Threat Hunting Early Experiment through Event Correlation and Memory Forensic

Arif D Purnomo¹, Charles Lim¹* and Burman Noviansyah¹

¹ Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia
* Corresponding author, email: charles.lim@sgu.ac.id

Abstract. The cyber threat landscapes nowadays are dynamically evolving over time, the cyber security practitioner in corporations need to adapt with more sophisticated way with the latest cyber threat attacks are launched. Cyber Threat Intelligence is one of the tools that can be utilized as a cyber threat detection. Generally, CTI operates by integrating its directory with events collected from Security Information and Event Management (SIEM) to correlates all of the appliances logs within corporation and providing summarized and meaningful information that can be reviewed to identify legitimate malicious cyber threat activity. However, relying only CTI subscription that only contains blacklist domain and ip addresses integrated with SIEM will only provide passive detection for known cyber threats. The needs for proactive cyber threat detection is required to compete with the modern threat landscape. This research work will try to explore the possibility of detecting unknown or undetected cyber threats using network event correlation and memory forensic to validate its existence. Throughout this research time span, we’re able to discover malicious network pattern that is proven to be undetected within internal organization endpoint protection. Therefore, this research will provide baseline for threat hunting activity based on network behavioural pattern.

1. Introduction

Many organizations nowadays rely on Indicator of Compromise (IOC), manual analysis, utilizing existing tools in related with detecting internal or external threat. For that reason, they need to get to the point where they could automate those processes on a regular basis and obviously have the skill set and capability to fulfill the maximum potential (Cole, 2016). Another aspect that Organization or Information Security practitioners need to pay more attention is that threat landscape is always changing throughout each year, that’s why traditional Security Operations Centre (SOC) that relies only on SIEM cannot cope with the dynamic movement of the threat adversaries. Cyber Threat Intelligence is one of the key points to turn things around against the fast-paced cyber security threats. According to SANS, Cyber Threat Intelligence (CTI) is a “collection, classification, and exploitation of knowledge about adversaries. CTI is analysed information about the intent, opportunity and capability of cyber threats” (Shackleford, 2018).

CTI is just an element that works as a complementary factor for the role of Security Operation Center (SOC) team within the organization, in the end it will take more than just blacklist domain and blacklist ip addresses to conduct proper Cyber Threat Hunting (CTH) activity. Cases where threats from within organization goes undetected by the network and endpoint protection have been around and a new perspective to overcome them should be evaluated. One thing that also needs to be considered is, Cyber Threat Hunting is not all about data feed, CTH should also contain key points that will answer the adversaries’ methodologies, tactics, techniques, knowledge gap that will put the defenders the upper hand in combating cyber security threat actors. IT Security Professionals or Security Operations Center (SOC) team must proactively observe and intelligently discover ways to reveal the potentially undetected threats within the organization, so that a descent SOC or incident response team are continuous process in the making.
2. Materials and Methods

2.1 Related Work Materials

Jakhaele (2017) on her journal which titled “Design of Anomaly Detection Framework by Data Mining Algorithm for Network Flow” uses data mining techniques with sliding window to capture network traffic, which will then capture the anomaly of the network that is compared with the normal traffic flow. She emphasizes the importance of anomaly-based detection for the unknown threats that will provide better detection rate compared to signature-based detection model.

Al-Mohannadi et al. (2018) on their journal use event analysis log data from cloud service honeypot to uncover attack pattern by the adversaries. They then perform event correlation based on the cyber incident log from AWS platform on Elasticsearch, Logstash, Kibana, which also known as ELK.

John (2017) elaborates all of the techniques required that can be done for detecting APT in his journal “State of The Art Analysis of Defense Techniques Against Advanced Persistent Threat”. He explains about the approach of the academic society and commercial solutions for detecting malicious content of APT and how to identify them based on the methodologies of the proposed solution. APT identification techniques such as machine learning classification, attack intelligence, context-based detection framework, honeypots and intrusion kill chain methods are highlighted in this research.

Divakaran et al. (2017) performed a research regarding detection of fundamental anomalous patterns in network traffic. Research conducted by evaluating the regression model from number of gathered malwares and normal traffic.

Mavroeidis and Josang (2018) performed a research back in 2018 regarding threat hunting activity relying on Sysmon log. They created a system that integrate the ontology from sharing threat intelligence platform and compare the sysmon log that is fed into the machine and then compare the activity based on the database of the shared threat intelligence platform.

2.2 Methods

This research work will only focus on the activity of cyber threat hunting by integrating existing event correlation appliance within organization with memory forensic activity to validate the threat hunting activity. The cyber threat hunting activity in this case will be performed by creating use case that is constantly monitoring the common ports used by windows OS service on existing SIEM. The cyber threat hunting activity will also integrate with the cyber threat intelligence on existing SIEM. When interesting traffic occur, the author tries to perform memory forensic to investigate the hypothesis of the undetected threat from the suspicious host captured on the event correlation. This research will be limited within specific organization network environment.

This research will be using existing devices for SIEM appliances, whereas the author also builds a cyber threat intelligence Minemeld from Palo Alto and threat intelligence feeds from OTX AlienVault feeding. The architecture of the research is depicted as Figure 1 below.
This research will be using below proposed framework in order to conduct threat hunting program. In which the proposed framework derived from MITRE ATT&CK framework especially from “Lateral Movement” section with a few modifications necessary for conducting this research. The diagram of research methodology framework can be found on Figure 2. This framework represents the action that will be taken during the research, which consists of four phases, Collection, Preliminary Analysis Correlation, Platform Analysis & Evaluation.
**Collection** - In this phase, we gather all log files necessary from disparate log files correlated to our System Information and Event Management (SIEM). Based on this event logs, we should create event correlation that could identify the suspicious events initiated by suspicious host or potentially infected host.

**Preliminary Analysis** - The process of creating event correlation that could capture the suspicious network traffic will be done in this phase. And based on the captive event, we should be able to identify the platform fingerprint of the suspected host. Define hypothesis if network traffic initiated by specific host is having a suspicious behavior. Each captured event will have different methods to analyze because each captured event will require different method of investigation depending on its Operating System platform. On this phase, we will acquire the running process or any historical event of the suspected host to investigate if there’s any malicious activity exist on the suspected host. This phase will analyze if certain conditions are met prior further checking into memory forensic investigation. This research focus on internal hosts within organization and not intended to “BYOD” host in particular.

**Platform Analysis** - This phase will validate the suspected host is legitimately infected and do remediation and necessarily contain the infected host. On this phase will also confirm if the signature-based detection mechanism running on the infected machine will do the protection feature properly.

**Evaluation** - This phase will evaluate if the preceding step are properly conducted and meet the objectives stated at previous phases by validating the results of memory forensic analysis to independent & credible 3rd party to identify the finding results of the memory forensic analysis process. The memory forensic analysis results can also be shared to vendor-related party to justify the findings of the memory forensic analysis process. This phase will also review the lesson learned and make room for
Annual Conference on Management and Information Technology (ACMIT) 2019

improvement of the things need to be done to contain, remediate and mitigate the undetected or even unknown threat from future reoccurrence as part of Security Incident Response Life Cycle Process. And can also be used as a starting point to set up new objectives for the next threat hunting activity.

3. Results and Discussion

3.1 Collection
This phase results in all the related devices and appliances must be sending through its log to correlation tools (SIEM) and should be displayed on SIEM dashboard. This phase will be the fundamental of all remaining phases that come right after this first one.

3.2 Preliminary Analysis
On this Preliminary Analysis phase, the author creates hypothesis of threat hunting. The author filters all the logs collected in hoping that it will display more meaningful information, such as anomaly of network traffic generated by specific host. This phase will mark the event correlation rules created by the analyst, it should represent the intrinsic value of the IOC (Indicator of Compromise) or the TTPs (Tactics, Techniques & Procedure) from Network perspective or Host generated-event regarding the threat that is being hunted. Figure 3 represents the event correlation filter that is created to trigger the undetected or unknown threat.

![Figure 3. Event Correlation Filter Rule](image)

After the creation of Event Correlation Filter, the analyst should monitor the SIEM dashboard in order to justify the hypothesis of the correlation filter that is previously generated. Figure 4 below depicts the result of event log generation of the previous phase that shows the event of the potentially infected host that remains hidden or undetected if the author would not create the event correlation filter to identify the TTPs of the potentially infected host.
3.3 Platform Analysis
On this phase the author starts the memory forensic activity of the potentially suspected host. Throughout this research, the author managed to gather two captures of live memory acquisition. The one that is generating numerous attempts of network scanning and the other is triggering the rule of threat intelligence. The process of memory acquisition itself conducted by using two different applications, which are dumpit and Belkasoft. The process of the memory acquisition using the mentioned tools itself is pretty straightforward, the author only run the tools and select the directory of the acquired memory from the host. The memory dump acquired will be further analysed by using different kind of tool. During the memory forensic process, the author uses Volatility and its plugins as main tool. Volatility is an open source, advanced tools for memory forensics written on python and runs on Linux, Windows & Mac OS (Ligh et al., 2014). Various processes can be gathered from memory forensic analysis, even potentially malware hidden can be uncover by performing memory forensic analysis.
3.4 Evaluation
The Evaluation phase of the memory forensic analysis process results in successfully found the undetected or unknown threat for the specific endpoint protection product by the time this writing is published.

![VirusTotal results of the suspected host](image)

Figure 6. VirusTotal results of the suspected host

From Figure 6 can be stated that the threat hunting process generates the expected outcome to identify the previously undetected or even unknown threats within organization.

4. Conclusion
Network Event Correlation that is gathered by mainly network security devices, such as firewalls, IPS, APT and also other appliances, whereas performed throughout this research is able to identify network behavior of potentially infected host. It can also be used as early indication or early detection to identify potential internal threat that cannot be detected by endpoint or network protection within organization. Simple idea such as inspecting common port that is generally used by Windows operating system, can lead to investigation process of potentially undetected malware infected host.

Memory forensic that is performed during this research also complement the network event correlation activity. It acts as a mandatory action to emphasize the legitimacy of early detection that is initially performed by network event correlation. It can become a thrilling activity for IT Security Incident Responder or other Cyber Security Professionals to investigate a cyber security case from different perspective and not solely rely on robust Information Security solutions available on the market. Memory forensic also will broaden the knowledge of the cyber security professionals to better understand the TTP (Techniques, Tactics & Procedures) of the adversaries.
References

Cole, Dr.E., 2016. Threat Hunting: Open Season on The Adversary. SANS.