The Role of Threat Intelligence in Risk Management and Incident Response for Native Cloud

Quang Tran Minh

Director of Intelligence Center – Viettel Cyber Security

viettel security

CONTENT

01 INTRODUCTION

02 THE CLOUD SECURITY LANDSCAPE

03 CTI IN CLOUD RISK MANAGEMENT & INCIDENT RESPONSE

04 STRATEGIES FOR INTEGRATING CTI IN CLOUD SECURITY

05 CONCLUSION

06 Q&A

Image generated by Microsoft Copilot.

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

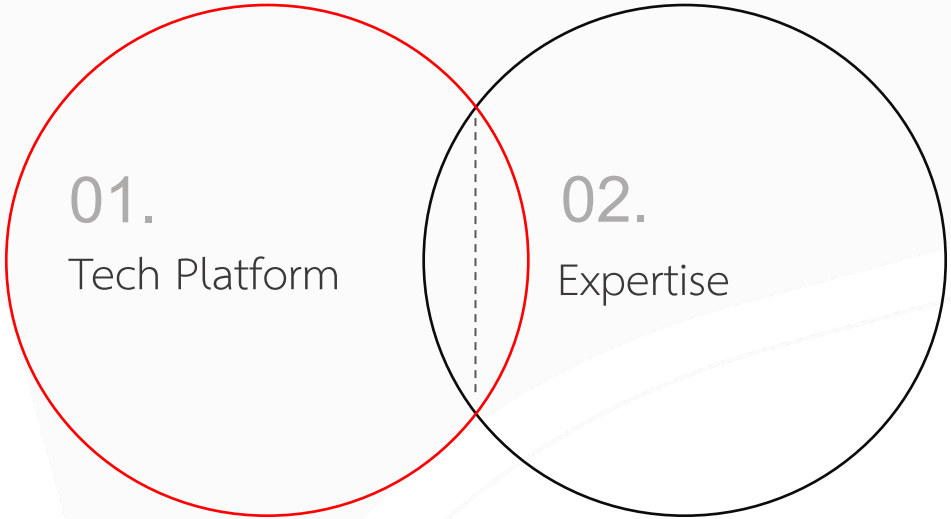
15 countries
Where customers come from

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

Master of Pwn
Pwn2Own
(2023, 2024)

viettel security **THREAT INTELLIGENCE**

100% BY VCS



For more information: https://cyberintel.io

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

Comprehensive Service
Localized Intelligence
& Expert Support

THE CLOUD SECURITY LANDSCAPE

CLOUD-NATIVE CYBER SECURITY

“The Cloud is Secure… But Are You Using It Securely?”

The cloud offers **scalability, flexibility, and agility**, but also introduces new attack surfaces and evolving threats.

Threat actors are adapting their techniques to exploit cloud environments.

Traditional security models are no longer enough—organizations need intelligence-driven security strategies.

Victim

LinkedIn

Industry

Social Media

Attack Vector

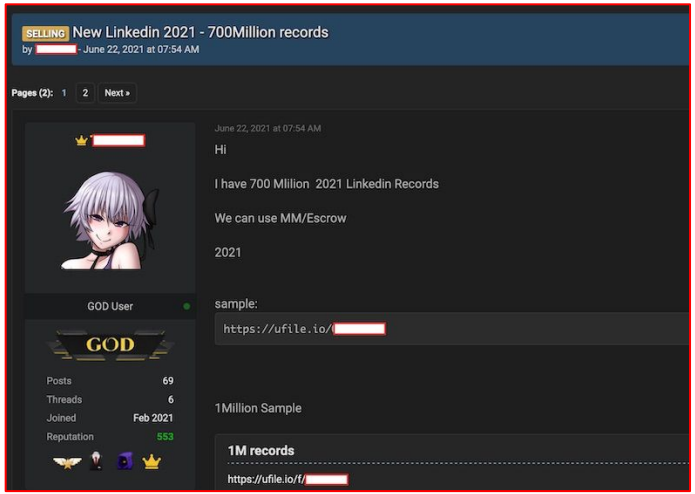
Insecure API

Time

June 2021

700 million

User Records



LinkedIn's 700M user data leak exposed emails, phone numbers, and job details, increasing risks of phishing, identity theft, and social engineering attacks.

https://cyberinsider.com/linkedin-data-leak-700-million-users/

Victim

Toyota Motor

Industry

Automotive

Attack Vector

Cloud Misconfiguration

Time

May 2023

260.000

Customer Data

May 31, 2023

Apology and Notice Concerning Newly Discovered Potential Data Leakage of Customer Information Due to Cloud Settings

Announcement

Print

On May 12, Toyota Motor Corporation (TMC) announced "Apology and Notice Concerning Potential Data Leakage of of Customer Information Due to Misconfiguration of Cloud Environment (Japanese only)" Subsequently, we conducted an investigation for all cloud environments managed by TOYOTA Connected Corporation (TC). It was further discovered that a part of the data containing customer information had been potentially accessible externally. We would like to inform you of the incident that has been identified as of today.

As we believe that this incident also was caused by insufficient dissemination and enforcement of data handling rules, since our last announcement, we have implemented a system to monitor cloud configurations. Currently, the system is in operation to check the settings of all cloud environments and to monitor the settings on an ongoing basis. In addition, we will work closely again with TC to explain and thoroughly enforce the rules for data handling. We will also work to prevent a recurrence by thoroughly educating our employees once again. We sincerely apologize to our customers and all relevant parties for any concern and inconvenience this may have caused.

Massive data breach caused by a cloud misconfiguration, exposing vehicle and customer data for over eight years, affecting more than 260,000 customers.

https://www.csoonline.com/article/575483/cloud-misconfiguration-causes-massive-data-breach-at-toyota-motor.html

Victim

Toyota Motor

Industry

Automotive

Attack Vector

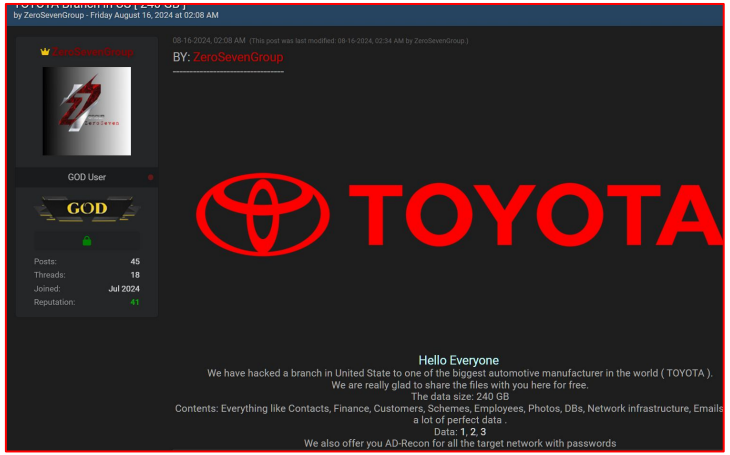
Third-party Compromise

Time

August 2024

240GB

Sensitive Information



*Toyota's U.S. branch suffered a 240GB data breach due to a **third-party compromise**, exposing employee, customer, contract, financial, and network credentials.*

https://www.bleepingcomputer.com/news/security/toyota-confirms-third-party-data-breach-impacting-customers

CLOUD CYBER THREAT STATISTICS

80%

of companies have encountered an increase in the **frequency of cloud attacks.**

23%

of cloud security incidents are a result of **cloud misconfiguration**.

$4.88 million

The average cost of a data breach has increased to $4.88 million in 2024, which represents not only direct losses related to stolen records but also includes long-term reputation loss and compliance fines.

51%

of organizations have reported that **phishing is one of the most prevalent attacks** launched by malicious actors to steal cloud security credentials.

82%

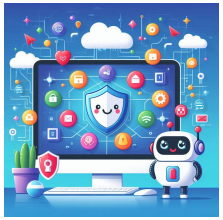
of cloud misconfigurations stem from **human error** and not software defects.

https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/

CLOUD-NATIVE SECURITY - THE NEW BATTLEFIELD

Shared Responsibility Model

Security is a joint effort between cloud providers and customers.



Expanded Attack Surface

APIs, containers, serverless functions, and third-party integrations introduce new risks.

Dynamic & Distributed Infrastructure

Workloads are constantly changing, making static defenses ineffective.

Sophisticated Threats

Attackers exploit misconfigurations, compromised credentials, and supply chain vulnerabilities.

📌 **Key Question: How can organizations proactively manage risks and respond effectively to incidents in the cloud?**

THE ROLE OF THREAT INTELLIGENCE IN CLOUD SECURITY

Proactive Risk Identification

Continuously analyze cloud environments to detect vulnerabilities, misconfigurations, and abnormal activities early. By identifying risks proactively, organizations can strengthen defenses and prevent security incidents before they escalate.

Threat Intelligence

Smarter Incident Response

Real-time intelligence enables security teams to quickly assess threats, isolate affected systems, and take immediate action. By leveraging up-to-date threat data, organizations can respond faster, minimizing impact and reducing downtime.

Image generated by Microsoft Copilot.

THREAT INTELLIGENCE IN CLOUD RISK MANAGEMENT

CLOUD-SPECIFIC THREATS ADDRESSED BY TI

Misconfigurations

- Unsecured cloud settings, such as open storage buckets or excessive permissions, expose systems to attacks.
- *Example*: TI detects publicly exposed S3 buckets with sensitive data, alerting security teams before attackers exploit them.

Vulnerability Exploitation

- Attackers exploit unpatched cloud services, APIs, or containers to gain unauthorized access.
- *Example*: TI tracks zero-day vulnerabilities in cloud platforms and alerts organizations to apply security patches before exploitation.

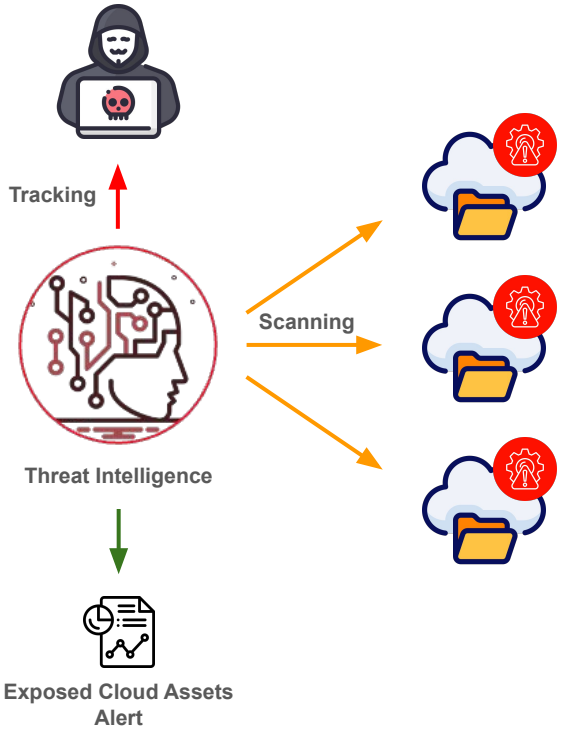
Insider Threats

- Malicious or negligent employees misuse access, leading to data breaches or system compromise.
- *Example*: TI identifies leaked employee credentials on dark web forums, helping organizations revoke compromised accounts.

Supply Chain Risks

- Weak security in third-party providers exposes organizations to indirect cyberattacks.
- *Example*: TI monitors vendor infrastructure for breaches, alerting organizations when a supplier's systems are compromised.

PROACTIVE RISK IDENTIFICATION



Identifying Emerging Threats

- Cybercriminals continuously develop new tactics to exploit weaknesses in cloud-based infrastructures.
- Tracking attacker behavior helps predict threats targeting APIs, containers, and cloud-native services.

Cloud-Specific TI Sources

- Specialized threat intelligence feeds focus on vulnerabilities and misconfigurations in cloud environments.
- These sources analyze security risks in APIs, containers, and serverless computing platforms.

Real-World Example: Early Detection of Exposed Cloud Assets

- **Misconfigured cloud assets** often expose sensitive data, making them prime targets for attackers.
- **Threat Intelligence continuously scans** for exposed databases, open storage buckets, and unprotected cloud resources.
- **Threat Intelligence** alerts a company about an **unsecured cloud database** before attackers can exploit it.

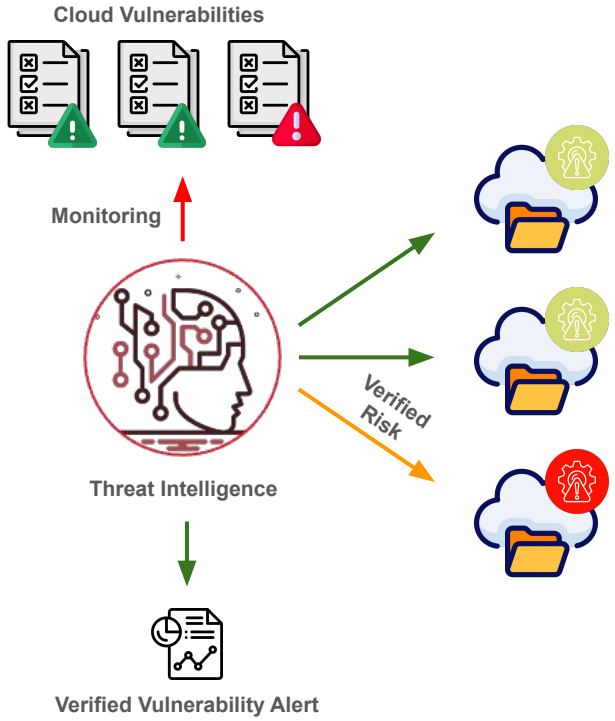
VULNERABILITY MANAGEMENT

Using TI to Prioritize Vulnerabilities in Cloud Infrastructure

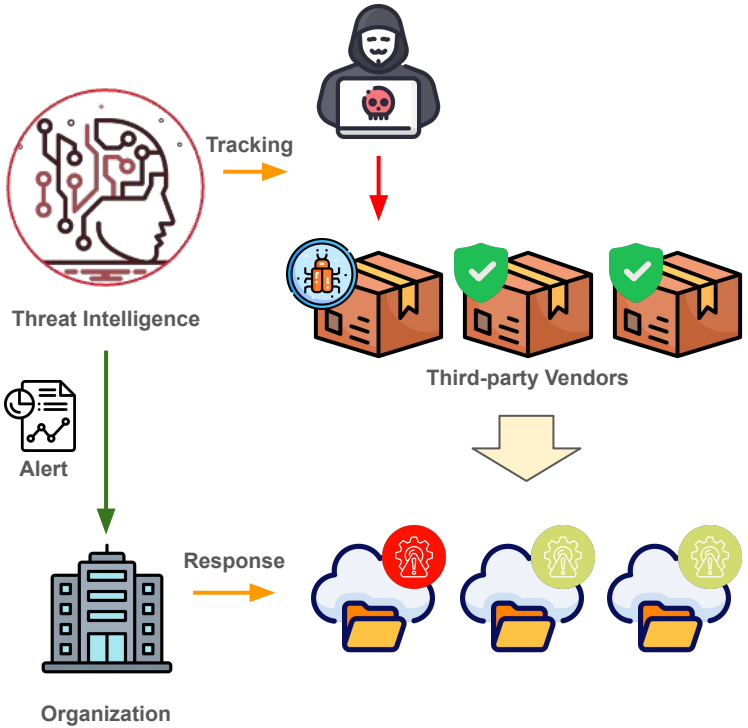
- Threat Intelligence helps detect **high-risk CVEs** that specifically impact cloud environments and services.
- Security teams can assess **which vulnerabilities are actively exploited** to prioritize patching efforts efficiently.
- By **contextualizing risks with real-world attack data**, organizations can focus on the most critical cloud threats.

Case Study: Applying TI to Mitigate a Vulnerability in a Cloud Platform

- A newly discovered **cloud API vulnerability** allows attackers to escalate privileges and access sensitive data.
- **Threat Intelligence identifies active exploitation attempts**, enabling security teams to deploy patches immediately.
- As a result, **potential breaches are prevented**, and the cloud environment remains secure from future attacks.



THIRD-PARTY RISK MANAGEMENT



Identifying Threats Linked to Third-Party Integrations

- Third-party vendors often introduce security risks through misconfigurations, weak authentication, or outdated software.
- Attackers exploit these vulnerabilities to gain unauthorized access or move laterally within cloud environments.

Key Metrics for Evaluating Third-Party Security Posture

- **Known incidents** provide insight into past breaches, helping assess a vendor's security history.
- **Shared Indicators of Compromise (IoCs)** reveal whether a vendor is linked to active attack campaigns.
- **Patching practices** indicate how quickly a vendor addresses vulnerabilities and mitigates security risks.

Real-World Scenario: Preventing a Supply Chain Attack Using TI

- A vendor's **compromised software update** introduces malware, threatening cloud infrastructure security.
- **Threat Intelligence detects IoCs early**, enabling organizations to isolate and mitigate risks proactively.

THREAT HUNTING IN CLOUD ENVIRONMENTS

Using TI for Proactive Threat Hunting

- Threat Intelligence helps **identify Indicators of Compromise (IoCs)** linked to cloud-specific attack campaigns.
- Security teams analyze **Tactics, Techniques, and Procedures (TTPs)** used by attackers targeting cloud environments.
- Proactive threat hunting **uncovers hidden threats** before they escalate into full-scale security incidents.

Example: Threat Hunting for Lateral Movement Using Cloud-Native Services

- Attackers abuse cloud-native tools, such as IAM roles or API calls, for lateral movement.
- Threat hunters use intelligence on suspicious access patterns to detect unauthorized privilege escalation.
- Early detection prevents attackers from moving deeper into cloud infrastructure and exfiltrating sensitive data.

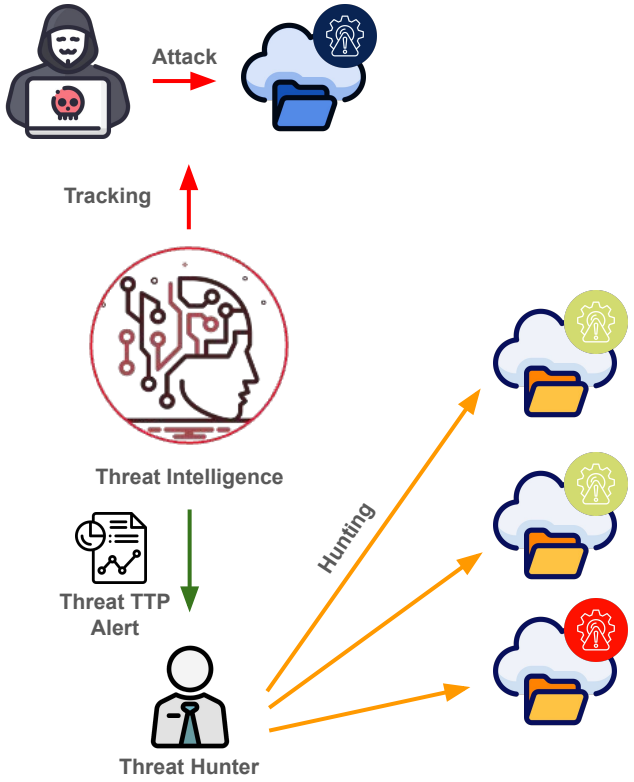


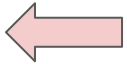

Image generated by Microsoft Copilot.

THREAT INTELLIGENCE IN INCIDENT RESPONSE

INCIDENT RESPONSE IN CLOUD ENVIRONMENTS

Challenges of Incident Response in Cloud-Native Environments

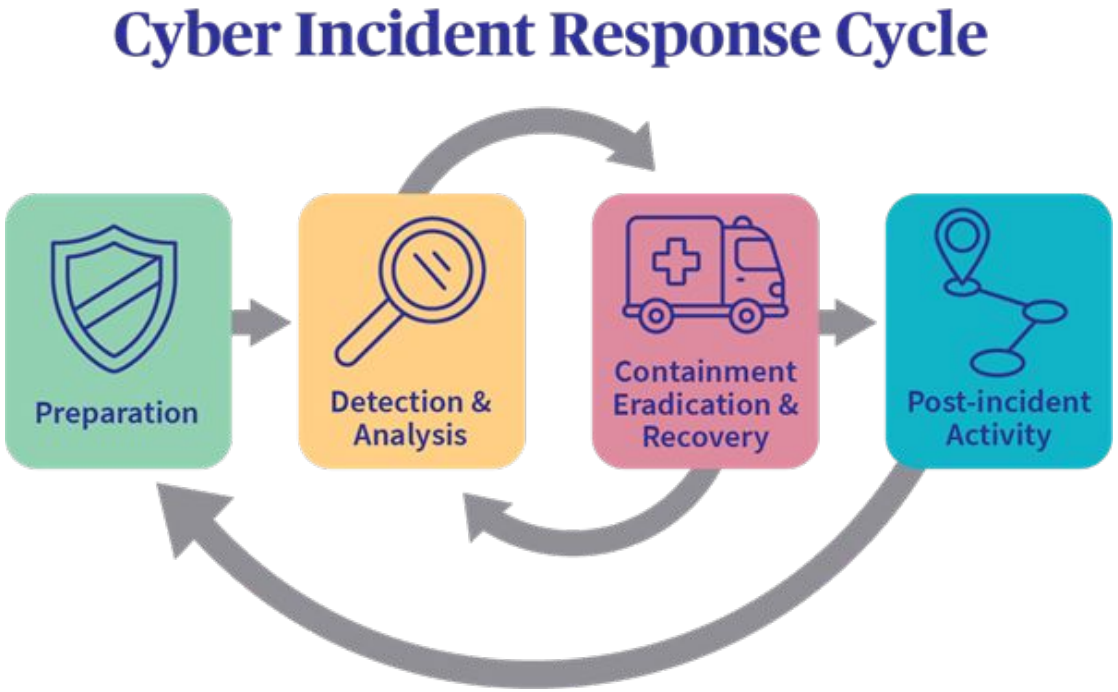
- Distributed systems make it harder to track and contain security incidents across multiple cloud services.
- Lack of visibility into cloud workloads, APIs, and third-party integrations delays threat detection.
- Dynamic scaling complicates forensic analysis, as logs and compromised resources may disappear quickly.



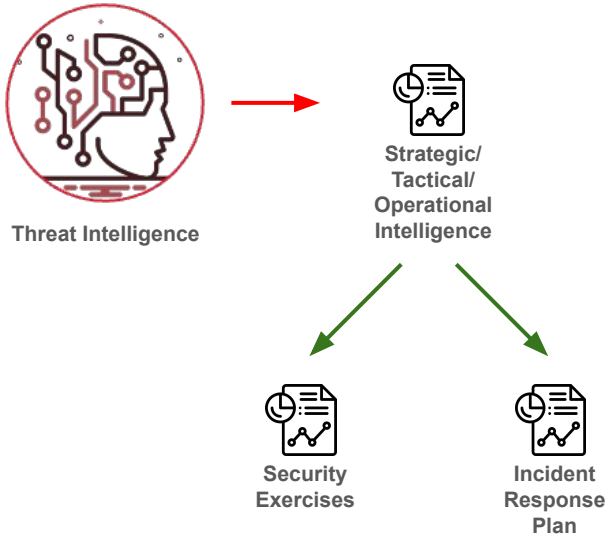
Role of Threat Intelligence (TI) in Addressing These Challenges

- TI provides real-time insights into emerging threats, improving visibility across cloud environments.
- By analyzing attack patterns and Indicators of Compromise (IoCs), TI accelerates threat detection.
- Automated TI integration enhances incident response, enabling faster containment and remediation of threats.

INCIDENT RESPONSE LIFE-CYCLE



PREPARATION PHASE



Using TI to Build Readiness

- **Developing cloud-specific playbooks** ensures incident response teams follow standardized procedures for cloud threats.
- **Identifying likely threats** helps tailor security defenses to real-world attack scenarios and emerging risks.

Example: Leveraging TI to Simulate Cloud-Native Attack Scenarios for Tabletop Exercises

- **Threat Intelligence provides real-world attack data** to create realistic cloud security incident simulations.
- **Tabletop exercises test response strategies**, helping teams improve detection and mitigation of cloud-based threats.

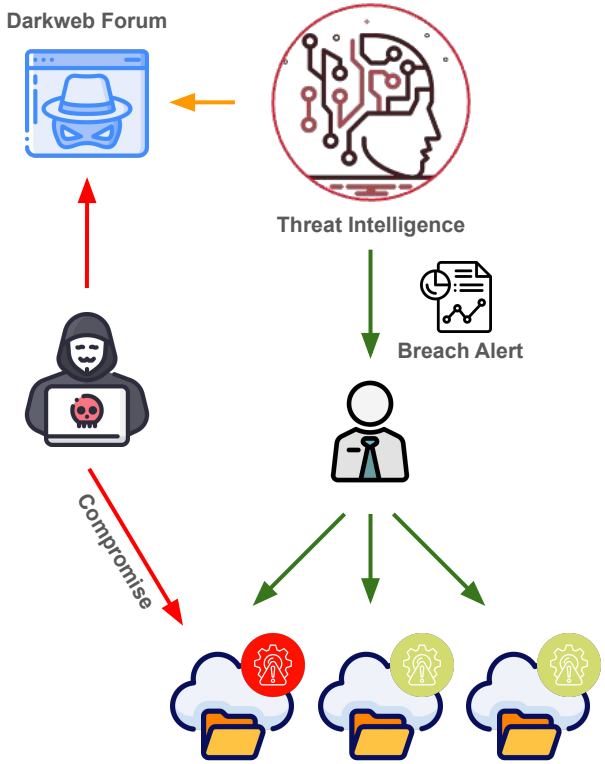
DETECTION AND ANALYSIS

How TI Accelerates Detection

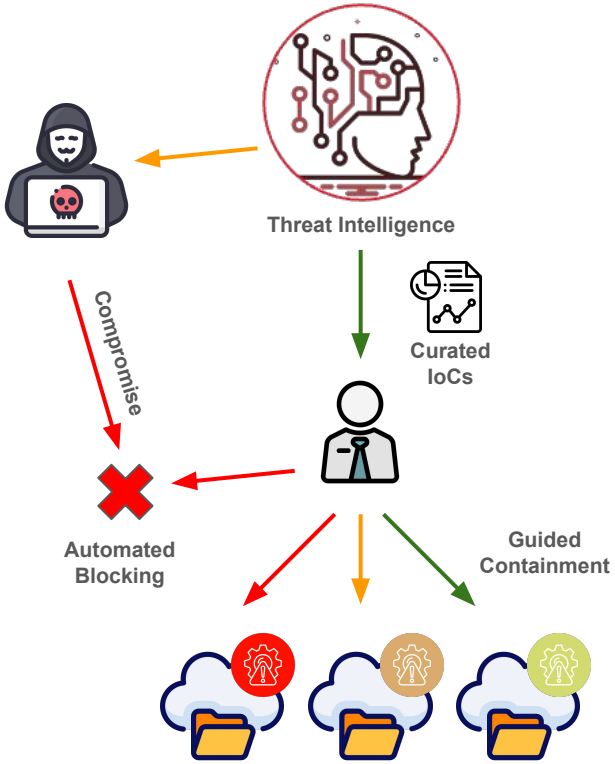
- **Threat Intelligence helps identify Indicators of Compromise (IoCs)** related to cloud-specific attack patterns.
- **TI enriches security alerts with real-time context**, linking threats to known attacker behaviors.
- **By analyzing IoCs and attack trends, TI enables faster detection** of malicious activity in cloud environments.

Case Study: Using TI to Detect an Active Exploitation of Cloud Storage Misconfigurations

- **A misconfigured cloud storage bucket exposed sensitive data**, making it vulnerable to unauthorized access.
- **TI detected hacker discussions on underground forums**, indicating active exploitation of similar misconfigurations.
- **Security teams received early warnings and secured the storage**, preventing data breaches before exploitation.



CONTAINMENT STRATEGIES WITH TI



Guiding Containment Decisions

- Threat Intelligence helps prioritize high-impact threats, ensuring critical incidents are addressed first.
- IoCs and TTPs provide actionable insights, enabling security teams to contain threats efficiently.
- In cloud environments, TI helps limit lateral movement, preventing attackers from spreading further.

Example: Isolating Affected Workloads and Blocking Malicious IPs Using Real-Time TI

- TI identifies malicious IPs communicating with compromised cloud workloads, enabling rapid response.
- Security teams use TI to isolate affected virtual machines, stopping further damage or data theft.
- Automated blocking of malicious IPs prevents reinfection and strengthens overall cloud security.

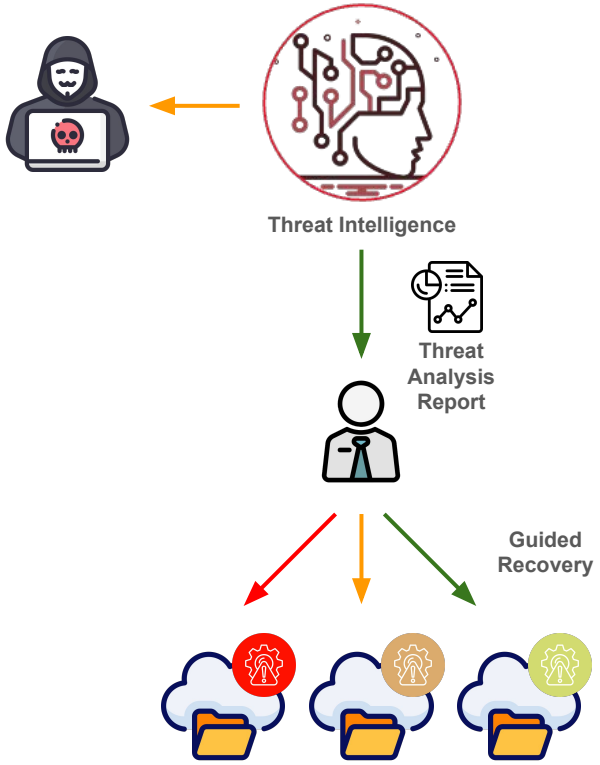
ERADICATION AND RECOVERY

Using TI to Guide Cleanup and Recovery Efforts

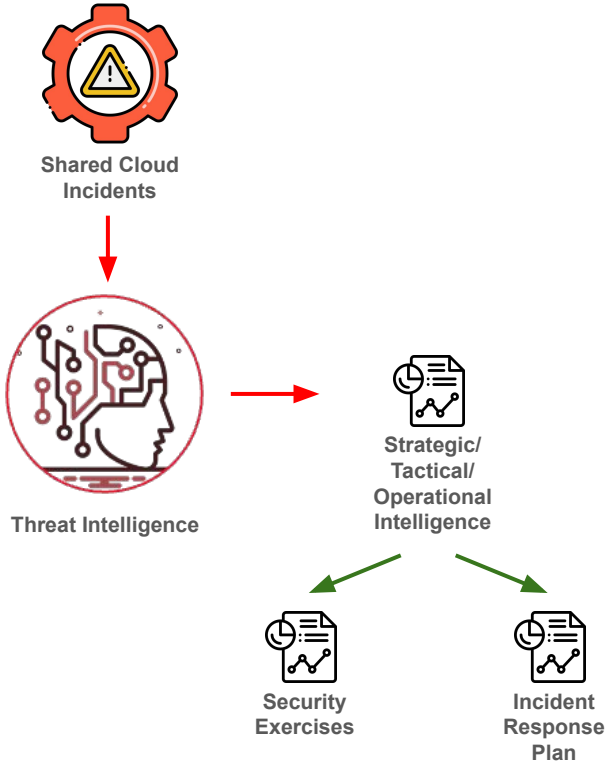
- Threat Intelligence helps identify the root cause of incidents, ensuring effective remediation.
- Analyzing attacker tactics provides insights into associated threats and potential lingering risks.
- Closing known vulnerabilities highlighted by TI prevents reinfection and strengthens cloud security.

Example: Recovering from Ransomware Attacks Targeting Cloud Backups with TI-Driven Guidance

- TI detects ransomware campaigns targeting cloud storage, enabling early mitigation strategies.
- Security teams use TI insights to identify compromised backups, preventing further data loss.
- Applying TI-driven recovery plans ensures system restoration without reinfecting cloud environments.



POST-INCIDENT ACTIVITY



Improving Future Defenses with TI

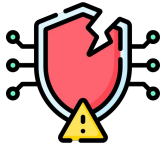
- New Indicators of Compromise (IoCs) from past incidents enhance threat detection capabilities.
- Lessons learned help refine security policies and improve cloud incident response strategies.
- Updating cloud security configurations ensures stronger defenses against similar future attacks.

Example: Sharing IoCs with Industry Peers and Leveraging TI-Sharing Platforms

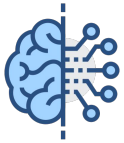
- Organizations share newly discovered IoCs to help industry peers detect emerging threats early.
- Threat Intelligence-sharing platforms provide real-time updates on evolving attack techniques.
- Collaborative TI-sharing strengthens cloud security by improving industry-wide threat awareness.

STRATEGIES FOR INTEGRATING CTI IN CLOUD SECURITY

CLOUD-FOCUSED THREAT DATA COLLECTION



Identify emerging threats in cloud environments by continuously monitoring vulnerabilities, misconfigurations, and attack patterns across APIs, containers, and serverless services to detect potential risks before exploitation occurs.



Gather real-time intelligence from multiple sources including security feeds, threat-sharing platforms, cloud provider telemetry, and underground forums to track malicious activities targeting cloud-based infrastructure.

Analyze and correlate attack trends by examining Indicators of Compromise (IoCs) and Tactics, Techniques, and Procedures (TTPs) used in cloud attacks to enhance proactive defense strategies.

AUTOMATING THREAT INTELLIGENCE PROCESS

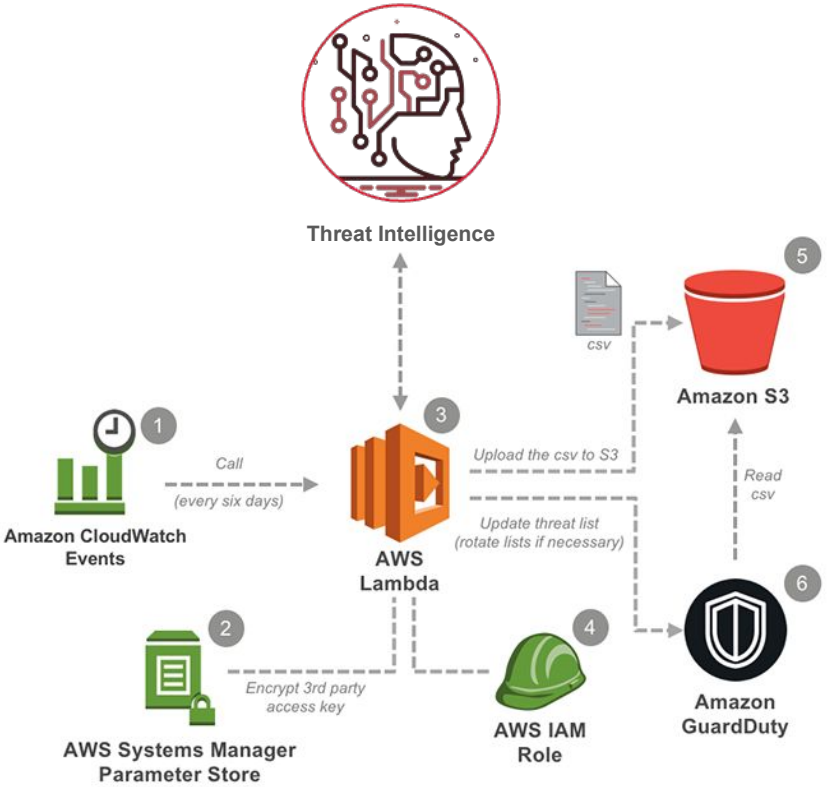
Automating Threat Intelligence Process

- **Automate threat data ingestion** to collect real-time intelligence from multiple sources, reducing manual effort and response time.
- **Use AI and machine learning** to analyze threats, detect patterns, and prioritize risks in cloud environments efficiently.
- **Automate threat distribution** by integrating intelligence feeds with security tools for faster incident response and mitigation actions.

Tools for automation

- Threat Intelligence Platforms (TIPs).
- Integration with cloud-native tools (e.g., AWS Security Hub, Azure Sentinel).

INTEGRATING TI WITH CLOUD SECURITY TOOLS



Cloud-Native Security Tools Enhanced by TI:

- CSPM (Cloud Security Posture Management): Continuous monitoring of cloud configurations for vulnerabilities.
- CWPP (Cloud Workload Protection Platforms): Threat detection for containers, virtual machines, and serverless environments
- SIEM/SOAR: Real-time threat monitoring and automated response workflows.
- ***Practical example:*** Enhancing AWS GuardDuty or Azure Defender with TI feeds.

METRICS FOR MEASURING THE SUCCESS OF TI INTEGRATION

Reduction in False Positives and Response Times

- *Measurement*: Compare the percentage of false alerts before and after implementing TI-driven filtering. Track MTTD and MTTR.

Number of Threats Detected or Mitigated Through TI

- *Measurement*: Count security incidents detected, blocked, or mitigated using TI-driven alerts and automation.

Improved Compliance with Security Frameworks (e.g., NIST, ISO 27001)

- *Measurement*: Track adherence to security policies, audit results, and incident reports related to compliance gaps.

Threat Intelligence Accuracy and Actionability

- *Measurement*: Evaluate how many IoCs and threat reports lead to actual detections or security actions.

Effectiveness of Automated Threat Intelligence Integration

- *Measurement*: Measure the percentage of security alerts enriched with TI, leading to automated response actions.

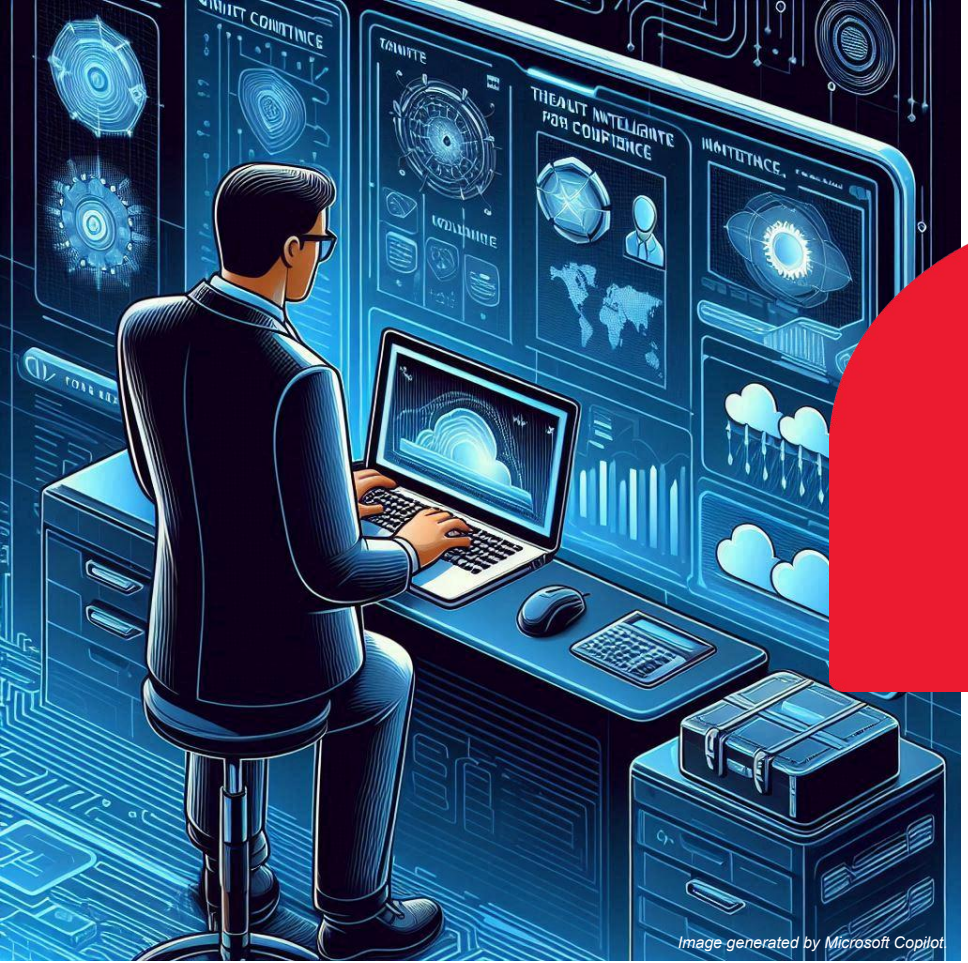


Image generated by Microsoft Copilot

CONCLUSION

KEY TAKEAWAYS

Threat Intelligence Strengthens Cloud Security Posture

Helps identify, analyze, and respond early to threats in cloud environments.

Proactive Risk Management is Essential

Leveraging Threat Intelligence to assess risks, detect vulnerabilities, and safeguard systems before attacks occur.

Incident Response Must Be Intelligence-Driven

Integrating Threat Intelligence into incident response processes enables faster detection, efficient mitigation, and minimized impact.

Automation and Integration Improve Efficiency

Embedding Threat Intelligence into cloud security tools (SIEM, SOAR, etc.) enhances automation and optimizes security workflows.

Continuous Adaptation is Crucial

The threat landscape is constantly evolving, requiring organizations to update intelligence, share insights, and refine cloud security strategies regularly.

QUESTION & ANSWER

viettel
security

Thank you

For attention!