flow:

- PowerShell invoked via %COMSPEC% (cmd.exe) with flags: -nop -w hidden -noni.
- Scripts encoded in base64 and XOR-obfuscated to bypass static signatures.

Lateral Discovery:

- Reconnaissance output redirected to \\hostname\C$__output.
- Service-based propagation across peer systems observed via repeated 7045 logs.

Evasion Techniques:

- PowerShell logging disabled (ScriptBlock Logging, ModuleLogging) prior to payload execution.
- Audit logs for local admin authentication and service installs were cleared post-operation.

MITRE ATT&CK Mapping

Tactic	Technique & Sub-Technique	ID	Observed Procedures & Tooling
Initial Access	Valid Accounts: Default & Admin	T1078.001	Adversaries abused the pre-installed DefaultAccount and local Administrator, using unchanged credentials.
	Remote Services: RDP	T1021.001	RDP sessions initiated by DefaultAccount; used for enumeration and access.
Execution	Command & Scripting: PowerShell via %COMSPEC%	T1059.001	PowerShell launched with flags: -nop -w hidden -noni from within cmd bat wrappers.
	Windows Command Shell	T1059.003	Self-deleting .bat files executed system recon commands (ipconfig, netstat, etc.) via obfuscated paths.
Persistence	Create or Modify System Process: Windows Service	T1543.003	Services like CloudRaService.exe, RustDesk.exe installed via Event ID 7045, persisted via auto-start.
	Install Util: NSSM for Service Wrapper	T1547.001	nssm.exe used to wrap custom payloads and deploy them as persistent Windows services.
Privilege Escalation	Token Manipulation: LocalSystem Execution	T1134.001	All suspicious services ran as LocalSystem, granting SYSTEM-level privileges.
Defense Evasion	Obfuscated Files/Scripts: PowerShell Compression & XOR	T1027.009	Complex PowerShell scripts were double-encoded, XOR-encrypted and embedded into services.
	Indicator Removal: Log Clearance	T1070.001	Admin logs wiped (Event ID for Microsoft-Windows-VerifyHardwareSecurity)
Discovery	Account Discovery	T1087.001	query user, whoami and group enumeration used via batch scripts.
	Network Configuration Discovery	T1016	netstat -a, ipconfig /all and DNS pings logged from bat files.
Lateral Movement	Admin Shares (C$, Temp)	T1021.002	Recon outputs piped to \\%COMPUTERNAME%\ C$__output, avoiding network transfers.
	Service Install Across Hosts	T1021.004	Repeated 7045 events across endpoints suggest pivoting via malicious service deployment.
Collection	Data Staging via Batch Output	T1074.001	Bat files stored output in %SYSTEMROOT%, redirected to admin shares (C$).
Exfiltration	Custom C2 via Encrypted Channels	T1041	enq.exe attempted to contact internal IP likely for staging or lateral movement.
Impact	Application Access – Web.config Targeting	T1499.001	extract sensitive app data via batch file.

Africa's Emerging Cyber Threats: A Penetration Tester's Perspective

www.esemtry.io

Africa's Emerging Cyber Threats: A Penetration Tester's Perspective

In the first quarter of the year, our offensive team carried out comprehensive penetration testing engagements across financial services, fintechs, energy and government sectors within Africa. These assessments aimed to evaluate the resilience of enterprise systems against evolving threat actors and techniques.

Through these engagements, a troubling pattern has emerged: attackers are increasingly leveraging **region-specific tactics** tailored to the unique operational environments of African organizations. These tactics are not only bypassing conventional security controls but also exposing critical gaps in detection, response and infrastructure hardening.

Unlike globally recognized threat patterns, these attack techniques are tailored to local technology infrastructure, social behaviors and economic systems. Most significantly, these approaches aren't from threat feeds or global advisories but from hands-on offensive security assessments conducted across financial, telecom, food and hospitality and logistics sectors. These tactics often remain undetected using common detection systems and are underrepresented in global cybersecurity news.

What makes them especially dangerous is their adaptability and design, taking advantage of local weaknesses in regulations, user behavior and rapid digitization.

Let's look at how emerging threats are being actively weaponized in African environments.

Mobile-First Financial Exploitation

Africa's mobile banking boom, driven by high mobile penetration and low banking access, has inadvertently opened unique threat vectors:

USSD Session Hijacking:

In telecom-focused pentests, we discovered that over 78% of USSD banking implementations failed to validate sessions adequately. Attackers can inject commands or replay USSD requests to perform unauthorized transactions.

Fake Loan App Ecosystems:

Malicious actors are cloning legitimate fintech apps with near-perfect branding and functionality. These fake apps often include bogus support channels, request biometric data and mobile money PINs and mimic local loan schemes. Victims rarely suspect fraud until funds disappear or devices are compromised.

Security Gap: Financial institutions tend to over-index on SMS phishing, while USSD and APK integrity remain grossly under-protected.

Ransomware's African Evolution

Unlike global ransomware groups, which operate via indiscriminate campaigns, African ransomware operators have localized their strategies:

Ransomware Delivery via Exposed APIs and Insecure CI/CD

In several Q1 pentests, exposed DevOps endpoints, unauthenticated API routes and misconfigured CI/CD pipelines were found. These could be leveraged to **drop ransomware payloads into internal environments**, especially in cases where internal scanning or access control was weak.

Supply Chain Ransomware in Logistics & Food Services

Many African businesses rely on third-party delivery systems, POS integrations and mobile payment APIs. If any of these vendors are compromised, ransomware could be **injected upstream**.

Testing Data: Over 75% of the assessed systems had not implemented internal network segmentation, allowing ransomware to spread laterally unchecked.

Exploitation of Misconfigured Cloud Storage and API Leaks

As more African startups and businesses adopt cloud technologies, rapid cloud adoption has outpaced secure implementation:

Firebase and S3 Exposure Abuse

Misconfigured cloud storage services exposed API keys, user tokens and backend data. These are easily discoverable and exploitable using public tools.

API Enumeration via Mobile Apps

Reverse-engineered mobile apps revealed hardcoded endpoints, secrets and tokens, enabling attackers to perform IDOR attacks and data scraping.

Security Gap: A lack of access controls, API rate limiting and secure coding practices leaves backend services dangerously exposed.

Abusing Token Reuse and Weak Session Management

Our testing revealed that many apps continue to mishandle session management:

Token Persistence Post-Logout

In many apps, tokens remained valid even after user logout, allowing attackers to reuse captured tokens for unauthorized access.

Session Fixation Attacks

Predictable or unrotated session tokens allowed impersonation, especially in admin panels or privileged roles.

Testing Data: Over 75% of the assessed systems had not implemented internal network segmentation, allowing ransomware to spread laterally unchecked.

Insecure Default Cryptography in Locally Developed Apps

Local development teams often use outdated or insecure cryptographic practices due to inadequate setup time and budget constraints:

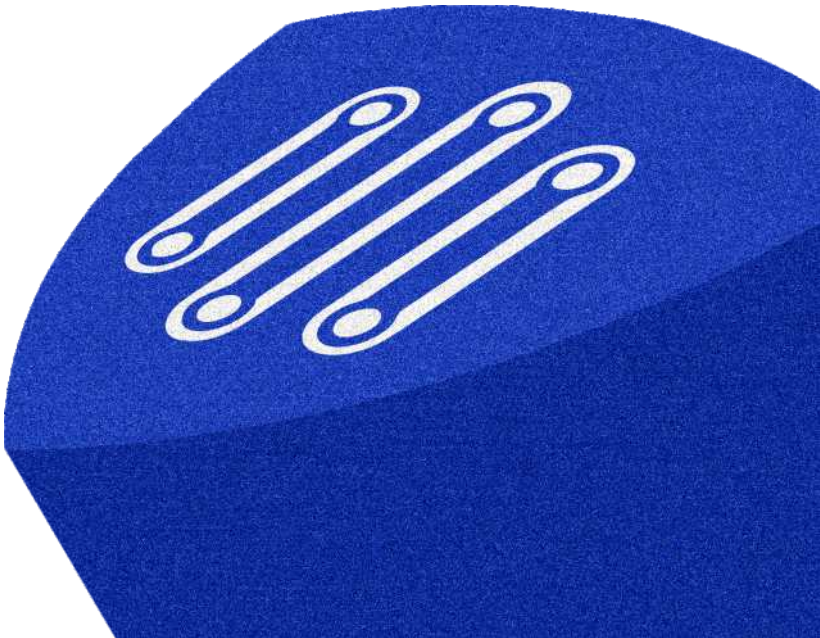
Use of AES-CBC with PKCS5/7 Padding

A vulnerable encryption mode is still widely used without integrity checks, exposing apps to padding oracle attacks.

Hardcoded Keys and Ivs

Several apps had static keys embedded in the code, allowing attackers to decrypt traffic or stored data effortlessly.

Impact: These flaws can completely undermine any encryption-dependent security promises within the app.



Connecting the Dots: Observations from Q1

Across the different enterprise pentests we conducted in Q1, several recurring vulnerabilities were identified:

- Hardcoded credentials in mobile APKs and config files.
- Improper session management and token reuse post-logout.
- Improper session management and token reuse post-logout.
- Insecure Firebase and S3 bucket exposures, often leaking user data.
- Outdated cryptographic implementations, including AES-CBC with PKCS5 padding.

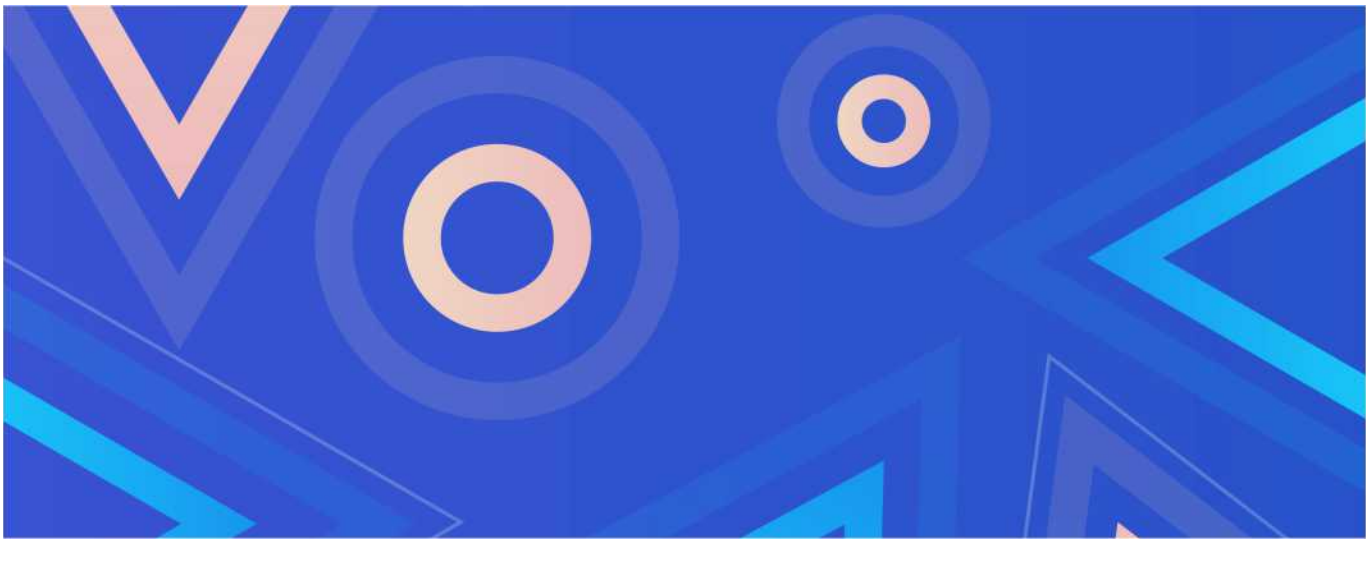
These were not isolated to one industry; Fintechs, e-commerce platforms, logistics apps and health-tech solutions showed similar oversights, indicating a systemic gap between app delivery speed and secure development practices.

Importantly, in several cases, our red team simulated full kill chains, from initial phishing to lateral movement and data exfiltration, using only publicly available infrastructure. These were not zero-day attacks, they were failures in basic system configurations and inadequate threat awareness.

Why This Matters Now

The attacks documented here are not future risks; they are active campaigns being executed today across African networks. Yet, they are often overlooked by global research and poorly addressed by traditional tools.

As a security-focused organization, our responsibility extends beyond testing, it includes reporting what's real, urgent and regionally specific. By highlighting these trends through continuous field work, we aim to drive security programs that are proactive, contextual and resilient.



Shield Matrix: A Cyber Defense Directive

www.esentry.io

Shield Matrix: A Cyber Defense Directive

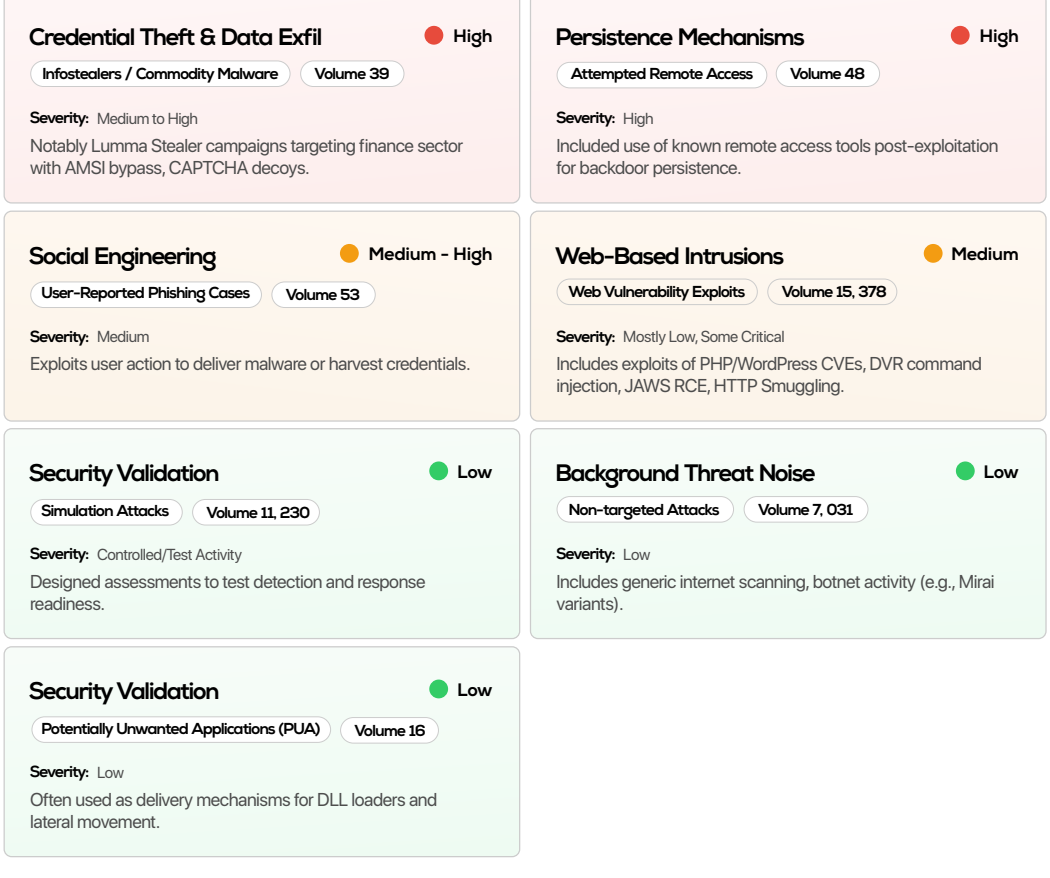
The first quarter of 2025 witnessed an unprecedented evolution in the cyber threat landscape, with sophisticated actors demonstrating enhanced capabilities against critical infrastructure sectors. Our 24/7 monitoring operations detected and responded to a diverse array of threats targeting telecommunications networks and enterprise IT infrastructures across our protected environments.

Our findings feature:

- A severity-weighted breakdown of incidents categorized by impact potential.
- Detailed examination of emerging adversary techniques and tradecraft.
- Contextual analysis of threat actor motivations and strategic objectives.
- Recommendations for enhanced defensive postures based on observed patterns

As threat actors continue to refine their methodologies, our continuous monitoring and rapid response capabilities have proven essential in maintaining the integrity and availability of critical systems. The technical assessment that follows outlines specific vulnerabilities exploited, detection metrics and mitigation strategies implemented throughout this dynamic quarter.

Figure 2:
Card view of the incident landscape across monitored tools.



Incident Landscape Dashboard

Comprehensive overview of security incidents for Q1 2025

Total Incidents	Threat Vectors	High Risk Incidents
33,745	7	87
Across all threat vectors	Distinct attack categories	High Priority 2 critical incidents

Figure 3:
Q1 2025 distribution of incidents

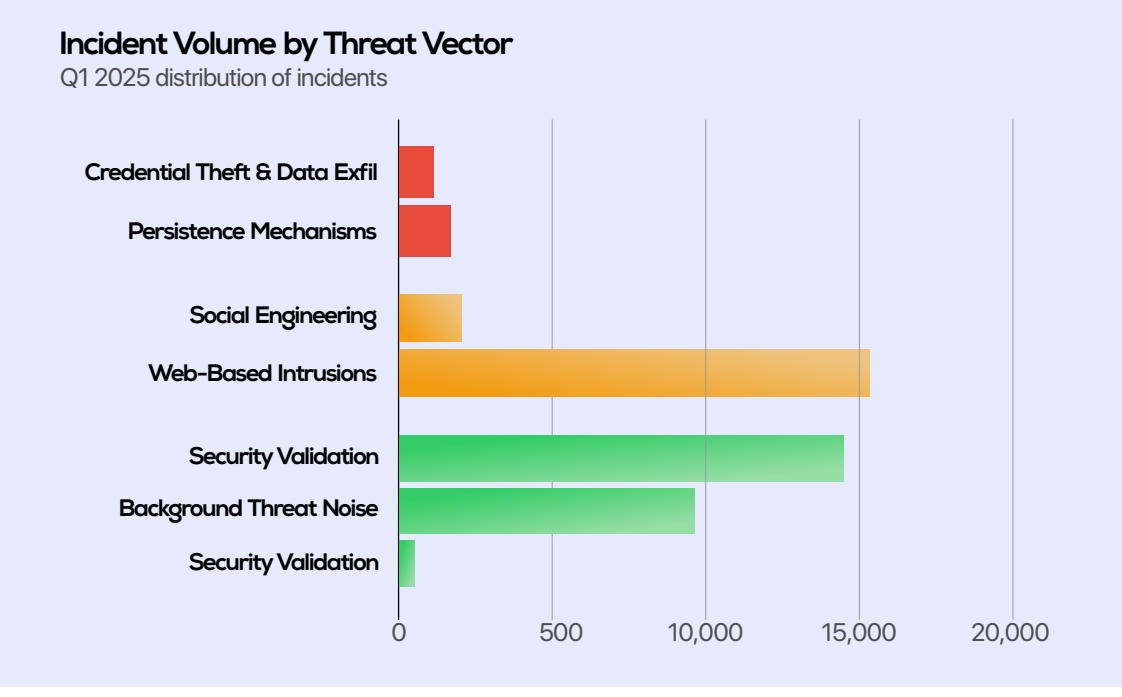
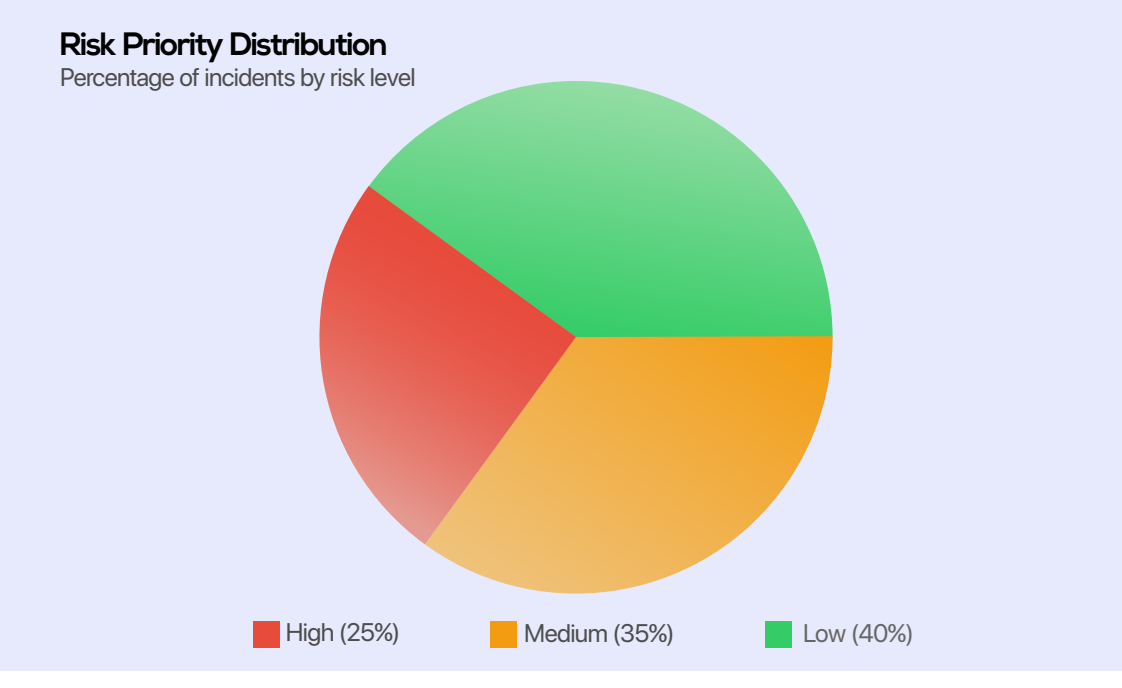


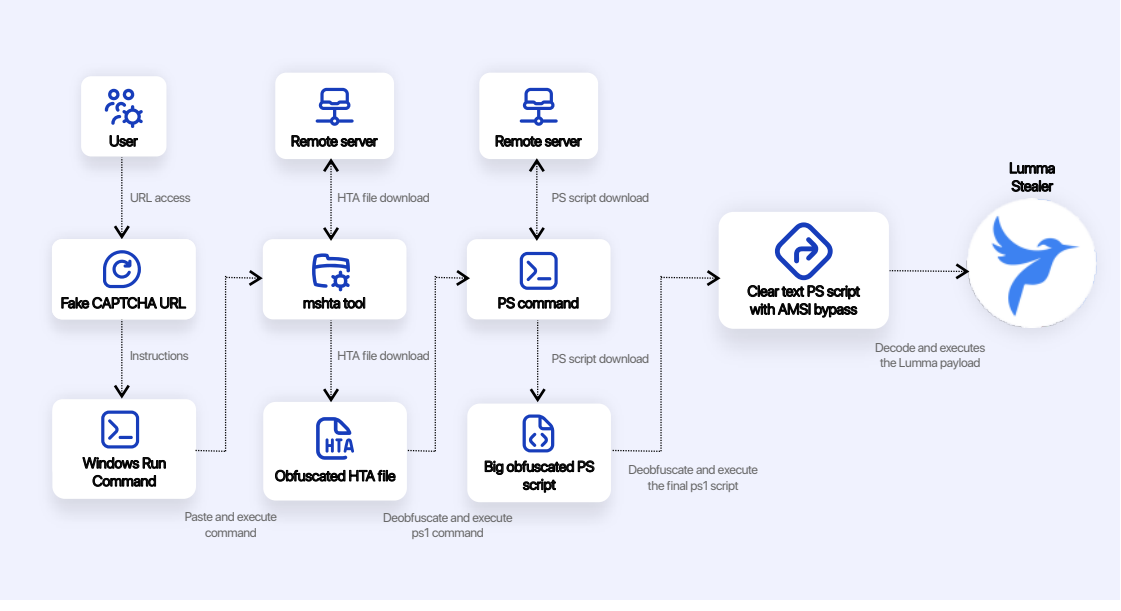
Figure 4:
A pie chart of the percentage of incidents by risk levels



Threat Campaign Spotlight: Lumma Stealer Infection Chain New Tactics

In Q1 2025, **Lumma Stealer** emerged prominently in targeted finance-sector intrusions. Malvertising techniques redirected users to attacker-controlled CAPTCHA decoy pages that initiated clipboard-based infection chains, evading traditional detection tools.

Figure 5:
An image of the flow of an Infection chain



Observed MITRE Techniques:

Figure 6:
The Observed MITRE techniques from the infection chain.

ID	TECHNIQUE	Details
T1189	Drive-by Compromise	Redirects from compromised websites to malicious CAPTCHA landing pages.
T1059	User Interaction	Clipboard abuse delivering mshta.exe commands instructing manual Run execution.
T1218.005	Living-off-the-Land Execution	mshta.exe fetched remote .hta scripts containing obfuscated loaders.
T1562.001	Defense Evasion	AMSI bypass via memory patching within HTA payloads.
T1041	Data Exfiltration	In-memory credential harvesting and HTTPS-based transmission to C2 servers.

Technical Observations

- Clipboard scripting via navigator.clipboard.writeText
- Abuse of mshta.exe as LOLBIN to evade disk-based detection
- In-memory payload delivery, bypassing EDR artifact scanning
- Targeting of autofill data, browser sessions, and cryptowallets

Exploitation Trends: Web Vulnerabilities

Across various monitored telemetry layers, a high volume of exploit attempts was identified many targeting outdated or poorly secured systems in **PHP and WordPress** environments mostly. The most notable critical attempts include:

- **JAWS Webserver RCE** (Unauthenticated Shell Execution)
- **Apache HTTP Smuggling** (CVE-2023-25690)
- **MVPower DVR Shell Exploit**
- **TBK DVR Command Injection** (CVE-2024-3721)
- **PHP CGI Argument Injection** (CVE-2024-4577)
- **WordPress Plugin Exploits** (e.g., WP Automatic <3.92.1 RCE, CVE-2024-2142)

These exploit chains typically used POST-based payload delivery mechanisms and focused on unauthenticated execution paths, with some attempts originating from compromised IoT devices and recycled botnet infrastructure (Mirai variants).

Technical Advisory

- Expand detection around clipboard access and mshta.exe usage patterns.
- Monitor LOLBins that execute out-of-browser scripts to bypass traditional web security layers.
- Disable or restrict scripting languages from executing externally fetched HTA payloads.
- Employ behavioural and signature-based protections for AMSI evasion techniques.
- Harden PHP/WordPress deployments with timely CVE patching and plugin minimization.

Emerging Risk from PUAs

Though statistically lower in volume, **Potentially Unwanted Applications (PUAs)** remain notable due to their **dual-use functionality.**

In Q1, we observed multiple PUA instances used to:

- Load malicious DLLs during startup
- Establish persistence using scheduled tasks or registry run keys
- Deploy proxy tools under the guise of legitimate software installers

Continued diligence in classifying borderline binaries and applying application whitelisting is advised.

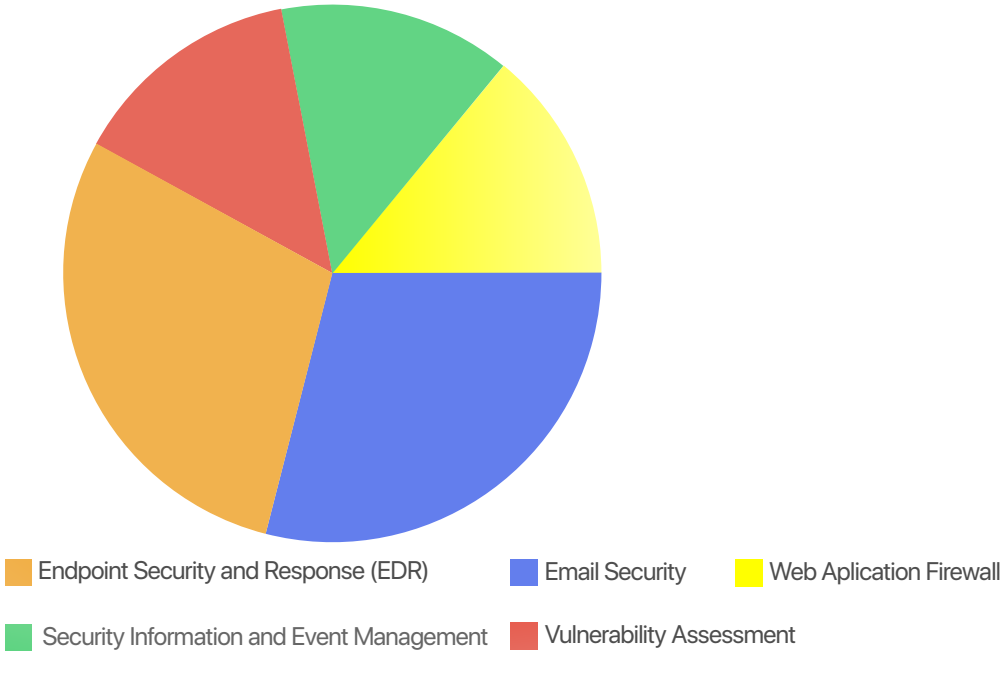
Security Engineering

Security Engineering

In Q1 2025, **our security engineering team** successfully implemented seven security solutions across multiple financial sector clients. These deployments addressed critical cybersecurity challenges ranging from regulatory compliance requirements to emerging threat vectors.

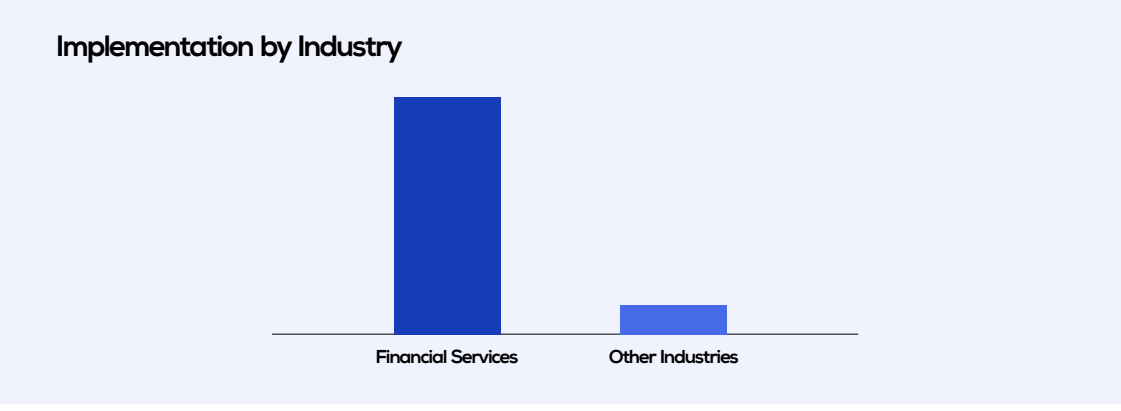
Solution Deployment Analysis

During Q1, we focused on delivering targeted security solutions to address specific client vulnerabilities and compliance requirements. Our implementations were driven by increasing regulatory pressures, sophisticated phishing campaigns, web application threats and advanced malware concerns.



Industry Sector Focus

All Q1 implementations were conducted for clients in the financial sector, reflecting the heightened security requirements and regulatory scrutiny this industry faces. Financial institutions continue to be prime targets for cybercriminals due to the sensitive nature of their data and the potential for financial gain.



Client Challenge Analysis

Regulatory Compliance Requirements

Regulatory bodies continue to update their guidelines, compelling organizations to maintain vigilant and proactive cybersecurity postures. One prominent example involved a client seeking PCI DSS certification, which required comprehensive network monitoring and event aggregation capabilities.

Case Study: Enabling Compliance Through Proactive Monitoring

While preparing for its PCI DSS certification, an institution reached out to the team with a critical need. To satisfy certification requirements, the organization needed a solution that would continuously monitor its network and aggregate security events across its infrastructure providing real-time visibility and operational insights.

After a thorough assessment, the team deployed a combination of Endpoint Detection & Response (EDR) and Security Information and Event Management (SIEM) solutions. EDR provided detailed threat detection and response capabilities at the endpoint level, while the SIEM platform enabled centralized log aggregation, correlation and alerting across the environment.

The deployment was completed within 7 to 14 days, aligning with the organization's audit timeline. Following implementation, the company successfully passed its PCI DSS certification audit and is now projected to see a 75% reduction in compliance-related incidents driven by improved visibility, faster incident response and more informed risk management.

Phishing and Social Engineering Threats

As social engineering tactics continue to evolve, phishing has become one of the most persistent and damaging threats facing modern organizations. Traditional security controls are increasingly ineffective against the more sophisticated techniques being used to exploit human behavior, often bypassing firewalls and antivirus tools without detection.

Case Study: Strengthening Email Security Against Phishing Threats

A financial institution approached the team with concerns about a noticeable spike in phishing emails targeting employees. These emails were not only frequent but also highly convincing, creating a significant risk of credential theft, malware infection and reputational damage.

To address the challenge, we implemented an advanced email security solution equipped with inbound email scanning, real-time link protection and sandboxing for suspicious attachments. This multilayered approach was designed to detect and block malicious emails before they could reach users' inboxes.

The full deployment was completed in **7 days,** with immediate impact. Post-implementation monitoring revealed a **complete elimination of spam and phishing emails reaching end users,** significantly reducing the organization's exposure to email-based threats and enhancing its overall cyber resilience.

Web Application Vulnerabilities

One of the most pressing challenges reported by organizations in Q1 was the rise in targeted attacks on web applications. These threats often came in the form of **unauthorized scanning activities, SQL injection attempts, and exploitation of application-level vulnerabilities** all of which posed a serious risk to operational continuity and data integrity.

Case Study: Web Application Protection

A growing e-commerce platform engaged the team after experiencing repeated web-based intrusion attempts that threatened the availability and security of their services. The attacks were not only persistent but increasingly automated, making them difficult to detect and block using basic perimeter defenses.

To counter this, we deployed a Web Application Firewall (WAF) designed to provide real-time inspection and filtering of incoming traffic to the organization's web applications. The WAF was configured to block malicious payloads, restrict unauthorized access attempts and log suspicious activity for ongoing analysis.

The entire deployment was completed in **5 days,** after which the organization experienced a **significant reduction in successful attack attempts.** The WAF now acts as a first line of defense, ensuring that web-facing resources are protected from both known and emerging threats—allowing the business to operate securely and without disruption.

Advanced Malware and Ransomware

The rise in sophisticated malware campaigns, particularly ransomware, has added a new layer of complexity to the cybersecurity challenges faced by modern organizations. Cybercriminals are deploying advanced malware variants capable of crippling operations, encrypting critical systems and triggering significant financial and reputational losses. These threats are often accompanied by the risk of data breaches, pushing businesses to urgently seek comprehensive protection for their digital assets.

This urgency was clear when a **client with critical infrastructure assets** reached out to the **team** following a close call involving a suspected compromise. The organization needed a solution that could offer robust protection for all critical assets and quickly detect and contain future threats.

In response, we deployed a **cutting-edge Endpoint Detection and Response (EDR)** solution, designed to provide multi-layered protection using **static analysis, artificial intelligence and behavioral analytics**. The deployment was completed in **7 days**, ensuring minimal disruption to the client's operations.

Post-deployment, the EDR solution began delivering results almost immediately blocking **threats in real-time**, reducing the client's **meantime to detect and respond to malware** and successfully **preventing ransomware encryption attempts**. With increased visibility across endpoints and improved threat detection accuracy, the client significantly enhanced its security posture and regained confidence in the resilience of its critical systems.

Threat Vector Analysis

Figure 9:
A pie chart of the percentage of incidents by risk levels

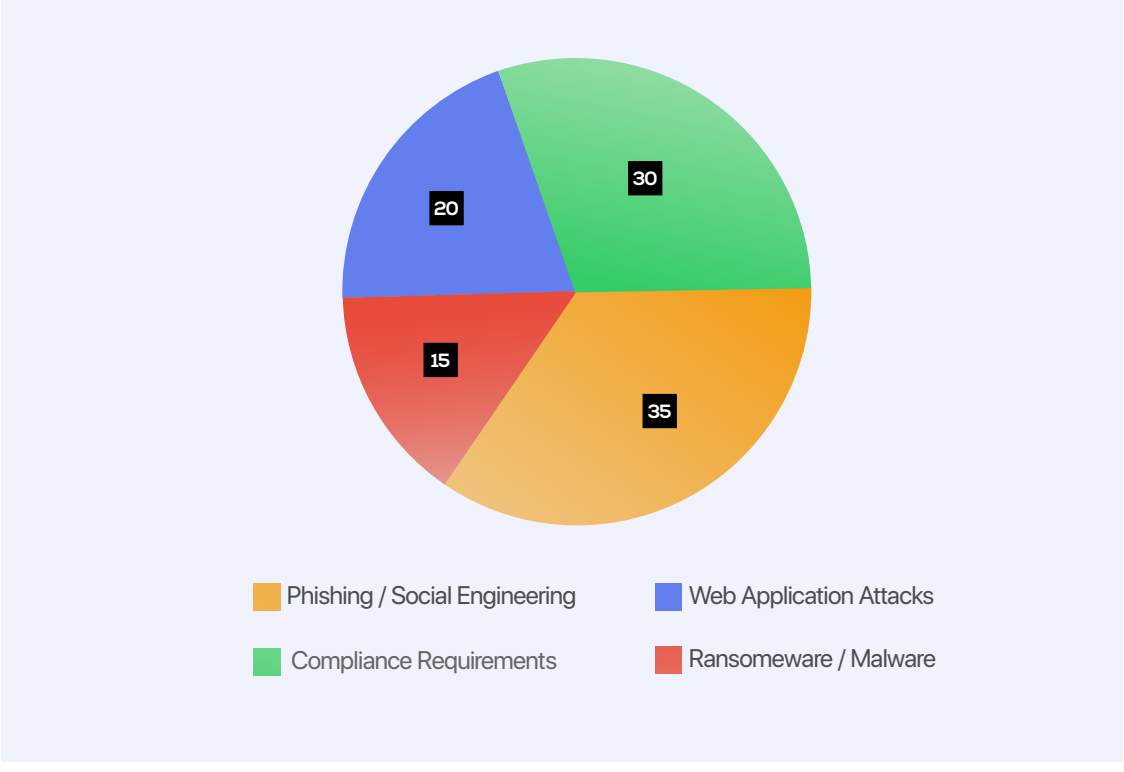
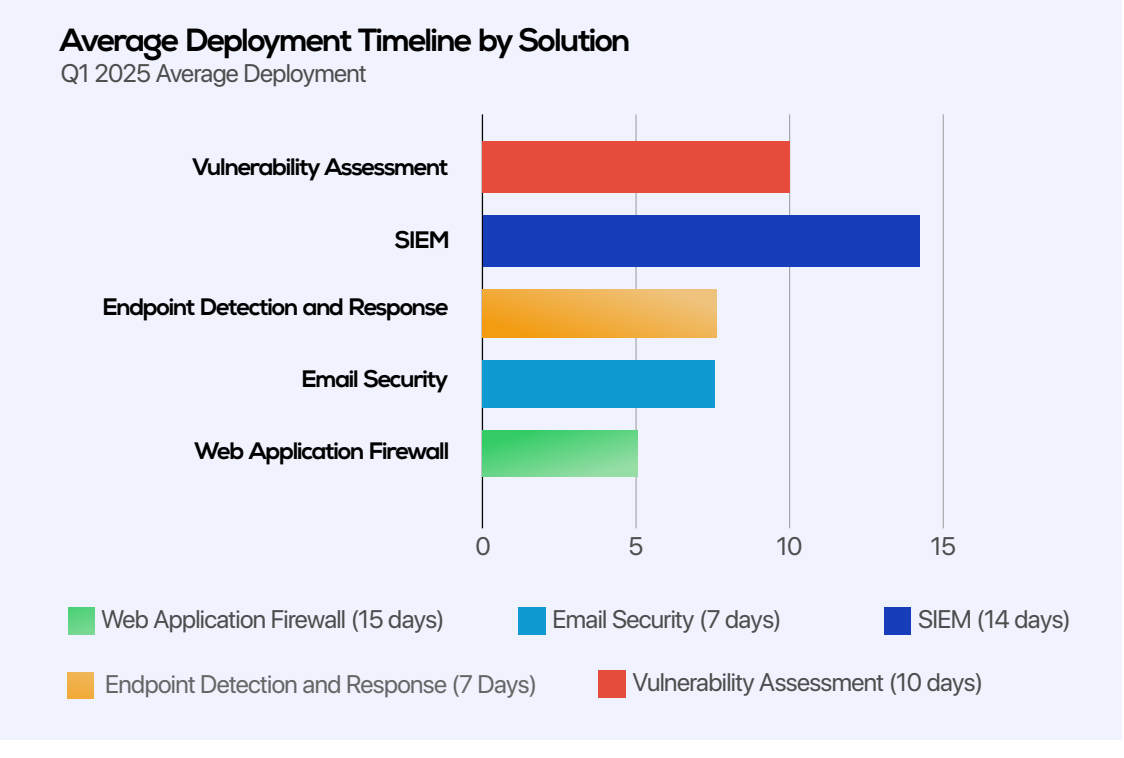


Figure 10:
Q1 2025 distribution of incidents



Cybersecurity Outlook for 2025

www.esentry.io

Cybersecurity Outlook for 2025

As we analyze the findings from Q1, a concerning picture emerges for the cybersecurity landscape in the coming quarter. Organizations should brace for an intensification of the sophisticated threat actor behaviors observed in Q1, with adversaries continuing to operate with enterprise-like structures complete with advanced tooling pipelines, operational discipline and unprecedented adaptability.

The traditional attack vector of phishing appears to be giving way to more insidious methods, as threat actors increasingly bypass social engineering in favor of directly exploiting default credentials, misconfigured accounts, and leaked credentials sourced from dark web marketplaces. Over 500 compromised user accounts discovered on these underground forums in Q1 alone signals that credential-based attacks will remain a preferred and highly effective vector in Q2.

Rather than developing entirely new malware families, attackers are likely to continue refining proven toolsets like Lumma Stealer, enhancing them with improved anti-analysis techniques, encrypted communications and more sophisticated stealth mechanisms. This evolution reflects a strategic shift toward persistence and evasion rather than rapid smash-and-grab operations.

The abuse of legitimate system tools will almost certainly increase, with native Windows binaries such as `rundll32.exe` and `mshta.exe` being weaponized for malicious purposes. This "Living-Off-the-Land" approach complicates detection efforts by blending malicious activity with legitimate administrative tasks, placing greater pressure on behavioral analysis and telemetry correlation.

Edge devices remain particularly vulnerable, with the exploitation window for newly disclosed vulnerabilities continuing to shrink. Organizations should expect attacks targeting VPN gateways, firewalls and remote access appliances within just 48-72 hours of exploit disclosure. The dramatic 913% increase in DDoS attacks observed in Q1 will likely persist as both primary disruption mechanisms and smokescreens for concurrent intrusion attempts.

Service-based persistence mechanisms will become more prevalent, with threat actors deploying remote access tools like RustDesk and SupremoRemoteDesktop as Windows services with obfuscated names to maintain long-term network presence. These services, often mimicking critical system processes, will allow attackers to evade routine service audits while maintaining administrative access.

Regional variations in attack methodologies will continue to develop, particularly in rapidly digitizing economies. In Africa, mobile-first financial exploitation targeting USSD banking implementations and deployment of clone fintech applications will remain significant threats. Cloud misconfigurations, particularly involving Firebase and S3 exposures, will be increasingly targeted as organizations rush cloud adoption without adequate security protocols.

Nation-state threat actors, particularly those associated with China, Russia and Iran, will maintain their strategic operations focused on long-term access, credential harvesting and internal reconnaissance rather than immediately disruptive attacks. Their campaigns will continue exploiting credential reuse and lateral movement through unmanaged assets.

On the technical front, clipboard-based infection chains using CAPTCHA decoys and clipboard abuse will grow more common as methods to deliver malicious payloads while evading traditional detection mechanisms. Web vulnerabilities, especially in PHP/WordPress environments, JAWS Webserver, Apache HTTP Smuggling and DVR command injection, will remain prime targets. Default account abuse will increase as attackers exploit gaps in identity lifecycle management to gain authenticated access without triggering intrusion detection systems.

In response to these evolving threats, organizations will likely prioritize several key security solutions in Q2. Email security implementations featuring advanced filtering and anti-phishing capabilities will see increased adoption. Endpoint Detection and Response (EDR) solutions will be in high demand, particularly for businesses operating in remote or hybrid environments requiring enhanced visibility into endpoint activities. Web Application Firewalls with specific capabilities for API protection will grow in importance as API-driven applications expand the attack surface. Finally, more comprehensive Security Information and Event Management (SIEM) solutions will be sought after to meet regulatory compliance requirements and improve threat visibility across complex infrastructures.

For organizations to effectively navigate this challenging landscape, they must implement proper security controls, improve identity management practices, enhance monitoring capabilities and accelerate vulnerability remediation cycles. The most successful security programs will focus not only on technical defenses but also on operational discipline, ensuring that basic security hygiene measures are consistently applied across their entire digital ecosystem.

Q1 2025 Cybersecurity Threat Highlights

500+

Compromised user accounts discovered on dark web forums, signaling increased credential-based attacks.

900%+

Increase in DDoS attacks, used both for disruption and to mask intrusions.

48–72 Hours

Timeframe in which edge device exploits (VPNs, firewalls) are launched post-vulnerability disclosure.

Top Malware

Refinements observed in known tools like Lumma Stealer, emphasizing stealth and persistence.

Living-Off-the-Land

Malicious use of native binaries (e.g., `rundll32.exe`, `mshta.exe`) to evade detection continues to rise.

Remote Access Abuse

Tools like **RustDesk** and **Supremo RemoteDesktop** deployed as hidden Windows services.

Regional Threats

In Africa, USSD banking fraud and clone fintech apps dominate threat landscape.

Cloud Risks

Misconfigured **Firebase and Amazon S3** buckets increasingly exploited during rapid cloud adoption.

Nation-State Focus

Actors from China, Russia and Iran prioritize long-term access and credential harvesting over disruption.

New Infection Vectors

Clipboard-based chains using **CAPTCHA decoys, and PHP/WordPress, JAWS Webserver and Apache HTTP** smuggling remain high-risk.

Contact Us

services@esentry.io

www.esentry.io

212/214 Herbert Macaulay Way,
Yaba, Lagos, Nigeria

About esentry

esentry delivers customized cybersecurity services based on the unique needs of each customer segment. Our portfolio encompasses end-to-end cybersecurity services and products, catering to diverse business scales worldwide. With a deep understanding of all facets of cyber protection, we deliver tailor-made solutions that meet each organisation's s pecific requirements.

An **esentry** Q1 Report 2025