解析網絡安全情報的實施：
增強網路防禦的關鍵策略

Understanding CTI Implementation to Strengthen Cyber Defense

Frankie Wong

CTI - Cyber Threat Intelligence

Who am I

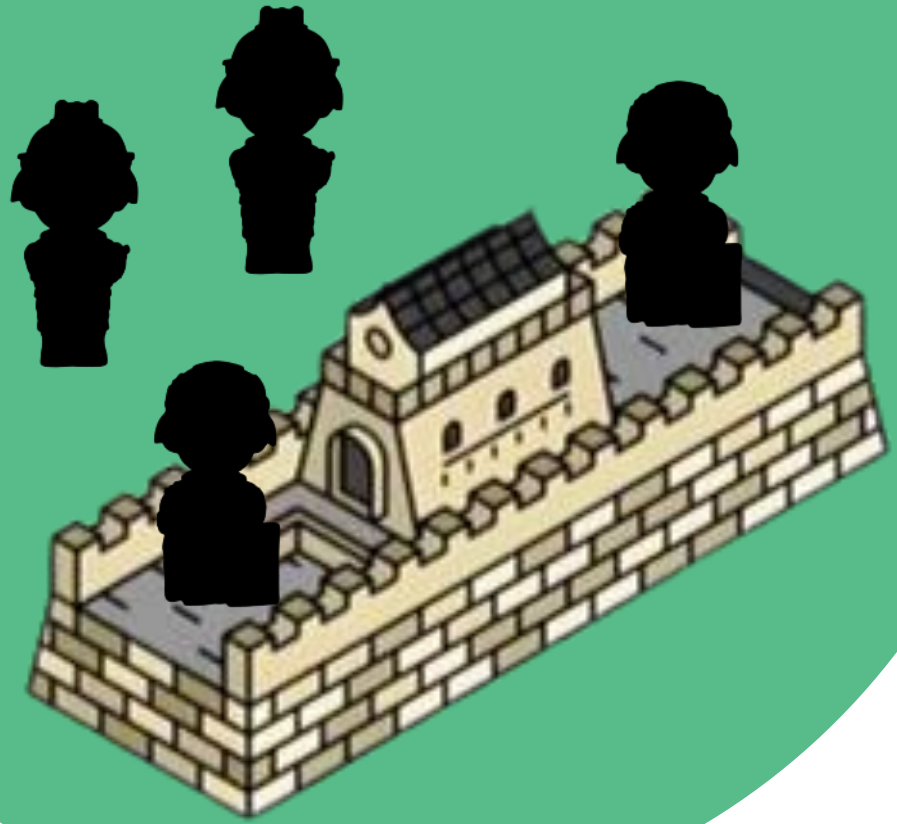
Mr. Frankie Wong (GCTI, GCFA, GCFR, CISSP, CISA)

- 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

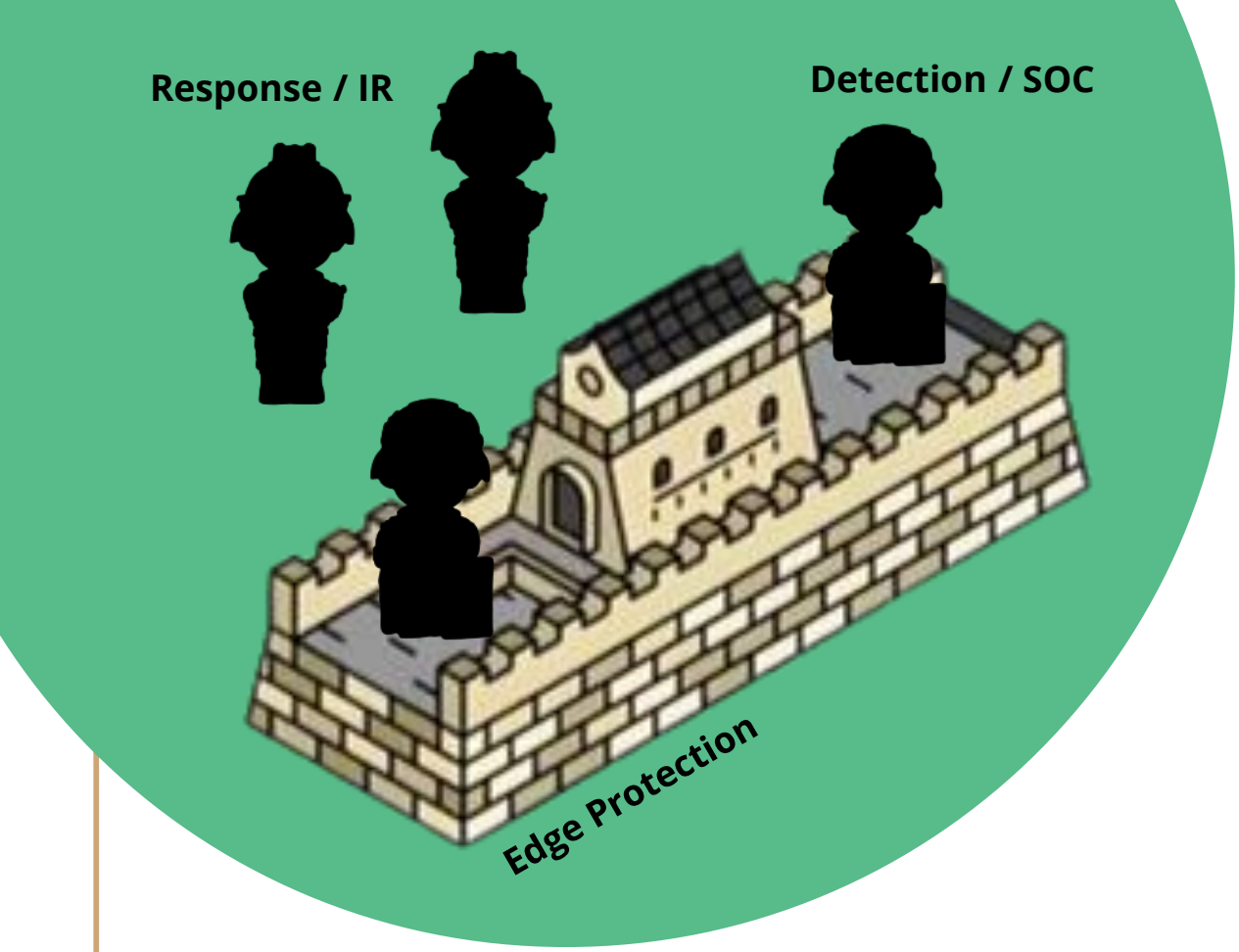
Agenda

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

Cyber Threat Intelligence (CTI)

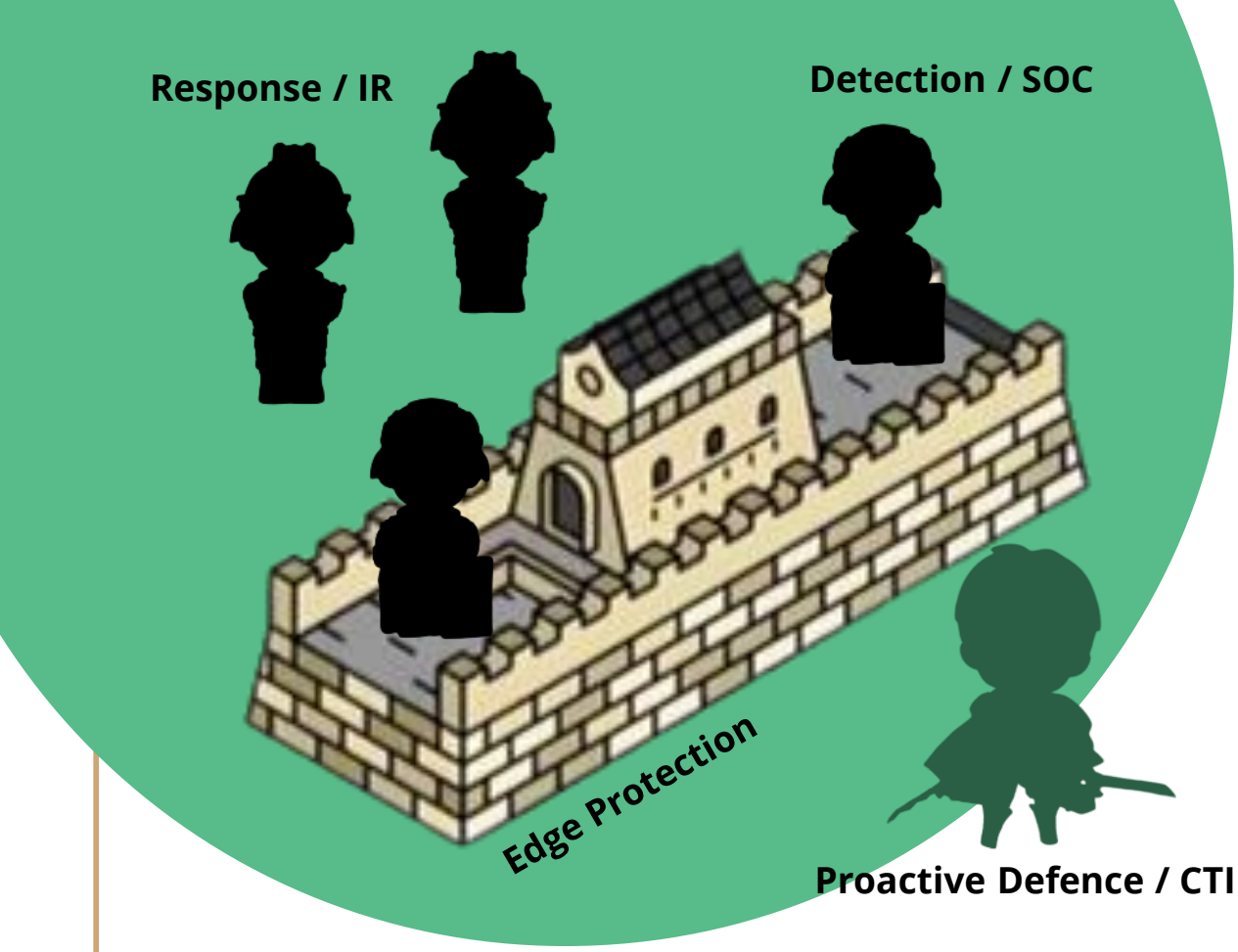


Traditional Cyber Defence



Unknown
Threat Actors

Traditional Cyber Defence



Unknown
Threat Actors

Intelligence-driven Cyber Defence

What is Intelligence

History

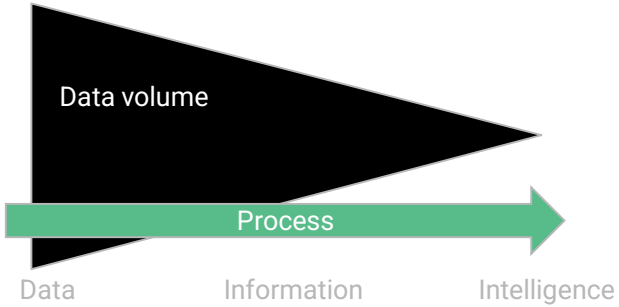
- Intelligence - for Military
- Information with Action

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 → Cyber Threats
- Objectives
  - Proactive Defense
  - Enhance Incident Response
  - Informed Decision Making

IOC - Indicator of Compromise

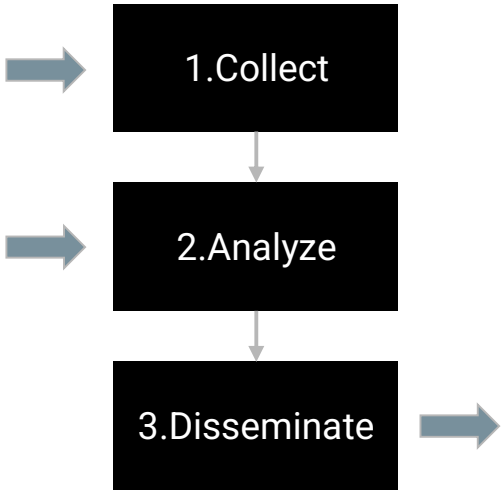
Cyber Threat Intelligence (CTI) Operations

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



CVE - Common Vulnerabilities and Exposures; TTPs - Tactics, Techniques, and Procedures

[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

TIP - Threat Intelligence Platform

[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

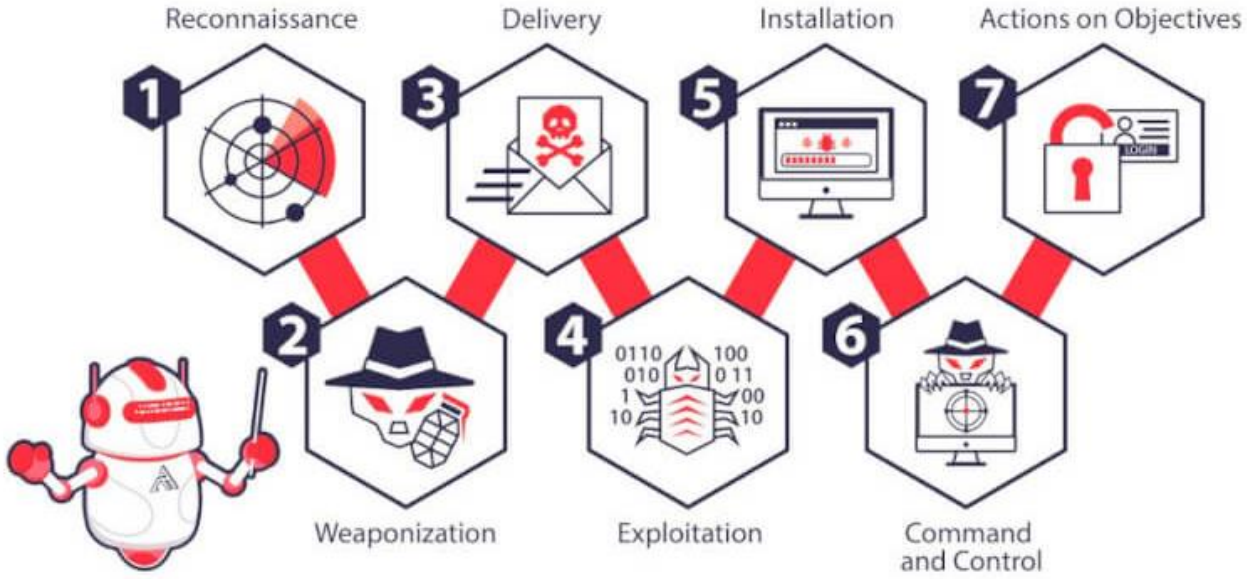
- Operational
  - Understand the attack path and TTPs
  - Leverage
    - Diamond model
    - Cyber Kill Chain
    - MITRE ATT&CK framework
  - Action: vulnerability patching, use case tuning, threat hunting
- Tools
  - Any analysis tools + CTI Analyst

[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

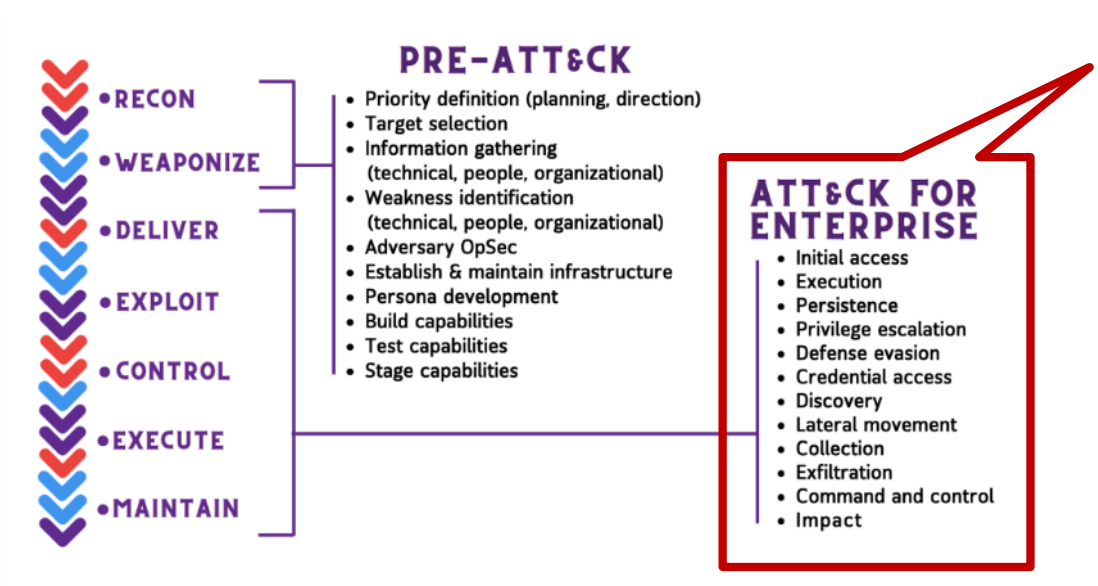
- Developed by Lockheed Martin, the Cyber Kill Chain® framework is part of the **Intelligence Driven Defense® model** for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.



Ref: https://www.cycraft.com/en/post/mitre20200701

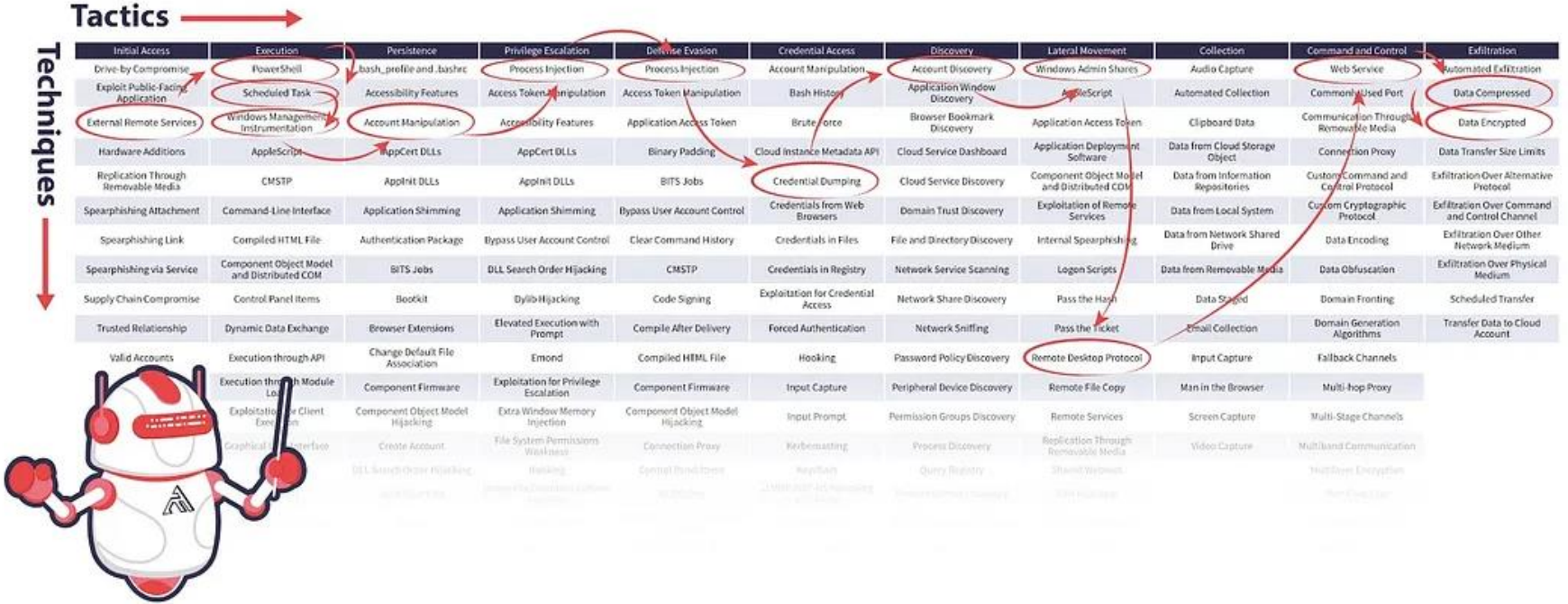
[2b] CTI Analysis - MITRE ATT&CK framework

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



Ref: https://attack.mitre.org/

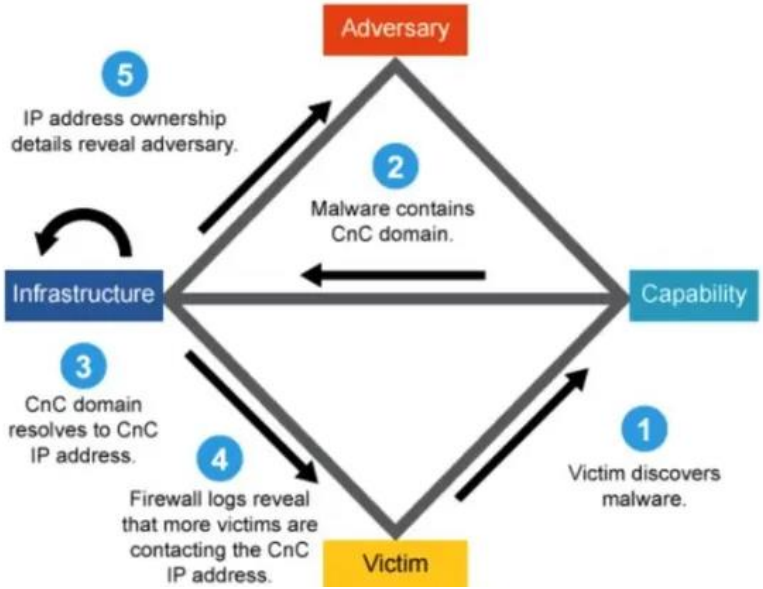
[2b] CTI Analysis - MITRE ATT&CK framework (cont.)

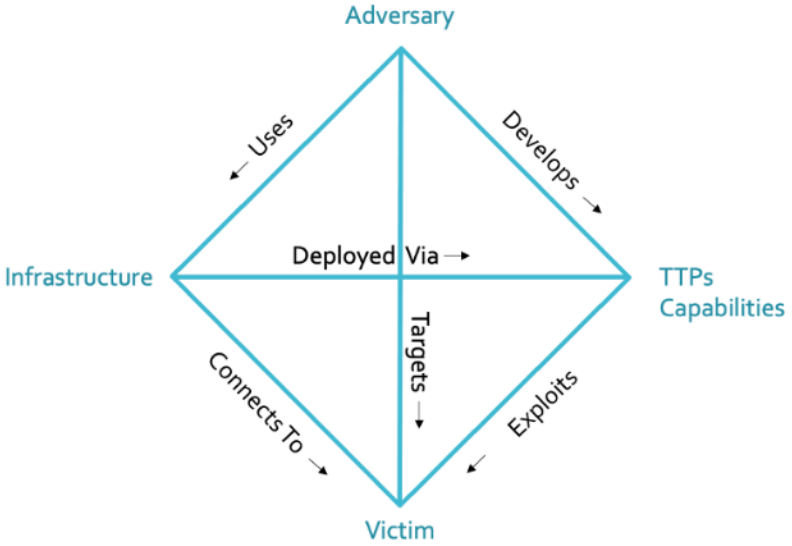


Ref: https://www.cycraft.com/en/post/mitre20200701

[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**.



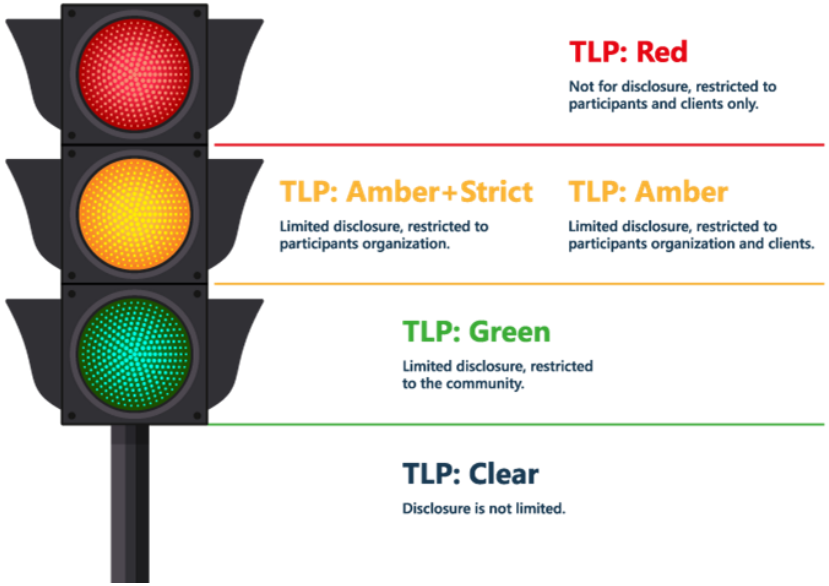


[3] CTI Dissemination

- 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 color-coded labels to indicate **sharing restrictions**.



Ref: https://www.first.org/tlp/

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
  - → Data breach ~400G data, Ransomware Trigona

- Analysis and correlation:
  - → Trigona
    - What's the initial access, CVE, TTPs, etc.?
    - Recent attacks? IOC for detection?
  - → DLS
    - Data accessible? Download and study the leaked data.

Use Case

[Sept 2023] Cyberport incident

- Dissemination
  - IOC collection → SOC for backward search and detection
  - TTPs → SOC for building use cases/ detection rules
  - CVE → vuln. mgt. team for evaluation
  - Contextual study → security awareness team for broadcasting
  - Leaked data → IR for handling

  - Comprehensive threat analysis study on both the Attacks & Controls sides and providing recommendations if a strategic solution is available.

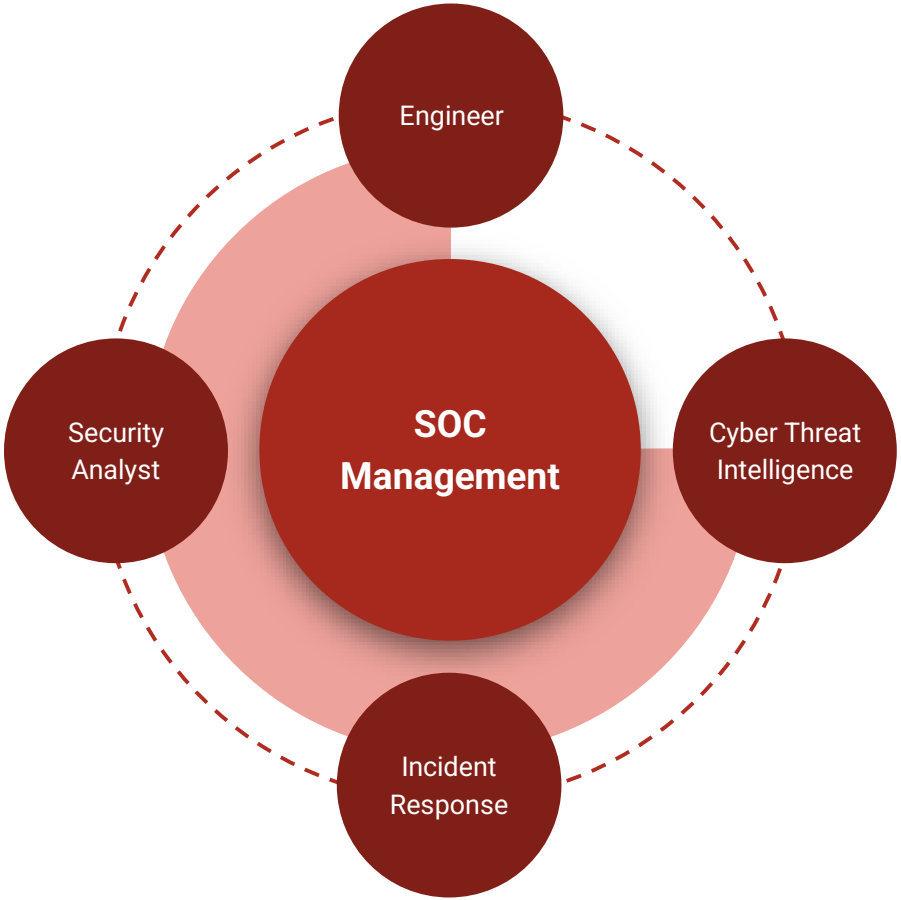
Security Operations Centre (SOC)

What is Security Operations Centre

- A Security Operations Center (SOC) is a dedicated team that **monitors**, **detects**, and **responds** to cybersecurity threats in real-time.
    - 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

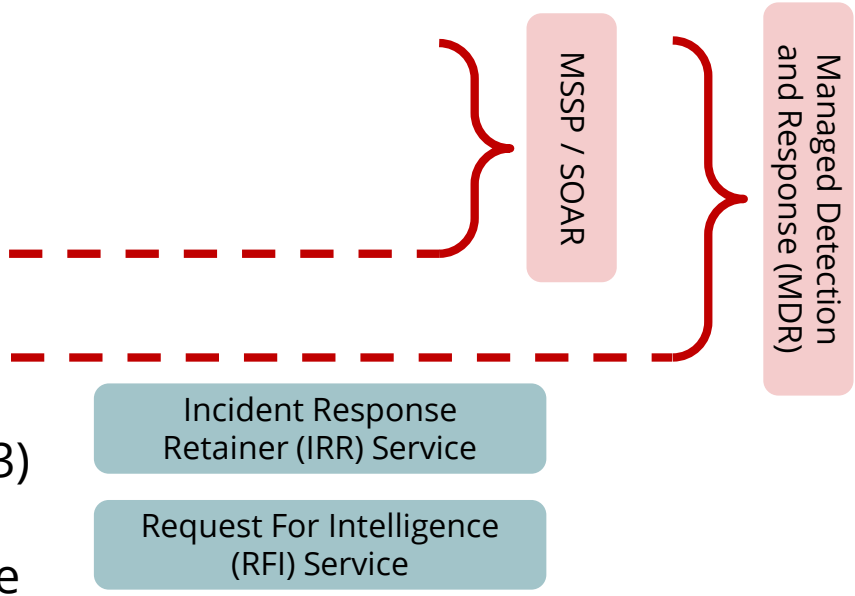
- Engineer
  - Managing Log collection, SIEM, SOAR, TIP, Ticketing System, etc.
- Security Analyst (tier 1) - Triage
  - Alerting
- Security Analyst (tier 2) - Analysis
  - Understanding the threat and initial investigation
- Incident Response (tier 3)
  - Investigation, Containment, and Recovery

Incident Escalation

- 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



MSSP - Managed Security Service Provider; SOAR - Security Orchestration, Automation and Response

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)

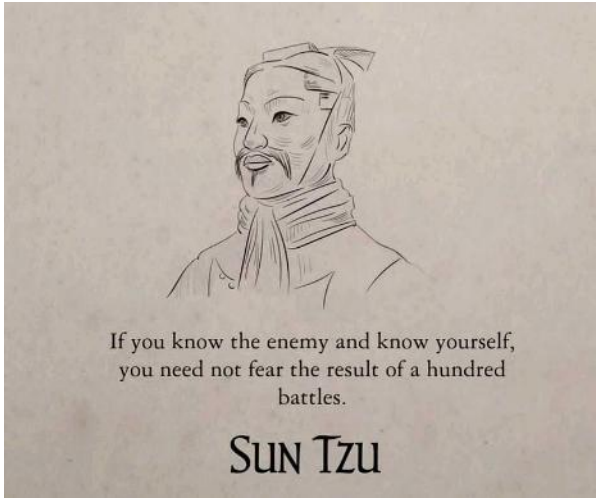
Intelligence-driven SOC

- 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



知己知彼 百戰不殆

先發制人

Q & A

Thank you

Frankie Wong

m.me/fankewong