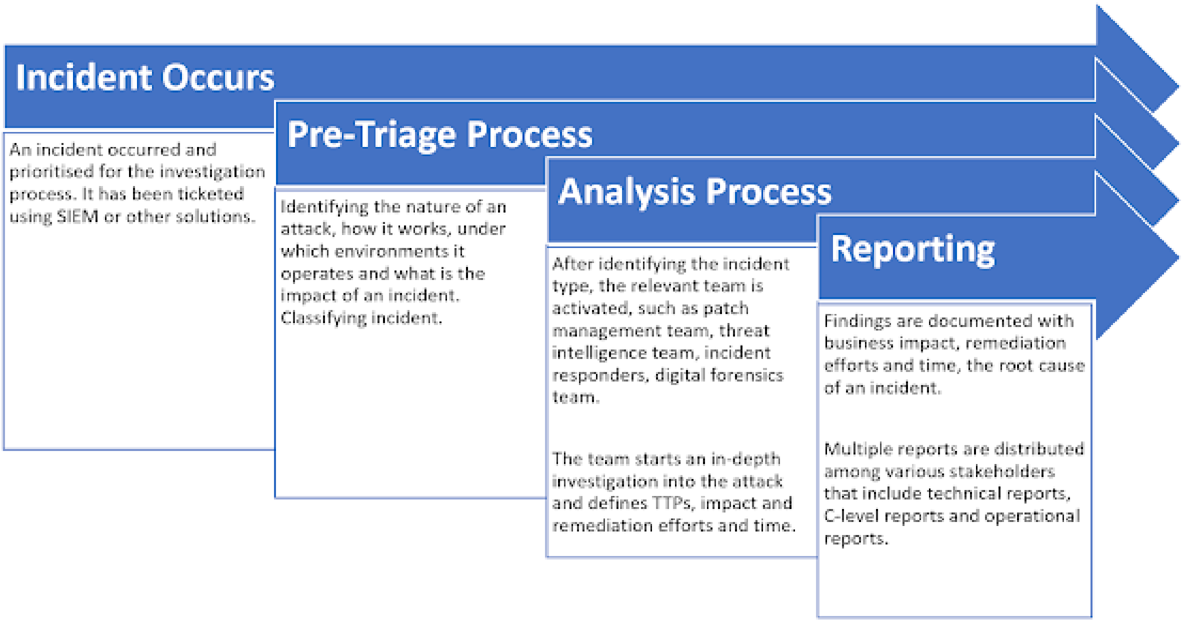
Integrate Threat Intelligence program into your daily security operations - Phase 3 - Effectiveness of the Analysis Process

In the previous three articles, we have gathered requirements of intelligence and formalised a process of collecting intelligence. It is now time to formalise processes for analysing anomalies using threat intelligence. Following diagram shows an overview of the analysis process and its phases.



Incident Occurs

An incident occurred and prioritised for the investigation process. It has been ticketed using SIEM or other solutions.

Pre-Triage Process

Identifying the nature of an attack, how it works, under which environments it operates and what is the impact of an incident. Classifying incident.

Analysis Process

After identifying the incident type, the relevant team is activated, such as patch management team, threat intelligence team, incident responders, digital forensics team.

The team starts an in-depth investigation into the attack and defines TTPs, impact and remediation efforts and time.

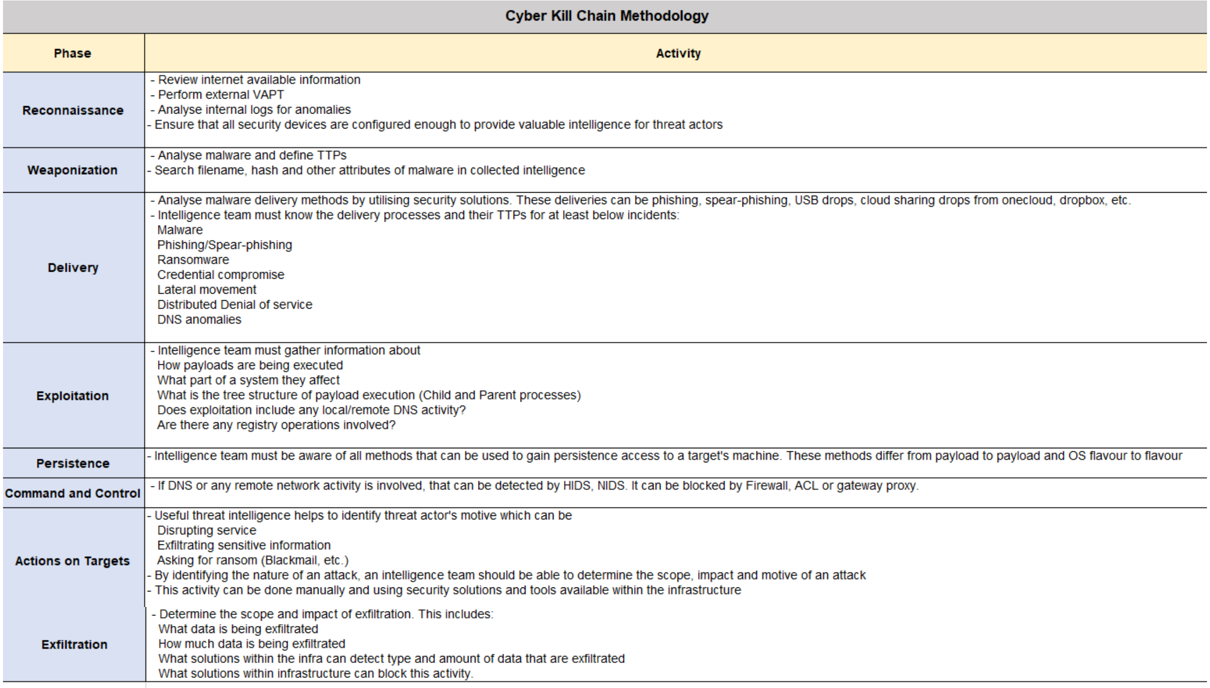
Reporting

Findings are documented with business impact, remediation efforts and time, the root cause of an incident.

Multiple reports are distributed among various stakeholders that include technical reports, C-level reports and operational reports.

Threat intelligence process must be aligned with the cyber kill chain methodology. Proactive intelligence involves many steps in each and every phase of the cyber kill chain methodology.

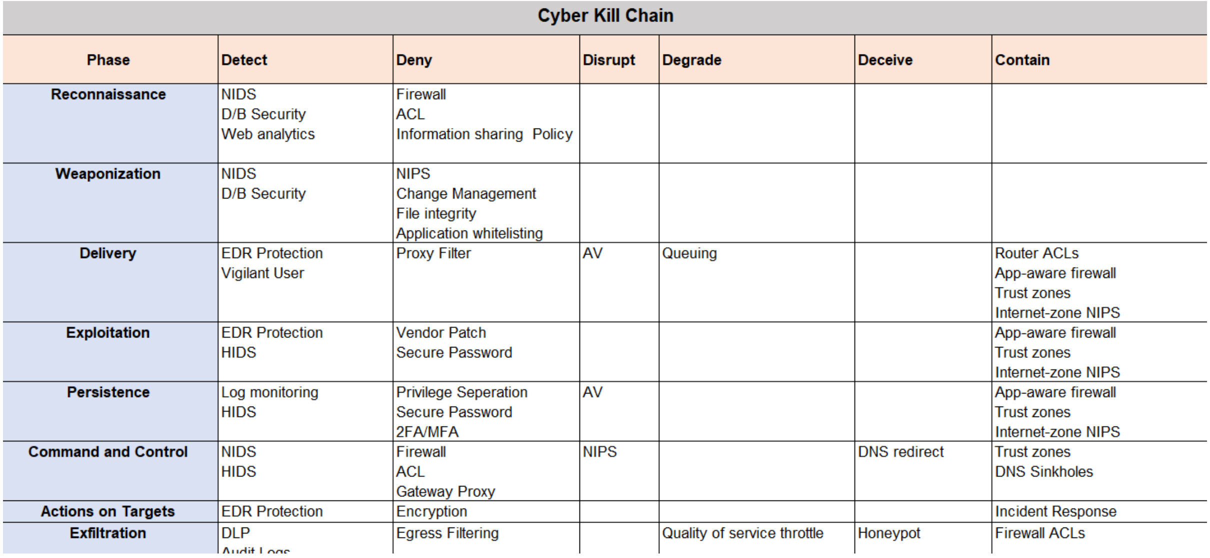
In this section, I will discuss how we can leverage threat intelligence by utilising the cyber kill chain methodology. Not only that, but I will also discuss various phases of incident response where we can utilise internal defences in order to align threat intelligence monitoring, detection and blocking process.



Cyber Kill Chain Methodology

Phase	Activity
Reconnaissance	- Review internet available information - Perform external VAPT - Analyse internal logs for anomalies - Ensure that all security devices are configured enough to provide valuable intelligence for threat actors
Weaponization	- Analyse malware and define TTPs - Search filename, hash and other attributes of malware in collected intelligence
Delivery	- Analyse malware delivery methods by utilising security solutions. These deliveries can be phishing, spear-phishing, USB drops, cloud sharing drops from onecloud, dropbox, etc. - Intelligence team must know the delivery processes and their TTPs for at least below incidents: Malware Phishing/Spear-phishing Ransomware Credential compromise Lateral movement Distributed Denial of service DNS anomalies
Exploitation	- Intelligence team must gather information about How payloads are being executed What part of a system they affect What is the tree structure of payload execution (Child and Parent processes) Does exploitation include any local/remote DNS activity? Are there any registry operations involved?
Persistence	- Intelligence team must be aware of all methods that can be used to gain persistence access to a target's machine. These methods differ from payload to payload and OS flavour to flavour
Command and Control	- If DNS or any remote network activity is involved, that can be detected by HIDS, NIDS. It can be blocked by Firewall, ACL or gateway proxy.
Actions on Targets	- Useful threat intelligence helps to identify threat actor's motive which can be Disrupting service Exfiltrating sensitive information Asking for ransom (Blackmail, etc.) - By identifying the nature of an attack, an intelligence team should be able to determine the scope, impact and motive of an attack - This activity can be done manually and using security solutions and tools available within the infrastructure
Exfiltration	- Determine the scope and impact of exfiltration. This includes: What data is being exfiltrated How much data is being exfiltrated What solutions within the infra can detect type and amount of data that are exfiltrated What solutions within infrastructure can block this activity.

Now that we know that what activities to be performed in order to determine each phase of cyber kill chain methodology, below is the sample table in which I tried to include all possible solutions that we can manually or automatically monitor in order to detect and respond anomalies.



Cyber Kill Chain

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Contain
Reconnaissance	NIDS D/B Security Web analytics	Firewall ACL Information sharing Policy				
Weaponization	NIDS D/B Security	NIPS Change Management File integrity Application whitelisting				
Delivery	EDR Protection Vigilant User	Proxy Filter	AV	Queuing		Router ACLs App-aware firewall Trust zones Internet-zone NIPS
Exploitation	EDR Protection HIDS	Vendor Patch Secure Password				App-aware firewall Trust zones Internet-zone NIPS
Persistence	Log monitoring HIDS	Privilege Seperation Secure Password 2FA/MFA	AV			App-aware firewall Trust zones Internet-zone NIPS
Command and Control	NIDS HIDS	Firewall ACL Gateway Proxy	NIPS		DNS redirect	Trust zones DNS Sinkholes
Actions on Targets	EDR Protection	Encryption				Incident Response
Exfiltration	DLP Audit Logs	Egress Filtering		Quality of service throttle	Honeypot	Firewall ACLs

Above example, a table is taken from two references that are included within this blog.

The Analysis Process

There are multiple methods of the analysis process, and an organisation should use according to their best need. Here I am going to explain the simplest way **(Diamond method)** that we can use for the analysis process within the threat intelligence.

This method has basically four components:

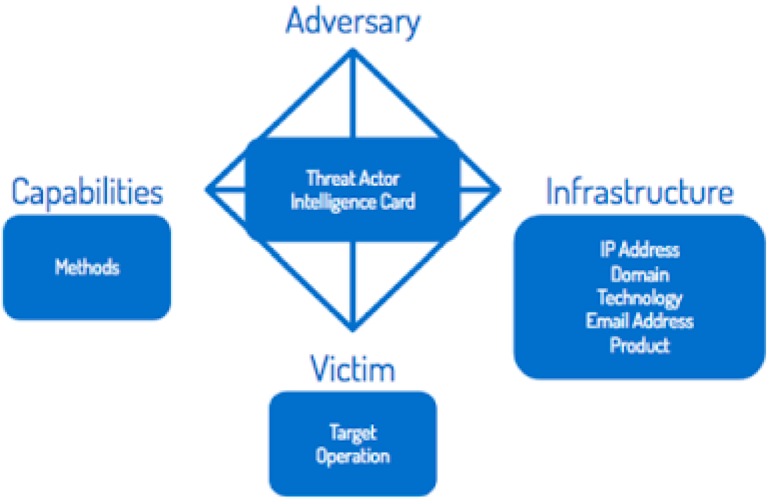
1) Adversary - Threat actor who can be an individual, group of hackers, nation, organisation, etc.

2) Infrastructure - An environment that threat actors use to attack their victims.

3) Victim - A threat actor's target.

4) Capabilities - Techniques, Tactics and Procedures used by threat actors are defined as capabilities.

Every component is directly connected to one another and creates a diamond.



There are main 3 deliverables of the analysis process:

1) Identification of TTP
2) Escalation process and operational guidelines for mitigations
3) Stakeholder reports for C-level executives, IR team, VM team and other teams.

A threat analyst reviews structured and unstructured data and produce above three types of reports.

Correlation of indicators

Correlation of indicators is vital to understand adversary's motive and a broader scope of an event. This helps identify severity, relevance, validity and a more widespread threat.

An event is a combination of multiple indicators. Therefore, linking all indicators help us to identify a broader scope and impact of an event.

Analysis of indicators must be:

Victim focused: Analyse data related victim in order to know what adversary

Adversary focused: Learn about adversary their actions, nature, potential targets and motivations of an attack on other organisations. This information may help us to identify adversary's actions and motives on our organisations.

Capability focused: Analyse data related to adversary's capabilities that help us to identify potential victims, technologies, infrastructure that supports capabilities.

Infrastructure focused: Monitor adversary's infrastructure, which identifies victims and capabilities.

Identifying actionable intelligence

In threat intelligence processes must be defined to provide an urgency of an incident. Either it should be escalated immediately to the IR team or ignored or investigate when time permits. SIEM can be used to perform the entire process seamlessly. Prioritising events can save a lot of time for an analyst.

Events must be prioritised based on severity against threat landscape.

Severity - Critical, Severe, Medium, Low, Info

Threat landscape - Global, Company-specific industry, Company itself

For example - A group of attackers are targeting an entertainment company of a specific country then options from the above list must be selected in the matrix in order to prioritise alerts, events regarding it.

Let's automate everything

Automation of the above things can reduce time and cost of resources whether they are doing hunting or investigation.

Intelligence software includes:

- automated information gathering
- ticket allocation
- incident analysis workflow
- prioritisation of alerts
- ready-made remediation steps

SIEM includes:

- environment visibility
- correlation of entities
- advance alerting
- advance ticket processing
- remediation steps

Along with the above solutions/software, tags can also be used. For example, the tag 'e-commerce' can be used to find malware, APT targeted to the e-commerce industry. Below is the list of some crucial tags that can be used in two ways.

1) Tags pertaining to targeted industries -

- Government
- Financial
- Aviation
- Banking
- Insurance
- Defense
- Energy
- Media
- Telecommunication
- Healthcare
- Oil and gas
- Academic
- Retail
- Legal
- Manufacturing
- Transportation
- any more...

2) Tags pertaining to the motivation of an attack

- Espionage
- Criminal
- Hacktivist
- Destruction

Using these tags (and many more which are not listed here, an organisation can have the latest alerts targeting to their company or industry). It is useful in proactive monitoring of new attacks targeting them.

Choose your threat intelligence software very carefully
Make sure that your Threat intelligence solution has at least below capabilities:

- data normalisation
- data integration
- tagging and ticketing
- threat knowledge portal
- tailored reports for C level executives, tactical reports and technical reports
- performance and value metrics
- many more...

I am not disclosing the entire list I prepared for myself, but this is just a hint to go ahead and evaluate and analyse things in all areas very carefully before making any decisions.

Then define the threat escalation matrix. In this activity, we have to create an escalation matrix to address a couple of challenges:

- How to inform stakeholders about any particular alert
- What to inform stakeholders about any particular alert
- When to inform stakeholders about any particular alert
- What communication methods to be used to inform stakeholders
- Which stakeholders to be informed

Based on company type, the requirement of intelligence gathering and analysis, this matrix can vary.

Importance of runbooks

It is essential to create runbooks as they are faster, handy, formalised and streamlined. They save time at the time of the incident.

Here is one of the standard formats for incident handling/response runbook.
https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/security_incident_response_plan_-_template.docx

Make sure runbooks should be created incident-specific such as:

- Credential theft incident response runbook
- Ransomware incident response runbook
- Malware incident response runbook
- Privilege escalation incident response runbook
- Insider threat incident response runbook
- Data breach incident response runbook
- Third-party incident response runbook

Finally, make sure that your threat intelligence is shared and stored on the threat knowledge portal, which can be accessible by a vulnerability management team, IR team, CTI team, and forensics team. It should have an ability to prioritise tickets, assign tickets, pivoting feature internally to access all relevant data and event timelines.

References

https://news.shack15.com/many-ai-startups-across-europe-dont-actually-use-artificial-intelligence/
https://www.webopedia.com/imagesvr_ce/5715/cyber-kill-threat.jpg
https://www.recordedfuture.com/diamond-model-intrusion-analysis/
https://img.deusm.com/darkreading/MarilynCohodas/killchainchart.jpg