Analysis of Honeypot Data utilizing Elasticsearch for Cyber Threat Intelligence

Mrs. Veena R C[1], Dr. Brahmananda S H[2]

[1] *Research Scholar, Department of Computer Science and Engineering, GITAM University, Bengaluru, India*

[2] *Research Guide, Department of Computer Science and Engineering, GITAM University, Bengaluru, India*

veenavn288@gmail.com, shbrahma@gmail.com

Abstract

In a real-time environment there are more cyber-attacks arising which require cybersecurity specialists to identify, investigate and protect from the cyber threats. In general, the timely managing of such a huge number of attacks is not feasible without thoroughly analyzing the features of the threat and taking appropriate intelligent protective measures in which it defines the term cyber threat intelligence. However, this is not a simplistic method, since the IDSs produce a significant volume of notifications that might or may not be correct eventually leading to a significant number of false positives. It is difficult to avoid cyber threats just by existing utilizing tools and techniques. Instead the analysis has been done for how the attacker's intension would evaluating via various means such as Indicator of Compromise (IoC). In this article, a new threat intelligence technique has been proposed to examine the log data of honeypots to detect the attacker's activities an attacker's target and acts as an objective, to accomplish this objective honeypot AWS has been installed in the cloud to obtain cyber incident log and the elastic search technology is used to examine the log data.

Keywords: *Threat Hunting, Hunting Maturity Model, Pyramid of Pain, Indicator of Compromise.*

1. Introduction

The cyber threat hunting is an important cybersecurity operation. It is the process of looking across networks to identify and classify emerging threats that bypass the current security solution. In any organization security providing employee or Network Admin takes place this threat hunting process to detect threats from notifications which are created by the IDSs to protect the critical resources of the corporate network. Analyzing and preventing cyber threats is an essential and dynamic operation. One of the best way to hunt the cyber threats through the Honeypot Data Analysis. A Honeypot is a network-connected device installed to attract the cybercriminals and to identify, prevent and analyze intrusion efforts to obtain the unauthorized access to the information systems and also it records the all activities and conversation of the users since it doesn't provide any legitimate assistance so all the activities are considered as unauthorized.

The Honeypots are divided into three categories based on their design viz. Low, Medium and High Interaction Honeypots. Honeypots generate a tremendous volume of information and no normal data processing systems can examine this volume of data. The Honeypots and Honeynets are untraditional security mechanisms that enable security providing users to acquire and examine the data to know more about the cyber-attacks. To secure the servers, network and other applications which are the essential components of any enterprise technology and information, several IDSs and IPSs are existing in the market. These mechanisms for detecting and mitigating threats could be automated but automating cybersecurity techniques is no the ultimate answer for securing the sensitive resource inside an enterprise. To analyze the attacker's behaviors for providing the stronger security the automation is necessary.

On the other side, cybersecurity is not a service but it is a mechanism that requires continuous supervision and enhancement. Thus it is necessary to think more analytically regarding the advances in cyber threat management. The detection of new threats is more sophisticated than the conventional rule-based identification method. Typically, the threats are designed by using various design strategies. It works as assistance in case of attacks and helps to identify many situations for every mitigation technique. There are several cyber-attack design strategies is used during the cyber-attack evaluation. Such design strategies may be performed independently or along with other design strategies. Cyber-attack design is primarily used for detecting the opponent's attack behavior.

2. Literature Survey

C. Seifert, I. Welch, P. Komisarczuk et al. have expressed their views towards Honeypot Client(HoneyC) [1] that it is one of the Client based Low Interaction Honeypot that captures only the key features of the intended users and it can identify only the Client-side attacks. Essentially the virtual clients are used to communicate with actual servers. The HoneyC is a network independent system composed of three key components such as queue, visitor and the Review engine.

J. van der Lelie-jop and R. Breuk-rory et al. evaluated the Secure Shell (SSH) [2] Honeypots during process in the session is operating and information is decoded using visual analytical method. R. Jasek, M. Kolarik, and T. Vymola et al. analysed the Advanced Persistent Threats [3] which are very effective and knowledgeable where it constantly collects the data and information on particular targets by using the different attack methods to analyze the weakness of the target system and conduct on the information obtained. The main attention of APT is particular target systems. Honeypots mainly used to identify cyber threats. Honeypots are outstanding devices because they have more number of resources for detecting a cyber-attack than any other technology. The Honeypot Data Analysis detects the abnormalities to identify the suspected cyber threats. N. Weiler et. al explained about the Distributed Denial of Service Attack(DDoS) [4] which is one of the major serious threats for any organization, by using Honeypots can understand more regarding cyber-attacks on the network infrastructure.

S. Liebergeld, M. Lange, and C. Mulliner et.al explained about the Nomadic [5] which is one of the types of Honeypots which is having capable to identify the threat on the mobile phones, it actual imitate like actual phone and gather all data to recognize what kind of malware is in infecting on the smartphones and also gives the resources to gather the details on threat intelligence information. Tracking is often taken on utilizing simulation methods. Dionaea is the Low Interaction Honeypot, used to gather information on attacks and evaluates to identify the pattern of cyber-attacks and also it often creates a profile for every attacker by evaluating the data collected. The C. Moore and A. Al-Nemrat et al. defined Honeypots can capture information of an attacker through IP address [7]. J. Song, H. Takakura, Y. Okabe, M. Eto et.al Analysed about cyber threats which is the essential for hunting of threats. Cyber threat hunting is a mechanism of evaluating specific data-sets to look for possible cyber-attacks across the network. Data examination may be conducted by utilizing current automated tools or performed manually as an option. Cyber threat hunting maturity within an organization relies on the abilities to acquire and examine data. Information, based on the most useful source for detecting cyber-attacks, maybe past or current. Threat data should be obtained using honeypots and evaluated until they occur to identify threats [9]. G. Portokalidis, A. Slowinska, and H. Bos et.al provides Information about specific incident that occurred in cybersecurity. Examination of this information provides an indicator that most security attacks do not arise as zero-day attacks [10], are very common and have trends in most situations. Appropriate collection and analysis of the data may contribute to other IoC components.

3. Analysis of Threat Hunting

3.1 HMM – Hunting Maturity Model

There are three aspects to require to be included during evaluating the hunting ability of any organization [8].

- The quantity and quality of the information they obtain for hunting.
- The tools and techniques they have for obtaining and evaluating the information.
- The skill abilities of the analysts who are specifically using the information and tools to identify the violations of security.

For these aspects, the abilities of the analysts are perhaps the most essential, as they are what helps them to convert information into detection methods. The quantity and quality of the information that any organization gets regularly from the IT environment is often a significant factor when defining the degree of HMM. The Hunting Maturity Model defines five stages of organizational ability for hunting which are ranging from HMM 0 to HMM 4 i.e. from the Least Capable to the Most Capable. The key concept behind the HMM is that it continuously requires enhancement.

3.1.1 Level 0: Initial

In any organization at level 0 of HMM mainly relies on automatic alert tools like IDSs, SIEM, antivirus, etc. to identify suspicious behavior within the organization. They may integrate sign update inputs or signals of the threat intelligence and may also generate their signature or signals but these are transferred directly into the surveillance systems.

At HMM 0 the human activity is based mainly on alert response. Also HMM 0 organizations don't gather any information from IT systems and their capability to detect threats proactively in extremely restricted. Level 0 is not considered for hunting.

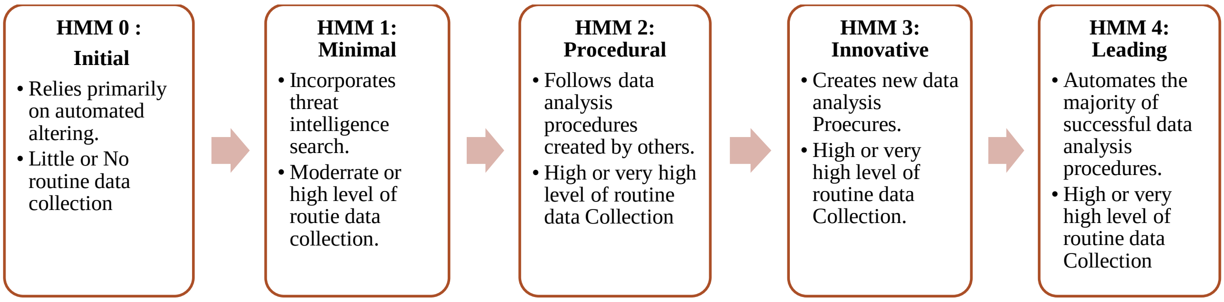
HMM 0 : Initial
• Relies primarily on automated altering.
• Little or No routine data collection
HMM 1: Minimal
• Incorporates threat intelligence search.
• Moderrate or high level of routie data collection.
HMM 2: Procedural
• Follows data analysis procedures created by others.
• High or very high level of routine data Collection
HMM 3: Innovative
• Creates new data analysis Proecures.
• High or very high level of routine data Collection.
HMM 4: Leading
• Automates the majority of successful data analysis procedures.
• High or very high level of routine data Collection

Figure 1: Hunting Maturity Model

3.1.2 Level 1: Minimal

An enterprise at HMM 1 often depends mainly on automatic alerting to support the incident response mechanism, although in addition they have at least certain routine IT data gathering. Such organizations also adhere to intellectual identification (i.e., they primarily base their identification decisions on their accessible information regarding threats). They also monitor the latest reports on threats from a combination of closed and open sources. HMM 1 organization usually accumulate at least certain types of information such as log monitoring systems or SIEM across their organization and store in a single location. Others can also collect more information. Thus as new threats arise to their notice, analysts can identify the core indicators from such reports and analyze historical records to determine if they were present in any recent times.

3.1.3 Level 2: Procedural

Most frequently, procedures integrate the desired form of input data with a particular analysis method to identify a specific type of malicious behavior (e.g., malware detection by gathering data regarding which programs are scheduled to automatically start on hosts). Although most of the easily available procedures depend on lesser-frequency analysis in any manner, HMM 2 organizations typically gather significant volumes of data from around the organization. HMM 2 is the most popular ability level for organizations with effective hunting schemes.

3.1.4 Level 3: Innovative

HMM 3 companies include a few hunters who know and can apply a variety of various types of data analysis techniques to detect malicious activity. Instead of focusing on other-developed procedures (as is the case with HMM 2), such organizations are usually the ones that develop and publish the procedures. Analytical expertise may be as simplistic as simple statistics or include more advanced topics such as related data interpretation, data visualization or machine learning. The aim at this point is for analysts to use such techniques to create repeatable procedures, which are regularly reported and conducted. If not even more advanced, data collection at HMM 3 is at least as usual as at HMM 2. HMM 3 organizations, in detecting and mitigating threat attacker behavior, may be very efficient. Nevertheless, as the amount of hunting processes they grow exponentially increases, they may face issues of scalability attempting to conduct them all on a reasonable plan because they expand the number of analysts necessary to fit.

3.1.5 Level 4: Leading

The HMM4 organization, with one key difference: automation, is the same as that at HMM3. Every effective hunting cycle at HMM4 will be operationalized and transformed to automatic detection. This relieves the analysts from the responsibility of constantly operating the same procedures and then helps them to concentrate on developing current processes or designing new ones. HMM4 organizations are extremely successful at preventing acts against opponents. The high degree of efficiency enables them to focus their attention on developing a stream of innovative hunting procedures, culminating in the continual enhancement of the whole detection system.

3.2 Threat Hunting Loop in HMM

Hunting of threat isn't a one-off activity, it is an operation. It focuses on several factors like Developing a Hypothesis, Analyse Hypothesis using Tools and Techniques, Discovering New Patterns and Tactics, Techniques and Procedures(TTP) and Enhancing Analytics Automation. To determine the effectiveness of the organization's data collection process, the loop elements should be compared to the Hunting Maturity Model. If the process operates with a hunting threat, it can be automated and communicated with other team managers to tackle specific cyber threats.

The most critical role is to hunt specific threats inside the network or to gather information from hosts. Data can be obtained from various sources. These data may be various forms including Syslog, data from firewalls, logs from the servers, data from honeypots, that could be used to develop a hypothesis. The collection of data could be automated in most scenarios and could be fed into an analytical framework or the visualization tools [8]. The Following Figure 2 illustrates the Threat Hunting Loop

.

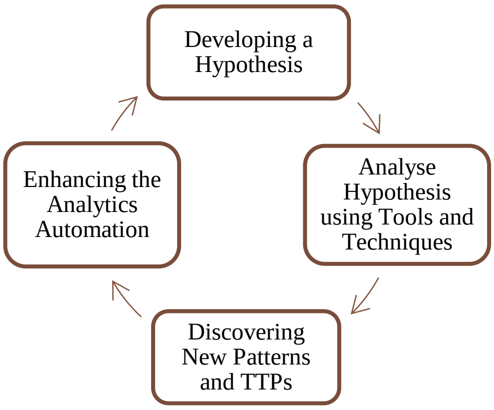
Developing a Hypothesis
Analyse Hypothesis using Tools and Techniques
Discovering New Patterns and TTPs
Enhancing the Analytics Automation

Figure 2: Threat Hunting Loop

The below steps are followed to perform the HMM process.

3.2.1 Developing a Hypothesis

The current alert based mechanisms like Firewalls, IDSs, IPSs, SIEM, etc. may not identify a significant threat so it essential to create a new hypothesis to evaluate and examine historical information. Inside a standard network the hypothesis is required to check regularly. When threat is detected, analysis and enhancement of the hypothesis are required and also new hypothesis may also be developed based on the cyber incident event.

3.2.2 Analyse Hypothesis using Tools and Techniques

There are several tools and techniques necessary to search for a threat, from data collection to automation. For Advanced hunting the Basic log analysis software, or SIEM, has limited flexibility. A hypothesis must be submitted to the test against the tools and techniques used to hunt threats. Advanced visualization grades will aid in most cases to check and build a new hypothesis.

3.2.3 Discovering New Patterns and TTP

It is hard identifying the Zero Day Attack or Advanced Persistent Threat ahead of time. It's particularly important with an attack on a Zero Day because this does not suit any defined pattern of attack. It is essential to develop patterns for recognizing typical attacks and to continue to search for new and evolving patterns of threat.

3.2.4 Enhancing the Analytics Automation

Managing manually with existing tools and techniques is practically difficult in cyber threat hunting. In these conditions, automation plays a crucial role. Alternatively, developing a hypothesis to Identification has to be automated to handle the events of the cyber-attacks incident effectively.

3.3 Pyramid of Pain

The following Figure 3 shows the Pyramid of Pain, every level of the pyramid describes various kinds of attack indicators that you may use to monitor the behavior of an attacker and is divided by how much pain it can create when you will deny such indications. Pyramid of Pain consisting of six varieties of IoC organized in that order of effect on the opponent and on the analyst's effort, respectively. The types of IoC positioned in a pyramid from bottom to top are listed below.

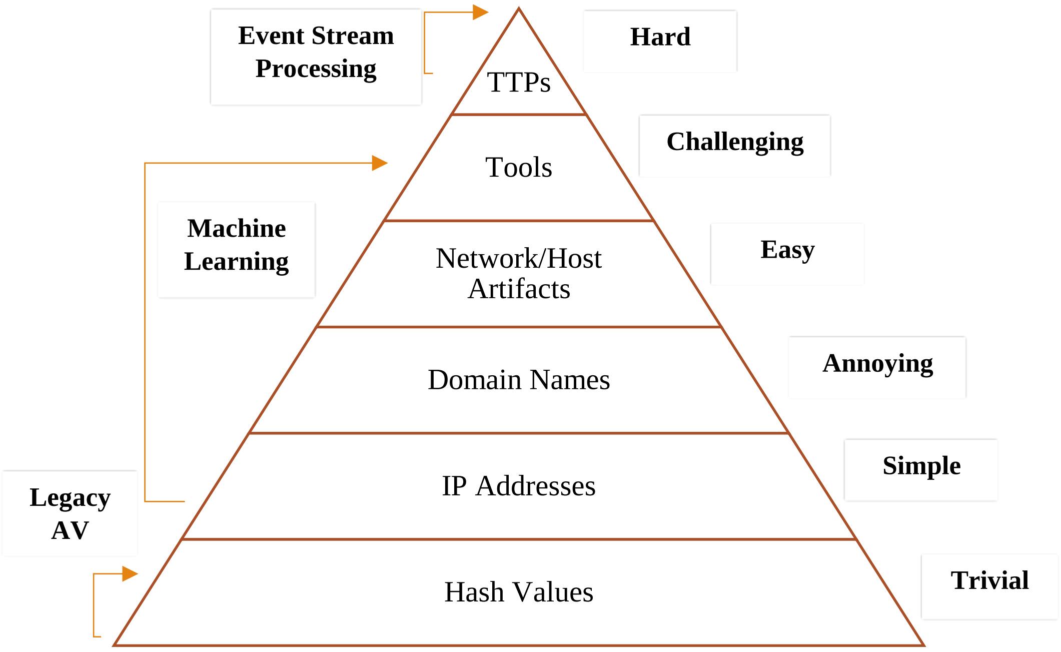

Figure 3. Pyramid of Pain

The bottom of the pyramid of pain has less effect on the opponents, while IoC on the top will not only have a major impact on the analyst's report but will also require a lot of effort. The color and width play a significant role in understanding the value of the specific IoC. During cyber-attack, the attacker usually leaves some kind of footprints that may be a mixture of the components of the Pyramid of Pain. Analyzing a Pyramid of Pain may, therefore, disclose an attacker's intent and purpose that could be used to make educated decisions regarding threat information.

Hash values have a unique identifier for particular malware or the payload used for the attack. For instance, hash values may be altered by a slight adjustment and there is also change in the payload as well. Therefore, it is not required to keep track of the new values which are produced more regularly and continuously. This ensures that threats use hash values can be quickly detected and handled.

IP addresses are incredibly simple criteria for detecting an intruder in any cyber-attack event. During a cyber-attack activity, it is impossible to mask IP addresses. To an intruder, modifying the IP address after attacking or masquerading before an attack happens quite simple. In reality it's not practically possible to investigate each single IP address that has attempted to break a network

The opponent must also have registered with a hosting organization to get a domain name. Tracing back to the roots of the domain is fairly easy; however, the attackers may be masked. Domain names on the other side may be modified at any time. Because domain name users have to sign, the changing of domain names relative to IP addresses is more complicated.

The next indication is the artifact of the network, which may separate the opponent's malicious activities from legitimate users. Hosts participating in a cybercrime also provide a considerable amount of data concerning the threat. Host Artifacts are indications of the host's malicious operations. This may be used to differentiate between the legitimate user and the attacker's reaction.

The tools the attacker uses to launch an attack. Such tools used for deploying the payload can be software or hardware-dependent in essence a variety of existing or modified tools will be a big challenge for the analyst.

Tactics, Techniques and Procedure (TTP) are the main and highest element of the pyramid. It is the point where the adversary's actions may be detected by either the malicious program or the payload.

3.3.1 IoC- Indicator of Compromise

IOC is a forensic concept that applies to the facts on a system indicating a breach of security. IOC data is obtained during a malicious event, security breach or unintended network call-outs. Also, regular checking of IOC data is standard practice to identify suspicious behavior and vulnerabilities. Any cyber-attack occurrence, or even a cyber-attack attempt, leaves several digital footprints (IOCs) with the malicious behavior behind it. In the case of a violation these traces may be tracked by organizations or security specialists to examine the total effect and severity of the violation. The indicator is analyzed using three different parameters such as Trace, Identification and Respond against IoC for improved analysis of such metrics are addressed in the following.

Trace: It's necessary to track an intruder on a network or host during their access. Trying to trace a hash value isn't necessarily helpful because the attacker may alter values during the next attack. Alternatively, if payload gets alter there will be different hash value. Hence it is hard to determine if the same intruder attempts any additional attack. The IP address is essential to have a connection between networks as each computer will have an IP address inside the network. The attacker can modify the IP address whenever they conduct an attack, which refers the same to domain names. The intruder can exit from the Host or Network though the domain or IP address has been changed. Such Host or Network artifact are also essential components for future analysis. Many users regularly use the same tool to perform a cyber-attack, because modifying the tool can involve design and testing which could be costly. Thus, tools may be used to detect attackers whether or not they use the same tool. The TTP is the most critical and difficult indicator on top of the pyramid. Since TTP primarily describes the attacker’s expertise and practice, they will enhance their skills over the period, allowing threat hunter difficult to think for the next acts of attackers.

Identification: Tracing enables threat hunters to detect an attacker's footprint. The traces created by the offender may be included in a possible attempt to recognize the attacker. Tracking mechanisms can be used, for instance, to compare specified components such as IP address, hash values, and domain name. Recognizing the network or host artifact could help analyze the behavior of an attack.

Respond: If a threat is identified and traced it is important to prevent any future events. For Instance, where an IP address is known as a data collection threat component, it may be blacklisted for any events in the future. If the recognized component is responded immediately, the protection has become an offense.

Deployment has been done on 2 low-interaction honeypots called Kippo and Dionaea [11] on Amazon cloud services to improve hunting. Input Data obtained more than 500 MB of log data for Kippo. The log data consists of all attempts to log in to the honeypots. The log also contains timestamps which signify whenever the event occurred. The cyber threat intelligence model has been introduced before evaluating the log data of the honeypots, which will allow us to analyze the data gathered effectively.

3.4 Threat intelligence

There are three key components are involved in cyber-attack detection viz., intrusions, Actions and Patterns. An intrusion is a strategic approach by an intruder to obtain access to a system, a network or a host. An intrusion derives from an intruder to a system that can be captured by gathering data. The attacker's actions may be detected from the gathered data because multiple attacks were performed by the same intruder. An intruder is either a person or a computer. The behavior for both situations is an example of the process used. Therefore, the relationship between human activity and cyber-attacks is good [12].

If we consider just the quantity of the data collection, evaluating and describing may require different techniques. The Figure 4 shows that a data-set on a cyber event includes details on the attack, and can be evaluated through data processing. Attack information may be isolated and viewed in a more accessible way from usual events. And even the attack launched by the attackers, in this case, shows the attacker's behaviors. Through incorporating information such as data analysis, we will detect patterns of the attack on such two factors. Patterns of attack may be essential to prevent upcoming cyberattacks.

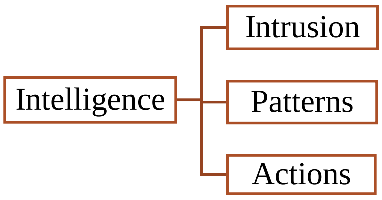

Figure 4: Concept of Cyber Attack

4 Experiment and Results

The term ‘ELK’ refers to 3 different open source projects viz., Elasticsearch, Logstash, and Kibana, where Elasticsearch is an engine for both analytics and search, Logstash is severed side information processing pipeline that takes information from multiple sources and again transfers it into ‘stash’, Kibana allows users to represent the data with charts, graphs, etc. ELK is used to create a visualization for any data volume to display the information. The main advantage of ELK is doesn’t have a scalability issue and is capable to handle large amounts of data and also scans faster.

The Five Hundred Megabytes of honeypot log data has been collected through a server called Amazon Web Services(AWS), then the two honeypots like Kippo which is low and Dionea is medium honeypots are used to establish. The honeypots act like original Operating systems that invites a lot of attackers such Log details consists of various timestamps and events with different dates. Each and everything is recorded in case if anyone tries to interact with honeypots. Usually log information is massive in terms of volume and which will be difficult to examine by looking at the log files. To know the actual value which exists in the log files the ELK Method is used. The key merit of ELK being that it integrates both visualization and Elasticsearch because it is extremely scalable, this can be searched within any data volume. It is also capable to perform all database operations and also connect all various related Application Programming Interfaces(APIs)for data search and analysis. The Elasticsearch [14] is used in many organizations and entrepreneurs to find the context and meaning of the data.

4.1 Analysis of Data using Kibana Honeypot

By using Elasticsearch in Kibana we conducted multiple varieties of keyword searches, the primary objective of detecting the attacks in the honeypot and a lot of activities from the analysis of the log information had observed. Figure 5 shows Kippo honeypot’s activities of the attacks. We have listed seven keywords that can be identified in honeypot activities that take place. This should be observed that every activity was not linked to the assault. It is being noticed that five keywords among seven are assault based and connection link lost and remote server error are not belonging to any security breach.

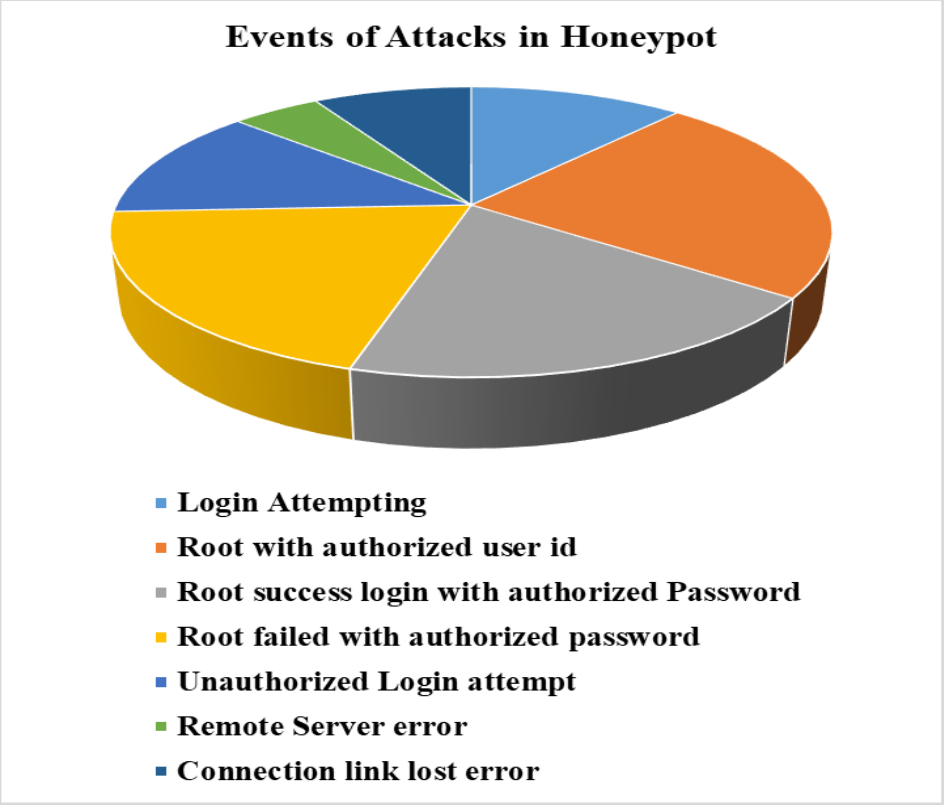

Figure 5: Using Kibana Event Log visualization of Kippo Honeypot.

The following Figure 6 illustrated the log details per keywords. It indicates that every assault is happening inside the honeypot. The honeypot offenders don't have a clue that they are communicating with the honeypot device. It can represent the intensity of an attack concerning a legitimate device. Table 1 Summarized the statistics of the events which have been taken place in the honeypot.

Name of the Event	Total Number of Time Event Occurred	Percentage of Event Occurred
Login Attempting	19,78,137	11.9%
Root with authorized user id	39,40,832	24.47%
Root success login with authorized Password	32,83,702	20.11%
Root failed with authorized password	32,94,818	20.45%
Unauthorized Login attempt	19,90,157	12.9%
Remote Server error	7,37,547	4.96%
Connection link lost error	13,31,368	8.79%

Table 1: Analysis of various Attack Events

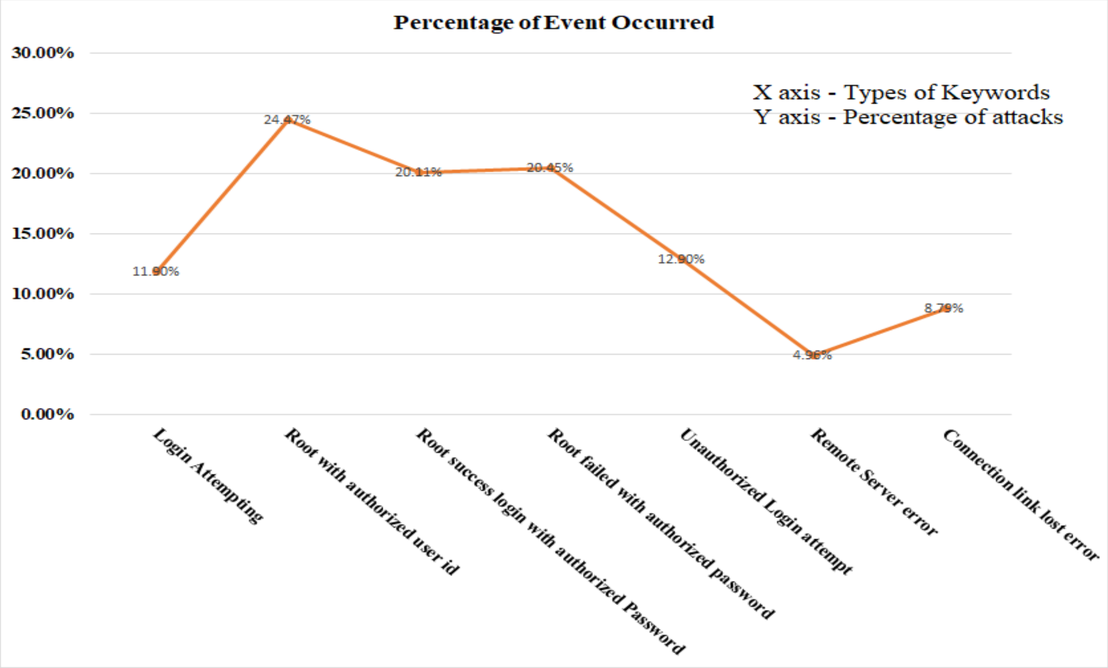

Figure 6: Percentage of Events Attacks

5 Conclusion

This article analysed a modern model of threat intelligence showing that threats, activities and patterns are a significant and appropriate consideration for all organizations. It's as necessary to consider the behavior of the attackers in our analysis of a cyber-attack. The pattern of attack can thus be detected from the attack and behaviors. The design only operates where there is a large volume of data relevant to the network event for evaluation. Using honeypot information gathered from AWS, we evaluated cyber-threat information. The Elasticsearch attempts to classify the different kinds of cyber incidents activities. It’s been known that attackers are actively attacking honeypots, some of the assaults are identical when attackers try to enter into the network. This study in cyber intelligence honeypot data is useful because it can be used to detect and prevent potential cyber-attacks. The greatest benefit of utilizing threat intelligence honeypot data is that there is no side impact on the development method. Such an evaluation may help create potential development IDS and IPS.

References

1. C. Seifert, I. Welch, P. Komisarczuk., “Honeyc-the low-interaction client honeypot,” Proceedings of the 2007 NZCSRCS, Waikato University, Hamilton, New Zealand, 2007.
2. J. van der Lelie-jop and R. Breuk-rory, “A visual analytic approach for analyzing ssh honeypots.”
3. R. Jasek, M. Kolarik, and T. Vymola, “Apt detection system using honeypots,” in Proceedings of the 13th International Conference on Applied Informatics and Communications (AIC’13), WSEAS Press, 2013, pp. 25– 29.
4. N. Weiler, “Honeypots for distributed denial-of-service attacks,” in Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on. IEEE, 2002, pp. 109–114.
5. S. Liebergeld, M. Lange, and C. Mulliner, “Nomadic honeypots: A novel concept for smartphone honeypots,” in Proc. Wshop on Mobile Security Technologies (MoST13), together with 34th IEEE Symp. on Security and Privacy, 2013.

6. G. Kelly and D. Gan, "Analysis of attacks using a honeypot," in International Cybercrime, Security and Digital Forensics Conference, 2011.
7. C. Moore and A. Al-Nemrat, "An analysis of honeypot programs and the attack data collected," in International Conference on Global Security, Safety, and Sustainability. Springer, 2015, pp. 228–238.
8. SQRRL, "A framework for cyber threat hunting," 2016.
9. J. Song, H. Takakura, Y. Okabe, M. Eto, D. Inoue, and K. Nakao, "Statistical analysis of honeypot data and building of kyoto 2006+ dataset for nids evaluation," in Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security. ACM, 2011, pp. 29–36.
10. G. Portokalidis, A. Slowinska, and H. Bos, "Argos: an emulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation," in ACM SIGOPS Operating Systems Review, vol. 40, no. 4. ACM, 2006, pp. 15–27.
11. T. Sochor and M. Zuzcak, Study of Internet Threats and Attack Methods Using Honeypots and Honeynets. Cham: Springer International Publishing, 2014, pp. 118–127.
12. M. Ovelg¨onne, T. Dumitras, B. A. Prakash, V. Subrahmanian, and B. Wang, "Understanding the relationship between human behaviour and susceptibility to cyber-attacks: A data-driven approach," ACM Transactions on Intelligent Systems and Technology (TIST), vol. 8, no. 4, p. 51, 2017.
13. M. Hilbert, "Big data for development: A review of promises and challenges. development policy review," martinhilbert. net. Retrieved, pp. 10–07, 2015.
14. C. Gormley and Z. Tong, Elasticsearch: The Definitive Guide: A Distributed Real-Time Search and Analytics Engine. " O'Reilly Media, Inc.", 2015.
15. Mauro Conti, Tooska Dargahi, and Ali Dehghantanha Cyber Threat Intelligence: Challenges and Opportunities 2018.
16. Hamad al-mohannadi, Irfan awan, andrea J Cullen, Loma Armitage cyber threat intelligence from honey pot data using elastic search. 2018.
17. P. Sokol, P. Pekarˇc´ık, and T. Bajtoˇs, "Data collection and data analysis in honeypots and honeynets," Proceedings of the Security and Protection of Information. University of Defence, 2015
18. D. Binaco, "A framework for cyber threat hunting part 1: The pyramid of pain," 2015. [Online]. Available: http://blog.sqrrl.com/a-frameworkfor- threat-hunting-part-1-the-pyramid-of-pain.
19. X. Lin, P. Zavarsky, R. Ruhl, and D. Lindskog, "Threat modeling for csrf attacks," 2013 IEEE 16th International Conference on Computational Science and Engineering, vol. 3, pp. 486–491, 2009
20. H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, and J. Disso, "Cyber-attack modeling analysis techniques: An overview," in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Aug 2016, pp. 69–76.
21. P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in Communications and Multimedia Security. Springer, 2014, pp. 63–72.

Authors

Mrs. Veena R C, working as an Assistant Professor in the Department of Computer Science and Engineering, GITAM Deemed to be University, Bengaluru Karnataka, India and having 5 years of teaching experience. she received B. E from B.M.S Institute of Technology, Bangalore, M. Tech from Visveswaraya Institute of Advanced Studies Muddenahalli (VTU PG Centre, Bangalore Region) and pursing Ph.D. from GITAM University Bangalore. She is certified trainee associate by DELL EMC for Data Analytics with R and Area of Interest is Internet of Things, Cyber Security and Threat Intelligence.

Dr. Brahmananda S H received B. E from Sri Siddhartha Institute of Technology, Tumkur, M. Tech from NITK Surthkal, and Ph.D. from DR.MGR University Chennai, he has 20 years of experience in teaching. He has published research papers in various reputated national and international journals. He is working currently as head of the Computer Science and Engineering Department, GITAM Deemed to be University, Bengaluru, Karnataka, India. and his area of interest cyber security**.**