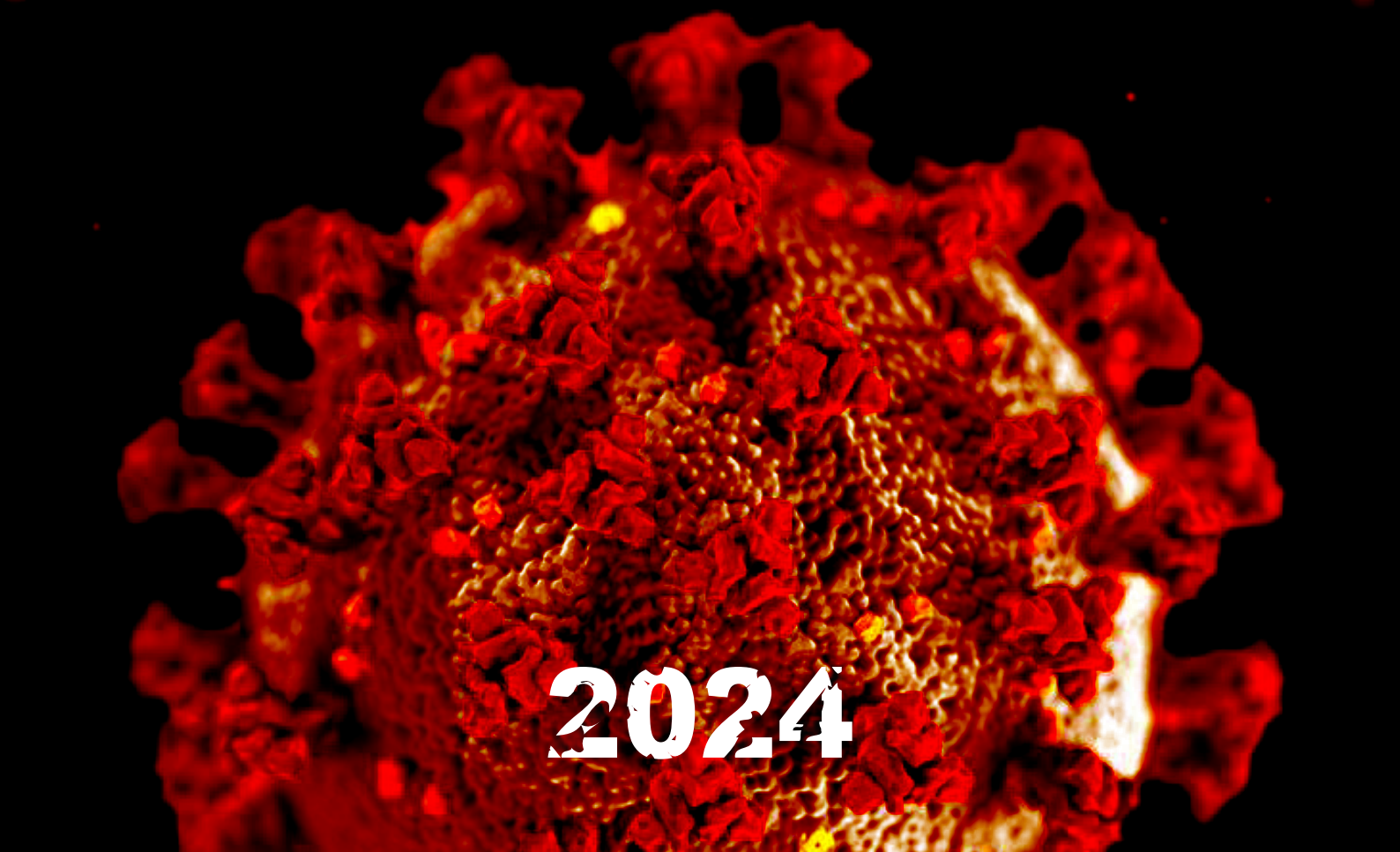
MALAYSIA THREAT REPORT



2024

TOTAL LOGS COLLECTED

71,880,607,531

This report provides a comprehensive analysis of Malaysia's threat landscape in 2024, based on extensive log data collected through our Security Operations Center (SOC) activities. It offers critical insights into cybersecurity incidents and trends, equipping IT teams with the knowledge to strengthen their defenses and prepare for future challenges.

The report covers the following key areas:

NUMBER OF INCIDENTS
A BREAKDOWN OF SECURITY INCIDENTS OBSERVED THROUGHOUT THE YEAR.

TOP THREAT ACTORS
IDENTIFICATION OF THE MOST ACTIVE MALICIOUS ENTITIES TARGETING MALAYSIA.

TOP INCIDENTS
AN ANALYSIS OF THE MOST FREQUENT AND IMPACTFUL INCIDENT TYPES.

MITRE TACTICS AND TECHNIQUES
A DETAILED MAPPING OF PREVALENT ADVERSARY BEHAVIORS.

ATTACK ORIGINS
INSIGHTS INTO THE TOP COUNTRIES FROM WHICH CYBERATTACKS ORIGINATED.

OBSERVED RISKS
HIGHLIGHTS OF THE PRIMARY CYBERSECURITY RISKS FACED BY ORGANIZATIONS.

2025 PREDICTIONS
STRATEGIC FORECASTS FOR KEY THREATS AND TRENDS EXPECTED IN THE UPCOMING YEAR.

Key findings from the report include:

MOST VALUABLE LOGS	MALICIOUS IP ACTIVITY	TOP RISK IDENTIFIED
IDENTIFICATION OF LOG SOURCES THAT PROVIDED THE MOST ACTIONABLE INTELLIGENCE.	AN AVERAGE DAILYCOUNT OF BAD IP ADDRESSES COMMUNICATING WITH CUSTOMER ENVIRONMENTS.	A CLEAR UNDERSTANDING OF THE MOST SIGNIFICANT RISK AWECTING ORGANIZATIONS IN MALAYSIA.

In addition to reflecting on the challenges of 2024, this report projects the emerging threats of 2025, providing actionable predictions to guide IT teams in prioritizing resources and enhancing their cybersecurity posture. It serves as a critical resource for understanding and mitigating the challenges faced by organizations operating in Malaysia.

CUSTOMER INDUSTRY


LARGE CONGLOMERATE


DATACENTRE PROVIDER


GOVERNMENT AGENCIES


EDUCATION


PROPERTY DEVELOPERS


ENERGY


LOGISTICS


MEDIA AND ENTERTAINMENT

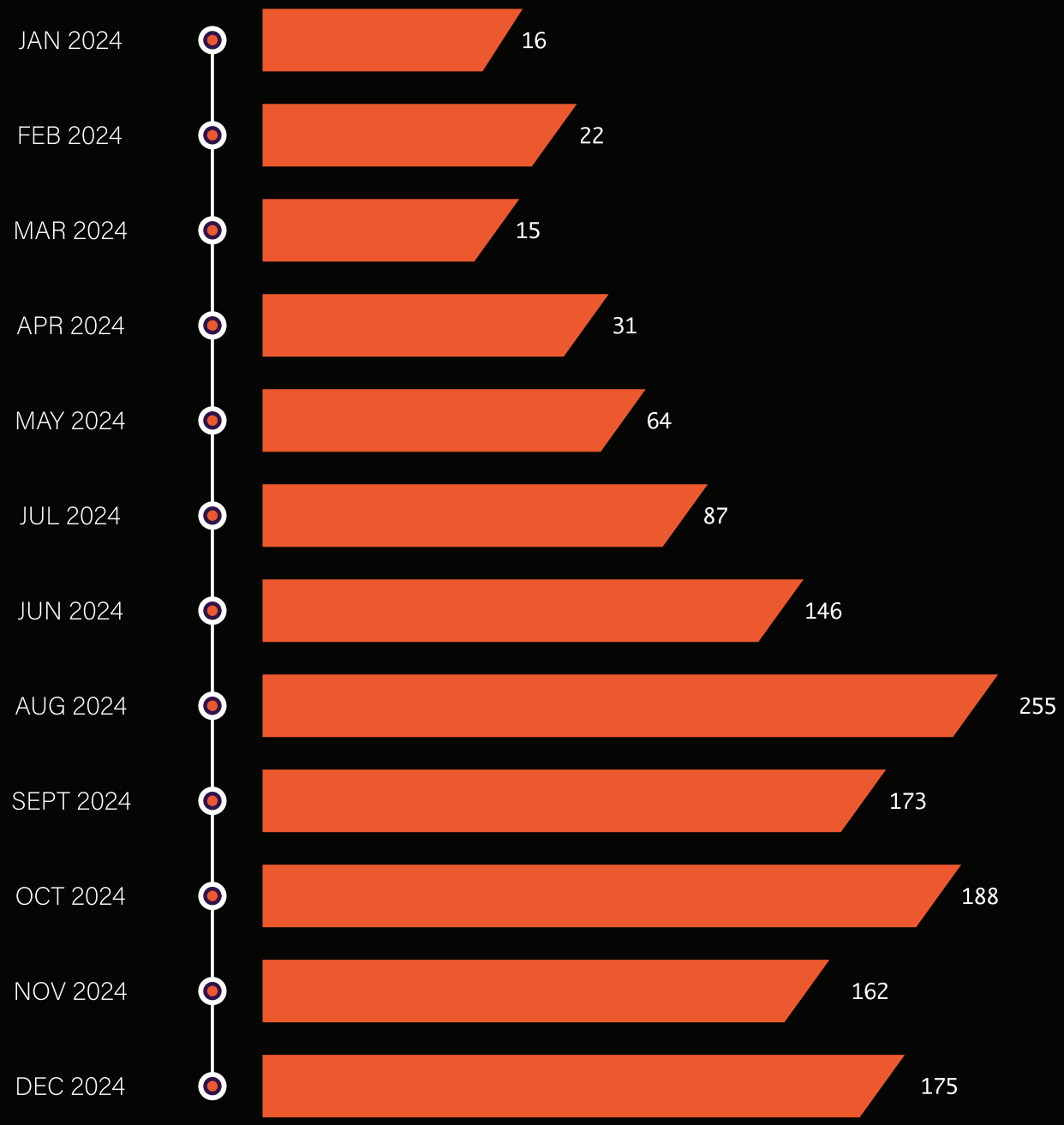

MANUFACTURING


FINANCE

INCIDENTS

How many total alerts triggered on SIEM: **139,764,986**

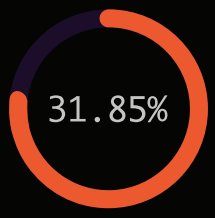
Total incidents escalated: **1334**



Based on Simply Data's proprietary data

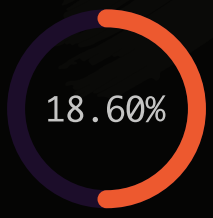
INCIDENTS BY LOG SOURCES

Top 5 by Ranking :



OPERATING SYSTEM LOGS

MICROSOFT 365 LOGS



FIREWALL LOGS

ENDPOINT DETECTION & RESPONSE (EDR) LOGS

PUBLIC CLOUD LOGS
(AWS, AZURE, GCP)

Top 5 incidents by name:

1. POTENTIAL PASSWORD SPRAYING OF MICROSOFT 365 ACCOUNTS
2. BRUTE FORCE ATTEMPTS ON PRIVILEGED ACCOUNT
3. PERSISTENT BLOCKED THREATS BY FIREWALL
4. FILE CHANGES AT SENSITIVE DIRECTORY (FIM)
5. THREAT INTELLIGENCE IOC MATCHED

Based on Simply Data's proprietary data

Top 3 MITRE Tactics and Techniques:

MITRE TACTICS	: TA0006 (CREDENTIAL ACCESS)
MITRE TECHNIQUES	: T1110 (BRUTE FORCE)
MITRE TACTICS	: COMMAND AND CONTROL (TA0011)
MITRE TECHNIQUES	: HIDE INFRASTRUCTURE (T1665)
MITRE TACTICS	: TA0040 (IMPACT)
MITRE TECHNIQUES	: T1485 (DATA DESTRUCTION)

Top industries (with most incidents):

LARGE CONGLOMERATE LOGISTICS EDUCATION

TOP THREAT ACTORS

Top Threat Actors
FLAX TYPHOON ◀ SIDEWINDER ◀ APT32 ◀ RIPPERSEC ◀ GAMAREDON GROUP ◀

Top Ransomware Groups
HUNTERS ◀ RANSOMHUB ◀ LOCKBIT ◀ RHYSIDA ◀ BLACKCAT ◀

Based on SOCRadar research

THREAT INTELLIGENCE

TOTAL THREAT INTELLIGENCE LOOKUP (UNIQUE IOCS)	THREAT INTELLIGENCE MATCHED
13,466,797	3.95%

TOTAL BAD REPUTATION IOCS MATCHED WITH THREAT INTELLIGENCE (UNIQUE IOCS)
532,228

*When matching threat intelligence, the average feeds matched is 12.86

Threat intelligence matched by countries (Top 5 by ranking)

Our threat intelligence leverages over 150 databases, supported by in-house mechanisms that query IP and URL reputations for every traffic passing through the customer environment, ensuring 100% threat intelligence coverage. Any indicators of compromise (IOCs) matching multiple databases are automatically blocked through seamless integration with the customer's firewall system. While blocking is essential, we also recognize the dynamic nature of IOC reputations and have implemented internal mechanisms to automatically unblock IOCs once their reputations improve. Additionally, we continuously review and enhance our databases and integration processes to maintain a robust and secure system.

RISK

TOP RISKS IDENTIFIED ARE:

LACK OF CONTINUOUS FINE-TUNING OF SECURITY SOLUTIONS

Without regular fine-tuning of security solutions, organizations risk leaving gaps in their defense systems. Cyber threats evolve rapidly, and static configurations can lead to ineffective detection and prevention of new attack vectors. Security tools such as intrusion prevention systems, firewalls, and endpoint protection require ongoing adjustments to adapt to the latest threat intelligence, customer-specific environment changes, and compliance requirements. Failure to continuously refine these solutions can result in attacks bypassing security measures, exposing critical systems and data to potential breaches.

ABSENCE OF VULNERABILITY LIFECYCLE MANAGEMENT

A lack of effective vulnerability lifecycle management poses a significant risk to organizations. This includes failing to address vulnerabilities identified during penetration testing or security assessments promptly. Without a structured process to track, prioritize, and remediate vulnerabilities, attackers can exploit known weaknesses, leading to potential breaches. Timely patching, vulnerability assessment, and remediation workflows are essential for minimizing the window of exposure. An absence of these practices not only leaves systems open to compromise but also undermines compliance with regulatory standards.

NON-HARDENED FIREWALL CONFIGURATIONS

Improperly configured firewalls, particularly those exposing SSLVPN or management interfaces to the public, present a critical risk to organizations. These interfaces are prime targets for attackers and are frequently linked to zero-day vulnerabilities and firewall firmware exploits. When these interfaces are exposed, they become susceptible to brute-force attacks, credential theft, and unauthorized access, which can lead to full system compromise. Many high-profile attacks leverage such vulnerabilities to bypass perimeter defenses.To mitigate this risk, organizations must adhere to strict hardening practices, including restricting access to trusted IP ranges, implementing multi-factor authentication (MFA), disabling unnecessary services, and ensuring firewall firmware is regularly updated. Additionally, regular vulnerability scans and proactive patching are essential to addresszero-day risks and reduce the attack surface, safeguarding critical systems from exploitation.

INSIGHTS FROM 2024 DATA

TOP RISKS RELATED TO MISCONFIGURATION AND LACK OF FINE-TUNING

The primary risks identified stem from misconfigurations and the absence of regular fine-tuning in existing security solutions. These issues can result in reduced effectiveness of security controls and increased exposure to potential threats. To mitigate these risks, detailed configuration-based auditing is necessary, such as leveraging CIS benchmarks. These benchmarks provide industry-standard best practices to ensure optimal configuration of key security solutions, particularly firewalls and Endpoint Detection and Response (EDR) systems. Regular audits and adjustments are critical to maintain a robust security posture.

TIME-CONSUMING IOC BLOCKING PROCESS

On average, a single customer needs to block 91 unique indicators of compromise (IOCs) daily, year-round. If manual blocking of each IOC takes approximately two minutes, this translates to 182 minutes—over three hours—dedicated daily to IOC blocking. This process is resource-intensive and unsustainable for long-term operations.To address this challenge, automated IOC blocking mechanisms are strongly recommended. Automation not only reduces the time burden but also enhances accuracy and response times, allowing IT teams to focus on other critical security tasks.

PRIORITIZATION OF VALUABLE LOGS FOR COLLECTION

Not all logs hold equal value in detecting and responding to incidents. Based on incident statistics, certain logs, such as those from operating systems (OS), are more “valuable” and impactful in identifying threats. It is crucial to prioritize the collection of OS logs while also aiming to gather logs from all available data sources whenever feasible. Comprehensive log collection enables better visibility and analysis, ensuring critical threats are detected promptly and reducing the likelihood of missed indicators of malicious activity.

PREDICTION AND RECOMMENDATIONS FOR 2025

Rise of Supply Chain Compromise

Supply chain compromises are becoming increasingly prevalent. While organizations may have limited control over these external vendors, they must remain vigilant in their threat-hunting efforts, particularly by focusing on administrative activities and SOC use cases that involve living-off-the-land techniques linked to supply chain vendors.

Password Compromise and Social Engineering

Password compromise and social engineering attacks are not new, but this trend is expected to persist, especially with the advancement of generative AI. In Q2 2024, the National Institute of Standards and Technology (NIST) issued new guidelines on password policies. However, adopting these guidelines will take time, as many cybersecurity auditors still refers to older password standards.

Ransomware and Security Practices

Ransomware will continue to be a major threat, fuelled by the increased adoption of Ransomware-as-a-Service (RaaS) and advanced security bypass techniques like “EDR killer” tools. Security personnel must ensure that all security solutions are configured optimally and aligned with industry best practices. Although technology vendors will undoubtedly continue to innovate, these innovations are rendered ineffective if not implemented or utilized correctly. It is crucial to remember that “Technology” is just one-third of the cybersecurity equation—equal emphasis must be placed on “People” and “Processes”.

ABOUT SIMPLY DATA

Simply Data is a data-focused company specializing in analysing, harvesting, and providing insights based on security and performance related data.

Powered by Elastic and various in-house built tools to automate analysis. Some tools are built in-house such as attack surface management and real-time threat intelligence lookup to provide additional value to our customers. Our aim is to deliver insights that enables our customers to make the right decisions.

We have also obtained CREST certification and started to venture into Red Teaming exercises.

No Shortcuts, No Limits – Simply Data, 100% Raw and Ready"

At Simply Data, we believe in providing unfiltered, complete access to your data, ready for any use case. Whether you're analyzing network performance, application behavior, or business metrics, our 100% raw and unprocessed data offers you the flexibility and depth to unlock actionable insights. With Simply Data, you get the full picture—no compromises, no limits—empowering you to make smarter, more informed decisions.

Contact Details:

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

contactus@simplydata.com.my

+6016 - 208 8000

LinkedIn

Youtube