2025

MALAYSIA THREAT REPORT

SIMPLYDATA

TOTAL LOGS COLLECTED

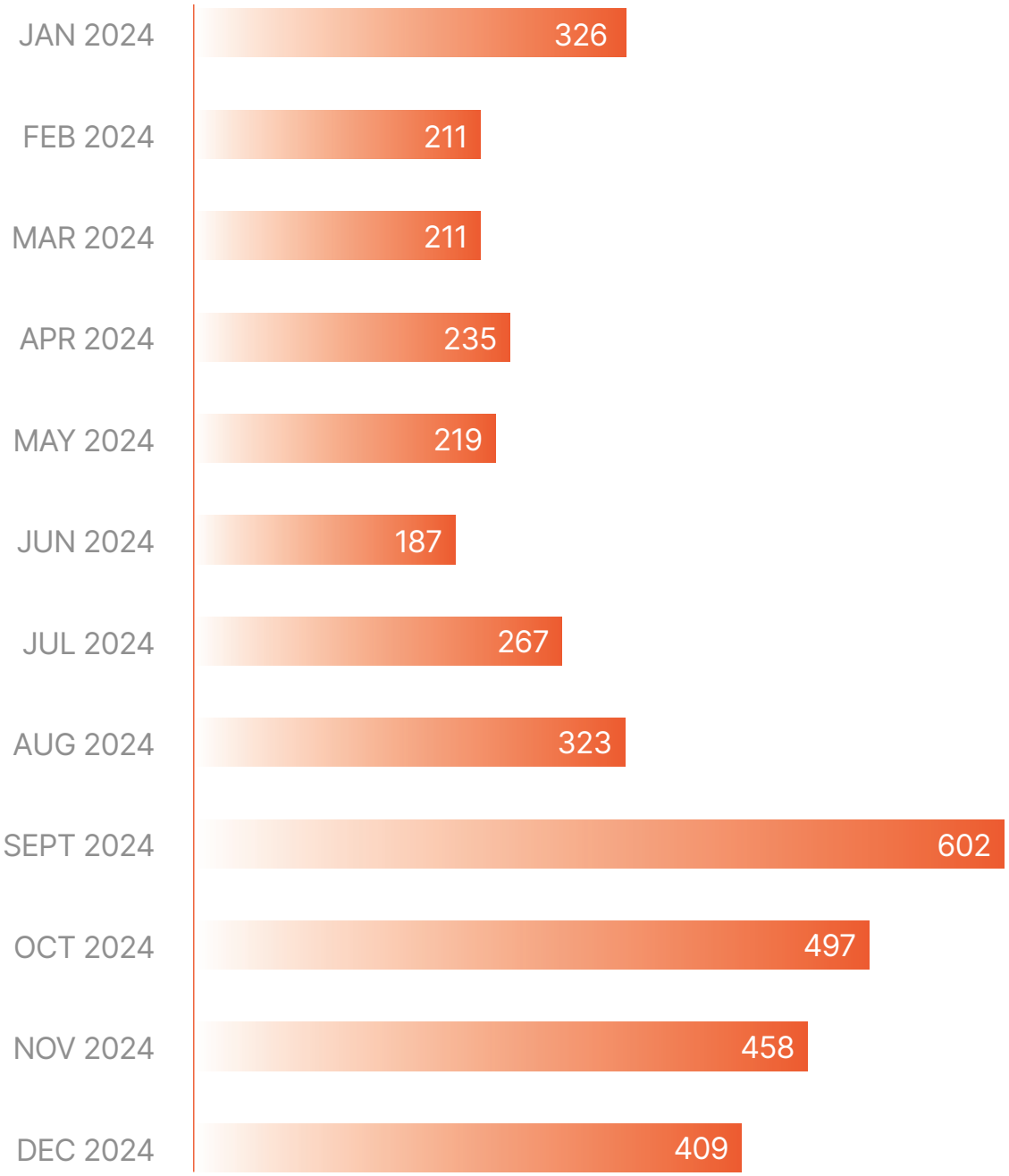
120,650,644,601

Customer Industry

- Finance & Insurance
- Large Conglomerate
- Datacentre Provider
- Government Agencies
- Education
- Property Developers
- Energy
- Logistics
- Media And Entertainment
- Manufacturing

INCIDENTS

How many total alerts triggered on SIEM: **12,379,396**
Total incidents escalated: **3945**



INCIDENTS BY LOG SOURCES

TOP 3 BY RANKING

Top 10 incidents by name

6.53% Potential Password Spraying of Microsoft 365 User Accounts

6.20% Microsoft 365 Portal Logins from Impossible Travel Locations

4.74% Successful O365 Login from Blacklisted IP

2.78% Sensitive Directory Service Object Changed

2.43% SMB (Windows File Sharing) Activity to the Internet

1.90% Account Configured with Never-Expiring Password

1.65% New User Created Login Using Admin Privileges

1.41% Successful Root SSH Login

1.17% Privileged Account Brute Force

1.17% File Changes at Sensitive Directory (FIM)

Based on Simply Data's proprietary data

TOP INDUSTRIES

(with most incidents)

EDUCATION **LOGISTICS** **LARGE CONGLOMERATE**

Top 5 MITRE Tactics and Techniques

Tactics (Top 5)

25.38%
TA0006
(Credential Access)

22.79%
TA0001
(Initial Access)

11.53%
TA0003
(Persistence)

9.45%
TA0010
(Exfiltration)

8.29%
TA0011
(Command and Control)

Techniques (Top 5)

18.71%
T1078
(Valid Accounts)

15.17%
T1110
(Brute Force)

8.54%
T1098
(Account Manipulation)

5.77%
T1190
(Exploit Public-Facing Application)

3.90%
T1048
(Exfiltration Over Alternative Protocol)

Based on Simply Data's proprietary data

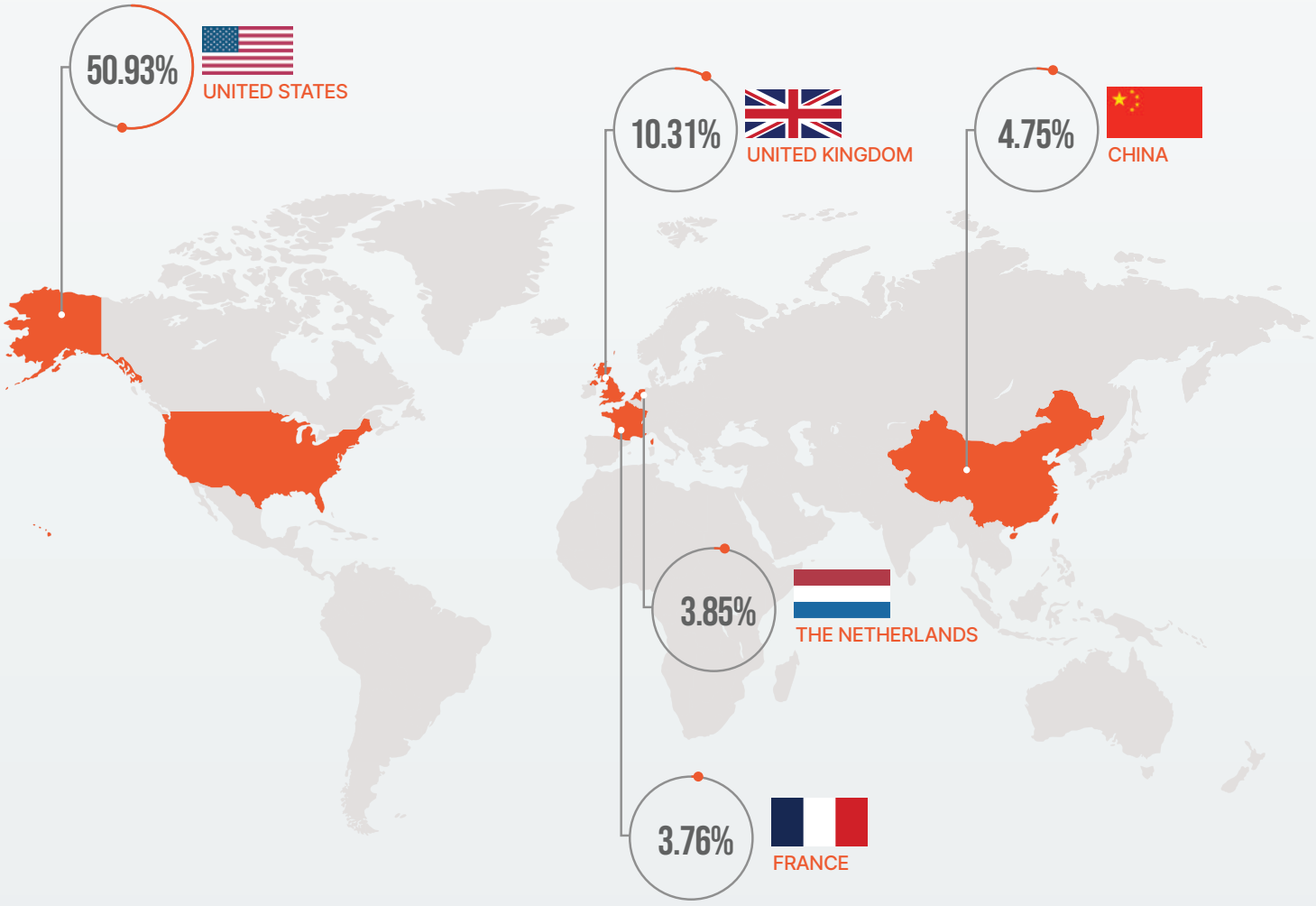
THREAT INTELLIGENCE

428,681,768
Total threat intelligence lookup (unique IOCs)

33,213,117
Total bad reputation IOCs matched with threat intelligence (unique IOCs)

7.75%
% threat intelligence matched

When matching threat intelligence, the average feeds matched is **18.027**



Based on Simply Data's proprietary data

RISKS
TOP RISKS IDENTIFIED ARE

01 Identity and Credential Compromise

Identity and credential compromise represents the most significant risk observed during the reporting period. Password spraying, brute-force attempts, and impossible travel login events account for the majority of detected incidents. This trend is strongly supported by MITRE ATT&CK mappings, where Credential Access is the most prevalent tactic (25.38%) and Valid Accounts is the most frequently observed technique (18.71%). Adversaries are primarily targeting user credentials to gain initial access, with Microsoft 365 environments being a common entry point.

02 Weak Access Controls and Privilege Management

The data indicates systemic weaknesses in identity governance and access control enforcement. Indicators include accounts configured with non-expiring passwords, newly created users being granted administrative privileges immediately, and unauthorized or high-risk directory object modifications. These conditions significantly increase exposure to persistence mechanisms, which account for 11.53% of observed tactics. In particular, Account Manipulation (T1098) represents 8.54% of techniques, highlighting the risk of privilege escalation and lateral movement once initial access is obtained.

03 Data Exfiltration Exposure

Data exfiltration activity ranks as the fourth most common tactic, accounting for 9.45% of observed behaviors. Notable indicators include SMB traffic to external destinations and exfiltration over alternative protocols. When viewed alongside Command-and-Control activity (8.29%), this suggests that successful intrusions frequently progress to active data extraction attempts. Affected sectors such as education and logistics typically manage sensitive personal and operational data, increasing the potential impact of these incidents.

Based on Simply Data's proprietary data

INSIGHTS FROM 2025 DATA

Identity-Centric and Supply Chain–Amplified Attack Patterns

The analysis shows that identity infrastructure is the primary attack surface, with Microsoft 365 consistently targeted as the initial entry point. Adversaries predominantly rely on credential-based techniques such as password spraying, brute force, and anomalous login activity to gain access.

This risk is further amplified by extensive third-party and supply chain integrations with Microsoft 365, where compromised external applications, OAuth permissions, or automation workflows can be leveraged to abuse trusted access paths. As a result, identity compromise is not confined to direct user activity but extends to integrated tools and services, increasing overall exposure.

Control and Governance Weaknesses Enable Attack Progression

Once initial access is obtained, weaknesses in access controls, privilege management, and identity governance frequently allow attackers to progress through multiple stages of the attack lifecycle. Indicators such as excessive privileges, non-expiring passwords, rapid elevation of newly created accounts, and risky directory changes point to configuration and enforcement gaps rather than a lack of detection capability.

The observed attack sequences spanning persistence, account manipulation, and command-and-control suggest that attackers can operate beyond initial compromise due to insufficient preventative controls and privilege hygiene.

Concentrated Risk Driven by High-Value Targets and Data Sensitivity

The observed threat activity is highly concentrated around a limited number of attack techniques that directly enable access to sensitive systems and data. Credential Access, Valid Accounts, Persistence, and Exfiltration consistently appear together, indicating that attackers are prioritizing efficiency and impact rather than breadth. Sectors such as education and logistics are disproportionately affected due to the nature of the data they manage, including personal information and critical operational data.

This concentration of activity suggests that attackers are selectively targeting environments where successful compromise is more likely to result in meaningful data access or operational leverage.

REFLECTING ON 2024 REPORT

2024 Prediction	
Rise of Supply Chain Compromise	Yes
Password Compromise and Social Engineering	Yes
Ransomware and Security Practices	Partial

REFLECTING ON OUR 2024 PREDICTIONS,

the majority proved accurate. The rise of supply chain compromises was fully validated, with several notable incidents throughout the year highlighting the growing risk posed by third-party vendors.

Organizations that invested in threat-hunting focused on living-off-the-land techniques linked to supply chain actors were better positioned to detect and respond to these threats.

Password compromise and social engineering also played out as expected. Generative AI significantly elevated the quality and scale of phishing and impersonation attacks, making them harder to detect. NIST's updated password guidelines in Q2 2024 were a positive step, but adoption has been slow, with many auditors still relying on outdated standards.

Ransomware predictions were partially realized. Ransomware-as-a-Service and advanced techniques like EDR killer tools continued to fuel attacks, confirming the threat landscape we anticipated. However, progress on the broader recommendation balancing People, Processes, and Technology remained uneven. Many organizations still struggled with proper configuration and adoption of security best practices, underscoring that technology alone is not enough.

STARLIGHT
THREAT INTELLIGENCE

Ransomware Statistics for Malaysia

2023	2024	2025
20	21	45

Top 10 Threat Actors

Threat Actor	Incidents	Threat Actor	Incidents
LockBit 3.0	17	Hunter	4
Qilin	13	Babuk2	4
Direwolf	9	TheGentlemen	4
Ransomhub	6	Akira	3
Obscura	5	Lv	2

Key Threat Actor Profiles

Threat Actor	Affiliations/Origins	Strategic Focus & Tactics
LockBit (3.0/5.0)	Global RaaS / Eastern Europe	Uses "invisible mode" and API harvesting; targets manufacturing.
Qilin (Agenda)	Russia-linked RaaS	Uses Rust language for speed; primary threat to aviation and healthcare.
Direwolf	SE Asia (Human-operated)	Specialized in double-extortion against tech and legal sectors.
INDOHAXSEC	Indonesia-based Hacktivist	Ideologically motivated; targets government for data leaks.
Akira	Global RaaS	Focuses on Windows and ESXi; highly prolific in late 2025.

OUTLOOK: PREPARING FOR 2026

AI is no longer a future concept but a functional "double-edged sword" in the 2026 landscape.

Offensive AI

- High-value Business Email Compromise (BEC) now uses AI-generated voice and video to impersonate CEOs.
- Natural Language Processing (NLP) is used to craft "Manglish" (Malaysian English) localized phishing lures that bypass traditional filters.
- Strains like LAMEHUG and PROMPTFLUX use LLM interactions to re-generate source code on execution, making them "invisible" to traditional signature-based EDR.

Defensive AI

- AI agents now handle the "volume problem," triaging thousands of alerts to identify true positives in milliseconds.
- Shifting from detection to anticipation by identifying pattern anomalies before a breach occurs.

High Risk Targeted Sectors for 2026

- Healthcare, Remains the primary target due to the critical nature of patient records and zero downtime tolerance.
- Manufacturing & Energy, Increasing risk due to IT-OT convergence, where corporate breaches can lead to physical production halts.
- Critical Infrastructure, Targeted by state-sponsored actors to sow economic chaos and disrupt essential public services.

This report was meticulously prepared by Starlight Intelligence.

About Starlight Intelligence

Founded in 2019, Starlight Intelligence is a premier cybersecurity firm dedicated to transforming the industry through locally developed, cost-effective solutions that bridge the gap between high-end protection and budgetary constraints. As a NACSA-licensed service provider and a Malaysia Digital Status company recognized for its innovation in Artificial Intelligence, the firm leverages its proprietary Starlight Neural Networks (SNN) to generate high-fidelity threat intelligence and assess risks with precision. Committed to the highest levels of data integrity, Starlight Intelligence is BSI-certified to ISO 27001:2022 standards and actively supports organizations in building a secure, AI-driven, and compliant digital future.

External References:

- *CyberSecurity Malaysia (MyCERT) - Quarterly Summary Report Q1/Q2 2025.*
- *SOCRadar - Malaysia Threat Landscape Report 2026.*
- *EC-Council - The Role of AI in Cybersecurity 2026.*
- *Bursa Malaysia Berhad - Media Release: Cyber Resilience Enhancements (Nov 2025).*
- *Google Cloud - Cybersecurity Forecast 2026 Report.*

FLAWTRACK

EXTERNAL EXPOSURE & DARK WEB OBSERVATIONS

Data Source : Flawtrack Intelligence Platform
Period : 2025 Statistics

To complement our internal SOC findings, we collaborated with Flawtrack to analyse external exposure and dark web intelligence trends observed across Malaysian organizations.

1. Overall Exposure Statistics

Metric	Value
Total Malaysian Domains Exposed	44,593
Total Credentials Compromised	5,776,612
Unique Users Affected	2,408,402
Government Domains (.gov.my)	3,980
Commercial Domains (.com.my)	21,451
Educational Domains (.edu.my)	5,404

2. Sector Breakdown

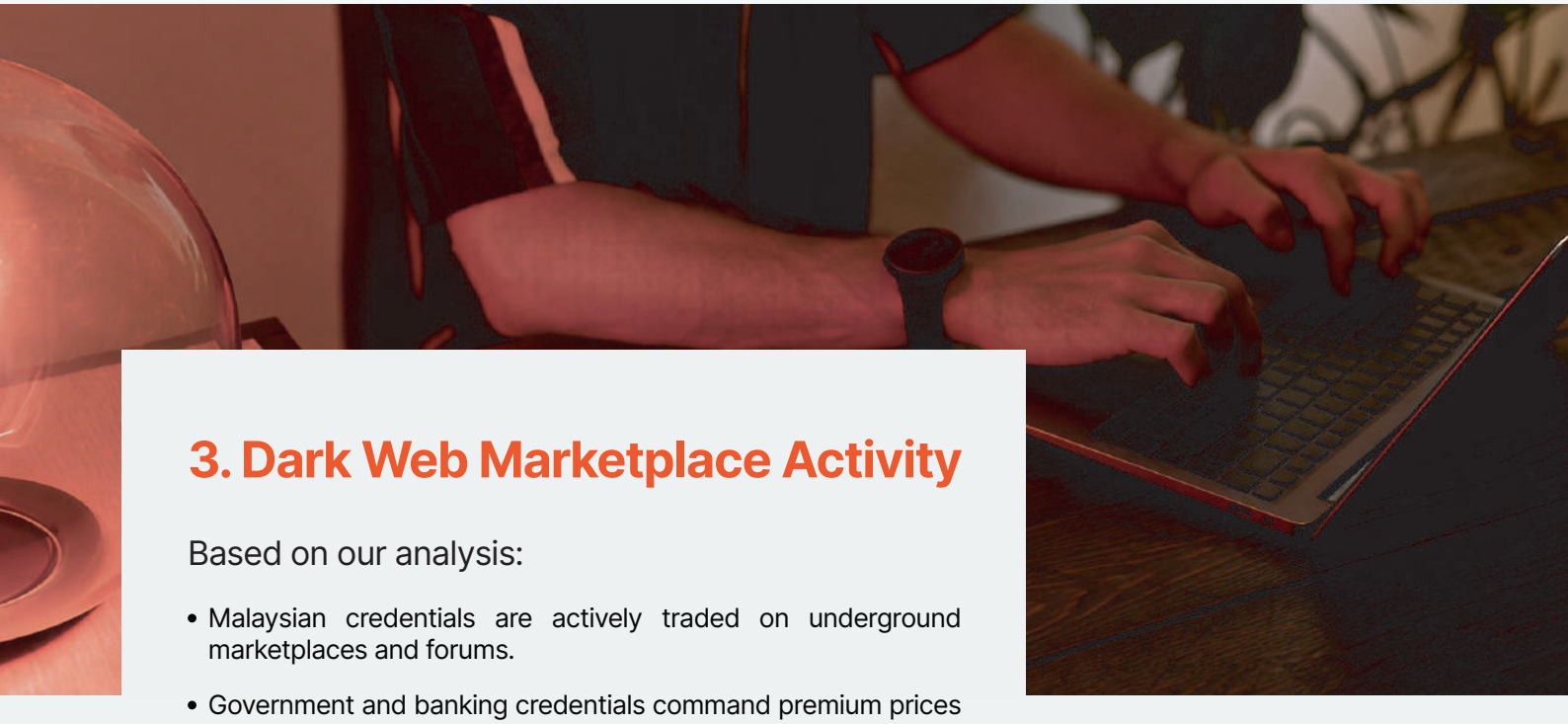
Sector	Domains Affected	Total Credentials	Unique Users	% of Total
Commercial	21,451	2,249,263	973,998	38.9%
Government	3,980	1,619,708	712,996	28.0%
Education	5,404	1,013,829	317,859	17.5%
Other	13,753	893,812	403,549	15.5%

Sector Breakdown (Compromised Endpoints)

Sector	Endpoints	Credentials	Unique Users
Commercial	499,265	1,909,848	158,913
Government	460,825	1,832,196	159,825
Education	189,339	918,724	72,024
Other	182,867	702,948	58,135

Operating System Distribution

OS	Devices	Credentials	% of Devices	Avg Creds/Device
Windows 10	54,994	8,307,511	71.3%	151
Windows 11	17,185	4,297,128	22.3%	250
Other	3,103	557,506	4.0%	180
Windows 7	1,787	143,644	2.3%	80
Windows Server	17	5,673	<0.1%	334



3. Dark Web Marketplace Activity

Based on our analysis:

- Malaysian credentials are actively traded on underground marketplaces and forums.
- Government and banking credentials command premium prices in dark web listings.
- Combo lists containing Malaysian emails are frequently updated and redistributed.
- Stealer logs from Malaysian endpoints are bundled and sold in bulk packages.
- Credential reuse across services significantly amplifies the impact of each breach.

PREDICTION AND RECOMMENDATIONS FOR 2026

AI Agents Security Risk

The adoption of AI agents and AI-driven workflows will introduce new attack vectors that are not fully addressed by traditional application security controls. Prompt injection attacks are expected to increase, enabling attackers to manipulate agent behaviour to extract sensitive information such as API keys, credentials, system prompts, or internal logic. In addition, agent-to-agent phishing where malicious agents impersonate trusted agents or inject malicious instructions into multi-agent workflows is likely to emerge as a viable attack technique, particularly in automated business processes.

RECOMMENDATIONS

Organizations should implement strict input validation and output filtering for AI agents, enforce least-privilege access for APIs and secrets, and isolate agent execution environments. Secrets should never be embedded directly in prompts or agent memory. Continuous monitoring of agent behaviour, strong authentication between agents, and human-in-the-loop controls for high-risk actions are critical to reducing the blast radius of successful prompt manipulation.

Supply Chain

Supply chain risk will remain a significant and persistent threat in 2026, particularly as organizations continue to rely on interconnected SaaS platforms, cloud services, and third-party integrations. Compromises affecting vendors, software dependencies, or trusted external services are expected to continue enabling indirect access to enterprise environments, including identity systems such as Microsoft 365.

RECOMMENDATIONS

Organizations should strengthen third-party risk management by integrating threat intelligence feeds, attack surface management (ASM), and brand monitoring capabilities. Continuous visibility into exposed assets, abused domains, and impersonation activity can help detect supply chain related threats earlier. Governance over third-party access, OAuth permissions, and API integrations should be regularly reviewed to reduce implicit trust relationships.

IoT Threats

IoT-related threats are expected to increase in 2026, particularly in regions where IoT security adoption remains low. Poorly secured IoT devices continue to present attractive, low-effort entry points for attackers. As a result, network-based attacks leveraging compromised IoT devices such as lateral movement, botnet activity, and internal reconnaissance are likely to rise.

RECOMMENDATIONS

Organizations should adopt network-centric IoT security controls, including proper network segmentation to isolate IoT traffic from core business systems. Dedicated inspection and monitoring of IoT communications should be enforced to ensure visibility into anomalous behaviour. Secure architecture design, combined with continuous traffic inspection and device inventory management, is essential to reducing IoT-driven risk.

SECURING MALAYSIA'S DIGITAL FUTURE

Delivering intelligence-driven cybersecurity across Malaysia, Indonesia, and Singapore.

About SIMPLY DATA

Simply Data is an innovation-led cybersecurity company experiencing strong regional growth across Malaysia, Indonesia, and Singapore. In 2025, the company was recognized for its award-winning Security Operations Center (SOC), reflecting its operational excellence and commitment to high-performance security monitoring.

Simply Data holds key industry credentials, including ISO/IEC 27001 certification, CREST accreditation, CSM Collaboration Partner recognition, and Penetration Testing Service Provider (PTSP) certification. These credentials reinforce its adherence to international standards and best practices in cybersecurity governance and operations.

Driven by continuous innovation, Simply Data has developed three proprietary security platforms deployed across enterprise environments to enhance detection, response, and operational visibility. The company is also an early adopter of internally developed AI-driven workflows, leveraging automation and intelligence to strengthen security operations and deliver scalable, future-ready protection for modern organizations.

Our Core Capabilities

- 24/7 Managed SOC & SIEM Monitoring
- Identity Threat Detection & Response (ITDR)
- Microsoft 365 & Cloud Security Monitoring
- Threat Intelligence & IOC Correlation
- Incident Response & Digital Forensics
- Vulnerability Assessment & Penetration Testing
- AI-Driven Security Automation & Analytics
- Supply Chain & Third-Party Risk Monitoring

Operational Scale & Intelligence Depth

- Over 120 billion security logs analysed annually.
- More than 12 million security alerts processed.
- Over 33 million malicious IOCs identified and correlated.
- Supporting critical sectors including education, logistics, finance, government, manufacturing, energy, and conglomerates.

This scale enables Simply Data to detect emerging attack patterns early, reduce attacker dwell time, and provide actionable intelligence tailored to the evolving Malaysian threat landscape.

Partner With Us

Organizations seeking to strengthen their cybersecurity posture may engage Simply Data for:

- *SOC Health & Detection Effectiveness Review*
- *Identity Security & Privilege Governance Assessment*
- *Threat Exposure & Attack Surface Evaluation*
- *AI & Automation Security Risk Advisory*

MALAYSIA CYBER SECURITY AWARDS

MSC MALAYSIA Spearheading Transformation

CREST

ISO 27001 Certified

B-03A-03, 3RD Floor, Block B Setiawalk, Persiaran Wawasan, Pusat Bandar Puchong, 47100 Puchong, Selangor.

contactus@simplydata.com.my

+6016 - 208 8000

simplydata.com.my

LinkedIn