增強網路防禦的關鍵策略 Understanding CTI Implementation to Strengthen Cyber Defense

解析網絡安全情報的實施:

Frankie Wong

CTI - Cyber Threat Intelligence

#### Who am I

Mr. Frankie Wong (GCTI, GCFA, GCFR, CISSP, CISA)

- Executive Committee Member of Cyber Security Specialist Group Hong Kong Computer Society
- 10+ year cyber security experience
- SOC / IR / CTI in Cybersecurity
- Web application / Mobile application

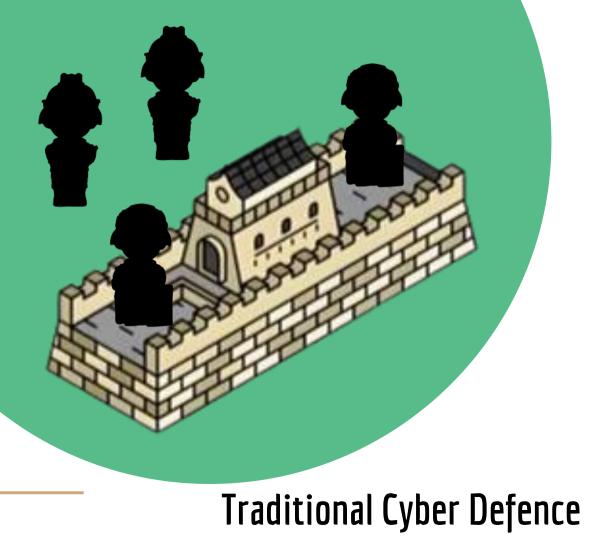


#### Agenda

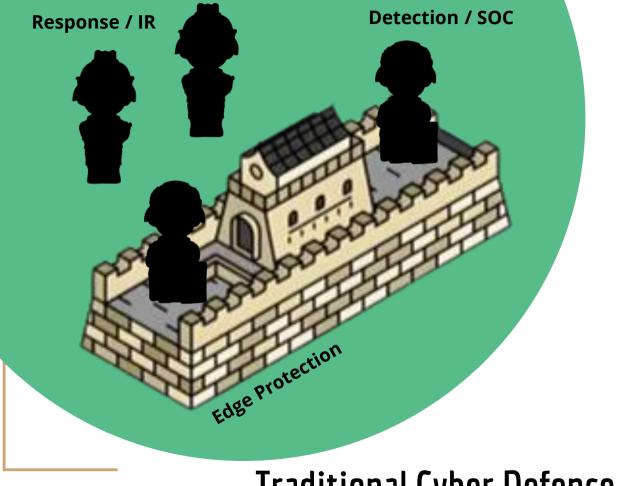
- Cyber Threat Intelligence (CTI)
  - What-is
  - CTI Operations
  - Use Case
- Security Operations Centre (SOC)
  - Functions, Roles & Operations
- Intelligence-driven SOC



# Cyber Threat Intelligence (CTI)



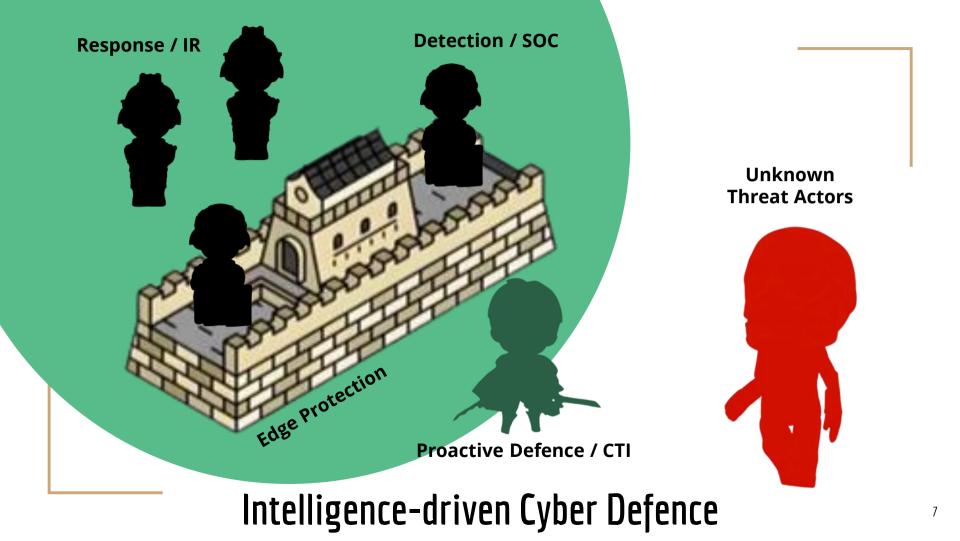




Unknown Threat Actors



#### **Traditional Cyber Defence**



### What is Intelligence

History

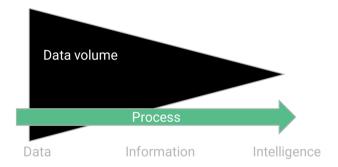
- Intelligence for Military
- Information with Action

Data > Information > Intelligence

• Raw data > Informative > Actionable

Forms of Intelligence

• HUMINT, SIGINT, GEOINT, SOCMINT, OSINT



## Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence != Anything found on the Internet

Threat Intelligence != IOC Feed

- Define roles and functions
- Scoping of intelligence  $\rightarrow$  Cyber Threats
- Objectives
  - Proactive Defense
  - Enhance Incident Response
  - Informed Decision Making



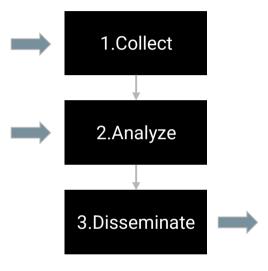
# Cyber Threat Intelligence (CTI) Operations

# 6 Stages CTI Life Cycle



#### **CTI** Operations

- 1. Data Collection
  - Security blogs/articles, Social media
  - Dark Web
  - Intel Sharing Platforms
- 2. Analysis and Correlation
  - Technical understanding + OSINT tools
  - Review Internal Controls against External Threats
- 3. Dissemination
  - Data feeds, e.g. IOC
  - Threat Intelligence Records, e.g. CVE, TTPs
  - Threat Intelligence Reports, e.g. Contextual analysis with Suggestions



# [1] CTI Monitoring / Collection

- Continuous monitoring 24/7?
- Scope of monitoring
  - Cyber Threats
  - Adversaries vs. Targets
  - Digital Risk Protection, including clear net, dark web, social media, etc.
- Tools
  - Feed aggregator
  - Intelligence platforms, including OS TIP, commercial TIP, sharing platform
  - Email subscription



# [2] CTI Process and Analysis

#### • Tactical

- Normalization for Data Feed, e.g. IOC
- Enrichment, e.g. GeoInfo, confidence level
- Action: immediate detection or blocking

#### • Tools

- TIP
- IP / domain enrichment service
- Sandbox



# [2] CTI Process and Analysis

- Operational
  - Understand the attack path and TTPs
  - Leverage
    - Diamond model
    - Cyber Kill Chain
    - MITRE ATT&CK framework
  - Action: vulnerability patching, use case tuning, threat hunting
- Tools
  - Any analysis tools + CTI Analyst



# [2] CTI Process and Analysis

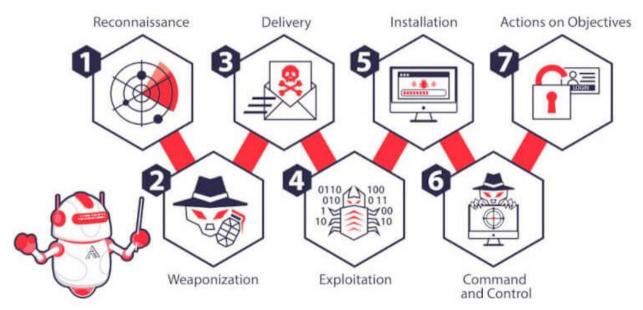
#### • Strategic

- Contextualize the attacks (incidents)
- Understanding threat actors, and targets (victims)
- Threat landscape / Security trends
- Action: provide high-level overview for decision making
- Tools
  - CTI Analyst + Experience



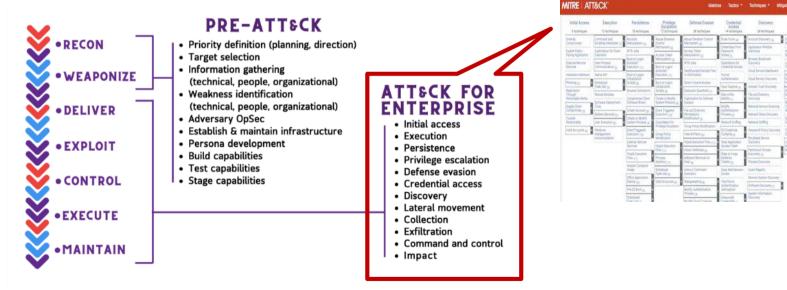
## [2a] CTI Analysis - Cyber Kill Chain

• Developed by Lockheed Martin, the Cyber Kill Chain® framework is part of the **Intelligence Driven Defense® model** for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.



### [2b] CTI Analysis - MITRE ATT&CK framework

• The MITRE ATT&CK Framework is a knowledge base of adversary **tactics** and **techniques** used to enhance cybersecurity defenses against threats.



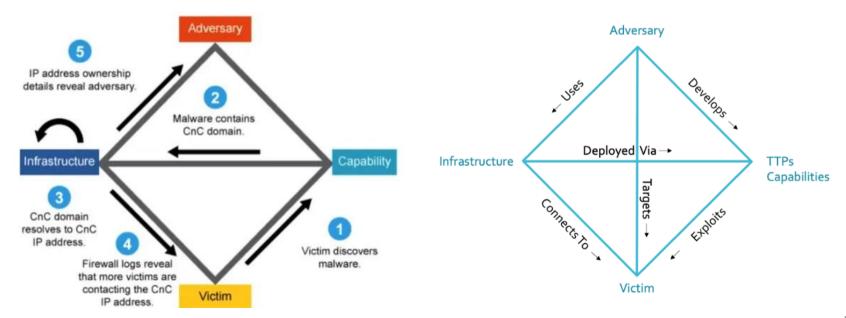
#### [2b] CTI Analysis - MITRE ATT&CK framework (cont.)

	Initial Access	Execution	Persistence	Privilege Escalation	Detense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exhibitration
C	Drive-by Compromise	( PowerShell )	bash_profile and .bashrc	Process Injection	Process Injection	Account Manipulation	(Account Discovery)	(Windows Admin Shares)	Audio Capture	Web Service	Automated Exfittration
- 1	Exploit Public-Facing Application	Scheduled Task	Accessibility Features	Access Token apripulation	Access Token Manipulation	Bash History	Application Window Discovery	AppleScript	Automated Collection	CommonlyUsed Port	Data Compressed
Est	ternal Remote Services	Windows Managements	Account Manipulation	Accessibility Features	Application Access Token	Brite orce	Browser Bookmark Discovery	Application Access Token	Clipboard Data	Communication Through	Data Encrypted
13	Hardware Additions	AppleScript	AppCert DLLs	AppCert DLLs	Binary Padding	Cloud instance Metadata API	Cloud Service Dashboard	Application Deployment Software	Data from Cloud Storage Object	Connection Proxy	Data Transfer Size Limits
	Replication Through Removable Media	CMSTP	AppInit DLLs	Appinit DLLs	BITS Jobs	Credential Dumping	Cloud Service Discovery	Component Object Model and Distributed CDM	Data from Information Repositories	Custom Command and Control Protocol	Exhibitration Over Alternation Protocol
Spo	earphishing Attachment	Command-Line Interface	Application Shimming	Application Shimming	Bypass User Account Control	Credentials from Web Browsers	Domain Trust Discovery	Exploitation of Remote Services	Data from Local System	Currom Cryptographic Protocol	Exfiltration Over Comman and Control Channel
	Spearphishing Link	Compiled HTML File	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Files	File and Directory Discovery	Internal Spearphishing	Data from Network Shared Drive	Data Encoding	Exfiltration Over Other Network Medium
Sp	earphishing via Service	Component Object Model and Distributed COM	BITS Jobs	DLL Search Order Hijacking	CMSTP	Credentials in Registry	Network Service Scanning	Logon Scripts	Data from Removable Media	Data Obfuscation	Exfiltration Over Physica Medium
Sup	oply Chain Compromise	Control Panel Items	Bootkit	Dylib Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Hagh	Data Stated	Domain Fronting	Scheduled Transfer
1	Trusted Relationship	Dynamic Data Exchange	Browser Extensions	Elevated Execution with Prompt	Compile After Delivery	Forced Authentication	Network Sniffing	Pass the ficket	Email Collection	Domain Generation Algorithms	Transfer Data to Cloud Account
	Valid Accounts	Execution through AP1	Change Default File Association	Emond	Compiled HTML File	Hooking	Password Policy Discovery	Remote Desktop Protocol	Input Capture	Fallback Channels	
		Execution through Module	Component Firmware	Exploitation for Privilege Escalation	Component Firmware	Input Capture	Peripheral Device Discovery	Remote File Copy	Man in the Browser	Multi-hop Proxy	
6		Exploitation or Client Exert on	Component Object Model Hijacking	Extra Window Memory Injection	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Remote Services	Screen Capture	Multi-Stage Channels	
ľ		Cophicat	Create Account.	Tile System Permissions Wookness	Connection Praxy	Nethemasting	Process Discovery	Replication Through Removable Media	Video: Capture	Multiliand Communication	
5		K ( <b>1</b> )									
S											

...

#### [2c] CTI Analysis - Intrusion Diamond Model

• The Diamond Model of Intrusion Analysis is a framework that analyzes cyber intrusions by mapping **adversaries**, **infrastructure**, **capabilities**, and **targets**.



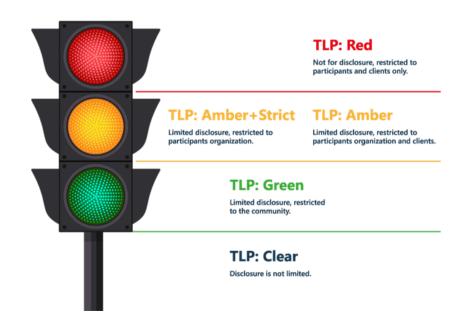
#### [3] CTI Dissemination

- Leverage TIP for tactical intelligence (automation + API)
- Distribute the intelligence to corresponding stakeholders
- Sample of Context
  - TLP (level of sharing)
  - Summary
  - Impact
  - Analysis
    - Adversaries, Targets, Capability, In-depth Malware Analysis, etc.
  - Recommendation
  - References
  - Appendix (e.g. IOC, TTPs)



## [3a] Traffic Light Protocol - TLP

• The Traffic Light Protocol (TLP) is a framework for sharing sensitive cyber intelligence, using colorcoded labels to indicate **sharing restrictions**.



#### **CTI** Cooperation

- Security Operations Centre (SOC) / SIEM
  - Threats detection IOC level
  - Preventive controls
- Incident Response (IR)
  - TTPs study
  - Threat Actor Profiling
  - Extending detection and prevention
- Threat Hunting (TH)
  - Proactive defense
  - Making use of external observations
- Cyber Risk and Awareness



## Challenges

**Common Challenges** 

- Data overloaded and Integrations
- Communications
- False alerts/ misinformation

Solutions?

- Automation Process / IOC level
- AI Context level
- Collaboration with external entities



# Cyber Threat Intelligence (CTI) Use Case

#### Use Case

[Sept 2023] Cyberport incident

When you are notified about this incident, you may have some questions that arise, such as...

- Are we also affected in the this incident?
- Are we well protected from the attack?



#### Use Case

[Sept 2023] Cyberport incident

- Information gathering ← news reader
  - $\circ \rightarrow$  Data breach ~400G data, Ransomware Trigona
- Analysis and correlation:
  - $\circ \rightarrow \text{Trigona}$ 
    - What's the initial access, CVE, TTPs, etc.?
    - Recent attacks? IOC for detection?
  - $\circ \rightarrow \mathsf{DLS}$ 
    - Data accessible? Download and study the leaked data.



Use Case

[Sept 2023] Cyberport incident

- Dissemination
  - $\circ$  IOC collection  $\rightarrow$  SOC for backward search and detection
  - $\circ$  TTPs  $\rightarrow$  SOC for building use cases/ detection rules
  - $\circ$  CVE  $\rightarrow$  vuln. mgt. team for evaluation
  - $\circ$  Contextual study  $\rightarrow$  security awareness team for broadcasting
  - $\circ$  Leaked data  $\rightarrow$  IR for handling
  - Comprehensive threat analysis study on both the Attacks & Controls sides and providing recommendations if a strategic solution is available.



# Security Operations Centre (SOC)

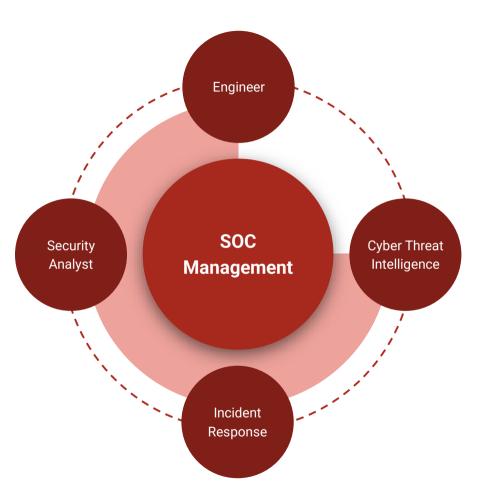
#### What is Security Operations Centre

- A Security Operations Center (SOC) is a dedicated team that **monitors**, **detects**, and **responds** to cybersecurity threats in realtime.
  - Continuous monitoring of security events
  - Incident detection and response
  - Threat intelligence integration



#### SOC Functional teams

- Engineer
- Security Analyst (tier 1)
- Security Analyst (tier 2)
- Incident Response (tier 3)
- Cyber Threat Intelligence



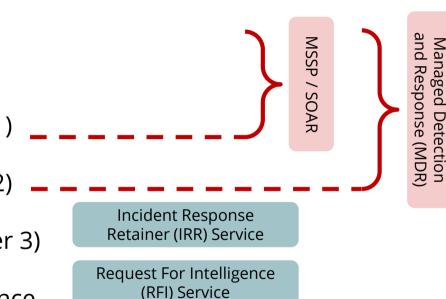
#### SOC Roles and Operations

- Engineer
  - Managing Log collection, SIEM, SOAR, TIP, Ticketing System, etc.
- Security Analyst (tier 1) Triage
  - Alerting
- Security Analyst (tier 2) Analysis
  - Understanding the threat and initial investigation
- Incident Response (tier 3)
  - Investigation, Containment, and Recovery
- Cyber Threat Intelligence
  - Understand and mitigate both external threats and internal vulnerabilities



#### Modern Hybrid SOC

- Engineer
- Security Analyst (tier 1)
- Security Analyst (tier 2)
- Incident Response (tier 3)
- Cyber Threat Intelligence



### SOC Operating and Procedures

- SOC leverages documents to enhance their operational efficiency and response capabilities.
  - Standard Operating Procedures (SOP)
    - E.g. Log Onboarding, Use Case Management
  - Incident Playbooks
    - How analysts/SOAR performs an investigation
  - Incident Response Plan (IRP)
    - How to respond to a confirmed incident, including containment, communication, recovery, etc.

# **Intelligence**-driven Security Operations Centre (SOC)

### Intelligence-driven SOC

- Traditional SOC ← Incident-driven, Reactive
- Intelligence-driven SOC approach enables SOC teams to implement **proactive**

#### threat detection and prevention strategies.

- Provide a direction of SOC, according to the latest threat landscape
- Understand your potential adversaries and TTPs
- Observe 0-day vulnerabilities and discussion
- Understand latest trends of RaaS, MaaS, PHaaS
- Monitoring potential incidents from Third-party vendors
- Monitoring deep dark web (DDW), i.e. leaked credentials

**Goal**: Kill the cyber chain before the attack.

### Intelligence-driven SOC

- Benefits of a Proactive Defense Approach
  - Efficient resource utilization
    optimizing security efforts and investments
  - Adaptability to Emerging Threats
    flexible in response to change
  - Enhanced Incident Response
    effectively to security incidents, reducing response times and minimizing impact



#### **Q & A** Thank you

#### Frankie Wong

m.me/fankewong