Localized Cyber Threat Intelligence: The Synergy of AI and Human Expertise in Addressing the Philippines Threat Landscape

Quang Tran Minh

Director of Intelligence Center – Viettel Cyber Security

viettel security

CONTENT

INTRODUCTION

ABOUT ME

QUANG TRAN MINH

Product Director

Viettel Cyber Security

CYBERSECURITY EXPERIENCE

- **15 years of experience** in Cyber Security
- Handled **100+ cyber security incidents** for various entities
- Conducted **10,000+ hours of research** in reverse engineering, malware, vulnerabilities, digital forensics and incident response, threat intelligence
- **Frequent speaker** at many conferences (FIRST, Security World, Security Summit, CIO/CSO, Security Bootcamp, botconf, tetcon, tradahacking…)
- **A member** of Vietnam CSIRT
- **International certifications include**: GIAC Cyber Threat Intelligence (GCTI), GIAC Certified Forensic Analyst (GCFA), Certified Threat Intelligence Analyst (C|TIA), Computer Hacking Forensic Investigator (CHFI), EC-Council Certified Incident Handler (ECIH), Certified Ethical Hacker (CEH)

ABOUT VIETTEL CYBER SECURITY

viettel security

#1 (*)

Best Cyber Security Company in Asia

(*): According to Cybersecurity Excellence Awards 2022-2023
(100 - 499 employees)

500+
EMPLOYEES

14 years
Experience

15 countries
Where customers come from

Japan, Philippines, Laos, Cambodia, Myanmar, Timo Leste, Tanzania, Mozambique, Burundi, Peru, Haiti, Vietnam, Hongkong, Singapore, South Africa

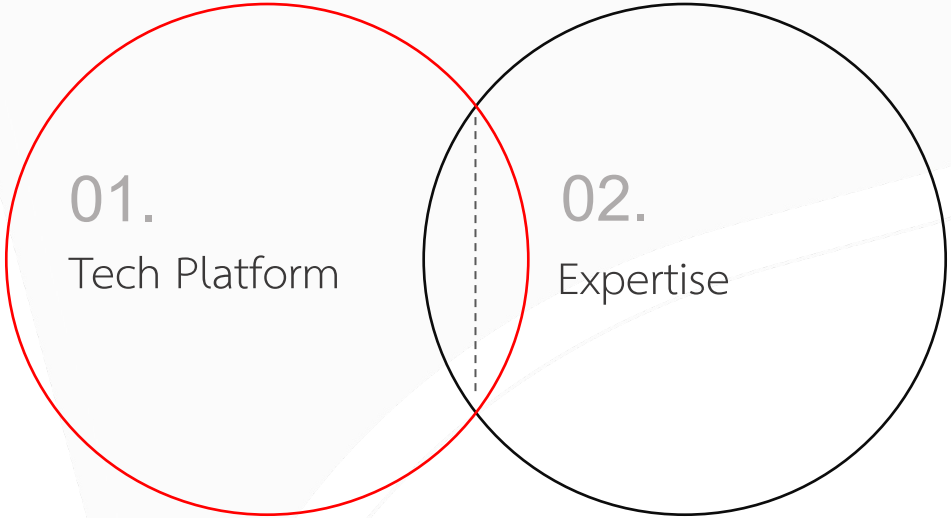
No1 CTF
Rootcon
(2024)

Master of Pwn
Pwn2Own
(2023, 2024)

Booth #G2

viettel security **THREAT INTELLIGENCE**

100% BY VCS



GCTI · GREM · GCFA · CompTIA PenTest+ · CISA · CISM · OSCP · OSWE · CISSP · CCSP · CHFI · ECIH · CTIA · CPENT · CEH · LPT

Comprehensive Service
Localized Intelligence
& Expert Support

THE PHILIPPINES THREAT LANDSCAPE

Victim

Department of Information and Communications Technology (DICT)

Industry

Government

Threat Actor

Unknown Hacktivist

Time

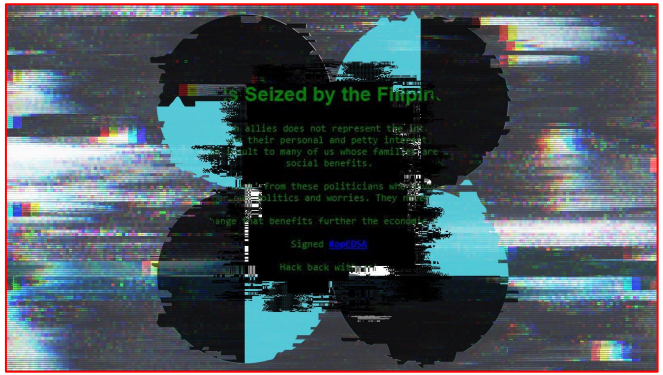
April 2024

n/a

Ransom Amount

2 TB

Affected Data Size



The attack compromised over two terabytes of data, locking the agency out of its systems. Local hackers, linked to the "#opEDSA" movement, claimed responsibility.

*Source: https://mb.com.ph/2024/4/3/hackers-strike-department-of-science-and-technology-servers

Victim

Department of Migrant Workers (DMW)

Industry

Government

Ransomware Group

n/a

Time

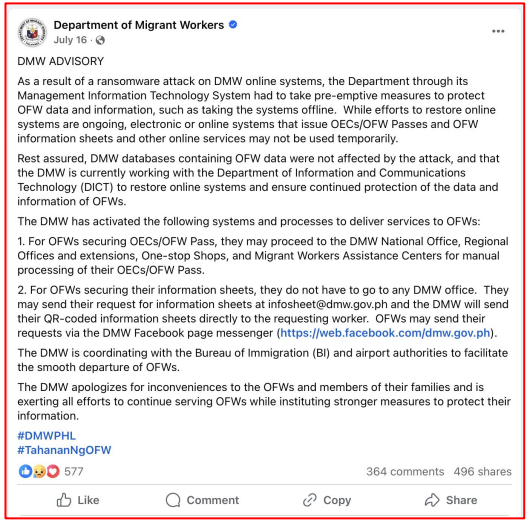
July 2024

n/a

Ransom Amount

n/a

Encrypted Data Size



Department of Migrant Workers
July 16 ·

DMW ADVISORY

As a result of a ransomware attack on DMW online systems, the Department through its Management Information Technology System had to take pre-emptive measures to protect OFW data and information, such as taking the systems offline. While efforts to restore online systems are ongoing, electronic or online systems that issue OECs/OFW Passes and OFW information sheets and other online services may not be used temporarily.

Rest assured, DMW databases containing OFW data were not affected by the attack, and that the DMW is currently working with the Department of Information and Communications Technology (DICT) to restore online systems and ensure continued protection of the data and information of OFWs.

The DMW has activated the following systems and processes to deliver services to OFWs:

1. For OFWs securing OECs/OFW Pass, they may proceed to the DMW National Office, Regional Offices and extensions, One-stop Shops, and Migrant Workers Assistance Centers for manual processing of their OECs/OFW Pass.

2. For OFWs securing their information sheets, they do not have to go to any DMW office. They may send their request for information sheets at infosheet@dmw.gov.ph and the DMW will send their QR-coded information sheets directly to the requesting worker. OFWs may send their requests via the DMW Facebook page messenger (https://web.facebook.com/dmw.gov.ph).

The DMW is coordinating with the Bureau of Immigration (BI) and airport authorities to facilitate the smooth departure of OFWs.

The DMW apologizes for inconveniences to the OFWs and members of their families and is exerting all efforts to continue serving OFWs while instituting stronger measures to protect their information.

#DMWPHL
#TahananNgOFW

577 364 comments 496 shares

Like Comment Copy Share

DMW took pre-emptive steps, including taking systems offline to protect OFW data. While unaffected data remains secure, online services like issuing OECs are temporarily unavailable.

Source: https://www.facebook.com/dmw.gov.ph/

Victim

Jollibee

Industry

Food and Beverage

Threat Actor

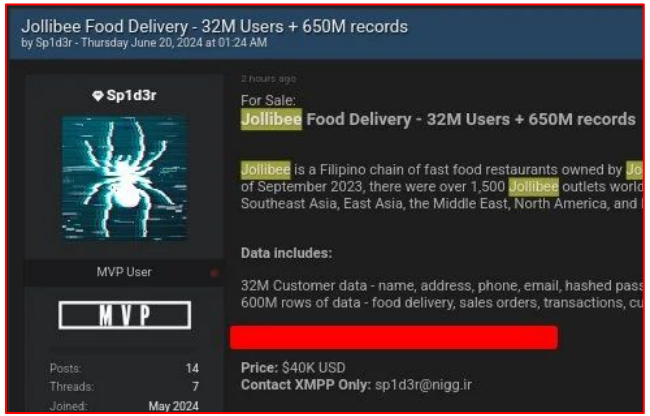
n/a

Time

June 2024

11.000.000

Affected Customers



The breach had compromised sensitive personal information in what is now the largest data breach in Philippine history. The exposed data included dates of birth and senior citizen identification numbers.

*Source: https://x.com/deepwebkonek/status/1803652654046048645

PHILIPPINE CYBER THREAT STATISTICS

Compromised Credentials & Data Breaches

Over **315,000**

Compromised credentials

47 data selling incidents:

- **660 Million** records
- **1TB** of data, **150GB** KYC data

Vulnerabilities

17,648 new

vulnerabilities worldwide

by **42%**

in comparison with H1 2023

- **71 new** vulnerabilities could potentially impact **Southeast Asia**.
- **Previously identified vulnerabilities** are being exploited for scanning and further attacks.

17,456 Phishing Attacks

by **27%**

in comparison with H1 2023

Top 3 targeted industries:

- **Financial–services**
- **E-commerce**
- **Government**

APT & Ransomware

7 APT Groups with **Significant Impact**

Most frequent Techniques: **DLL-Sideloading, CVE**

7 TERABYTES

encrypted data in **Southeast Asia**

Ransom amount: **~ $13 Million**

CHALLENGES

Rapidly Evolving Threat Landscape

The cyber threat landscape is constantly changing, with new attack vectors, malware, and phishing tactics emerging frequently. In the Philippines, sectors such as finance and government are increasingly targeted by sophisticated, localized cyber attacks.

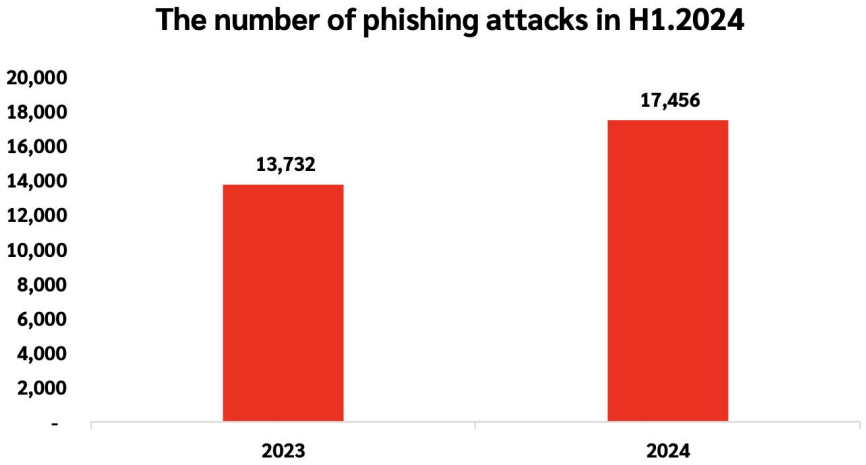
High Volume of Data and Alerts

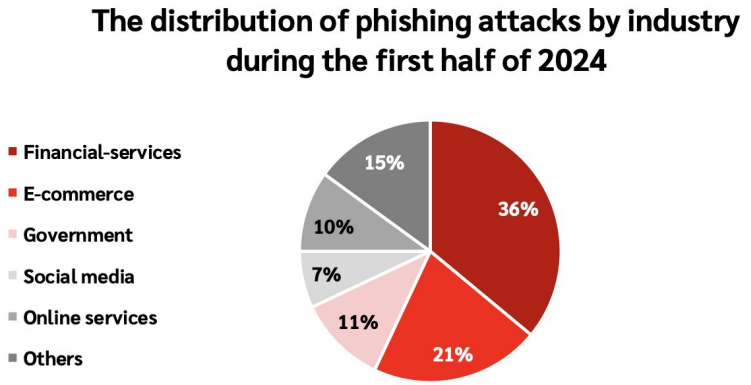
Organizations face overwhelming volumes of data and security alerts daily, making it difficult to identify genuine threats, especially with regional nuances and languages in the Philippines.

Resource Constraints and Skill Gaps

Cyber threats in the Philippines often have unique cultural and language factors, making it difficult for generic AI solutions to detect and categorize them accurately.

CHALLENGE #1: RAPIDLY EVOLVING THREAT LANDSCAPE

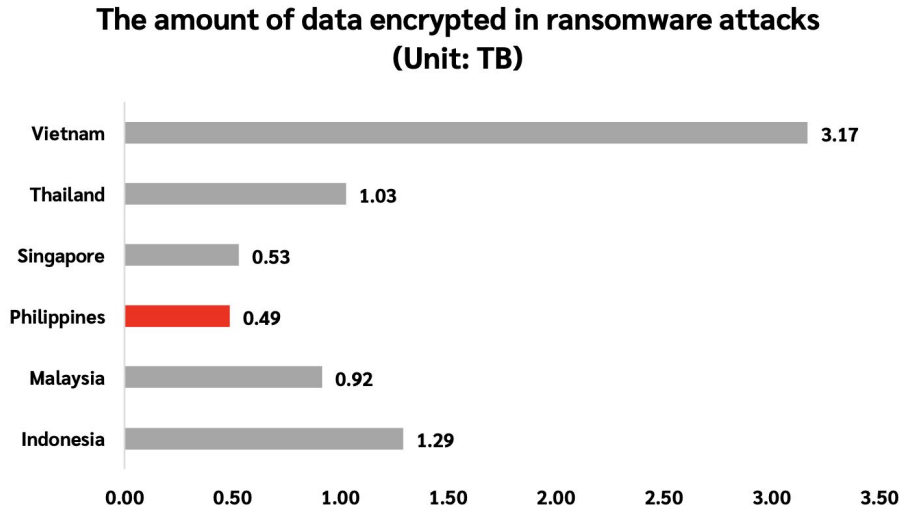




Increase In Phishing Attacks

Significant increase in phishing attacks, with incidents rising by over 23% in the past year, especially targeting financial, e-commerce and government sectors

CHALLENGE #1: RAPIDLY EVOLVING THREAT LANDSCAPE



Rise in Ransomware Incidents

In H1.2024, data encrypted in ransomware attacks across Southeast Asia reached more than 7 Terabytes, with the estimated total ransom amounting to approximately 13 million USD.

CHALLENGE #1: RAPIDLY EVOLVING THREAT LANDSCAPE

LOCKBIT

Ransomware

Russia

Revenue — **$ 91 Millions** (In the US alone)

Victim — **1700** (In the US alone)

Operation Model

- Sell malware, charge via profit sharing
- Widely malware spreading and system compromising
- Ransom demands

Lazarus

Revenue — **$ 900 Millions** (7/2022-7/2023)

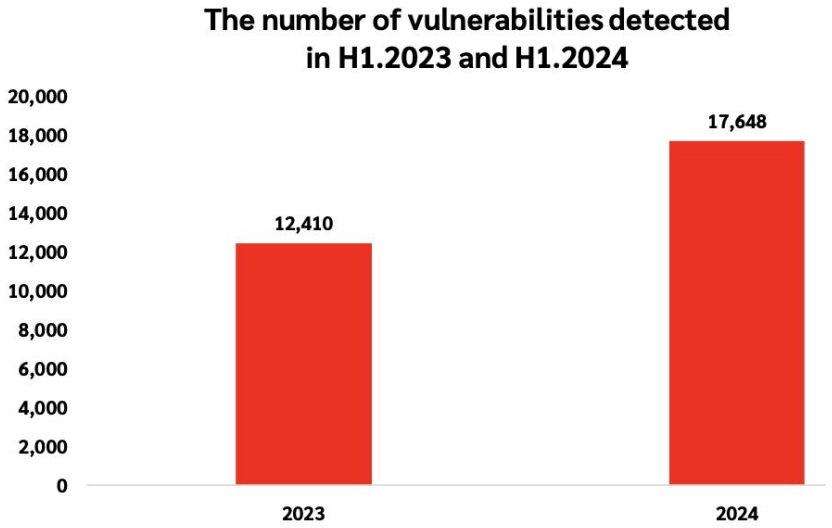
Operation Model

- Build new tools and exploit new vulnerabilities
- Install malware via phishing
- Launder cryptocurrency using cross-platform currency exchange methods

Sophistication of Attacks

Advanced Persistent Threat (APT) groups are increasingly shifting to more financially motivated attacks, including ransomware and data theft, posing a high-risk factor for Philippine critical infrastructure.

CHALLENGE #2: HIGH VOLUME OF DATA AND ALERTS



over 315,000 compromised credentials

Viettel Threat Intelligence has recorded **over 315,000 compromised credentials** in the Philippines in the first half of 2024. The rise of Stealer-as-a-service (SaaS) and Stealer Malware groups have contributed significantly to the increase of compromised credentials.

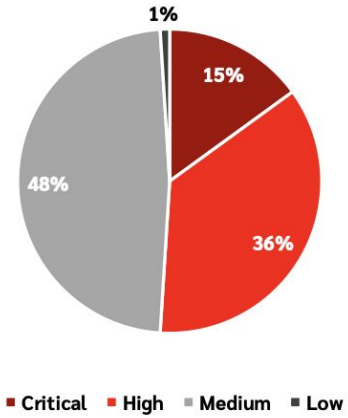
Numerous incidents involving the leak of privileged credentials for critical and sensitive systems, such as email systems, single sign-on (SSO) management systems, Active Directory (AD) systems, and internal access VPNs, have raised serious concerns. If this information falls into wrong hands, it could be used for malicious purposes, such as disrupting operations, stealing sensitive data, or conducting cyberattacks.

Explosion of Cybersecurity Alerts

A typical cybersecurity operations center (SOC) handles an average of 10,000–15,000 alerts daily, with larger enterprises sometimes managing up to 50,000 alerts per day.

CHALLENGE #2: HIGH VOLUME OF DATA AND ALERTS

The proportion of vulnerabilities by severity level in H1.2024



71 alerts
related to vulnerabilities

Through the assessment and analysis of vulnerabilities, Viettel Threat Intelligence has issued **71** alerts related to vulnerabilities that significantly impact organizations and enterprises in the Philippines, specifically as follows:

Table 2. The number of vulnerabilities recorded in H1.2024 by severity level

Severity	Amount
Critical	2
High	23
Medium	45
Low	1

False Positive Rates

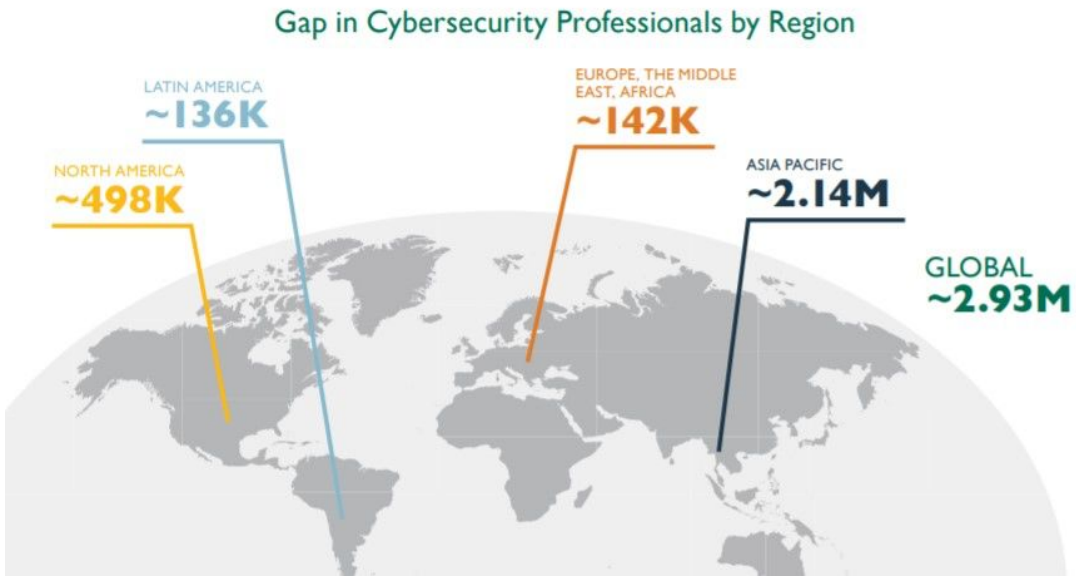
Around 45-50% of security alerts generated by detection systems are false positives, requiring manual review by analysts, which drains resources.

CHALLENGE #2: HIGH VOLUME OF DATA AND ALERTS

Increased Data from Digital Transformation

Organizations have seen an annual data growth rate of around 30%, primarily from digital transformation efforts, remote work setups, and IoT devices, increasing data volume and resulting alerts.

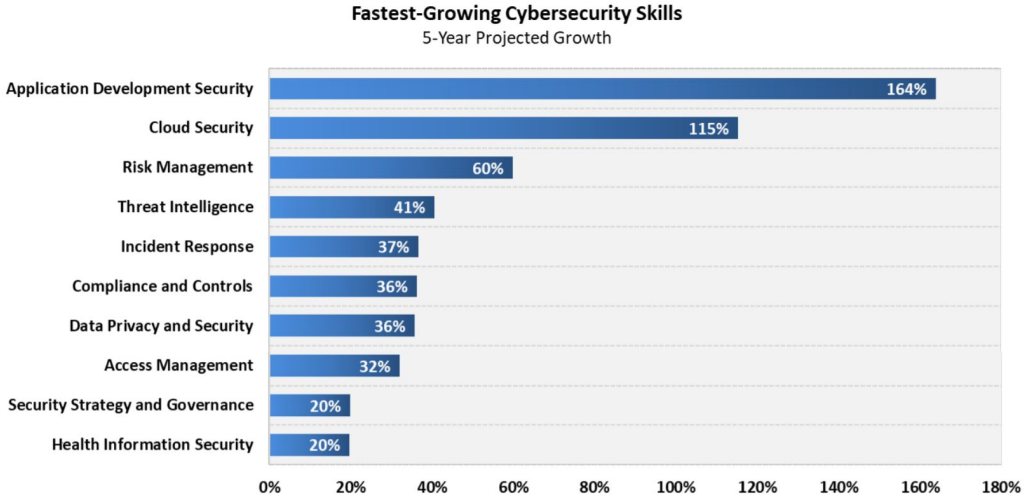
CHALLENGE #3: RESOURCE CONSTRAINTS AND SKILL GAPS



Cybersecurity Workforce Shortage

As of recent reports, there is a global shortage of 3.4 million cybersecurity professionals, with the gap projected to grow as demand outpaces supply. The Asia-Pacific region, including the Philippines, has one of the highest cybersecurity workforce gaps, with a shortage of over 2.1 million professionals in 2023, highlighting the need for skilled talent.

CHALLENGE #3: RESOURCE CONSTRAINTS AND SKILL GAPS



Increased Demand for Specialized Skills

Only 25% of cybersecurity professionals report having the necessary skills to interpret and act on threat intelligence effectively, contributing to delays in response and higher operational costs.

CHALLENGE #3: RESOURCE CONSTRAINTS AND SKILL GAPS

High Turnover and Analyst Burnout

A recent survey found that 68% of SOC analysts report burnout, with over half considering leaving their role due to overwhelming workloads and lack of resources.

AI & HUMAN EXPERTISE IN LOCALIZED TI

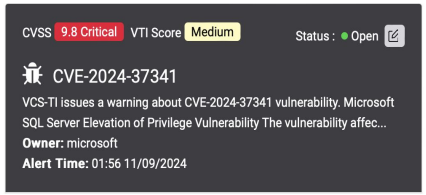
AI-POWERED THREAT DETECTION AND ANALYSIS

AI Capabilities:

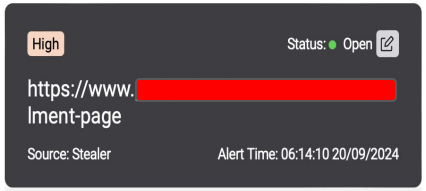
- AI's ability to process and analyze vast amounts of data in real time.
- Detection of complex and evolving attack patterns, including zero-day threats and advanced persistent threats (APTs) common to the Philippines.

Examples:

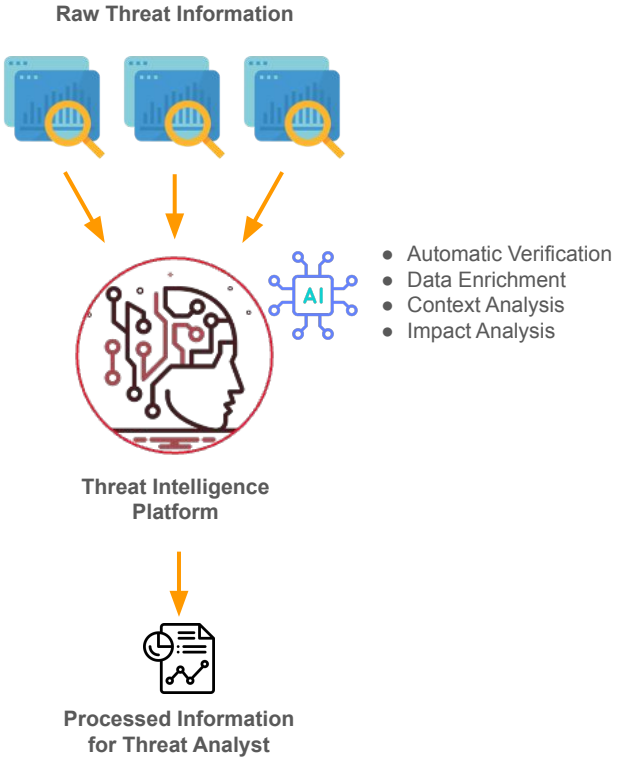
- Threats detected by AI:



New Vulnerability



Compromised Account



AUTOMATED LOCALIZATION AND ADAPTABILITY OF AI MODELS

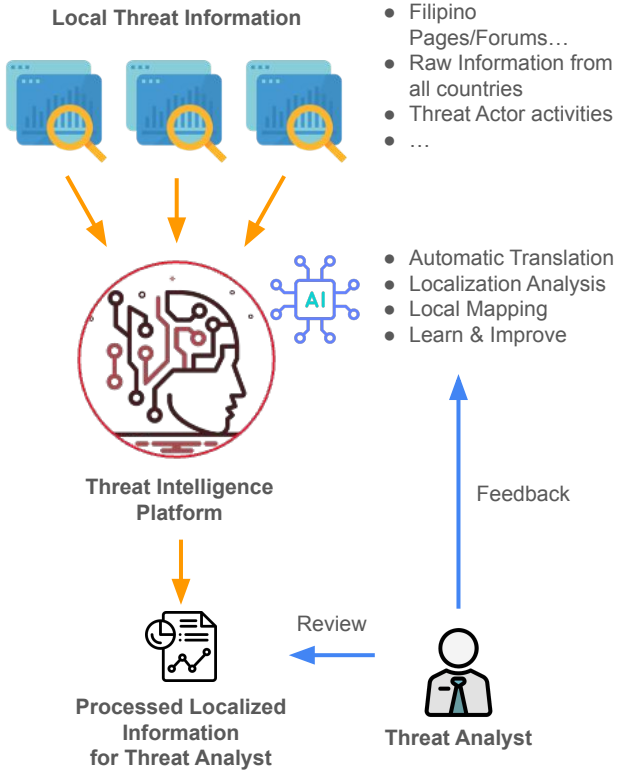
Localized Data Models:

- AI systems are capable of handling data from various multilingual sources, including Filipino, allowing more accurate threat detection in the local context.
- The AI automatically maps and analyzes information relevant to the Philippines, using indicators such as IP addresses, domain names, content, and organization names.

Continuous Learning:

- AI models are continuously improved by incorporating insights from threat analysts, who verify and tag local information sources, ensuring accuracy and relevance to the Philippines' threat landscape.

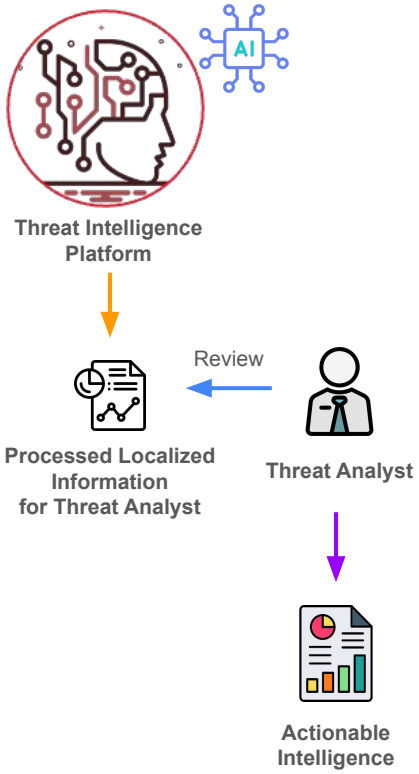
However, AI is not enough!



HUMAN INTELLIGENCE IN CONTEXTUAL ANALYSIS

Key Responsibilities of Analysts:

- Human analysts review and validate AI-generated threat alerts, ensuring the accuracy and relevance of detected threats.
- Analysts align threat attributes with the specific digital assets of the organization, clarifying potential impact and providing tailored response measures.



ENHANCED DECISION-MAKING AND CUSTOMIZED CLIENT SUPPORT

Client-Focused Intelligence:

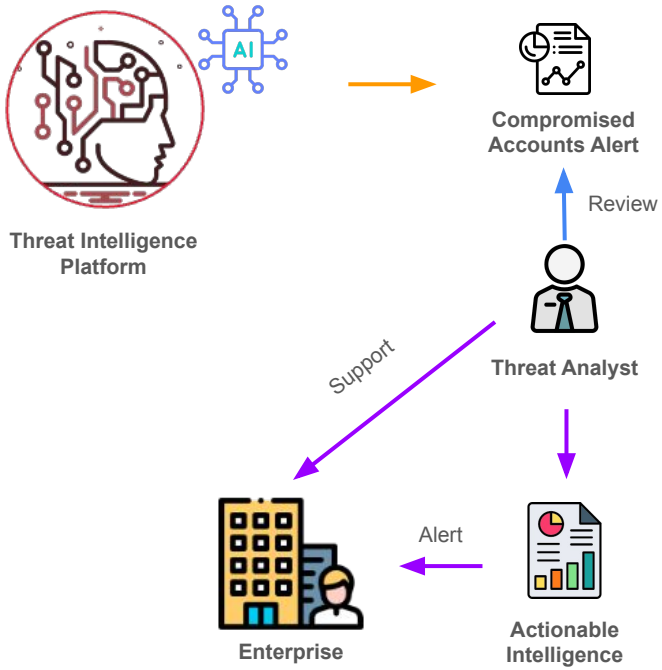
- Threat analysts provide tailored recommendations based on their knowledge of a client's industry, size, and risk profile.

Human Judgment in Critical Situations:

- Threat analysts recommend response actions with priority levels and customized insights to address the unique needs and context of each client.

Case-study: Alert and response on compromised accounts

- Threat Intelligence Collects, Analyzes, and Alerts on Compromised Accounts for Sale on the Deep Web.
- Threat Analyst Verifies Account Accuracy and Identifies High-Priority Accounts.
- Actionable Intelligence Report Tailored to the Organization's Digital Asset Profile
- Support for Organizational Response Measures



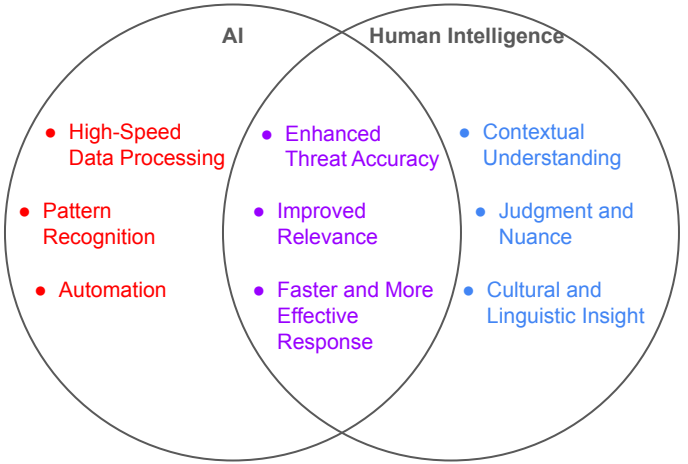
COMBINED INTELLIGENCE IN THREAT DETECTION

Overview of Synergy:

- AI rapidly processes large volumes of data, quickly detecting patterns and generating alerts. This allows for faster identification of potential threats, reducing the time needed for initial threat detection.
- Human analysts bring essential contextual knowledge and judgment, interpreting AI-generated alerts to ensure accuracy. By understanding the organization's specific environment, they can assess threats more effectively and tailor responses to be both relevant and impactful.

Enhanced Detection and Response:

- AI enables quicker identification of threats, allowing for prompt action and minimizing potential damage.
- Advanced filtering helps decrease false alerts, allowing analysts to focus on genuine threats.
- Threat intelligence is tailored to the specific needs and threat landscape of Philippine clients, ensuring actionable and localized insights.



CASE STUDY: RESPONDING TO A LOCALIZED PHISHING CAMPAIGN

Case Summary:

- AI-Powered Threat Intelligence detected unusual patterns indicative of a phishing campaign targeting Philippine organizations.

Role of Human Expertise:

- Human analysts added context, validating AI's findings and uncovering specific phishing lures tailored to Philippine users.

Outcome:

- This combined effort led to faster detection, client alerting, and prevention of broader exposure.

19/09/24:
- Phishing Domain Created
  - *philip[redacted]net*

19/09/24:
- Phishing Domain Detected by AI-Powered Threat Intelligence

19/09/24:
- Threat Verified by Human Threat Analyst
- Actionable Intelligence created and sent to Client

20/09/24:
- Takedown Request filed from Client
- Takedown Actions taken by Human Threat Analyst

21/09/24:
- Phishing Domain taken down
- AI-Powered Threat Intelligence continue monitoring for new phishing domains

AI-POWERED THREAT INTELLIGENCE WITH HUMAN SPECIALIST

<24h

Average Threat Detection Time

The combined power of AI and human expertise enables critical threat detection within 24 hours, ensuring timely response and mitigation before threats escalate.

90%

Reduction in Operational Analysis Costs

Automating data processing and preliminary analysis with AI reduces manual workload significantly, lowering operational costs associated with threat analysis and management by up to 90%.

80%

Decrease in False Positives

AI filters out false positives, leaving only high-confidence alerts for human review. This streamlining allows analysts to focus on actual threats, improving efficiency and overall security posture.

CONCLUSION

SUMMARY: KEY TAKEAWAYS

Rapid and Accurate Threat Detection

Combining AI's speed with human expertise enables threat detection within critical timeframes, ensuring timely response and risk mitigation.

Cost Efficiency Through Automation

AI reduces manual workload, achieving up to 90% in operational cost savings by automating data processing and initial analysis.

Enhanced Relevance for the Philippines

Localized threat intelligence tailored to the Philippines addresses region-specific risks, providing actionable insights relevant to clients' unique environments.

Reduced False Positives with Human Verification

AI filters low-priority alerts, while human specialists validate and contextualize findings, reducing false positives and improving focus on genuine threats.

Comprehensive, Client-Centric Support

The synergy between AI and human intelligence delivers precise, customized responses and recommendations, ensuring maximum protection and alignment with client needs

RECOMMENDATIONS ON TI PROGRAM

1. Implement a Comprehensive TI Program as Part of the Organization’s Security Strategy
2. Localize the TI Program for Organizational, Industry, and National Specifics
3. Ensure Timely Analyst Support for Rapid, Effective Threat Response
4. Maintain Flexibility for Integration with Other Security and IT Systems
5. Leverage AI in the TI Program to Address Big Data and Digital Transformation Challenges

QUESTION & ANSWER

viettel
security

Visit us at G2 booth for personalized threat check report!

Thank you

For attention!