Threat Intelligence

Research

1 Abstract

[a] The purpose to write a research paper on Threat intelligence is to understand real time cyber attacks through evidences of threat, hacker's motives, and dark web data and to provide recommendations on enhancing two aspects of the technology. **[b]**Organizations often want robust infrastructure security and invest on data driven tools/devices that help in defending cyber attacks but fail to use them effectively due to less knowledge of threat data or artifacts. These artifacts are evidence based threat data that is provided by Threat intelligence.**[c]**The research paper will recommend two aspects of Threat intelligence that needs to be explored more by first introducing the technology and provide its evolution with future scope, also discussing working and sources of threat data in TI, how organizations select threat intelligence platforms, types of intelligence that is needed and the Diamond model that helps in knowing the whole attack components by one evidence. The paper will also discuss about Indicators of threats and their usefulness with real evidences of analysis done on open source Threat intelligence. In the end, paper will include the Gartner reviews on best Threat intelligence platform available with evidences of how banking organization and teams of other industries use the technology. **[d]**The analysis approach helps organization selecting Threat Intelligence to make good decision in terms of what is needed and what is relevant also guide how to effectively use the technology and work on certain aspects that makes an organization infrastructure security robust. **[e]** A cyber attack can be fully defended if attacker motive, evidence of attack like tools used and procedure followed and dark web data that includes malicious intents, leaked data and relatable discussion is informed by Threat intelligence data.

[f] Cyber, dark web, artifacts, diamond model, indicator of threats

2 Introductions

Threat intelligence is evident based data collected, analyzed and processed through third party sources to understand a threat actor's motives and behaviors. [1]"Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets". **[g]** Evidences based data that shows the relation of it with some previous cyber attacks, ransomware or malicious activities on internet. The threat data (such as system logs or open source intelligence feeds) are generated from internal and external sources and help security teams in identifying the threats relevant to their organizations. TI provides proactive threat management by threat data from open sources that is formatted, correlated and feed to organizations security and alerting systems. **[h]**Infrastructure and network security is managed by data driven devices. Mostly these data are provided by humans after an attack but Threat intelligence is a technology that analyze real time malwares and provide threat data through various sources that is further used in data driven devices proactively before a cyber attack. **[i]** Mostly 95% organization use internet for operations and every organization that is using internet are exposed to cyber attack, a

technology that provides threat data that enables proactive actions/recommendation to defend atost cyber attacks to whole 95% organizations. **[j]** The research is promising as in the world with increasing cyber attacks an intelligence of threat is required that aware and provides necessary data for defense mechanism.

3 The misunderstood definition

[2]The data with no context is not threat intelligence. Threat intelligence is often misunderstood as data that helps in defending attacks but any data with no evidence can even trouble security teams with false alarms. For example, a third party provide an IP address as a malicious, this data is not considered threat intelligence data as the reason of it being malicious is not evident. In the same way, an admin while working in a shift came to know an internal data starts uploading to external sites and block the site on security device. The blocking evidence is not documented and the admin left the office, the other admin who was in other shift came to the office and found that a site is being blocked and could not find any evidence as to why it is blocked. The above scenarios identify non documented actions and no-evident data that will not be considered as threat intelligence.

4 Data, Information and Threat Intelligence

[k] The basic differences between Data, Information and Intelligence. [3.1]The data are simple logs in large volumes that are of limited utility. For example, raw data pertaining to logs of certain source IP in an infrastructure of an organization. Information is collected from data to give a particular output. For example, information that related to a suspicious activity of hike in traffic for a particular server. Processing and analyzing the information for a decision making is intelligence. For example, the information is correlated with past activity that is related to the current hike in traffic and made decision accordingly.

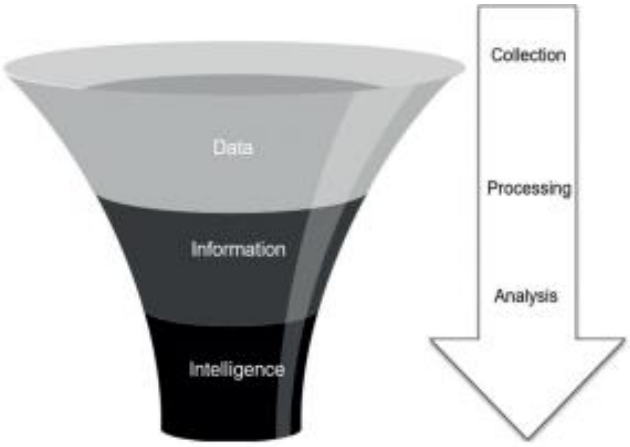


Figure 1: Producing intelligence from threat data.[3.2]

5 Evolution of Threat Intelligence

5.1 Before Threat Intelligence

[4]The methods used before threat intelligence. Cyber security is always about intelligence information that powers the tools and not to battle the minds that made the malware. The precursors for threat intelligence at first were IP and URL blacklists. Security researcher's use suspected IP's and URL's and add it to internal tools for alerting purpose. Security information and event management (SIEM) and next generation firewalls used the blacklists to give alerts and reports. In this way security researchers manually search for threats and sent report to customers. This process was challenging and time consuming and it turn do not ensure proactive security monitoring.

5.2 Idea of Threat Intelligence with Big Data Tools

The idea of threat intelligence developed in year 2010. The dark net activities and malign activities increased and hundreds of IP's, domains and other IOC's are tough to analyze and correlate with certain attack. The cyber security industry uses the Artificial intelligence and machine learning capabilities to automate and correlate data. Millions of sensors provide data feeds and this data is processed and analyzed by big data tools. The system gives extensive visibility and allows complex detection covering all attack surfaces. The ides gives birth to threat intelligence term.

5.3 The false alerts and usage of TI in security systems

Machine meets humans in 2015 as big data tools provide many false alerts. Machine capability to correlate and analyze data coming from millions of sensors generated false alerts for security teams. Security researchers started analyzing intelligence data by feeding data in security systems and analyzing the threats that is relevant to the organization. This involvement enables fast detections, reduced false positives and easy management with the help of other managing tools like SIEM.

5.4 The Increased popularity

By 2018 to 2020 threat intelligence concept ballooned. In 2018, hundreds of threat intelligence platforms were offered by different companies. By the beginning of 2019 companies of every infrastructure started adapting threat intelligence feeds for robust security. The market in growing and according to the usability and requirement of threat intelligence technology researchers suggested TI could be worth 13 billion US dollars by 2023.

6 Intelligence cycle

[I] The working or flow of Threat intelligence data is briefed in Intelligence cycle. [5.1] Threat intelligence has taken several years to build using analytical process by government and military agencies. TI focus on 6 different phases that is combined to called intelligence cycle. The six

phases are direction, collection, processing, analysis, dissemination, and feedback that define the analytical process and will be explained further.

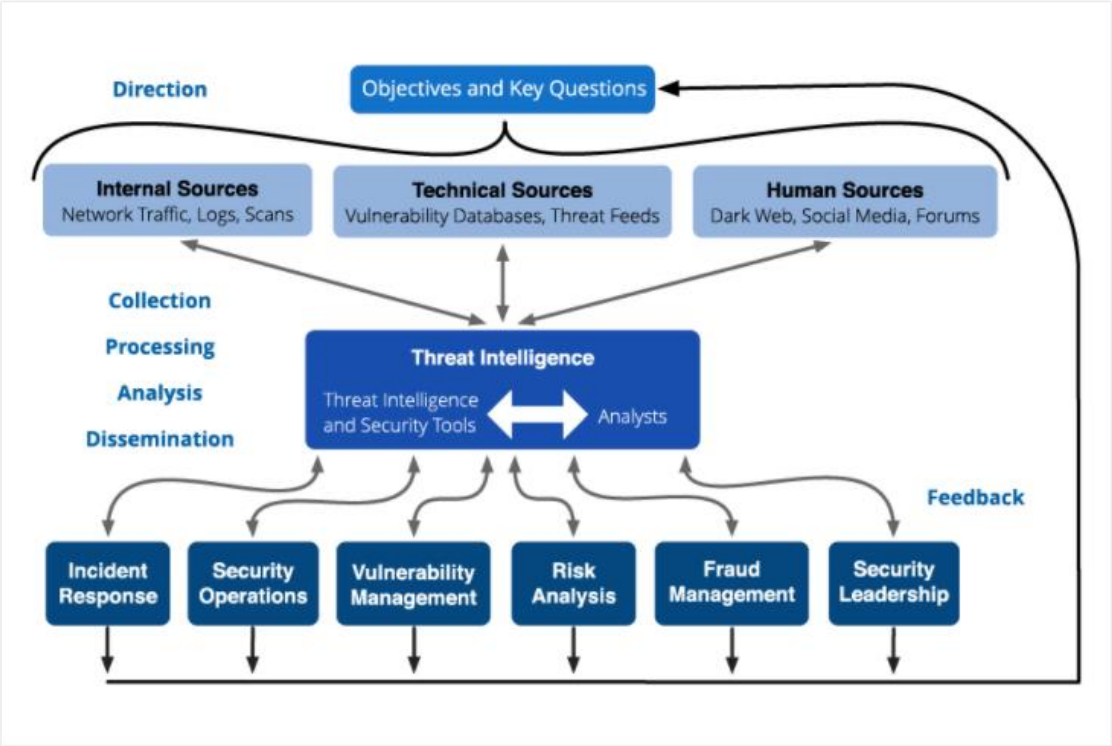


Figure 2: Threat intelligence and the six phases of the intelligence lifecycle. [5.2]

6.1 Direction

[6]The first phase is direction that is setting goal for threat intelligence. The goals involves setting priority of assets needs to be protected, impacts of losing that assets, selecting the best threat intelligence platform that provide expected requirement with less SLA(service level agreement). Organization often needs to decide the goal or actual need of threat intelligence to have the full privilege of the platform.

6.2 Collection

The second phase is collection of information to utilize most important intelligence. Information gathering sources are open source news and blogs, harvesting websites and forums, infiltration from dark web, metadata from internal networks and security devices, and subscription to threat data feeds from cyber security vendors. The collected data is a combined

finished data that is used on intelligent reports or other devices to make proactive monitoring and defense mechanism.

6.3 Processing

The third phase is processing of collected information into a usable format. The raw data from multiple sources comes in variable formats that are formatted into a usable report or readable view. For example, extracting IP addresses from vendors report in a CSV format an inducing it in SIEM for monitoring and alerting purpose. Extracting IOC's (Indicator of compromise) from an email with other information and then enabling endpoints protection tools for automatic blocking. Collecting information and putting in a format for usable inputs to security tools and human actions.

6.4 Analysis

The fourth phase is analysis of the processed information. Analysis is the human process that investigates the information and takes appropriate decisions. The decisions involve actions to avoid future cyber threat, recommendation for new security measures, realtime monitoring and identifying loopholes in organization infrastructure. The analysis stage is the decision making stage that signifies usage of the information provided by threat intelligence.

6.5 Dissemination

The fifth phase is dissemination that involves finished decided output to Threat intelligence utilizing teams. In an organization mainly six teams make use of the technology; incident response, security operations, vulnerability management, risk analysis, fraud management and security leadership. The teams utilize the intelligence data to enable better security for an organization.

6.6 Feedback

The sixth phase is feedback that involves regular response from teams about process betterment. Prioritizing needs of an organization and using TI with appropriate tools for better output is involved in this stage. Regular feedback makes sure the requirement of each group utilizing threat intelligence is adjusted according to change in priorities and change in cyber threat. Feedback is the last stage and it enables requirement adjustment according to priorities.

7 Sources of Threat Intelligence Data

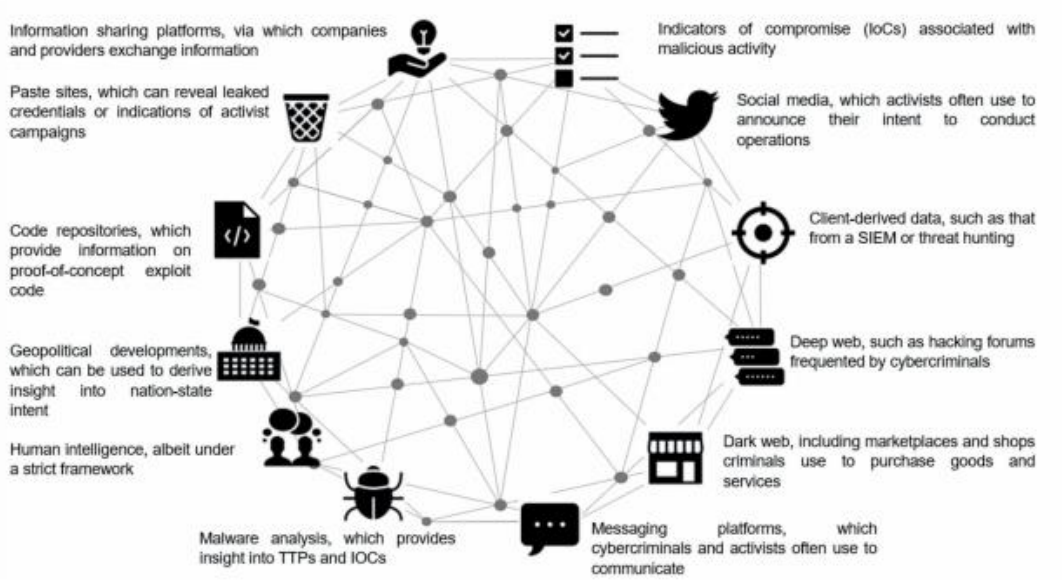


Figure 3: A summary of different sources typically used by threat intelligence providers[8.1]

Threat intelligence providers commonly use wide range of source for intelligence data. IOC's (Indicator of compromise) for cyber threats, TTP's (Technique, tactics and procedure) of adversaries, data leak scenarios and brand reputation of an organization is maintained through various sources providing data.[8.2]Multiple sources give holistic understanding of all the threats an organization face. The sources are client derived data, deep web, dark web, messaging platforms, human intelligence, malware analysis, code repositories, paste sites, and information sharing platforms or social media. These sources are divided into external and internal sources broadly. For proactive response to future cyber attack a threat intelligence platform that provides data from varied forms of sources is must.

7.1 External data

The external data for a threat intelligence platform includes feeds from third party vendors or externally exposed data. Human intelligence comes under external data in one scenario when incident response team member, analyst or engineer put their views and investigative data on external forums and platforms that help organizations in proactive defensive measures. Similarly data feed from dark web that includes discussion of hackers and leaked data information. Malware file information through open source feed from endpoint malware analysis platforms. Data leak information from social media, information sharing platform and paste sides (used for source code and sensitive information sharing) is collected by Threat

intelligence platforms. The external data is taken from varied sources and these sources depend on the organization choice and the platform used for an appropriate purpose.

7.1 External data

The internal data includes infrastructure configuration and on the field data. The infrastructure configuration involves regular analysis of networks for vulnerabilities in the systems. These vulnerabilities include internal website analysis, domain analysis, vulnerabilities in systems and brand reputation by analyzing internal data or copyright scenarios over internet. The on the field data includes investigation of past frauds and cyber forensic to get digital footprints of a cyber attack or crime.

8 Things to consider while selecting Threat intelligence for an Organization

[9]The decision of the appropriate Threat Intelligence for an organization depends on few requirements. Threat intelligence data has been put through analytical and logical process to have proper output in an organization. The process involves human at the end in most cases for evaluation, usage and better output. The decision rests on three requirements that the data should be relevant, actionable and valuable. For better output and relevant threat intelligence information, an organization should verify three requirements.

8.1 Relevant Data

The data should be relevant to an organization. Threat intelligence data or feeds should be relevant to business objective /enterprise/organization. For instance, a company 'A' uses Linux OS(Operating system) on their servers and all the desktops are Apple Macs is approached by a Threat Intelligence vendor that provides OS based vulnerability data. The vendor is best in the market but provide OS vulnerability data for Microsoft Windows. The data provided by the vendor is not relevant to company 'A' since they have no desktop that runs Windows OS. So, the data in itself can be best but needs to be relevant to an organization infrastructure.

8.2 Actionable Data

The data should be actionable. For a threat data to be actionable it should provide enough information so that actions can be taken on it. For example, information like anonymous has launched a phishing attack on the organizations internal users is not enough to take action. Instead a Threat Intelligence data with full evidence that shows phishing attack by certain sender email domains with relevant IP(Internet Protocol) addresses and cyber attack patterns is the actionable data. The security analyst can take actions of blocking and reporting through the information provided by Threat Intelligence.

8.3 Valuable Data

The data should be contextual or valuable. The contextual data provided by Threat intelligence provides security team to take actions and make decision that will robust the business and infrastructure of an organization. Data that helps in blocking cyber attacks from outside world to an organization, reducing false alarms and inform about the latest threat trends surely signifies valuable data.

9 Diamond Model

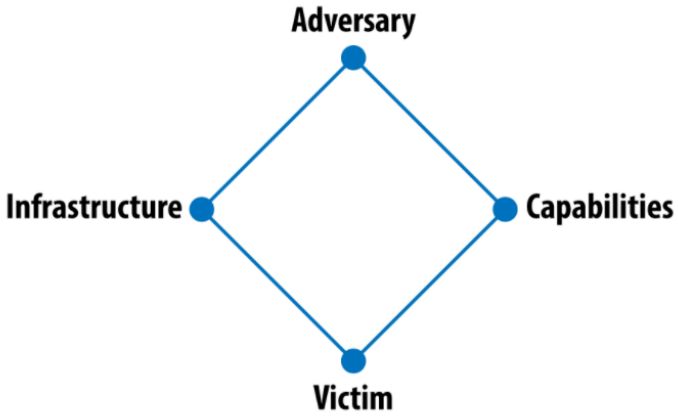


Figure 4: The Diamond Model

[10]Diamond model has four components that are the top information provided by Threat Intelligence. This information related to one another and any one component gives information about other components. The diamond model is a way to bifurcate all aspects of an intrusion that allows analyst to pivot from one point to other in a single attack. The diamond model is useful as it allows connecting information in a cyber attack. For example, a cyber attack occurs through phishing (a suspicious email) and an analyst gets a malicious sender IP behind it. Through intelligence the IP can be searched on Threat intelligence and the appropriate Threat groups and the attack vector is found. The diamond model comprises of four components that are the pivoting stages in diamond model.

9.1.1 First component

First component is Adversary. Adversary is the group or person behind the group. Usually cyber attacks happened by known group and the intentions or threat vectors are known. The diamond model helps in keeping track of the group and the associated indicators.

9.1.2 Second component

Second component is capabilities. The method of attacks, the procedure followed by hackers and the patterns of attacks comes under capabilities. The last cyber attack history helps in identifying till what extent the cyber attack can happen in an organization.

9.1.3 Third component

Third component is Infrastructure. The structures adversary has that are used in a cyber attack like tools, online data, networks, processing data and storages. The infrastructures used by hackers are highly correlated by the other components in diamond model in a certain cyber attack.

9.1.4 Fourth component

Fourth component is Victim. A victim is simply a targeted host, organization, network that is attacked by hackers. A past victim is simply an old cyber attacked host/organization that provides evidences to threat intelligence about the ramification of an attack.

9.2 Diamond model usage in real life example

Real life examples that signify diamond model usage in threat intelligence. In 2019, a Trojan was introduced that has targeted banking organizations specifically. The attacker groups are known as Emotet that has been active throughout history. The attack patterns show mainly these cyber attacks happen through phishing emails that delivers a malware. The attacker's intention is to steal sensitive user's data and sell it on dark web. Here the adversaries are Emotets that use sensitive information as their capabilities to hack through phishing emails as infrastructures on banking organizations as victims.

10 Three types of Intelligence

[11.1]Threat Intelligence provider comes up with three types of intelligence. Strategic, tactical and operational intelligence must be provided in a way using Diamond model. An organization uses any attack model weather it is Diamond model or "Cyber kill chain" the motive is to extract three types of intelligence.

Figure 5: The three components of Intelligence.[11.2]

10.1 Strategic Intelligence

Strategic intelligence directs budgets and resources towards robust security of an organization. In diamond model strategic intelligence aims knowing the adversary and the victim. For example, an organization found that there are 30 percent increase in the phishing attacks where emails with embedded malicious attachments are used. The third party intelligence providers confirm that hackers are investing more resources in such type of attacks. Senior management now has intelligence that allows them investing on more resources fighting those attacks. The organization decides budgeting and resources by knowing details about the group or person behind the attacks and the intentions behind it. From thousands of adversaries active throughout the world some are relevant to an organization. For instance, a banking organization would act on the adversaries that are targeting information such as credit cards and involves in fraud related activities. Finding relevant threat to an organization and the reason behind the threat being relevant is strategic intelligence.

10.1 Tactical Intelligence

Tactical intelligence focuses on the capabilities of the adversaries. In diamond model, tactical intelligence aims in knowing the capabilities of the attacking groups. The intelligence is more technical and aims in knowing how adversaries work. Tactical intelligence works on documenting TTP's (tactics, techniques and procedures) in a report or induce it inside incident response tools, SIEM (Security incident and event management) tools, ticketing tools or TIP (Threat intelligence platform). For example, an attack after breaching the network moves throughout network using Powershell then tactical intelligence helps in enabling Powershell related artifacts to detect/track lateral movement of an attacker inside a network. Tactical intelligence reveals the tools used by adversaries and the time when the attack usually occurs. The tactical intelligence combines information from various sources which is impossible for an organization to collect by itself. The Threat intelligence providers have resources and teams that work on collecting threat related data and provide tactical intelligence to the organizations.

10.2 Operational Intelligence

Commonly used threat intelligence amongst information security communities is Operational intelligence. Operation intelligence focuses on indicators and infrastructures in diamond model. The operational intelligence involves practical IOC's (Indicator of compromise) such as IP addresses, domain names, hashes, registry entries, filenames, email domain etc. This intelligence is fed into SIEM, TIP (Threat Intelligence Platform), endpoints, proxy and firewalls

for preventive actions like blocking. This intelligence helps analyst to figure out the back story of an attack through single IOC like an IP address is seen scanning a network and the analyst can trace back the history of that IP and got to know which past attack uses that IP and if it is relevant. Operational intelligence is timely unlike strategic and tactical intelligence. Often attacker changes the IP addresses, domain names reputation get fixed throughout time, hashes of the file often changes. So actions using operational intelligence are time based. Operational intelligence works on indicators and infrastructure and is used by security communities for blocking and other actions.

11 Pyramid of Pain

The pyramid of pain detects usefulness of the intelligence. The POP detects to which extent the intelligence or indicators are useful, measures the difficulty in finding that indicators or intelligence. Indicators involves hashes to least useful to TTP's the highest useful. Although indicators changes throughout, it is recommended and a good practice to take actions (like blocking on tools) on any indicator observed throughout a cyber attack without considering its usefulness. The pyramid explained and depicted below shows the indicators and their usefulness in detail.

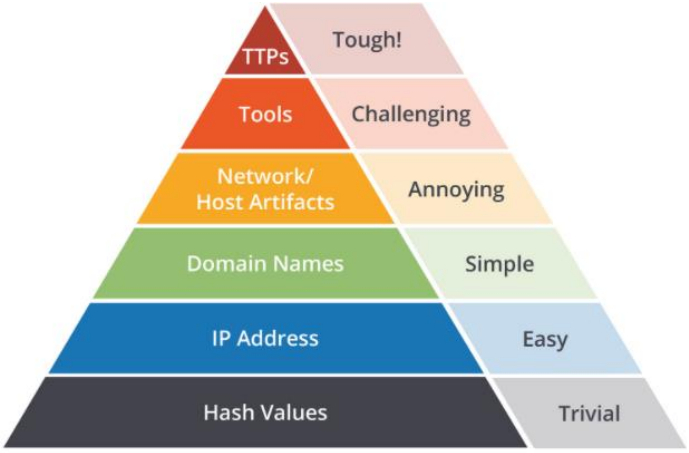


Figure 6: Pyramid of pain. Source: David J.Bianco, personal blog[12]

11.1 Hashes

[13]Hashes are least useful indicators. Hashes are alphanumeric code assign to a file. For every file hash is unique and slight change in file content changes the hash. The hash indicator is susceptible to change and least useful. For example, in a cyber attack a malicious file with virus is installed in the system that infects the network. Security analyst tends to block the file with hash values but this is timely because hashes changes if a slight change in file occurs. Hackers may change a character inside a file that changes the hash value and the old hash which is

blocked or put under tools for monitoring is of no use. Since hashes changes with a slight change in file it is least useful indicator.

11.2 IP (Internet Protocol) addresses

IP addresses do not remain same throughout and is the second last useful indictor. Hackers often use proxies, VPN or TOR nodes to initiate an attack and the IP's are untraceable. The one IP that is observe in a day scanning a system or targeting an organization may change the other day because of tools. For example, an IP belongs to a certain country started scanning a network suddenly and exploited a vulnerability in a system. The security analyst will observe the IP and put this under blocking and report it as malicious. But the group behind the cyber attack often changes IP and does the same attack again. So, keeping the old IP under the blocking and monitoring mode to detect and prevent future attacks sometimes work but may not work if the IP address is changed in another instance of an attack.

11.3 Domains/URL's

Domain names are as easy to change as IP addresses but are more useful than above discussed indicators. For example, a phishing email that has a malicious URL that takes users personal information is often seen in real cyber attacks. Security analysts usually report the domains and block it on proxies so that no one can access it from the organization and the intent of the hackers fails. But since domain names are registered and paid it can be redirected to different malicious destination using dynamic DNS systems. Most cyber attacks use limited domain names in an attack and auctioning on the domains indicators for preventive measure is a good practice. Although the domains can be changed too but require more work it is high useful than hashes and IP address.

11.4 Network and host artefacts

Network and host artifacts are the third most useful indicator. For example, an attack that use remote desktop protocol to get access to remote hosts and downloads a extracts data from one of the directory in Linux machines. Here network artifact is the protocol used and the host artifact is the Linux machine. Knowing these indicators related to an attack usually stops the attacks with same intent.

11.5 Tools

Tools are the second most useful indicator. Attackers use online resources and tools to initiate an attack. The intelligence that gives indicators that certain tools are used by particular adversary then analyzing the network logs and monitoring any activity coming through the

particular tools stops the attacks. In this way the adversaries have to change the tools that will increase the testing and training time for them and in turn increase your defense mechanism.

11.5 TTP's (Technique, tactics and procedure)

Indicators like tactic, technique and procedure is the most useful and hard to achieve indicator. Attackers put all their knowledge and training to perform an attack. The knowledge is evident in the tactic, technique and procedure followed by the attacker. For example, a ransomware attack happened in an organization that locks computers and asks for money to unlock or to retrieve data. The ransomware downloads occurs through a phishing email send to users with an attachment. The attachment is a RAR file that once clicks gets downloads and a script is used that executes commands and lock the systems. The TTP used here is the email with sender domain as ppp.com and RAR attachment that when downloaded runs JavaScript that execute certain processes. The whole procedure once known by the organization helps in defending 99 percent same type of attacks. An organization here can create monitoring and blocking mechanism of all RAR files through emails and block all email from certain subjects and senders and enables endpoints to block the automated scripts and processes involved. Another attack pattern example is (AES encryption, files of exactly 750,000 bytes, file copies via SMB). The TTP is the combination of lot of actions that ruins the whole mechanism of attack set by an attacker. This way, an attacker has to retrain and get more resources, knowledge and another method to attack the same organization.

12 Investigation on Threat intelligence platform

Internet Protocol addresses investigation on a Threat Intelligence Platform and a brief explanation on working of sample platform. Virus Total is an open source threat intelligence platform used for information on threat indicators. Figure 7.1 shows that the IP was marked as an indicator of malware on 7 engines. Virus total use feeds from more than 30 engines to get a verdict on any IOC searched. Humans feedback are also captured by the platform as seen in figure 7.2. Many researchers, analyst and other threat hunters investigate and put their comments that can be read and used for information. Figure 7.3 shows IP is used to deliver seen various files and communicate to outside domain. Figure 7.4 shows information of one file indicating as a malware. The file is an exe file that is a TROJAN by the adversary named Emotet. Emotet is a famous cyber attack adversary targeting banking organizations in 2019. As studied previously in diamond model, Threat intelligence helps analyst to jump to conclusion with one Indicator to others like in this case from IP to the files and the related cyber attack.

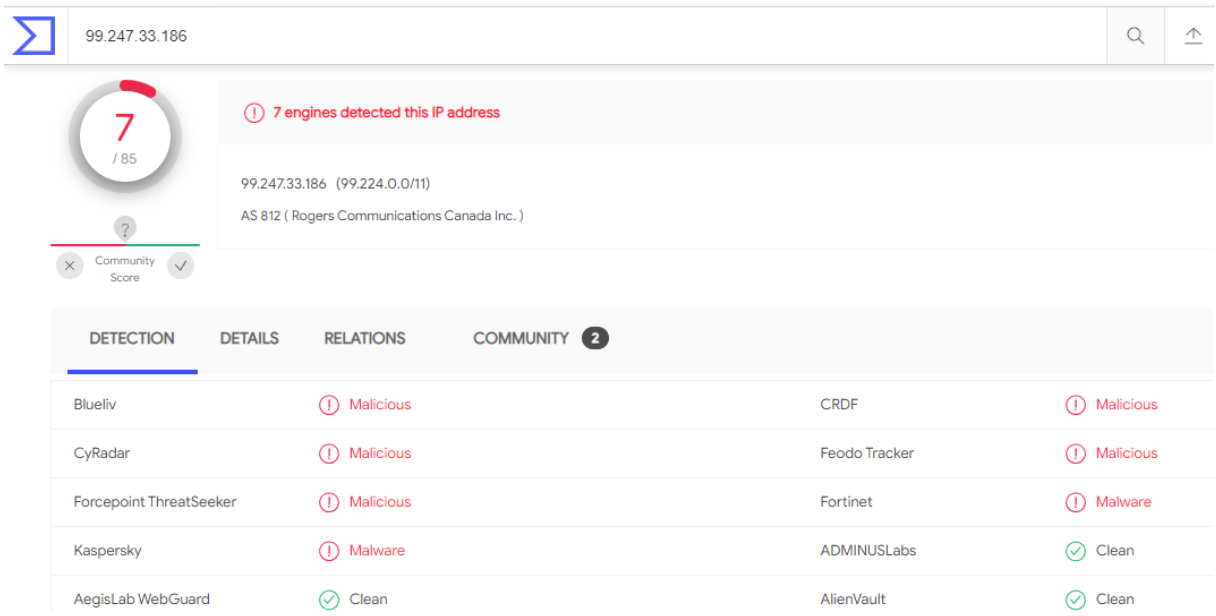


Figure 7.1: Virus Total portal[14]

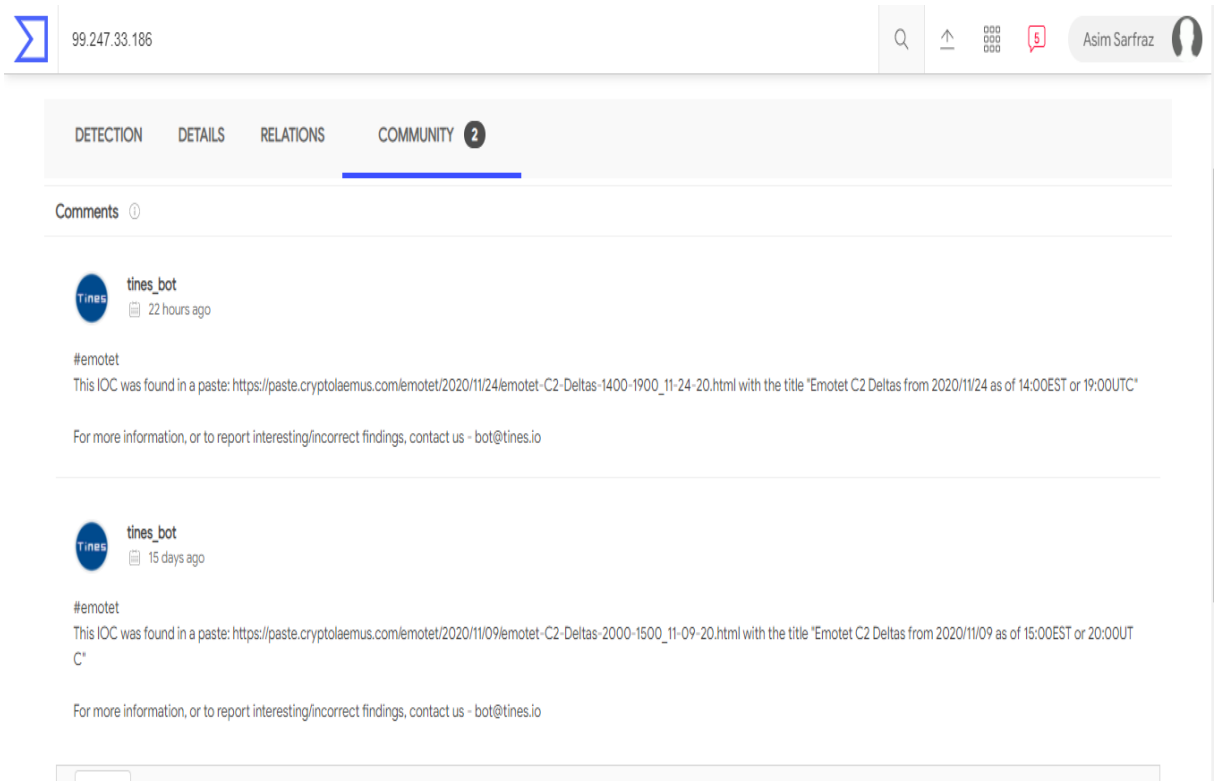


Figure 7.2: Virus Total portal[15]

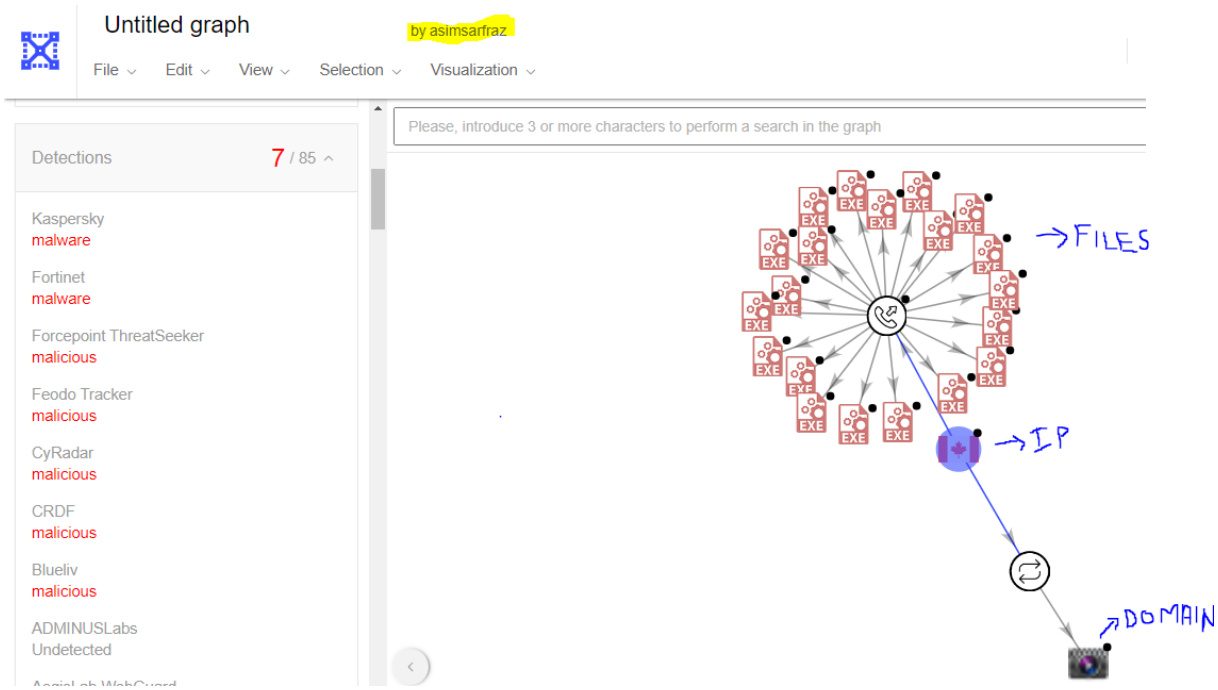


Figure 7.3: Virus Total portal[16.1]

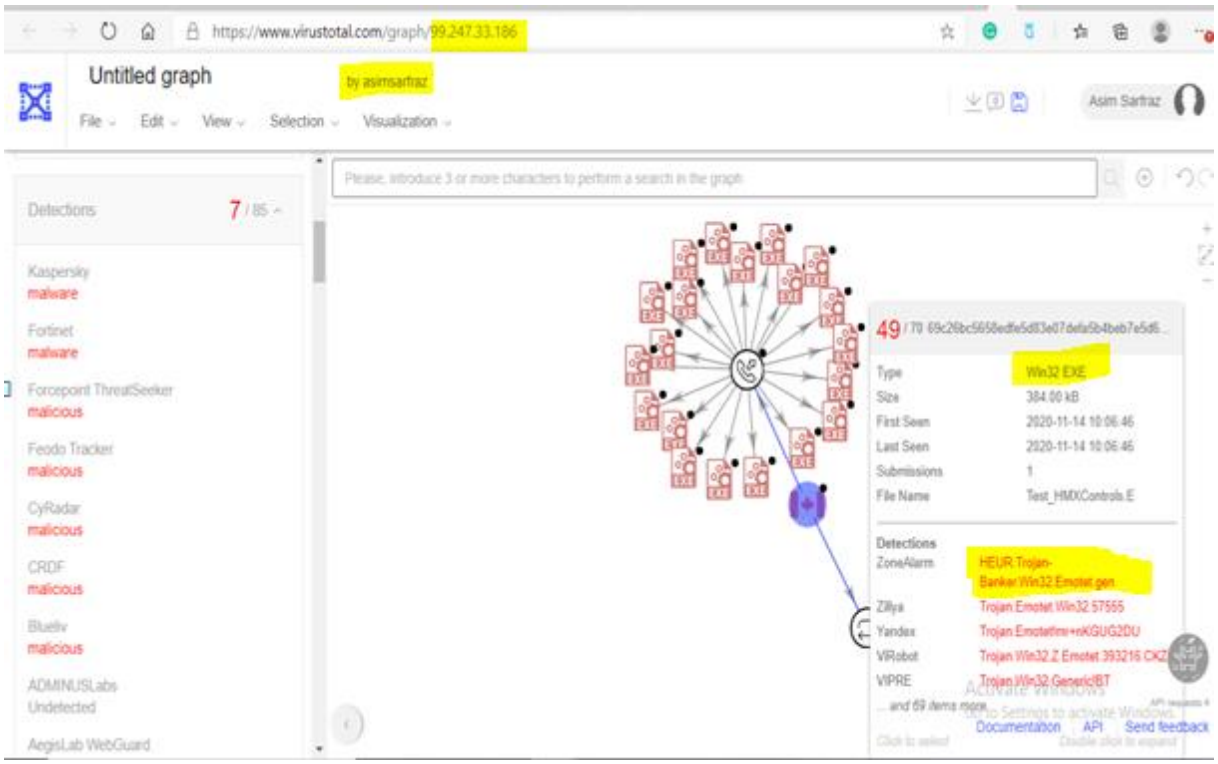


Figure 7.4: Virus Total portal[16.2]

13 How various organization teams use Threat intelligence data?

Teams in an organization use Cyber Threat intelligence data for various means. Security operation center uses threat intelligence data to create alerts or rule on SIEM (security incident and event management) tool and perform real time monitoring of cyber threat alerts. IT security management use threat intelligence data and attack scenarios to take appropriate decision on defensive measure for an organization. Vulnerability management team use latest information on OS patches and updates the organization infrastructure by proper patch management. Investigation and response team perform analysis of threat intelligence data and take proper tool update, involve defense against TTP's of adversaries and IOC deployment on firewalls, IPS (Intrusion prevention system), proxies etc. Training and awareness team study scenarios relevant to threat intelligence data and provide training to unaware non technical employees. For example cyber attacks happen through phishing so training team aware employees and users to avoid action on phishing emails and report. Phishing emails and vishing (Fraud through call) reporting and awareness scenarios is done by this team. Development team use threat intelligence data and work with IT security managers to handle technical aspect of deploying new defensive tools or updating the old ones. Threat intelligence data has major role in provide defensive measures and various teams use these data for maintaining robust security in an organization.

14 How banking organizations use Threat intelligence?

A banking organization use threat intelligence for various aspects. Brand reputation is the main aspect and banks often aim to maintain trust. Banking websites, apps, and social media accounts are even replicated by hackers for fraud or data leaks. Threat intelligence provides information on these replicating scenarios and proper actions are taken appropriately. Executive monitoring is the second aspect. Executives have senior management responsibilities often being approached on social media or conferences by hackers. Additionally executives often and unknowingly put sensitive information about new projects and infrastructure on Linkedin that is monitored by Threat intelligence platform taken by the organization to defend data leaks. Financial data like credit card information or client financial quotations related to projects are often being leaked or shared on open forums. The threat intelligence platform monitors these financial data to give remediation actions. Servers and systems used in organizations often have loopholes that need to be patched. For example, Microsoft often provide patched for new vulnerabilities on Windows OS (operating system). Threat intelligence informs these patches to an organization and gives thorough action plan to the number of system with old OS. Threat intelligence also provides cyber news from various sources for knowledge. Banking organization refers the relevant news and takes appropriate actions. Banking organizations use threat intelligence platform for most important aspects but in the real world every organization needs robust security of data and approach towards threat intelligence platforms.

15 Gartner peer reviews on Threat intelligence platforms

The best Threat intelligence Platform according to industries and regions as per Gartner reviews. One TI can be best for some organization but not up to the mark for the other. As per the reviews on Gartner in manufacturing, services and government industries Kapersky Threat Intelligence Services has better reviews due to sandboxing, lookup and Threat reporting capabilities. For communication industries Recorded future named TI has better reviews due to multiple sources, brand reputation monitoring and dark web feeds from relatable forums. Healthcare industries gave better reviews for Wildfire by Palo Alto due to easy and fast searching and unknown file malware detection/blocking. Consequently kaspersky has better reviews from organizations and customers from Europe, Middle East and Africa while North America gave good reviews to Recorded Future. As most of the organization in Middle East is construction and manufacturing related and North America has more communication industries which provide evidence for the reviews provided above that is according to industries. So, no TI can be concluded better than other as their usage depends on the feeds they provide that should be relevant to the organizations infrastructure.

16 The two aspects of threat Intelligence that needs to be worked on

16.1 Intelligence sharing

The first aspects that will make Threat intelligence more valuable are proper intelligence sharing mechanism. Collective defence and sharing of strategies amongst organization/industries is considered most valuable aspect. This is common old concept came from military strategies to ally forces against common enemies. The world is lacking in intelligence sharing. For example most of the organization in regions such as UAE after being a victim of Zero day attacked (attack pattern/way/scenario happened for the first time in world) does not share whole artefacts. The other organization will not be aware of all TTP's and IOC's and in turn their probability of getting cyber attacked from the same adversaries is more. The above scenario does not mean that Threat intelligence depend on reporting of the Zero day attacks and then only take actions. TI platform do anomaly and open source investigation for Zero day attacks but reporting by the victim gives more holistic understanding of the cyber attack that happened.

16.2 Dark web

The second aspect that will make Threat intelligence more valuable is having more exposure on dark web feeds. Everything we know as internet is the surface net. Hackers and fraudsters communicate on dark web related to selling or buying of illegal data or things and discussing future and past hacks. Threat intelligence platform companies often have people that camouflage in the discussing forums and get intelligence data but it is limited. Dark web is huge and getting relevant threat intelligence data from it is like finding a needle in a jungle. The dark web feeds are limited and more exposure and proper mechanism to get more feeds from it will surely reduce impact of future cyber threats.

17 Conclusion and recommendations

The research goal is to provide information on Threat intelligence technology that provide threat data for defense mechanism against cyber attacks through understanding of sources of TI, leveraging diamond model for knowing the attack components, using indicator of compromise for defensive and informational actions on cyber attacks, helping organizations to select relevant and appropriate Threat intelligence platform by Gartner reviews and providing evidences of how banking organization and other organization teams use TI. The recommendation on increasing exposure on Intelligence sharing and dark web can be achieved too. Properly designing forums for sharing and awarding victim organizations providing artifacts is the solution for better intelligence sharing. While increasing man power cover maximum forums on dark web and training capabilities of the employees involve helps in getting out relevant and important data more easily.

References:

[1] McMillan, Rob "Definition: Threat Intelligence." Gartner Research. Published :May 16, 2013. Accessed :November 10, 2020. Available: https://www.gartner.com/en/documents/2487216/definition-threat-intelligence

[2] Liska, Allan. "Threat Intelligence in Practice." Oreilly. Published: November 12, 2017. Accessed:November 2, 2020. Available: https://learning.oreilly.com/library/view/threat-intelligence-in/9781492049302/copyright-page01.html

[3] Crest. "What is Cyber Threat Intelligence and how is it used?" *Crest*. Accessed November 2, 2020. Available: https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf

[4] Karasev, Artem. "How threat intelligence evolved, and where it will go next" *Kaspersky*. Accessed: November 9, 2020. Available: https://www.kaspersky.com/blog/secure-futures-magazine/threat-intelligence-trends/35109/

[5] Baker, Kurt. "WHAT IS CYBER THREAT INTELLIGENCE?" *Crowdstrike*. Published July 12, 2019. Accessed October 25, 2020. Available: https://www.crowdstrike.com/epp-101/threat-intelligence/#:~:text=Threat intelligence benefits organizations of all shapes and,protection that would otherwise be out of reach.

[6] The recorded future team. "What the 6 Phases of the Threat Intelligence Lifecycle Mean for Your Team" *Recorded Future*. Published January 15, 2020. Accessed: October 30, 2020. Available: https://www.recordedfuture.com/threat-intelligence-lifecycle-phases/--

[7] RFSID. "Top 6 Sources for Identifying Threat Actor TTPs." *Recorded future*. Published: August 17, 2016. Accessed October 21, 2020. Available: https://www.recordedfuture.com/threat-actor-ttp-sources/

[8] Crest, “What is Cyber Threat Intelligence and how is it used?” in Title of Different sources of intelligence, 2019 ed. Sec 2, pp.11-13.

[9] Carnall, James and Olson, Eric. "How to Define and Build an Effective Cyber Threat Intelligence Capability" Syngress. Published 2014. Accessed Octber 30, 2020. Available: https://learning.oreilly.com/library/view/how-to-define/9780128027301/B9780128027301000028/B9780128027301000028.xhtml

[10] CARREON, CRIS. "Applying Threat Intelligence to the Diamond Model of Intrusion Analysis." Recorded Future. PublishedJuly 25, 2018. Accessed November 5, 2020. Available: https://www.recordedfuture.com/diamond-model-intrusion-analysis/

[11] Liska, Allan, "Threat Intelligence in Practice," in Chapter 1. *Defining Threat Intelligence*, 2018 ed. Sebastopol, CA. Courtney Allen. Chapter 1. Pubished 2018

[12] Fireye. "The Pyramid of Pain." Fireye. Published 2014. Accesses November 8, 2020. Available: https://rvasec.com/slides/2014/Bianco_Pyramid of Pain.pdf

[13] Sai, Niketan. "What is Pyramid of Pain ? & It’s types." Infosavvy. Accessed November 2, 2020. Available : https://info-savvy.com/what-is-pyramid-of-pain-its-types/#:~:text=Pyramid of pain represents the types of indicators,the indicators at each level are being denied.

[14]Virus total. "6 engines detected this IP address" Virus total. Accessed November 11, 2020. Available: https://www.virustotal.com/gui/ip-address/99.247.33.186/community

[15]Virus total. "6 engines detected this IP address" Virus total. Accessed November 11, 2020. Available: https://www.virustotal.com/gui/ip-address/99.247.33.186/detection

[16]Virus total. "Graph" Virus total. Accessed November 11, 2020. Available: https://www.virustotal.com/graph/99.247.33.186

[17] Crest, “What is Cyber Threat Intelligence and how is it used?” in Title of Different sources of intelligence, 2019 ed. Sec 2, pp.15-16.

[18]Gartner Peer insight. "Security Threat Intelligence Products and Services" Gartner. Accessed November 10, 2020. Available: https://www.gartner.com/reviews/market/security-threat-intelligence-services

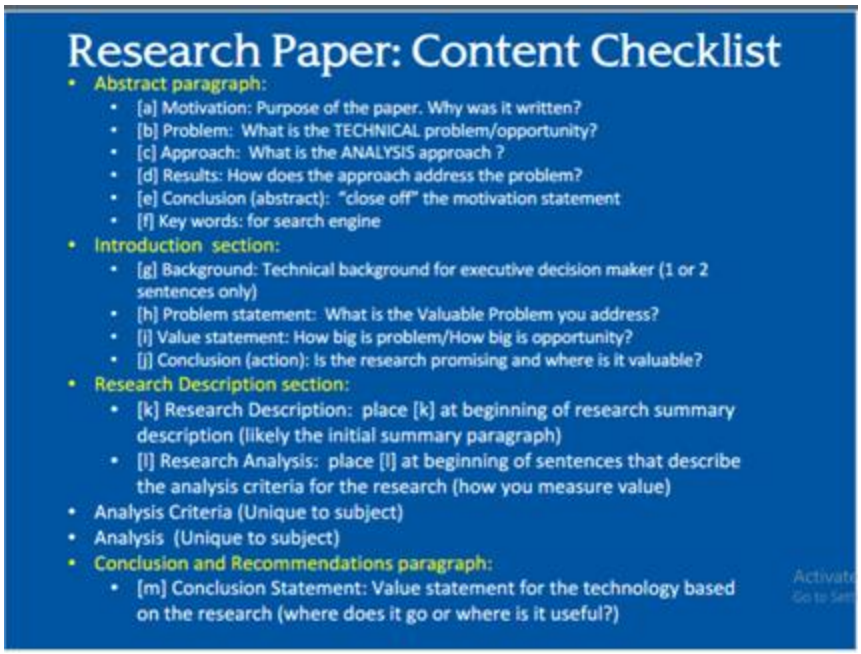
[19] CASSETTO, ORION. "Threat Intelligence: Threat Feeds, Tools, and Challenges." Exambeam. Published December 11, 2018. Accessed November 12, 2020. Available: https://www.exabeam.com/siem/4-layers-threat-intelligence/

[20] CYWARE. "The Role of Threat Intelligence Sharing in Collective Defense" Cyware. Published :June 11, 2020. Accessed October 29, 2020. Available: https://cyware.com/blog/the-role-of-threat-intelligence-sharing-in-collective-defense-6b9f/

[21] APMG International. "Using the Dark Web for Threat Intelligence" Blog. Published: February 25, 2020. Accessed October 20, 2020. Available: https://apmg-international.com/article/using-dark-web-threat-intelligence

[22] Express Journalr. (2020, October). CYBER THREAT INTELLIGENCE INDUSTRY MARKET WITH FUTURE PROSPECTS, KEY PLAYER SWOT ANALYSIS AND FORECAST TO 2025 [Online]. A vailable: https://www.express-journal.com/cyber-threat-intelligence-industry-market-216892/

Item	
Word Count (body of document only)	~5500
Underline all topic sentences (write topic sentences first, do not just check after the paragraph is complete. Sentences, not key words)	Confirmed
No personal pronouns (I, we, our, my…)	Confirmed
No instance of "very"	Confirmed
No use of passive voice	Confirmed (rarely used)
All paragraphs complete with at least 3 sentences	Confirmed


Research Paper: Content Checklist
Abstract paragraph:
[a] Motivation: Purpose of the paper. Why was it written?
[b] Problem: What is the TECHNICAL problem/opportunity?
[c] Approach: What is the ANALYSIS approach ?
[d] Results: How does the approach address the problem?
[e] Conclusion (abstract): "close off" the motivation statement
[f] Key words: for search engine
Introduction section:
[g] Background: Technical background for executive decision maker (1 or 2 sentences only)
[h] Problem statement: What is the Valuable Problem you address?
[i] Value statement: How big is problem/How big is opportunity?
[j] Conclusion (action): Is the research promising and where is it valuable?
Research Description section:
[k] Research Description: place [k] at beginning of research summary description (likely the initial summary paragraph)
[l] Research Analysis: place [l] at beginning of sentences that describe the analysis criteria for the research (how you measure value)
Analysis Criteria (Unique to subject)
Analysis (Unique to subject)
Conclusion and Recommendations paragraph:
[m] Conclusion Statement: Value statement for the technology based on the research (where does it go or where is it useful?)