International Journal of Digital Crime and Forensics
Volume 12 • Issue 4 • October-December 2020

A Summary of the Development of Cyber Security Threat Intelligence Sharing

Lili Du, JiLin University, China
Yaqin Fan, JiLin University, China
Lvyang Zhang, Yiwu Industrial and Commercial College, China
Lianying Wang, Tencent Security Xuanwu Lab, China
Tianhang Sun, Electrical Engineering and Telecommunications, University of New South Wales, Australia

ABSTRACT

In recent years, the sharing of cybersecurity threat intelligence (hereinafter referred to as threat intelligence) has received increasing attention from national network security management organizations and network security enterprises. Academia and industry have conducted research on threat intelligence analysis and sharing. This paper first introduces the value and significance of threat intelligence. Then it introduces the commonly used threat intelligence analysis model. Then it organizes and classifies the threat intelligence sharing norms and threat intelligence vendors. Then it starts from the main problems faced by threat intelligence sharing. A solution to build regional network security capabilities is presented; finally, the future research direction of threat intelligence sharing is explored.

KEYWORDS

Cyberspace Security, Intelligence Sharing, Regional Network Security Capabilities, Threat Intelligence

1. INTRODUCTION

1.1. Definition and Significance of Threat Intelligence

With the diversification, complexity and specialization of today's cyber-attacks, the passive protection methods of traditional security have gradually failed, and the defense against attacks has gradually turned to the active defense method based on detection and analysis. However, the current global detection of attacks is not optimistic. In order to effectively solve the problem of offensive and defensive information in the offensive and defensive process, more and more enterprises are beginning to pay attention to the construction of threat intelligence platforms, through the collection and sharing of threat intelligence. Improve the efficiency of the corporate security team (RFSID,2017).

The definition of threat intelligence in the industry is different. Most of the literature refers to the definition proposed by Gartner in the 2014 Market Guide for Security Threat Intelligence Service: Threat Intelligence is about IT. Evidence-based knowledge of existing or potential threats to information

DOI: 10.4018/IJDCF.2020100105

assets, including contexts, mechanisms, indicators, inferences, and feasible recommendations that can provide a basis for decision-making on threat response.

In the era of big data, any behavior can be recorded and analyzed. Once a cybersecurity incident occurs, the behavioral methods involved in the incident will be recorded and analyzed, and corresponding threat information will be generated for reference by other parties to avoid the trick. This is the meaning of threat intelligence. Threat Intelligence provides strong data support for all stages of security analysis with its highly standardized data format, high knowledge density of data content, high accuracy and strong correlation. As a result, security teams in various countries are actively exploring the value of threat intelligence data and researching threat intelligence analysis and sharing technologies(Solomon,2017).

1.2. Network Security Threat Intelligence Usage Scenario

1.2.1. Attack Detection and Defense

Based on threat intelligence data, you can create signatures for IDPs or AV products, or generate rules for products such as NFT (Network Forensics Tool), SIEM, TTDR (Terminal Threat Detection and Response) for attack detection. For example, IP, domain name, URL, etc. are used as machine-readable intelligence IOC (there are many internationally available machine-readable threat intelligence standards, including: STIX, OpenIOC, IODEF, CIF, OTX, etc.), which are directly imported into the device for access to import and export traffic. control.

1.2.2. Attack Source

Security analysis and attack source tracing in incident response is one of the important tasks. It can also rely on threat intelligence to process it more easily and efficiently. In the determination of attack scope, the predictive type of metric can be used to predict the possible malicious activities before or after the attack cues are discovered, so as to more clearly clarify the scope of the attack; at the same time, the early work results can be input into the SIEM type device as threat information. Conduct a historical index to get a more comprehensive list of assets that may be affected or other clues. In particular, the existing threat intelligence platform can be used to tighten some key information. For example, if some IP are found in the device log, then the threat intelligence search can be performed according to IP, and the history communication record of IP is used. It has been associated with malicious samples, PDNS, reverse domain name resolution results, etc. to determine the nature of IP. If it is malicious IP, it can be further queried according to the results.

1.2.3. Situational Awareness

Situational awareness, many security teams are also called security operations. Many security teams now have their own Security Operations Center (SOC). The role of the SOC is generally responsible for emergency response, security monitoring, and the development of an overall security strategy. With the rise of threat intelligence, the Intelligence-Driven Security Operations Center (ISOC) has begun to be proposed. ISOC has the ability to integrate and analyze big data. It can generate its own intelligence related to the enterprise and form its own perception (confidant). It can also call external open source or paid threat information interface to obtain the latest external consultation and form an external Perceived ability (knowing oneself), resulting in a certain situational awareness.

Threat intelligence was proposed a few years ago, and there has been some development at home and abroad. Many security vendors have begun to build their own threat intelligence platforms. Since the WannaCry incident, people have begun to appear on existing defense systems. The question is that threat intelligence has once again become a research hotspot. This paper mainly introduces threat intelligence from the perspective of intelligence sharing. Firstly, it introduces the common threat intelligence model. On this basis, it introduces the existing information sharing norms, then analyzes

the current problems in intelligence sharing, and finally proposes a construction area. Information sharing program for network security capabilities, providing reference for subsequent research

2. NET SECURITY THREAT INTELLIGENCE MODEL

The offensive and defensive confrontation is ultimately the confrontation of human beings and the confrontation of intelligence capabilities. All knowledge changes rapidly, from which process methods or basic principles must be summarized. The Threat Intelligence Model is an analytical model for the above challenges. It is expected to reduce the cost of defenders and increase the cost of attackers. It provides a way to integrate intelligence into the analytics platform, correlate, categorize, and predict events based on the attacker's activities while planning and implementing threat mitigation strategies (Gartner,2017).

In order to better carry out threat intelligence analysis, in recent years people have been committed to the research of threat intelligence analysis models. It is difficult to extract valuable information from a large amount of data. It is necessary to ensure the accuracy and timeliness of the results of data analysis as an intelligence input practice. The rapid change of network information is becoming more and more demanding for people's data analysis. An effective threat intelligence analysis model plays a vital role in the whole data analysis process. At present, practitioners have proposed different analysis models, including attack graph models based on attack perspectives, chain-killing models based on attack perspectives, and diamond models based on event perspectives.

2.1. Attack Graph Model Based on Attack Perspective

The attack graph was proposed by Cuningham et al. in 1985. They believe that the attack graph is composed of various components that are connected to each other by physical or logical methods. A typical cyber-attack graph consists of nodes and directed edges of connected nodes. The node indicates the state of the network, and the directed edge between the nodes indicates the transition relationship between the network states.

In order to generate an attack graph, the network modeling and modeling process first requires a large amount of security-related information in the network, such as host configuration information, host vulnerability information, network topology information, and network configuration information. In the process of generating a network attack graph, it is necessary to apply the knowledge of the relevant vulnerability database to determine the relationship between the various vulnerabilities existing in the network.

Network modeling and attack graph generation need to fully consider the final application of the generated attack graph. When performing penetration testing, it is necessary to find out all the attack paths. For risk analysis or finding the shortest attack path, you may need to consider the complexity of each atomic attack. Or the probability of success and the degree of harm caused by the successful exploitation of the vulnerability, etc., and the cost of each vulnerability patch needs to be calculated when guiding vulnerability patch management.

Therefore, the final application of the attack graph determines the model and generation method that needs to be established to some extent. The generation method of the attack graph is represented by the network model and the vulnerability database information data structure. At present, there are many methods for generating attack graphs. In order to facilitate the analysis, comparison and evaluation of these methods, it is necessary to analyze the attack graph generation mechanism, find out the attributes that can be used for analysis and comparison, and classify the generation methods. Identify problems and discover possible research findings.

2.2. Kill Chain Model Based on Attack Perspective

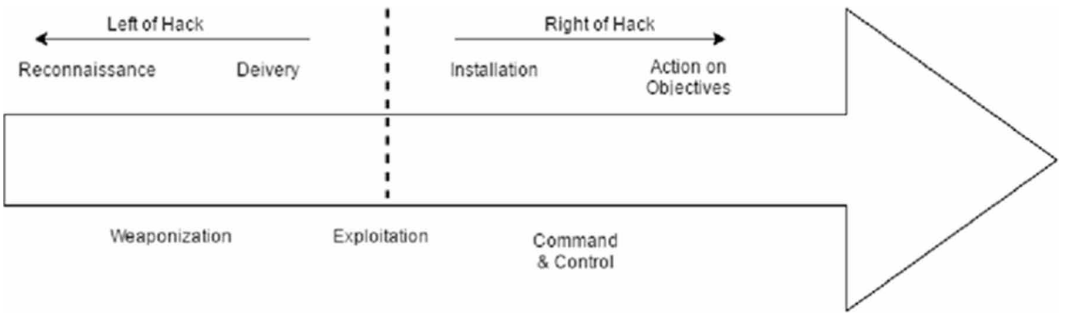
Kill chain is a model of the network intrusion attack kill chain proposed by Lockheed Martin in the United States in 2013, drawing on the concept of "kill chain" in the military field.

From the attacker's point of view, the Kill chain model performs a segmented task description of the attacker's network intrusion attack behavior process, thus forming a complete "kill chain":

- **Reconnaissance:** Find possible targets and track target dynamics;
- **Weaponization:** Put malware into valid payloads (such as Adobe Pdf and Microsoft Office files) to determine the attack mode and complete the attack preparation;
- **Delivery:** Targeted weapons (malicious code) to the target environment (eg via email attachments, websites or USB drives);
- **Exploitation:** Use malicious vulnerabilities or defects to trigger malicious code and gain system control rights;
- **Installation:** Implant malicious programs and backdoors to ensure the survival of malicious programs and maintain control rights continuously;
- **Command and Control:** Establish a communication connection with an external C2 server, and use a protocol such as Web, DNS, mail, etc. to hide the communication channel;
- **Action on Objectives:** Conduct direct intrusion attacks, steal data, disrupt system operations, or move further laterally within the internal network.

The essence of the Kill chain model (Figure 1) is to clearly propose that the attack and defense sides have their own advantages in the process of attack and defense. The Kill Chain model analyzes and describes external threats and intrusion attacks from the perspective of an attacker. According to this chain, the defender can construct a defense-based defense system based on threat intelligence to quickly detect external threats, accurately cut off the key nodes of the chain, and prevent or even counter the attacker's intrusion attacks. That is, in the seven steps in which the attack ultimately causes loss, the detection or blocking of any step can effectively block and block. Even if it is found to be compromised, there is still a chance to remedy the damage before it causes the final loss (Ashok, 2015).

Figure 1. Kill chain model



If the defender can find counterattacks faster than the attacker, then the cost of the attacker's intrusion will rise sharply. This model shows that compared to the traditional view, the intruder does not have many advantages over defenders.

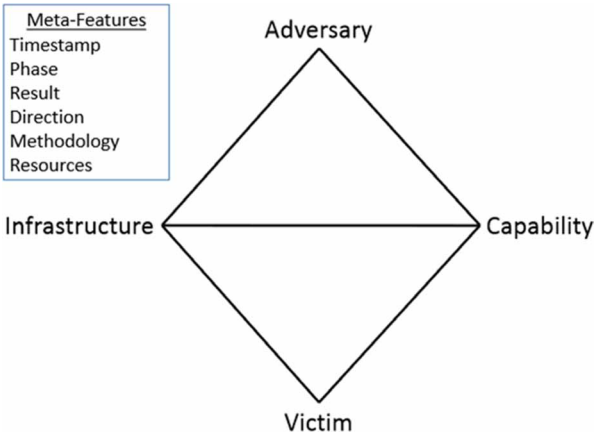
Currently, the Kill Chain model has been applied to the STIX 2.0 standard. ATT&CK can be seen as an enhanced knowledge framework for the last four links in the Kill Chain model.

2.3. Diamond Model Based on Event Perspective

The Diamond Model is an analytical framework model for network intrusion attacks proposed by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz in the 2013 paper "The Diamond Model of Intrusion Analysis."

Diamond model (Figure 2) considered that no matter what kind of intrusion, the basic elements are one of the event, and each event consists of the following four core features: the adversary, capability, infrastructure and the victim. The four core features are connected by lines to represent the basic relationship with each other and arranged in a diamond shape to form a structure resembling a "diamond" shape, hence the name "diamond model". At the same time, the model defines two important extended meta-characteristics of socio-political relationships (between opponents and victims) and technical capabilities (to ensure capacity and infrastructure operability).

Figure 2. Diamond model



Therefore, each event can be understood as a structured description of "what infrastructure is deployed on the victim's ability to invade the victim." In the analysis, the analyst can use the pivoting (also translated as "fulcrum") analysis, extract a single meta-feature as a starting point, and use the observable data sources such as intelligence and alarms, combined with the understanding and analysis of the relationship between meta-features. In turn, other relevant meta-features are discovered, more intelligence about the adversary, new attack capabilities, infrastructure and victims (including potential victims) that may have been attacked.

In terms of correlation analysis of events, the diamond model introduces the analysis concepts of "active thread", "activity map", and "attack activity map", combined with the Kill Chain model, by following the causal activity thread, or the activity group. Or an attack path diagram similar to an attack tree, correlating different events from various analysis dimensions and inferring undetected events.

Threat intelligence is one of the access data sources that the diamond model focuses on when conducting revolving analysis and correlation analysis. Therefore, when building a security analysis tool or platform based on a diamond model, compatibility issues with threat intelligence standards such as STIX/TAXII must be considered.

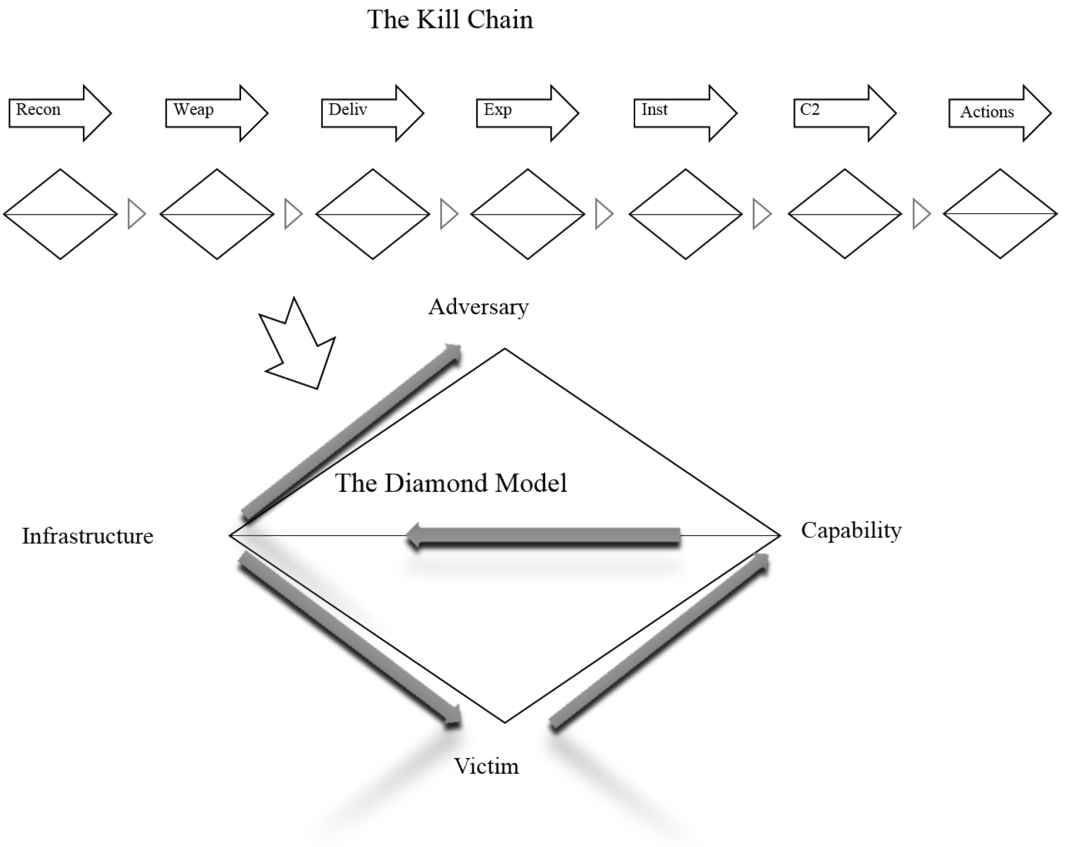
2.4. Active Defense Model Based on Combination of Kill Chain and Diamond Model

The kill chain and the diamond model each have their own characteristics and complement each other. The kill chain model focuses on describing the process, details the stages of the seven-step attack, extracts indicators for each phase, and conducts cross-stage tracking. The diamond model

directly complements each step of the attack chain analysis, using structured indicators to define and understand the activities of the opponents are conducive to the accumulation of knowledge. The combination of the two can not only complete the emergency, but also form knowledge precipitation and threat intelligence, and understand the attacker's intention.

The Active Cyber Defense Cycle (Figure 3) takes threat intelligence and attacker information generated using both the kill chain model and the diamond model to digest attack features within the organization. It is completed in four steps. The first step is to apply threat intelligence, and to analyze the characteristics of the attack behavior within the organization to find out the victims. The second step is to conduct security monitoring and model or extract the threat intelligence content as an organization asset. Input into the protective equipment; the third step is to carry out emergency response, and to deal with the new threats monitored and discovered after the application of intelligence; the fourth step is to strengthen the system vulnerability against external threats. The advantage of active defense is self-improvement through attack by attackers.

Figure 3. The active cyber defense cycle model



3. THREAT INTELLIGENCE PLATFORM

As can be seen from the hot words of the last three years, "Threat" and "Intelligence" are the focus of attention. Threat intelligence vendors have also sprung up in the field of network security. In addition to newcomers, many traditional security vendors have expanded their business into threat intelligence

and are rushing to launch their own threat intelligence products. Not all "threat intelligence" is the same. The information provided by some vendors is simply the meaning of the currently active IP address and URL. This information allows customers to respond quickly to current threat environments, but cannot predict future activities. (Yang Zeming et al,2015) Some vendors provide information on adversary information and related programs, but the price of such information is usually high and generally requires speculation based on a wealth of information. Table 1 summarizes the development and product information of these threat intelligence vendors. However, it should be noted that the threat intelligence market is still immature, and we can foresee that many vendors and their capabilities may change in the short to medium term.

4. THREAT INTELLIGENCE SHARING SPECIFICATION

All enterprises, organizations and organizations in the industry have carried out related research work according to the problems encountered in the actual business of intelligence sharing, and put forward some norms for threatening the expression and transmission of intelligence. (Yang Pei'an et al, 2018) Through the investigation and analysis of threat intelligence specifications, the characteristics and scope of the representative main specifications are summarized, as listed in Table 2.

The current mature foreign threat intelligence standards include network observable expression (CyboX), Structured Threat Information eXpression (STIX), and Trusted Automated eXchange of Indicator Information (TAXII).

Among them, the development of TAXII has been strongly supported by major security industry organizations, including IBM, HPE, Cisco and Dell, large financial institutions and US government agencies including the Ministry of National Defense and the National Security Agency. TAXII defines exchange protocols in the terms of standardized services and information exchange, and can support multiple sharing models. The main threat intelligence sharing models include peer-to-peer, source/subscriber, and Hub and Spoke three ways. See the following Figures 4-6.

Peer to Peer is a peer-to-peer sharing model that directly shares information between two or more organizations. A Peer to Peer sharing model may be ad-hoc, where information exchange is not coordinated ahead of time and is done on an as-needed basis, may be well defined with legal agreements and established procedures, or somewhere in the middle.

Source/Subscriber is a shared model in which an organization acts as a single source of information and sends that information to subscribers. As shown in Figure 5.

Hub and Spoke is a sharing model in which an organization acts as a central clearing house or hub to coordinate the exchange of information between partners or organizations. Spoke can generate or consume information from the Hub. As shown in Figure 6.

5. DIFFICULTIES IN NETWORK SECURITY THREAT INTELLIGENCE SHARING

Information sharing is an eternal and important topic in global cybersecurity. Curbing the momentum of cybercrime requires sharing of enforceable threat intelligence information between networks, borders, and vendors. The active sharing of information between all sectors and public or private organizations is a necessary condition for industrial development. Business organizations continue to face the challenges of evolving threats, a growing surface of attack, and a lack of security technologies. Executable information is the best way to move from passive to active, bringing cybercriminals to justice and punishing them. However, information sharing is difficult to say when it is easy to do. Many problems will become a barrier to threat intelligence sharing.

The benefits of cyber-security threat intelligence sharing are undeniable. However, various obstacles limit the possibility of cooperation. Next, we reveal the main reasons for not sharing threat information at present:

Table 1. Typical representative of threat intelligence vendors

Company/ Platform	Country	Business Description
FireEye	America	FireEye's services are based on its 2014 acquisition of Mandiant. FireEye started out as a research forensics service and incident response service. In early 2013, FireEye published a research report on APT attacks. Independent threat intelligence services are still relatively new to FireEye and may be slightly under-represented by some competitors. Major vertical industries include financial services, manufacturing and natural resources.
IsightPartners	America	Isight Partners has been focused on threat intelligence services and has since joined some incident response services. The core competence of the vendor is widely recognized, and analysts account for a large proportion. Isight Partners has intelligence gathering specialists in all major regions, including Eastern Europe, Western Europe, Asia, the Middle East and South America, which are rare among vendors. The main vertical industries are financial services and government.
Dell Security	America	Dell Security is a leading security services company. Customers can purchase threat information services on their own or as part of a complete security service solution. Its intelligence services are divided into two parts: global threat intelligence and targeted threat intelligence, which also provide general and more customized threat intelligence.
Symantec	America	In the threat intelligence market, Symantec is best known for its long-lived Deep-Sight service, which is part of real-time monitoring and notification. Symantec's higher-end services provide deeper analysis, and based on this, Symantec is not prominent in the acquisition and analysis of threat intelligence. Symantec is involved in many vertical industries and relies heavily on financial services.
Verisign iDenfense	America	Verisign entered the market earlier through the iDefense service, and its brand awareness was high. Verisign continues to optimize and attract customers, such as comprehensive services, powerful intelligence processing capabilities and a large number of analysts around the world (and multi-lingual background); Verisign's main vertical industry is financial services and media.
CrowdStrike	America	CrowdStrike is a relatively new company, but has a good reputation for its professionalism. Intelligence covers a wide range of decision-making levels, from short-term (for example, a few minutes) action decisions to long-term (for example, five-year) strategic decisions, including manual and automated decisions. CrowdStrike's main business focus areas span multiple vertical industries, including media, government and others.
Group-IB	Russia	Group IB's threat intelligence experience and capabilities have been integrated into high-complexity hardware and software ecosystem solutions to monitor, identify and prevent cyber threats. At the same time, Group IB also provides advanced threat intelligence consulting and emergency response services. The main vertical industry is financial services.
Kaspersky	Russia	HuMachine Intelligence is Kaspersky's behavioral analysis and machine learning algorithm-based protection, combining artificial intelligence technology with the strengths of Kaspersky's own security team, and is an advanced solution based on next-generation technology.
Sophos	England	Sophos provides high quality, accurate and easy to deploy Cyber Threat Intelligence (CTI) to combat modern malware and zero-day threats in real time. Sophos helps resource-constrained IT security teams and OEM partners provide easy-to-implement protection solutions for their network, email and web security solutions.
Digital Shadows	England	The vendor can generate content in real time and export it in a STIX-compatible format. The vendor believes that its strength lies in the wide range of threat sources it tracks. Digital Shadows' main vertical industry is financial services, and there are other scattered customers in the media, manufacturing and natural energy, public utilities and other industries.
Check Point	Israel	Check Point's services are limited to intelligence on existing activities, not predictive intelligence. The information sources provided by the vendor include malicious program signatures, file metrics, and address metrics that Check Point devices can use to determine policies in real time (Check Point's intelligence is only available to Check Point devices).
Qihoo 360	China	Its Tianyan system collects and correlates local information, and also integrates a series of information such as IP, domain name, malicious samples, attack techniques, and attack organizations.
ThreatBook	China	ThreatBook is the leading brand of China Threat Intelligence, dedicated to providing real-time, accurate and unique threat intelligence products and services. The micro-step online service provides threat information data API, threat detection platform Threat Detection Platform and multi-source threat intelligence management platform Threat Intelligence Platform.
Singhand	China	Based on the massive public data of the Internet, Singhand comprehensively uses cutting-edge technologies and methods such as natural language processing, deep learning, cognitive computing, knowledge extraction and deduction, and data mining to aggregate, analyze, and track the public information of specific targets, and present the target in an all-dimensional manner portrait.

Table 2. Typical threat intelligence specification

Standard/ Framework	Source	Characteristics
STIX	MTRE	STIX provides a structured language that provides a generic, general description of cyber security threat information so organizations can share, store, and use cyber security threat information in a standard format. Currently, STIX has become a formal international standard recognized by OASIS (Organizational Information Standards Promotion Organization) and has been released version 2.0 (released in 2017).
OpenIOC	Mandiant	OpenIOC provides users with a set of expression formats and frameworks for the proper recording, definition, and sharing of cybersecurity threat intelligence so that threat intelligence can support threat detection, incident response, and machine-readable technical indicators. Digital forensics work. As an enterprise standard (not an international standard), OpenIOC has gained a lot of recognition in the industry. Currently, the latest version is OpenIOC1.1 (released in 2013).
CybOX	MITRE	CybOX is a set of structured language standards proposed by the US MITRE organization. CybOX provides a structured language for the canonical and general description of network observable objects, so as to be specific when performing threat detection, event response or management. Threats and events provide standardized factual evidence based on different network observables and share attack-related threat indicators and test results across different organizations in a standard format. Currently, CybOX has been integrated into the STIX 2.0 standard and is no longer released and revised as a separate standard.
VERIS		VERIS is a framework designed to provide a common language for describing security events in a structured and repeatable manner. VERIS is a response to the lack of high quality information challenges in the security industry.
IODEF	IETF	IODEF (Incident Object Deion and Exchange Format) is a format used by CSIRTs (Computer Security Incident Response Teams) to exchange event information between themselves, their supporters and their partners, and can provide for the development of interoperable tools. basis. IODEF incorporates the data formats of many DHS series specifications and provides a format for exchanging information about operational statistical events and supports automatic processing.
TAXII	MITRE	TAXII is a set of application layer protocol standards proposed by US agencies. It aims to design an application layer protocol based on HTPS to support and standardize the trusted and automated exchange of network security threat information standardized by STIX. TAXII supports multiple sharing models (for example: peer-to-peer, subscription, and radiance), does not depend on any specific transport mechanism, and supports the exchange of threat information for non-STIX structures. At present, TAXII has become a formal international standard recognized by OASIS and has been released version 2.0.
TLP	FIRST	The Traffic Light Protocol specification provides a set of names, not a data format, but can be simply included in any relevant standard or specification. TLP classifies intelligence that may be shared to control the scope of sharing. It defines four levels of sharing (corresponding to four colors).
MAEC	MTRE	MAEC provides a structured language for describing and sharing malware based on attributes and characteristics such as behavior and attack patterns. It aims to standardize the description content and methods of malware, and eliminate the ubiquitous description ambiguity and inaccuracy. Reduce the dependence on signatures and improve the efficiency of malware information sharing. Compared with STIX, MAEC describes malware more comprehensively, with a finer granularity and a more specialized audience. Currently, MAEC has been updated to version 5.0. Like the STIX 2.0 standard, MAEC 5.0 is also starting to use the JSON format.
OVAL	MITRE	OVAL is an open language standard. OVAL aims to design a set of description language based on XML format, which is intended to define the definition and description of technical implementation details such as check/evaluation items and vulnerability points in security check/evaluation, such as: Windows, Linux System state, vulnerability, configuration, patch, etc. of Unix and various embedded operating systems. Designed to be machine readable, OVAL's description of checkpoints can be directly applied to a variety of automated scanning tools that support OVAL.

Figure 4. Peer to peer

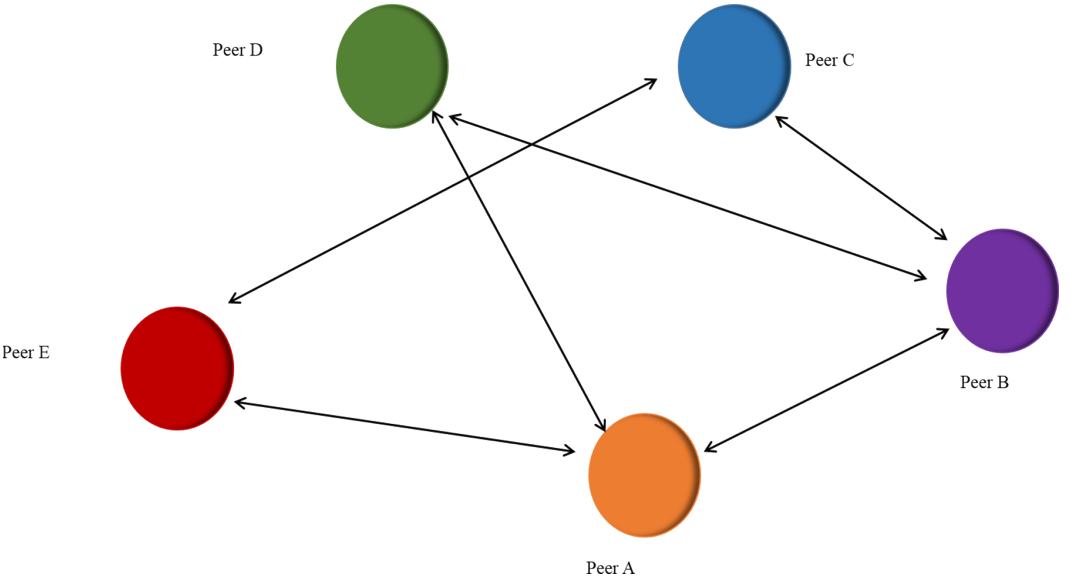
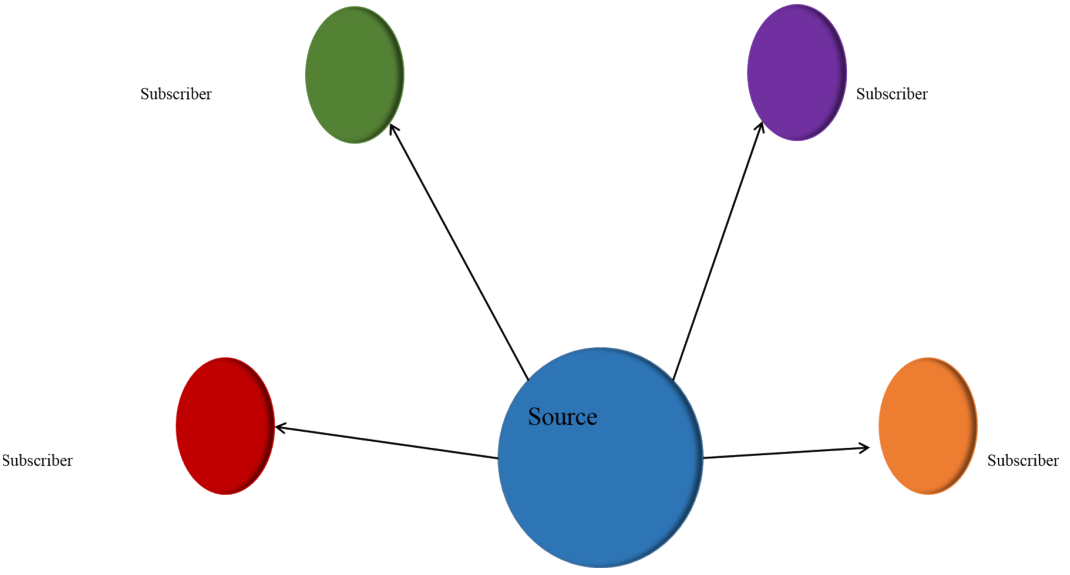


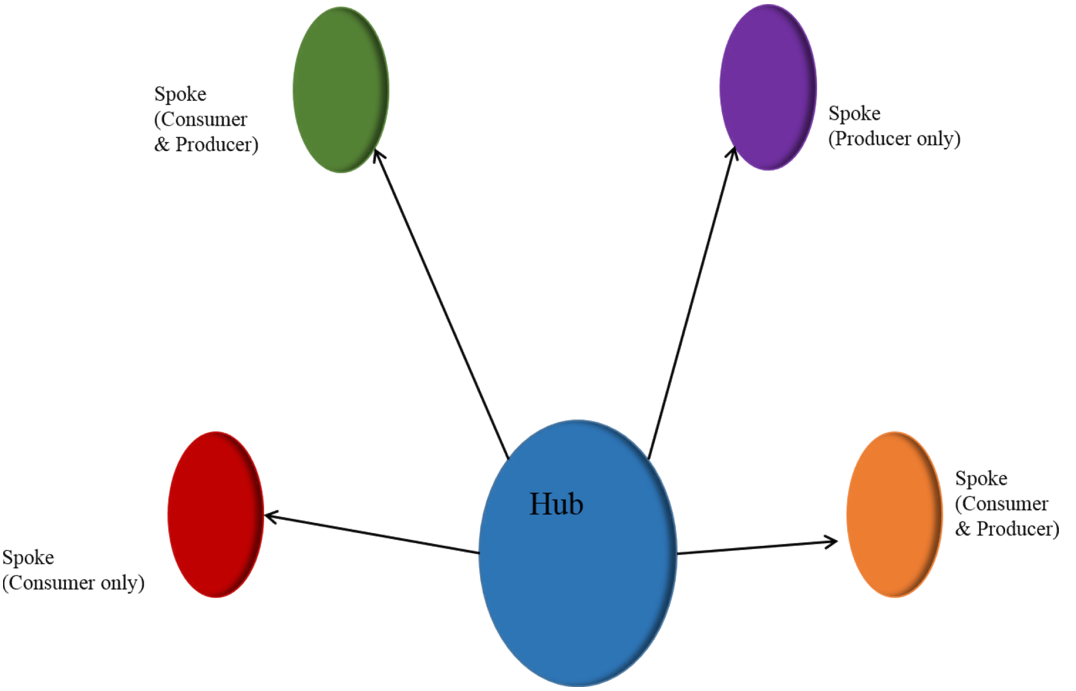
Figure 5. Source/Subscriber



1. Legal rules, privacy issues.

Legal rules, privacy issues are important reasons for the non-sharing of information. Different countries have different legal rules. For partners, the differences in legal rules will bring many problems. The reason many organizations are reluctant to share some events is because they are not sure what kind of events can avoid legal issues and privacy issues. (Yang Bohan et al,2018) Providing services to specific departments also requires service providers

Figure 6. Hub and SPOKE



to comply with specific laws and regulations. With regard to international cooperation, the two cooperative teams must comply with different legal environments in different countries, especially when sharing sensitive issues. This issue affects the way the team provides, thus limiting the possibility of cooperation.

2. Changes in the nature of cyber attacks.

Changes in the nature of cyber-attacks. The changes in cyber-attacks are changing with each passing day, and the nature of cyber-attacks is becoming more and more personalized. Even if the organization successfully shares the attack data, and when these organizations belong to the target range, the nature of the opponent's cyber-attack has changed, and the problem of personalized attack makes the shared intelligence information insufficient for them to defend themselves (Li Jianhua, 2016).

3. Quality problems.

The quality of information is one of the obstacles to information sharing. The quality of data includes timeliness, accuracy, relevance, comparability, confidentiality and so on. These will affect the decision-making behavior of threat intelligence gainers. Many intelligence sources say that many of the shared content is not timely, obsolete, or credible enough to help the decision-making process.

4. Think that this event is not worth sharing.

There are also a number of victim organizations that simply deal with the incident internally and believe that it is not serious enough to report and share to external parties, including law enforcement agencies and other competent agencies.

5. Budget issues.

Budget issues. The budget issue is the reason for limiting the construction of valuable information sharing cooperation platforms and organizations. Some organizations say that qualified real-time threat intelligence is often expensive.

6. Untrusted participants.

Untrusted participants. Some reports also mention key barriers to effective communication between untrusted participants. If an intelligence sharing alliance has only a few parties actively participating in the sharing plan, and without getting too much reward from it, trust will be damaged. As a result, it is no longer actively participating in the sharing program, which is an obstacle to participating in the threat intelligence sharing platform (Ma Minhu et al, 2016).

6. NETWORK SECURITY THREAT INTELLIGENCE SHARING SOLUTION

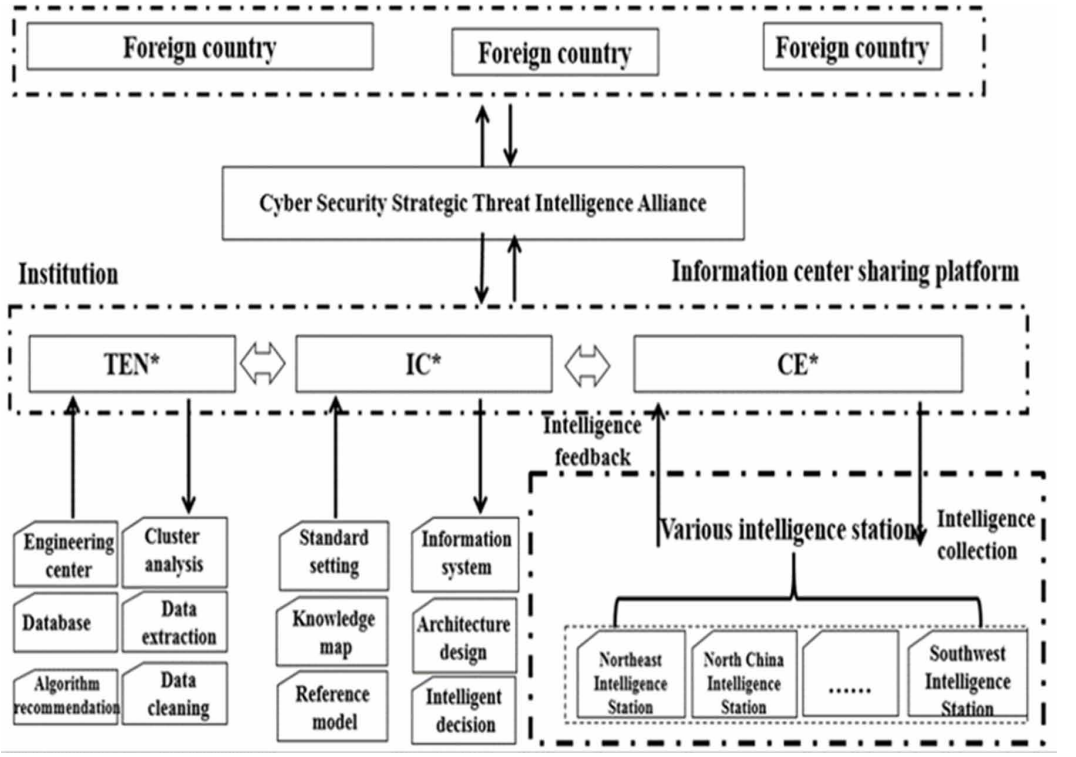
The essence of information security lies in the information asymmetry between the offensive and defensive sides. Whoever can grasp more information can achieve asymmetric strike or defense. Today's key issues in developing regional cybersecurity capabilities and implementable solutions are the creation of threat intelligence sharing and threat intelligence sharing platforms. Establishing a unified and efficient network security intelligence sharing mechanism to accurately grasp the rules, trends, and trends of network security risks can avoid many network security incidents.

In response to the above problems, this paper proposes a solution to develop regional network security capabilities - Firefly Action to establish a threat intelligence alliance, as shown in Figure 7.

The establishment of a threat intelligence alliance will solve the problem of intelligence sharing. Threat Intelligence Alliance is mainly composed of independent security software vendors (Internet companies, cloud security companies, traditional security companies, security researchers, and institutions in industries with high similarities such as finance and banking). Millions of threat-centric data points to provide threat data sources from around the world, as well as internal threats and incident data from corporate multi-layered defenses and businesses, providing massive threat intelligence. The Threat Intelligence Alliance will coordinate and integrate the intelligence forces of multiple departments to improve the ability of countries to prevent and respond to cyber attacks. It is the main department for preventing and responding to cyber threats and the nationwide cyber threat intelligence hub. Each corporate department has its own responsibilities, including the development of shared standards, the design of analytical models, the establishment of knowledge maps, and data cleansing. Through the threat intelligence alliance, the exchange of information between them can enhance the mutual trust and complementarity between enterprises, and promote the participants' understanding of the attackers and the overall strategy, so that the participants have the opportunity to obtain blind spots or narrow information channels due to their own vision. Information to arrive. These vendors that form alliances are generally more powerful in one area of security analysis, sharing threat intelligence in the form of alliances.

From the basic physical layer, computing storage environment, network boundary, architecture security, external supply chain, threat intelligence, public opinion and other aspects to comprehensive consideration, establish an information security field ecosystem program, through threat intelligence and security event information sharing, build joint defense The joint governance situation system

Figure 7. Threat intelligence sharing alliance architecture



uses open, shared, and win-win methods to proactively respond to external attacks and enhance the information security defense dimension.

7. CONCLUSION

The sharing of threat intelligence provides a strong support for dealing with cyber attacks in the new era. By analyzing the existing threat intelligence platform and sharing mechanism, this paper puts forward the key issues in the current threat intelligence sharing system and tries to give a solution for regional security capability improvement. Overall, China's research and construction in the field of threat intelligence sharing is still in its infancy. I hope this article will bring inspiration to readers and lead some thinking.

REFERENCES

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *Diamond Model of Intrusion Analysis*. Center for Cyber Threat Intelligence and Threat Research, Technical Report ADA586960.

Gartner, J. (2017). *Competitive Landscape: Threat Intelligence Services*. Worldwide.

Koujalagi, A. (2015). *Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Academic Press.

Li, J. (2016). A Survey of Network Space Threat Intelligence Perception, Sharing and Analysis Technology. *Journal of Network and Information Security*, *2*(02), 16–29.

Ma, Ting, & Yue. (2016). The US Network Security Information Sharing Mechanism and Its Enlightenment to China. *Journal of Information, 35*(3), 17-23.

OASIS. (n.d.). *TAXII 2.0 Specification Document*. https://oasis-open.github.io/cti-documentation/resources.html

RFSID. (2017). Threat Intelligence, Information, and Data: What Is the Difference? In *The ART of Making Threat Intelligence Actionable.* SecurityWeek.

Yang, Wu, Su, & Liu. (2018). A Survey of Cyberspace Threat Intelligence Sharing Technology. *Computer Science, 45*(6), 9-18.

Yang. (2018). Network security and intelligence analysis based on big data. *Modern Information Technology, 2*(7), 157-158.

Yang, Z., Qiang, L., Liu, J., & Liu, B. (2015). Research on Threat Intelligence Sharing and Utilization for Attack Source Tracing. *Information Security Research*, *1*(01), 31–36.