Cyber Threat Intelligence

VIT-AP UNIVERSITY

Guided by:

Dr. Sibi Chakkaravarthy S

Associate Professor Grade 1

Computer Science and Engineering
Vellore Institute of Technology Andhra Pradesh
Amaravati

Team Members:

Diya Gupta
Naveen Kumar N

Abstract:

An efficient method for obtaining Cyber Threat Intelligence (CTI) and thwarting cyberattacks is the integration of SIEM, Kill Chain, and OSINT. Integration of SIEM, Kill Chain, and OSINT is a successful strategy for gathering Cyber Threat Intelligence (CTI) and preventing cyberattacks. This integration of Kill chain, open-source intelligence (OSINT) and System Information and Event Management (SIEM) will enable security personnel to more effectively respond to incidents and identify threats earlier in the course of an attack by giving them a better understanding of potential risks and security problems. By creating a more comprehensive and effective incident response strategy, organisations can lower the impact of security breaches and reduce the amount of time required for clean-up.

A solid security posture and regulatory compliance standards can both be maintained by organisations with the use of CTI. In this document, we'll examine the benefits of combining SIEM, Kill Chain, and OSINT to accomplish CTI and how this strategy can assist businesses in fending off cyberattacks

Introduction:

Cyberattacks have grown in number and are now a significant hazard to both businesses and people. Due to the use of digital technology and the increasing reliance on the internet and networked systems, cybercriminals have developing new and sophisticated techniques to exploit flaws in software, hardware, and user behaviour in order to gain unauthorised access to sensitive data. Cyber-attacks have the potential to cause severe consequences, such as damage to one's reputation, financial losses, the disruption of essential infrastructure, and even the risk of human life.

Cyber-attacks, also known as cybersecurity breaches, refer to malicious activities that target computer systems, networks, or devices with the intent to gain unauthorized access, disrupt operations, steal sensitive information, or cause damage. Cyber-attacks can be perpetrated by individuals, groups, or even state-sponsored actors, and they can take various forms, including malware infections, phishing attacks, ransomware attacks, DDoS (Distributed Denial of Service) attacks, social engineering attacks, and more.

Because of this, it is essential for both businesses and individuals to comprehend the nature of cyberattacks, the various hazards they pose, and the best practises for thwarting and minimising them. We shall examine the fundamentals of cyberattacks in this document, as well as their potential effects and countermeasures.

Cyber Threat Intelligence

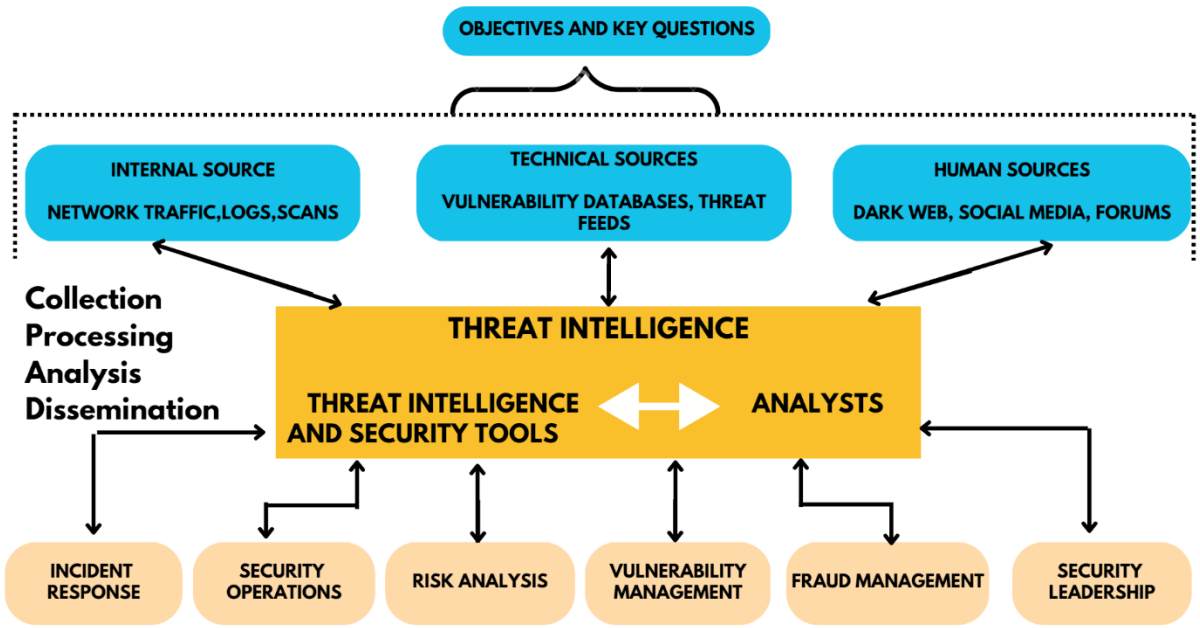
Cyber Threat Intelligence (CTI)

The process of gathering, examining, and sharing knowledge regarding future or current cyberthreats is known as cyber threat intelligence (CTI). Cyber Threat Intelligence's objective is to assist organisations in better comprehending the nature of cyber risks and taking preventative measures to avert or lessen assaults.

CTI encompasses a variety of tasks, including the gathering of information from several sources, including threat actors, dark web forums, and open-source intelligence. The analysed data is used to provide actionable insight by spotting patterns and trends. Risk evaluations, threat modelling, incident response planning, and other cybersecurity operations can all benefit from this information.

There are several types of CTI, including strategic, operational, and tactical. Strategic CTI focuses on the broader cybersecurity landscape, including emerging threats, geopolitical factors, and industry trends. Operational CTI is more focused on specific threats and attacks, providing insights into the tactics, techniques, and procedures used by threat actors. Tactical CTI is aimed at supporting real-time threat detection and response, providing detailed information on specific threats and indicators of compromise.

CTI is a crucial tool for businesses looking to strengthen their cybersecurity posture. Organisations may better understand the dangers they face and take preventative action to reduce those threats by utilising the intelligence offered by CTI. This might range from putting security policies in place and training staff to performing vulnerability analyses and penetration testing. The ultimate objective of CTI is to assist organisations in staying ahead of cyberthreats and safeguarding their sensitive data and vital infrastructure.



Stages in the CTI:

Stage 1: First stage in CTI Framework is to define the requirements and goals that are going to be achieved by using threat intelligence. After that we need to plan on how to collect the data with a proper permission and rights that obtained from the concerned authorities and administrators.

This is the crucial part of the CTI Framework because the output from of this phase is guidance on how to leverage the data on the following stages. This is usually defined by the security team leaders or organizational needs. For example, we can set the requirements as to collect unstructured data from threat advisory data using web mining techniques and integrate it with threat data feed to improve the cyber-attack attribution process in the threat data platform.

Stage 2: **Data Collection:**

The phase of data collecting involves gathering and analysing data from numerous publicly accessible sources. The data collecting step has two subprocesses: data collection and data analysis. The method of gathering data involves using a variety of security feeds, including free source CTI feeds, paid CTI feeds, security incident reports, and web crawling of linked websites. Data preparation, enrichment, and correlation are steps in the data analysis process that follows the collection of multiple security feeds from the Internet. A machine learning technique is used throughout the data preparation process to categorise the data as harmful or not. When the confirmed data is put in a database, a correlation and enrichment procedure is used to give context to that data.

Stage 3: **Data analysis:**

Data analysis is performed by an individual using OSINT analysis tools. The final phase of the OSINT analysis is the results submission, where the results are presented or communicated to the other team members

The analysis phase of the CTI framework involves two processes, which is Indicator of Compromise (IOC) generation and data correlation. In order to generate Indicator of Compromise, we need to have the correct value for each attribute related to the cyber incident (e.g., IP, domain, hash value) based on the data evaluation process in the data collection phase.

The data correlation in this phase can support the previous data correlation in the data collection phase to gain better insight into the cyber-attack.

Functions of CTI:

Threat detection: CTI assists businesses in identifying possible risks by keeping an eye out for any strange behaviour in their digital environment, such as the use of malicious software, phishing scams, or unauthorised access.

Risk Assessment: CTI gives businesses the ability to evaluate any risks connected to a specific threat, including the likelihood of an attack, the possible effects, and the weaknesses the threat may exploit.

Incident Response: CTI gives businesses the knowledge they need to react to online assaults correctly, including how to minimise and lessen their consequences as well as how to recover and restore systems and data.

Proactive Defense: Using CTI, organisations may proactively protect against cyber threats by seeing possible security holes in their systems and putting security precautions in place to stop assaults before they happen.

Strategic Planning: CTI helps strategic planning by giving businesses information about new risks and industry trends, enabling them to create efficient cybersecurity plans and spend resources appropriately.

Risks and challenges:

- **Sheer volume and complexity of data:** The sheer volume and complexity of data related to cyber threats can be overwhelming. CTI analysts must process and analyze huge amounts of data from multiple sources such as threat intelligence, incident reports, and open-source information to determine relevant and actionable information. Handling large amounts of data and ensuring data quality can be challenging.
- **Threat data overload:** Threat data has developed rapidly, and there are hundreds of threat data sets that are free, open-source, or both. Customers' prompt access to pertinent threat data that may be used to take appropriate action is crucial for cyberattack defence. However, a large number of them continue to struggle with an excessive volume of threat data and lack the knowledge necessary to maximise the effectiveness of their threat data programmes. Threat Data Quality

Threat data quality is a common problem in CTI (cyber threat intelligence). The quality of threat data depends on the source of the data and how it is collected. Some common issues with threat data quality are:

- **Inaccurate or incomplete data:** Threat data can be inaccurate or incomplete due to errors in collection, processing, or analysis.
- **Lack of context:** threat data may lack context, making it difficult to understand its relevance to an organization's security posture.
- **Data overload:** security teams can be overwhelmed with the amount of threat data they receive, making it difficult to identify and prioritize threats.
- **Data inconsistency:** threat data can be inconsistent across different sources, making comparison and analysis difficult.

To address these issues, organizations should establish clear processes for collecting, analysing and sharing threat data. They should also invest in tools and technologies that help automate threat data processes and reduce the risk of human error. Finally, organizations should partner with others in their industry to share threat data and improve their collective security posture**.**

- **Privacy & legal issues:**

Privacy and legal issues are a major concern in CTI (Cyber Threat Intelligence). Some of the key challenges are:

- **Privacy:** companies must ensure that the collection and sharing of threat intelligence is done in compliance with privacy regulations such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).
- **Intellectual property:** organizations must be careful not to infringe on the intellectual property rights of others when collecting and sharing threat data.
- **Ownership of data**: Organizations must establish clear ownership of threat data to avoid disputes over its use and distribution.
- **Accuracy of data:** To protect themselves from legal responsibility, businesses must make sure the threat data they gather and communicate is accurate and trustworthy.

Organisations should have clear rules and processes for gathering, evaluating, and exchanging threat data in order to address these issues. To make sure their practises adhere to pertinent rules and legislation, they should also collaborate with legal professionals. In order to exchange threat intelligence and strengthen their overall security posture, companies should collaborate with other companies in their sector.

OSINT

OSINT, or Open-Source Intelligence, it is the practice of gathering and analyzing information from publicly available sources to produce useful intelligence. OSINT is used in a wide range of fields, including law enforcement, business intelligence, and national security.

One of the key features of OSINT is that publicly available. which means that anyone with internet access can access OSINT sources. OSINT covers a wide range of sources, including social media platforms, public records, news articles, and more.

OSINT is a valuable tool for intelligence. It does not require any specialized equipment or resources to accessible to a wide range of users. OSINT is also legally permissible, as it does not involve any illegal or unethical methods of obtaining information. OSINT can be accessible by anyone.

OSINT serves a important roles in the Cyber threat intelligence:

1. **Threat Identification.**

OSINT can provide information about potential threat actors, their tactics, techniques, and procedures (TTPs), and their motivations. This information can help cyber threat hunters identify potential threats and take proactive steps to prevent them from causing harm.

OSINT can be used to analyze, monitor and track cyberthreats from targeted or indiscriminate attacks against an organization by malware and bad actors. It is an essential

element to strengthen any organization's proactive cybersecurity posture. An example of using OSINT for cyber threat intelligence (CTI), is when a company searches the internet for its email addresses. The search finding could be used to get information about potential threats targeting this company.

2. **Threat Analysis.**

   OSINT helps investigate security incidents and is leveraged by security teams, for example, when investigating a security breach. A primary reason enterprise use OSINT is utilizing it for cyber threat intelligence. This helps Security Operation Centre (SOC) teams get actionable information to prevent, detect, and respond to various cyberattacks.

   An example of using OSINT for cyber threat intelligence (CTI), is when a company searches the internet for its email addresses. The search finding could be used to get information about potential threats targeting this company. CTI platforms enable the creation of detailed threat analysis by working together among peer organizations by sharing relevant, structured and enriched threat information

   OSINT can be used to collect information from various sources such as social media platforms, blogs, forums, and other publicly available sources. This information can be used to identify potential threats and vulnerabilities that could be exploited by cybercriminals.

   OSINT can also be used to monitor the dark web for any potential threats or data breaches. This can help organizations take proactive steps to prevent data breaches and protect sensitive information.

3. **Vulnerability Assessment:**

OSINT can be used to identify vulnerabilities in an organization's security posture by collecting information from various sources such as social media platforms, blogs, forums, and other publicly available sources. This information can be used to reveal corporate information that the company may deem libellous, embarrassing, harassing, or otherwise harmful to a company's reputation.

An OSINT Corporate Vulnerability Assessment can help validate or disprove the open-source information that negatively influences your business. Depending on the amount or type of information available, it may be possible to determine the root or extent of the problem

4. **Incident response:**

OSINT can be used by incident response teams to gather intelligence on the source and nature of an incident, identify potential attackers, and assess the extent of the damage. In addition, OSINT teams can provide real-time intelligence to the incident response team during a security incident.

CTI (Cyber Threat Intelligence) can be used to understand the threats that have, will or are currently targeting an organization. It functions as a proactive extension to incident response by leveraging the output from existing cybersecurity monitoring tools.

5. Threat Intelligence sharing:

Open-source intelligence (OSINT) is an essential element to strengthen any organization's proactive cybersecurity posture. It provides unparalleled space to discover threatening information from publicly available sources. OSINT is now widely used in threat intelligence to detect and counter advanced cyber-attacks before turning into an immediate risk. By leveraging OSINT sources, organizations can detect internal and external security vulnerabilities in their IT environment and work to fix them quickly before they get exploited by malicious actors.

Sharing CTI (Cyber Threat Intelligence) helps security teams alert each other to new findings across the threat landscape and flag active cybercrime campaigns and Indicators of Compromise (IOCs) that the cybersecurity community should be immediately aware. The CTI platforms enable the creation of detailed threat analysis by working together among peer organizations by sharing relevant, structured and enriched threat information. The most important factor in the success of any open-source intelligence initiative is the presence of a clear strategy, understand the target and set the objectives to accomplish the goal accordingly.

Characteristics of OSINT:

- **Publicly available:** OSINT sources are available to anyone with Internet access.
- **Wide scope:** OSINT covers a wide range of sources, including social media, online forums, news articles, public records, and more.
- **Easy to access:** Many OSINT sources are easily accessible and do not require no special tools or skills to access.
- **Cost-effective:** OSINT is a cost-effective method of gathering information because it does not require expensive equipment or resources.
- **Legally permissible:** OSINT does not involve any illegal or unethical methods of information gathering.

The modern concept of OSINT as a systematic approach to collecting and analyzing publicly available information. OSINT can be classified into several categories based on the information sources of information being analyzed:

1. **social media:** Social media platforms are a rich source of OSINT, providing because they offer insights into the opinions, beliefs, and activities of individuals and groups.

2**. Web content:** Web content includes news articles, blogs, forums, and other publicly accessible online sources. This category of OSINT can provide valuable insights into events, trends, and public opinion.

3. **Public records:** Public records include government documents, court records, and other publicly available sources of information. This category of OSINT can provide valuable insights into the activities and behaviour of individuals and organizations.

4. **Geospatial data:** Geospatial data includes maps, satellite imagery, and other sources of location-based information. This category of OSINT can provide valuable insights into the movements and activities of individuals and groups.

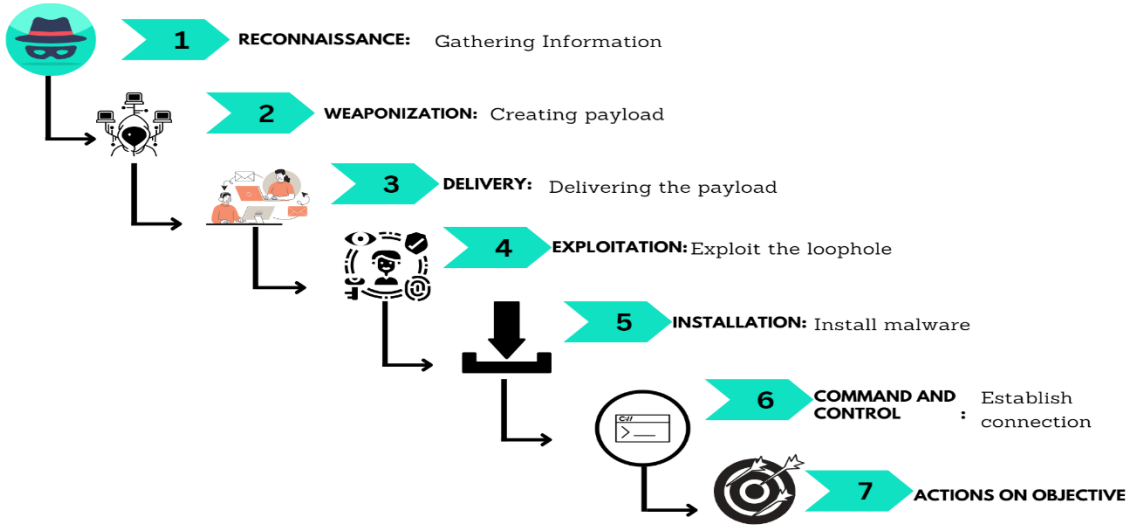
The best OSINT tools:

- **Sn1per Professional:** professional, open-source OSINT and vulnerability scanning tool that enables exploration, data collection and vulnerability scanning of target domains and networks.
- **SpiderFoot:** An open-source OSINT tool that automates the collection and analysis of data from multiple sources.
- **Shodan:** A search engine for Internet-connected devices that can be used to collect information about networks, servers and other devices.
- **Google Dorking (Advanced Google Hacking Techniques):** A powerful search engine that allows users to narrow down their search results based on specific criteria such as location, file type, etc.
- **Sublist3r:** Python-based open-source OSINT tool that enables subdomain discovery by searching various search engines, online forums and DNS data.
- **The Harvester**: Helps identify an organisation's "external threat landscape on the Internet" by searching "emails, names, subdomains,IPs and URLs.

Kill Chain

The Cyber Kill Chain is a framework that describes the phases of a cyber-attack how an attacker gathers information and perform the attack from initial reconnaissance to exfiltration of data. The framework was developed by Lockheed Martin and is widely used in the cybersecurity industry to help organizations understand and defend against cyberattacks.

The Cyber Kill Chain consists of seven stages:



Reconnaissance: Attackers obtain information on their target during this phase using a variety of techniques, including network scanning, social engineering, and open-source intelligence (OSINT). An attacker's initial step of information gathering about the target

system or business is at this stage. This might entail looking for weaknesses, locating possible targets, or gathering data about the infrastructure, people, or security precautions of the target. This stage is crucial for the attacker since it enables them to spot potential security flaws and vulnerabilities that may subsequently be exploited. In this phase the attacker will collect 90% of data of the victim.

Weaponization: in this stage, attackers create a weapon such as malware or exploit code to attack their target.

once the attacker has gathered enough information, he develops or acquires tools, techniques and malware to exploit the identified vulnerabilities. This may involve developing their own malware or using off-the-shelf malware or exploits. The attacker then prepares the weaponized payload for delivery to the target system.

Delivery: In this phase the attacker now sends the malicious payload which he created based on the loopholes which he gathers in the phase-1 to the network or target system. The payload can be delivered via a variety of techniques, including spearphishing, social engineering, and exploiting flaws in the target's software or systems. The attacker wants to get into the target system and establish a link for further action.

Exploitation: in this phase, the attackers exploit the weapon to exploit vulnerabilities in the target's systems or applications.

once the weaponized payload has been delivered, the attacker exploits vulnerabilities in the target system to gain unauthorized access. In this phase the attacker involves elevating privileges, installing backdoors or remote access tools, or manipulating the target system to gain control.

Installation: in this phase, the attackers install malware or other tools on their target's systems to gain access and control over them.

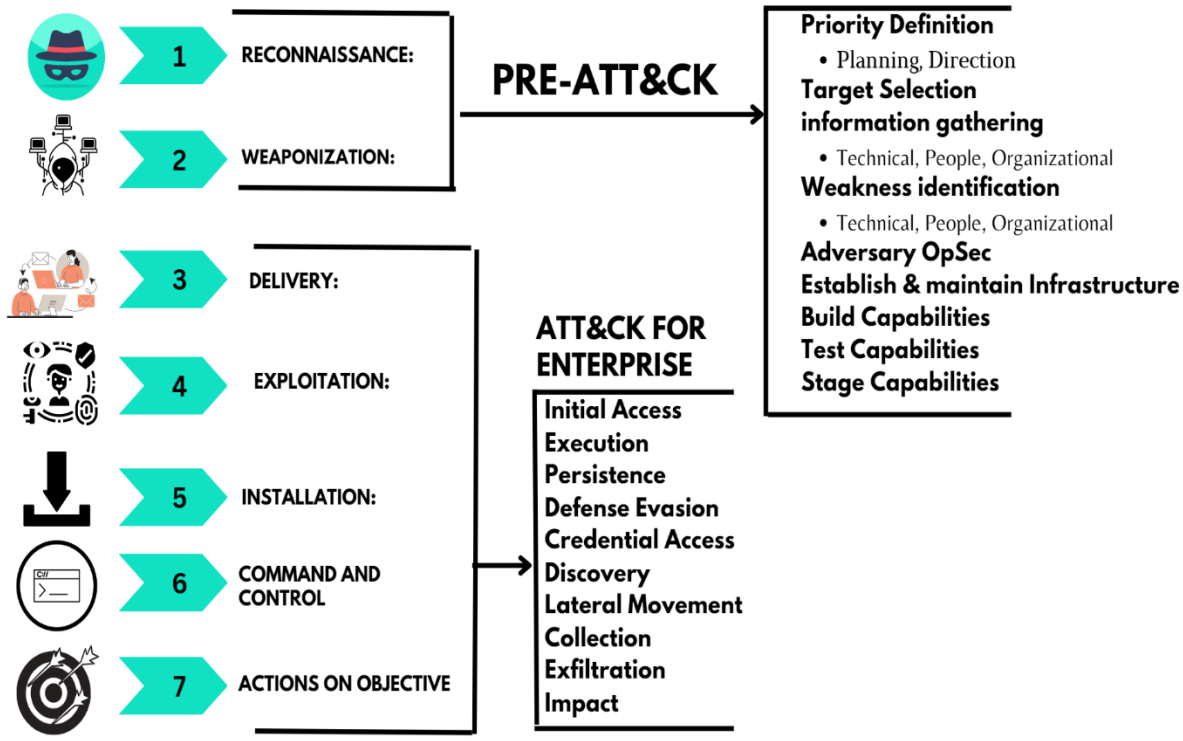
After gaining access, the attacker installs additional tools and malware to maintain and take control of the target system. This may include creating user accounts, modifying system settings, or installing rootkits.

Command and Control (C2): In this phase, the attacker establishes communication channels with the compromised system or network to remotely control and manage the attack. This may involve establishing backdoors, remote access tools, or other communication mechanisms to enable ongoing control and manipulation of the target system.

Actions on Objectives: Once the attacker gains control of the target system, they can pursue their primary objectives, such as data exfiltration, intellectual property theft, financial fraud, or service disruption. This phase can vary widely depending on the attacker's motives and goals, and may involve multiple actions over an extended period of time.

The role of the kill chain in OSINT

Kill chain offers a framework for comprehending the many actions an attacker takes during a cyberattack, from reconnaissance through operations at the target. The kill chain will reveal where he is in the attack's progression. The kill chain is crucial in the context of OSINT for recognising and minimising possible risks by utilising information that is readily accessible to the general public.



The first step in the kill chain, reconnaissance, is when an attacker learns 90% of the information about the victim. Because it entails acquiring and analysing open-source data from publicly accessible sources like social media, news articles, forums, and other online platforms, OSINT is crucial at this phase. By monitoring and examining material in the public domain, OSINT assists in locating possible weak points in the target's defences.

During the reconnaissance phase, information gathered by OSINT will give insight into the target's infrastructure, systems, networks, personnel, and other pertinent facts. The possible attack surface and potential entry points for an attacker may both be evaluated using this information. For instance, an attacker can utilise social media accounts to obtain data from the target company's workers and use that data to initiate social engineering or phishing assaults. In order to create weaponized malware at the weaponization stage, OSINT can also give knowledge on the target's technological stack, software versions, and known vulnerabilities.

OSINT may aid in identifying prospective threat actors as well as their goals, strategies, and equipment. OSINT will offer intelligence on recognised threat groups, their activities, and the tools they employ to carry out the assault by keeping an eye on online forums, the dark web, and other sources. This information may be used to identify individual threat actors responsible for cyberattacks and to comprehend how they operate, both of which are important for creating effective defences.

OSINT can be crucial at stages of the kill chain other than the reconnaissance stage. For instance, during the exploitation phase, OSINT might offer details about the target's systems and infrastructure that can be leveraged to create specialised assaults. OSINT can support the monitoring and analysis of the infrastructure and communication channels the attacker employs to control the systems under attack during the command-and-control phase. By keeping an eye out for indications of data breaches, interruptions, or other hostile behaviour, OSINT can also shed light on activities in the target phase.

The kill chain in OSINT is crucial because it offers a proactive and strategic approach to threat intelligence and defence against cyberattacks. Organisations may detect possible dangers early in the kill chain by understanding the different phases of a cyberattack and employing OSINT to obtain pertinent intelligence. Then, they can take the necessary steps to stop or lessen the effects of an attack. Insights from OSINT on threat actors' tactics, methods, and procedures may be leveraged to create efficient defences and strengthen an organization's overall cybersecurity posture.

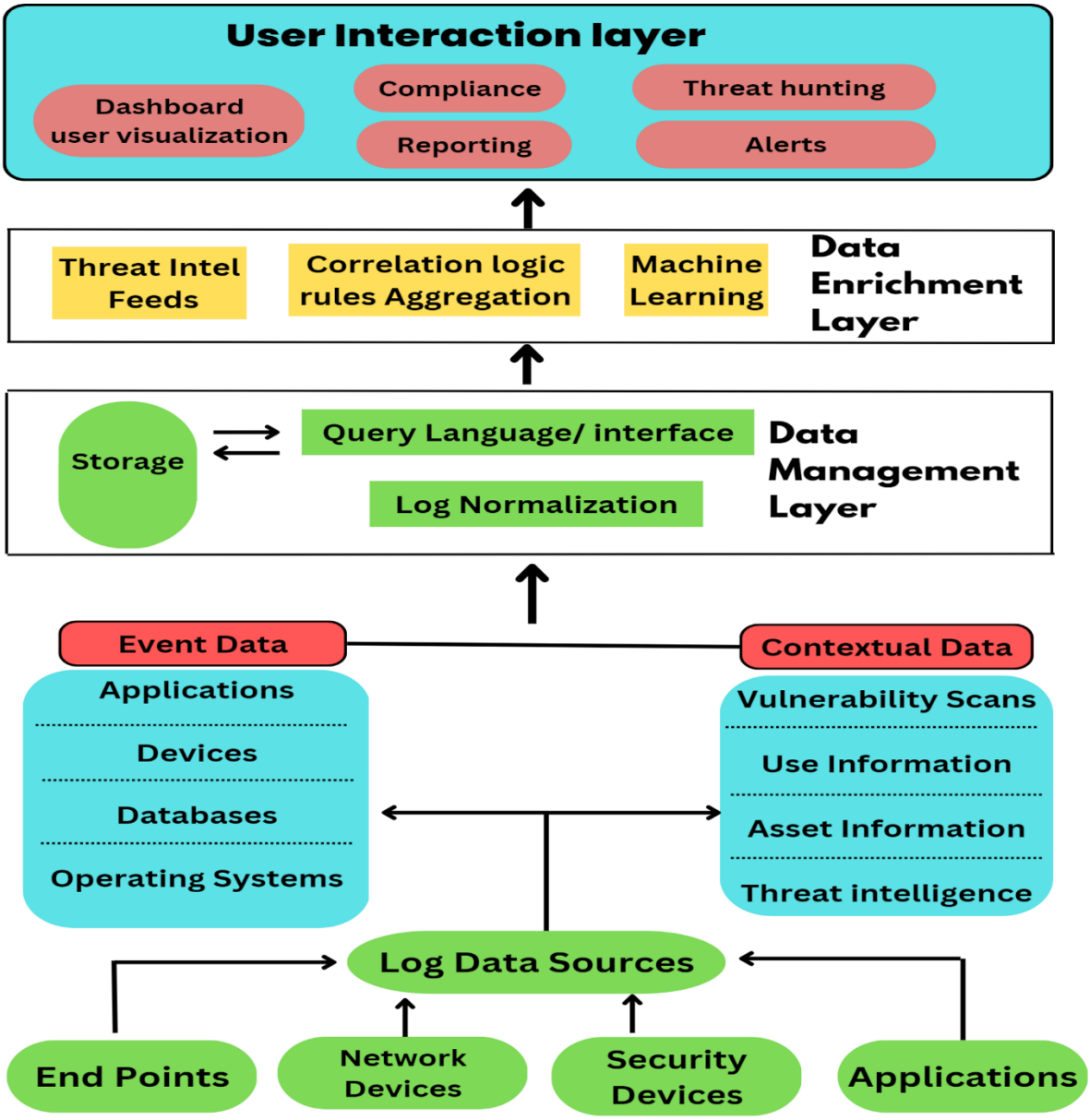
The kill chain is a critical concept in OSINT that helps organizations understand and systematically respond to cyber threats. OSINT plays an important role in several phases of the kill chain, particularly the reconnaissance phase, where open-source information is collected and analyzed to identify potential vulnerabilities and weaknesses in the target's defenses. By leveraging OSINT and understanding the kill chain, organizations can improve their threat intelligence capabilities, develop effective countermeasures, and proactively defend against potential cyber threats. By understanding each phase of the cyber kill chain, organizations can develop strategies to detect and prevent cyberattacks at each stage.

SIEM

Security Information and Event Management (SIEM):

SIEM or security information and event management allow us to monitor and analyse events and track and log data for compliance and auditing purpose. This helps the organisations to recognize security threats and vulnerabilities that may disrupt the organisation’s business in future. It combines security information management system (SIM) and security event management into one security management system.

SIEM works by deploying multiple agents at the endpoint that collect data related to security events from end point devices(users) or security devices like firewalls, antivirus etc. and forwards it to centralized management console, where security analysts recognise the unusual activities, identifies them and prioritize security incidents



Data analysis of the SIEM:

1. **Data Collection:** SIEM collects security data from various sources such as logs, events, and alerts generated by network devices, servers, applications, security appliances, and other sources. This data is typically stored in a centralized location for analysis.

2. **Data Normalization:** SIEM normalizes the collected data by converting it into a standardized format that can be easily analyzed and correlated. This step involves parsing and categorizing data into common fields, removing duplicates, and enriching the data with additional contextual information.

3. **Data Aggregation and Correlation:** SIEM aggregates and correlates data from different sources to identify patterns, relationships, and anomalies. This step involves correlating events and alerts based on time, location, user, and other contextual factors to identify potential security incidents or threats.

4. **Threat Detection:** SIEM uses pre-defined rules, signatures, machine learning algorithms, and behavioural analytics to detect known and unknown threats. This step involves analyzing aggregated and correlated data to identify potential security incidents or patterns of behaviour that may indicate a security threat.

5. **Incident Response:** SIEM gives security analysts the resources they need to look into and address security occurrences. In this stage, the security events that have been found are reviewed and analysed in order to determine their severity and effect. Following that, a suitable incident response procedure is started in order to contain, lessen, and ultimately resolve the occurrences.

6. **Reporting and Compliance:** For security analysts, IT administrators, and management to analyse and monitor security events, incidents, and compliance with security rules and laws, SIEM creates reports and offers dashboards. In order to give insight into the security posture of the organisation and show compliance with regulatory obligations, this phase entails producing reports, alerts, and notifications.

7. **Continuous Improvement:** SIEM allows organizations to continuously improve their security posture by analyzing historical data, identifying trends, and refining detection rules and policies. This step involves leveraging the insights gained from SIEM analysis to enhance security defenses, update security policies, and improve incident response processes.

OSINT and SIEM:

In SIEM, or Security Information and Event Management, OSINT, or Open-Source Intelligence, is crucial. Information that is publicly accessible and available, such as posts on social media, news stories, and blogs, is referred to as OSINT.

OSINT is used in the context of SIEM to enhance security data and strengthen threat detection capability. Security analysts can acquire a deeper picture of the security landscape and see potential dangers that could go unnoticed otherwise by integrating OSINT data into a SIEM system.

For example, OSINT can be used to keep an eye on social media sites for signs of a compromise, like mentions of shady behaviour or malware. A SIEM system can then be used to analyse this data along with other security data to look for trends and abnormalities that can point to a security breach.

Integration of OSINT with SIEM:

Find relevant OSINT sources: That can provide valuable information about potential threats, vulnerabilities, or indicators of compromise (IOCs). These sources may include threat intelligence platforms, vulnerability databases, social media, public threat intelligence, security blogs, and other openly available sources of security information.

Define an approach for acquiring and merging OSINT data into the SIEM: As an approach for gathering OSINT data. Depending on the situation, this may include manually compiling OSINT data and entering it into the SIEM or establishing automated processes to regularly collect and ingest it. Make sure the data is obtained swiftly and efficiently, and consider what categories of OSINT data are relevant to the security requirements of your firm.

Normalise and Improve OSINT Data: By placing the collected OSINT data in a common format, the SIEM can will analyse it and utilise it to compare it to other security data. To do this, it could be necessary to parse, classify, and enrich the OSINT data with additional contextual data, such as threat scores, indicators of compromise (IOCs), or other information.

Correlate OSINT Data with Other Security Data: Utilise the OSINT data and other security data that has been obtained from various sources inside the organisation by analysing and correlating them using the SIEM's correlation capabilities. Link OSINT data to other security information. Comparing OSINT data to logs, events, and warnings generated by servers, network devices, software, and security appliances may be necessary to do this. Correlation can be used to find potential dangers, behavioural patterns, or indications of compromise that might not be picked up by other security sources alone.

Develop OSINT-Based Detection Rules: Utilise the OSINT data to create unique detection rules or to adapt already-existing detection rules in accordance with known threat intelligence. By using the OSINT data to identify possible threats or suspicious activity, this can alert or notify the SIEM when pertinent occurrences or trends are found. This can also assist in finding new threats or zero-day vulnerabilities that conventional security solutions might not be able to address.

Enhance Incident Response with OSINT: Utilise OSINT data to amplify event data and offer more context for incident response when security incidents are noticed. In order to comprehend the capabilities, motives, and strategies of the IOCs or threat actors discovered in the event, this may involve conducting research using OSINT data. This can assist in developing a successful reaction strategy and quickly reducing the situation.

Stay Updated with Latest OSINT: Maintaining the OSINT data's relevancy and effectiveness in spotting and combating new threats requires ongoing monitoring and updating. It's critical to periodically assess and adapt the OSINT integration strategy since OSINT data might change over time and new intelligence sources can become accessible.

Advantages of integrating the SIEM with the OSINT:

Enhanced Threat Detection: Additional threat intelligence sources that may not be accessible through internal security data sources can be provided through OSINT. Information on well-known threat actors, indicators of compromise (IOCs), new threats, vulnerabilities, and other pertinent security data may all be found in OSINT. Integrating OSINT with SIEM can improve threat detection capabilities, enabling businesses to see security issues and possible threats that might have gone undiscovered otherwise.

Improved Incident Response: During an incident response, OSINT can offer helpful context and insights. When a security event is discovered, OSINT may be used to add more relevant information to the incident data, including more details on the threat actors and their tactics, methods, and procedures (TTPs). As a result, security analysts may be better able to prioritise incident response activities, develop an effective response plan, and promptly mitigate incidents.

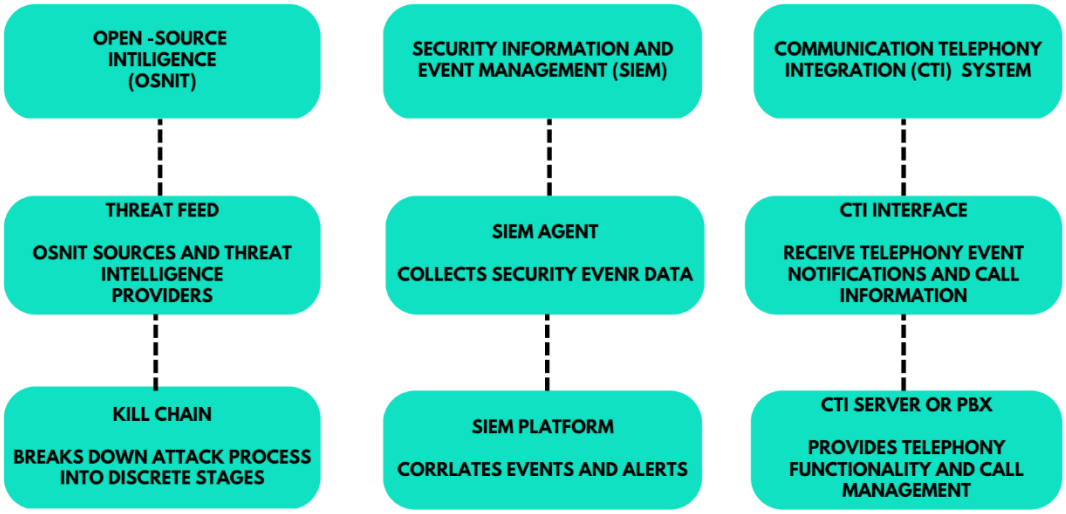
Better Situational Awareness: In addition to information regarding national risks, business-specific dangers, and developing threats, OSINT can offer a larger view of the threat landscape. Organisations may improve their knowledge of the present threat landscape, recognise prospective risks, and proactively change their security defences and incident response strategies by integrating OSINT with SIEM. This may lead to increased situational awareness and enhanced readiness for future online attacks.

Customized Threat Intelligence: Based on the unique requirements and industrial sector of an organisation, tailored threat intelligence may be created using OSINT data. Organisations may use the OSINT data at their disposal to develop detection rules, alerts, and notifications that are specifically suited to their environment by integrating OSINT with SIEM. As a result, organisations may be able to detect risks that are pertinent to their sector, region, or technology stack and increase the effectiveness of their threat detection efforts.

Cost-Effective Solution: As OSINT contains publicly accessible information, it is frequently free or inexpensive to access. The threat intelligence capabilities of an organisation can be improved without incurring major additional expenditures by integrating OSINT with SIEM. For small and medium-sized businesses with limited funding for cybersecurity expenditures, this can be very helpful.

Timely Threat Intelligence Updates: Organisations may receive the most recent threat intelligence since OSINT data is often updated in real-time or with little latency. Organisations may keep informed about the most recent threats, vulnerabilities, and other security information by combining OSINT with SIEM, and they can respond promptly and proactively to prospective risks.

Achieving Cyber Threat Intelligence with Kill Chain, OSINT and SIEM



In this image, the OSINT threat feed and intelligence providers are feeding the Kill Chain process data about potential dangers to the organisation. The Kill Chain is a concept that divides each stage of a cyber-attack into distinct stages, from reconnaissance through exfiltration, in order to better understand and defend against these attacks.

While the SIEM agent collects security event data from various endpoints, the CTI interface receives alerts of telephony events and call details from the PBX or CTI server. The SIEM platform receives this data and correlates the events and alarms to provide a comprehensive picture of the organization's security posture.

By combining the Kill Chain, OSINT, and SIEM, security teams can more accurately identify potential threats, comprehend the steps of an attack, and respond to any events quickly and effectively. The addition of telephony event notifications and call information through the CTI system also increases the organization's overall security posture by giving a more complete view of user activity and behaviour.

Advantages of integrating the OSINT, kill chain and SIEM.

Integrating Kill Chain, OSINT, and SIEM to achieve Cyber Threat Intelligence (CTI) provides several advantages, including:

- **Improved situational awareness:** By integrating these three components, more complete picture of prospective threats and security issues can be obtained by integrating these three elements by security personnel. Better situational awareness is made possible as a result, which is essential for seeing and avoiding potential cyberattacks.

- **Enhanced threat detection:** OSINT provides valuable information about potential threats and their tactics, techniques, and procedures (TTPs). Integrating this information with the Kill Chain process and SIEM event data can help security teams detect threats earlier in the attack process and respond more effectively.

- **Better incident response:** By integrating these three components, security teams can develop a more robust and effective incident response plan. This can help to minimize the impact of a security incident and reduce the time to remediation.

- **More efficient resource allocation:** Integrating Kill Chain, OSINT, and SIEM can help security teams to focus their resources on the most critical areas. This can help to ensure that resources are used effectively and efficiently.

- **Improved compliance**: CTI can also help organizations to meet regulatory compliance requirements by providing a more comprehensive view of their security posture.

Risks and challenges:

While integrating Kill Chain, OSINT, and SIEM can provide significant advantages in achieving Cyber Threat Intelligence (CTI), there are also limits and challenges that organizations need to be aware of, including:

Data overload: The amount of data that needs to be processed and analysed as a result of the integration of several data sources. As a result, security personnel may find it challenging to identify and prioritise possible threats due to data overload.

Complexity: Kill Chain, OSINT, and SIEM integration can be difficult and expensive because it required a lot of technical knowledge experts, effort, and money. For organisations to implement and manage this integration effectively, they must have the right tools and skills.

False positive and negative results: The identification of threats sometimes gives false positives and false negatives which can be time-consuming and difficult for security teams as a result of the integration of various data sources. Lack of standardization: Effectively integrating many data sources might be difficult due to the lack of standardisation in data collection and analysis.

Privacy concerns: When personal data is involved, the integration of data from many sources can cause privacy concerns. Companies must make sure they accept by data protection laws and preserve the privacy of their clients.

Limited visibility: An organization's security posture could still have gaps despite the integration of numerous data sources. As a result, the organisation may not be aware of possible dangers, leaving it open to cyberattacks.

Conclusion:

CTI, OSINT, Kill Chain, and SIEM are crucial parts of cybersecurity operations. Effective cyber threat detection, analysis, and response are made possible by these technologies for security professionals. Each tool, however, has unique difficulties and restrictions. While the Kill Chain concept might not be appropriate for all sorts of attacks, CTI and OSINT are reliant on the accuracy and usefulness of the data sources. SIEM has difficulties handling massive amounts of data and separating genuine from malicious activity.

Numerous benefits, such as a deeper comprehension of threats, quicker incident response times, and improved collaboration across security teams, might result from integrating these solutions. However, integrating these tools also involves risks and difficulties, including the requirement for specialised knowledge and skills. Therefore, organisations need to have a clear view of their goals and a well-defined strategy in order to properly incorporate these tools. This plan should include the proper tool selection, the creation of efficient workflows and procedures, and the ongoing training and assessment of the security operations centre.

References:

1. Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R. (2017). Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives.
2. Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. Computers & Security, 87, 101589.
3. Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security, 72, 212-233.
4. Guo, L., Wen, S., Wang, D., Wang, S., Wang, Q., & Liu, H. (2021, June). Overview of cyber threat intelligence description. In 2021 International Conference on Applications and Techniques in Cyber Intelligence: Applications and Techniques in Cyber Intelligence (ATCI 2021) Volume 1 (pp. 343-350). Cham: Springer International Publishing.
5. Sillaber, C., Sauerwein, C., Mussmann, A., & Breu, R. (2016, October). Data quality challenges and future research directions in threat intelligence sharing practice. In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (pp. 65-70).
6. Kotsias, J., Ahmad, A., & Scheepers, R. (2023). Adopting and integrating cyber-threat intelligence in a commercial organisation. European Journal of Information Systems, 32(1), 35-51.
7. Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence–issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(1), 371-379.
8. Czekster, R. M., Metere, R., & Morisset, C. (2022). cyberaCTIve: a STIX-based Tool for Cyber Threat Intelligence in Complex Models. *arXiv preprint arXiv:2204.03676*.
9. Veerasamy, N. (2017). Cyber threat intelligence exchange: A growing requirement.
10. Shouse, K. (2015). *Actionability of cyber threat intelligence* (Doctoral dissertation, Utica College).
11. Amthor, P., Fischer, D., Kühnhauser, W. E., & Stelzer, D. (2019, August). Automated cyber threat sensing and responding: integrating threat intelligence into security-policy-controlled systems. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (pp. 1-10).
12. Kure, H., & Islam, S. (2019). Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. *Journal of Universal Computer Science*, *25*(11), 1478-1502.
13. Fereidooni, H., Dmitrienko, A., Rieger, P., Miettinen, M., Sadeghi, A. R., & Madlener, F. (2022). Fedcri: Federated mobile cyber-risk intelligence. In *Network and Distributed Systems Security (NDSS) Symposium*.

14. Sillaber, C., Sauerwein, C., Mussmann, A., & Breu, R. (2016, October). Data quality challenges and future research directions in threat intelligence sharing practice. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security* (pp. 65-70).
15. Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & security*, *72*, 212-233.
16. Mtsweni, J., Mutemwa, M., & Mkhonto, N. (2016). Development of a cyber-threat intelligence-sharing model from big data sources. *Journal of Information Warfare*, *15*(3), 56-68.
17. Mtsweni, J. S., Shozi, N. A., Matenche, K., Mutemwa, M., Mkhonto, N., & Jansen van Vuuren, J. (2016). Development of a semantic-enabled cybersecurity threat intelligence sharing model.
18. Sauerwein, C., Sillaber, C., & Breu, R. (2018). Shadow cyber threat intelligence and its use in information security and risk management processes. *Multikonferenz Wirtschaftsinformatik (MKWI 2018)*, 1333-1344.
19. Tabak, I. (2018). Functional scientific literacy: disciplinary literacy meets multiple source use. In *Handbook of multiple source use* (pp. 221-237). Routledge.
20. Tziampazis, C. (2021). *Open Security Intelligence, analysis and countermeasures* (Master's thesis, Universitat Politècnica de Catalunya).
21. Tabatabaei, F., & Wells, D. (2016). OSINT in the Context of Cyber-Security. *Open Source Intelligence Investigation: From Strategy to Implementation*, 213-231.
22. Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, *28*(2), 673-682.
23. Hwang, Y. W., Lee, I. Y., Kim, H., Lee, H., & Kim, D. (2022). Current status and security trend of OSINT. *Wireless Communications and Mobile Computing*, *2022*.
24. Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defense enterprise*. Rand Corporation.
25. Riebe, T., Biselli, T., Kaufhold, M. A., & Reuter, C. (2023). Privacy Concerns and Acceptance Factors of OSINT for Cybersecurity: A Representative Survey. *Proceedings on Privacy Enhancing Technologies*, *1*, 477-493.
26. Hassan, N. A., Hijazi, R., Hassan, N. A., & Hijazi, R. (2018). The evolution of open source intelligence. *Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence*, 1-20.
27. Best Jr, R. A., & Cumming, A. (2007). Open source intelligence (OSINT): issues for congress. *December*, *5*, 28.
28. Gibson, S. D. (2014). Exploring the role and value of open source intelligence. *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities*, 9-23.
29. Davis, J. W. (2002). Application of OSINT. *OPEN SOURCE INTELLIGENCE READER*, 30.
30. Yadav, T., & Rao, A. M. (2015). Technical aspects of cyber kill chain. In *Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3* (pp. 438-452). Springer International Publishing.
31. Pols, P., & van den Berg, J. (2017). The unified kill chain. *CSA Thesis, Hague*, 1-104.
32. Mihai, I. C., Pruna, S., & Barbu, I. D. (2014). Cyber kill chain analysis. *Int'l J. Info. Sec. & Cybercrime*, *3*, 37.
33. Yamin, M. M., Ullah, M., Ullah, H., Katt, B., Hijji, M., & Muhammad, K. (2022). Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security. *Mathematics*, *10*(12), 2054.
34. Alendal, G., Dyrkolbotn, G. O., & Axelsson, S. (2021). Digital forensic acquisition kill chain–analysis and demonstration. In *Advances in Digital Forensics XVII: 17th IFIP WG 11.9 International Conference, Virtual Event, February 1–2, 2021, Revised Selected Papers 17* (pp. 3-19). Springer International Publishing.
35. Seker, E. (2019). Cyber Threat Intelligence Understanding Fundamentals. *MİLLİ TƏHLÜKƏSİZLİK VƏ HƏRBİ ELMLƏR*, 75.

36. Sekharan, S. S., & Kandasamy, K. (2017, March). Profiling SIEM tools and correlation engines for security analytics. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 717-721). IEEE.
37. Detken, K. O., Rix, T., Kleiner, C., Hellmann, B., & Renners, L. (2015, September). SIEM approach for a higher level of IT security in enterprise networks. In *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (Vol. 1, pp. 322-327). IEEE.
38. Hristov, M., Nenova, M., Iliev, G., & Avresky, D. (2021, November). Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT. In *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA)* (pp. 1-5). IEEE.
39. Zeinali, S. M. (2016). *Analysis of security information and event management (SIEM) evasion and detection methods* (Doctoral dissertation, Master Thesis, Tallinn University of Technology).
40. Motlhabi, M., Pantsi, P., Mangoale, B., Netshiya, R., & Chishiri, S. (2022, March). Context-aware cyber threat intelligence exchange platform. In *International Conference on Cyber Warfare and Security* (Vol. 17, No. 1, pp. 201-210).
41. Nikolaienko, B., & Vasylenko, S. (2021). Application of the Threat Intelligence platformto increase the security of governmentinformation resources. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*, *11*(4).
42. Irfan, A. N., Chuprat, S., Mahrin, M. N. R., & Ariffin, A. (2022, October). Taxonomy of Cyber Threat Intelligence Framework. In *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 1295-1300). IEEE.
43. Gonzalez-Granadillo, G., Faiella, M., Medeiros, I., Azevedo, R., & Gonzalez-Zarzosa, S. (2019, June). Enhancing Information Sharing and Visualization Capabilities in Security Data Analytic Platforms. In *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)* (pp. 1-8). IEEE.
44. Chung, M. H., Yang, Y., Wang, L., Cento, G., Jerath, K., Raman, A., ... & Chignell, M. H. (2023). Implementing Data Exfiltration Defense in Situ: A Survey of Countermeasures and Human Involvement. *ACM Computing Surveys*.
45. Thompson, E. C., & Thompson, E. C. (2020). Threat intelligence. *Designing a HIPAA-Compliant Security Operations Center: A Guide to Detecting and Responding to Healthcare Breaches and Events*, 37-63.
46. Kose, Y., Ozer, M., Bastug, M., Varlioglu, S., Basibuyuk, O., & Ponnakanti, H. P. (2021, December). Developing Cybersecurity Workforce: Introducing CyberSec Labs for Industry Standard Cybersecurity Training. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 716-721). IEEE.

https://opensourcery-io.ueniweb.com/blog/the-role-of-osint-in-cyber-threat-hunting

https://www.authentic8.com/blog/OSINT-2021-guide-tools-and-techniques

https://feedly.com/ahead/posts/defining-osint-and-its-role-in-cyber-threat-intelligence

https://portswigger.net/daily-swig/osint-what-is-open-source-intelligence-and-how-is-it-used

https://comsecllc.com/services/corporate-vulnerability-assessment/

https://www.linkedin.com/pulse/critical-role-osint-supporting-other-teams-within-mssp-groeneveld

https://feedly.com/ahead/posts/defining-osint-and-its-role-in-cyber-threat-intelligence

https://feedly.com/ahead/posts/defining-osint-and-its-role-in-cyber-threat-intelligence

https://www.domaintools.com/resources/blog/5-simple-steps-to-bring-cyber-threat-intelligence-cti-sharing-to-your-organ/

https://www.hawk-eye.io/2020/08/cyber-threat-intelligence-and-osint/