An Assay: Next Generation Automated Cyber Defense Mechanism against Advanced Phishing Attacks and Campaigns Using Threat Hunting and SOAR Capabilities

Dr. Mohan Mahanty[1]*, Dr. Rajendra kumar Ganiya[2]

Department of Computer Science and Engineering,
Vignan's Institute of Information Technology, Visakhapatnam, AP, India
**mahanty.mohan@vignaniit.edu.in[1], rajendragk@rediffmail.com[2]*

Indian Journal of Advances in Science Engineering and Technology
Vol 1 No 2 2022: 71-82

IJASET

Original Article

An Assay: Next Generation Automated Cyber Defense Mechanism against Advanced Phishing Attacks and Campaigns Using Threat Hunting and SOAR Capabilities

Dr. Mohan Mahanty[1*], Dr. Rajendra kumar Ganiya[2]

Department of Computer Science and Engineering, Vignan's Institute of Information Technology
Visakhapatname, Andhra Pradesh, India
**mahanty.mohan@vignaniit.edu.in[1], rajendragk@rediffmail.com[2]*

Abstract

We are in the new era of cyber security, now a day's, a lot of companies and organizations are facing issues against cybercriminals. They are getting more sophisticated attacks creatively and 50-60% of those attacks and incidents are coming through Phishing. Phishing is a type of attack that involves sending an email or making a similar attempt to obtain information from the recipient. To detect these attacks one of solution is Threat Hunting. This whole process takes tedious manual effort and time. To avoid manual intervention and vast time effort we have implemented a framework using different threat hunting approaches conducting an in-depth analysis of phishing emails, integrating with Security Information Event Management (SIEM) and Security Orchestration Automation Response (SOAR) tools and Automated Threat Intel Detection using Internal & External feeds. Here, we combine both automated workflows and Human Investigation to identify advanced persistent attacks. The experiments conducted ascertain that the proposed model can identify 80-90% of threats against any organization and generate accurate metrics & reports.

Keywords: **Cyber Defense, Threat Hunting, SOAR, Phishing Attacks, Threat Intelligence, SIEM**

1. Introduction

Cyber threats that can attack smartphones include viruses, spam, and phishing attacks. These types of attacks are designed to trick users into performing various actions in order to obtain financial or social gains from the attackers. In most cases, these types of attacks are carried out through social engineering messages that are sent over the internet. Despite the various technological advancements that have been made in the fight against cybercrime, phishing attacks are still considered to be one of the serious crimes on the Internet. The term phishing was first used in 1996. It is regarded as one of the most common cyber threats that organizations face. Phishing attack is a type of attack that uses victim's personal information to obtain unauthorized access to it. This attack is classified as social engineering, which means it doesn't have a technical vulnerability. In order to carry out this attack, the attacker uses a phony web page that looks like it's from a reputable source.

According to Proofpoint's, in 2020 77% of organisations saw bulk phishing attacks, 66% of organisations delt with spear phishing attacks and 65% of organisations faced BEC attacks [1]. In 2021, more than 80% of the organisations fall victim to at least one phishing attack(s) last year. There is an indiscriminate bulk phishing attacks rose 12% over year. According to a study conducted by the Webroot Threat Report (WTR), over 1.5 million numbers of phishing sites are created every month. The rise of web applications has changed the way information is delivered and exchanged in today's society. Due to the increasing number of web applications, there has been a rise in the number of security threats. These threats can lead to the exploitation of vulnerabilities in these applications, which can cause severe damage to online transactions.

Now a days phishing attacks are the most popular attack vectors in social engineering, malware infections, Advanced Persistent Threats (APT). It is arguably the most damaging and high-profile cybersecurity threat facing in different organizations. Cybercriminals can able to gain access to email accounts, sensitive business data like customer names, confidential documents and medical records, irrespective of different industrial sectors [2].

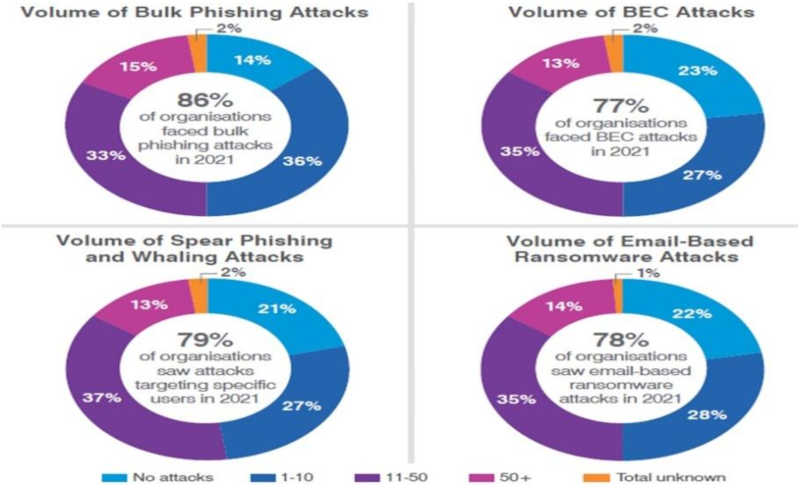


Figure – 1: Phishing attacks in 2021

In this case, threat hunting needs internal and external log data resources and threat intelligence feeds as well. Based on the raw data we can create a hypothesis and implement a real-time threat detection mechanism. Here, we are improving our detection capabilities using internal email data and external & internal threat intelligence feed data sources. There are various types of phishing attacks like, such as Email phishing, Whaling, Spear phishing, vishing, Smishing and Angler phishing.

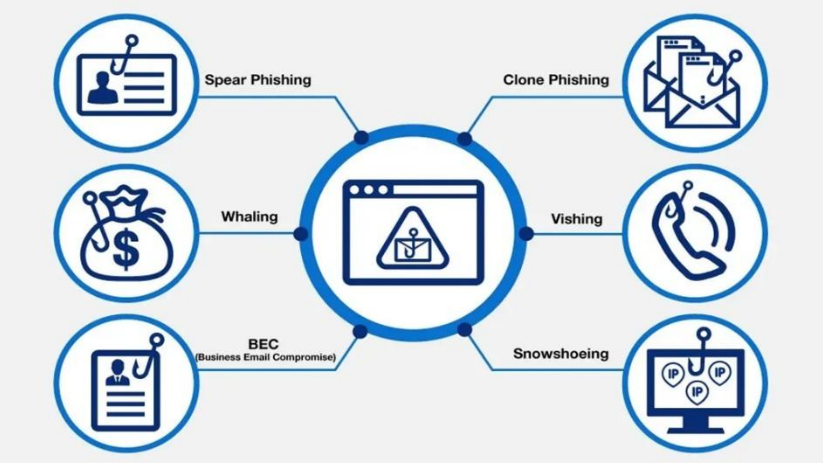


Figure – 2: Types of Phishing [3]

To detect these attacks one of solution is Threat Hunting. This whole process takes tedious manual effort and time. To avoid manual intervention and vast time effort we have implemented a framework using different threat hunting approaches conducting an in-depth analysis of phishing emails, integrating with Security Information Event Management (SIEM) and Security Orchestration Automation Response (SOAR) tools and Automated Threat Intel Detection using Internal & External feeds.

2. Related Work

The goal of phishing attack is to take the advantage of the weaknesses (vulnerabilities) in system processes that are caused by users. For instance, a user might not know that their passwords are being stolen, but they might accidentally leak them through a link in an email. This vulnerability could potentially affect the security of the entire system. Vulnerability in the DNS (Domain Name System) cache system could be used by attackers to create more convincing phishing messages. For instance, by tricking users into clicking on a link in an email, they could get more convincing messages by referring to spoofed or legitimate domains. This makes phishing attacks a complex issue that requires addressing both the technical and human layers.

Phishing is a type of that uses electronic messaging to trick users into providing their financial or personal information. It typically involves making users input their financial or personal information in order to gain access to a malicious site. A phishing attack usually begins by sending a link to a fake website that looks like it's legitimate. Dealing with this type of attack is a combination of technological and social engineering. Today most of the research work is going on malicious pattern identification, deep learning on malware samples and threat hunting hypothesis and processes. In our research work, we are automating existing processes and implementing advanced threat hunting approaches that can correlate with different log sources and detecting advanced threats in organization wide. Here we are integrating multiple log data sources, which include Phishing Email data, Security Logs, Threat Intelligence feeds and Certificate Transparency Logs.

Kiran D. Tandale [4] discussed the various types of phishing attacks and corresponding detection techniques. Most of these attacks are carried out through users weaknesses. They usually try to target the vulnerability that is already in the system. There are many techniques that one can use to mitigate the effects of phishing attacks. In this paper, authors presented various types of techniques that can be used to prevent the exploitation of the vulnerability.

Diksha Goel et.al discussed the various techniques used in mobile phishing attacks [5]. Due to portability and their small size, the use of smartphones has become more prevalent. Due to the increasing number of people using these devices, security threats related to them have also become more prevalent. Attackers often send out links to phishing websites or apps in an attempt to collect personal information. Mobile device users are more susceptible to phishing attacks than desktop users. Some of the factors that can increase the risk of getting attacked by these attacks include the size of the screen, lack of identity indicators, and the user's preference for different applications. Security requirements for mobile devices are also influenced by various factors. Since there is no way to check if the credentials sent to a rogue server are legitimate, attackers can easily access a mobile device's camera, contacts, and other sensitive information

Roberto O. Andrade et.al [6] discussed the rise of phishing attacks. Due to the emergence of the covid19 pandemic, the security risks associated with smart homes and smart buildings have become more relevant. The rise of telework mode and the increasing number of people working from home have created significant changes in the cybersecurity landscape. While the level of security at home is not as high as that of an organization, it can still be easily accessed by an attacker. This is because the home is often built with a smart infrastructure scheme, which can also increase the attack surface. In order to minimize the efficiency of VPN solutions, attackers have started to focus on social engineering attacks. The rise of the Internet of Things has allowed the creation of smart infrastructures that are designed to improve the resilience and sustainability of cities. Through the connections between devices and people, the data collected by these networks can be used to improve the efficiency of various organizations and consumers. According to various cybersecurity firms, the number of attacks during the covid19 pandemic has increased significantly.

They noted that the movement of people and activities from home has also increased the number of attacks. According to the FBI, business email compromise scams have cost companies around $3.1 billion in the past two years [7]. This is a huge amount of money for an organization, and it highlights the importance of having a strong understanding of how to prevent these types of attacks from happening. One of the biggest challenges that businesses face when it comes to cybersecurity is spear-phishing. Unfortunately, many organizations rely on their weakest link as their first line of defense against cybercrime. This allows cyber-criminals to easily access and steals data from their customers. In this article, authors discuss the primary ways that attackers can successfully carry out spear-phishing attacks.

Authors discussed about the cyber-attacks on various businesses organisations[8]. One of the biggest challenges that businesses face when it comes to fighting cybercrime is the number of and different types of phishing attacks that they can be subjected to. Although there are many common reasons why these types of attacks are carried out, one of the most common techniques used by scammers is by sending emails that appear to be from a reputable site. Although this technique is considered to be one of the oldest forms of phishing, it still remains one of the most effective. The goal of the scam is to trick the recipient into clicking on a link in an email, which will then lead to the download of malware. Despite the technological advancements that have been made in the past few years, email attachments still remain one of the most common ways that criminals can infect a user's computer. Despite the technological advancements that have occurred in the past few years, it's still important that businesses remain vigilant about the threats that they can still face. Unfortunately, criminals are still able to capitalize on the latest security measures.

Faran Sadique et.al [9] proposed an automated framework for Real-time Phishing URL Detection. Due to the increasing number of services being integrated with the internet, there has been a rise in the number of attacks that are designed to steal user information. One of these is phishing, which is a type of attack that uses fake websites to trick users into providing their personal information. One of the main strategies that users can use to prevent phishing is by maintaining a black list of web addresses. However, this method is reactive and cannot effectively defend against new phishing sites. In order to improve the effectiveness of this strategy, researchers have been developing machine learning techniques that can identify previously unseen phishing addresses. Unfortunately, there is currently a lack of an end-to-end framework that can effectively implement the techniques used in machine learning to identify phishing sites. This is because the lack of a comprehensive framework for developing and implementing these techniques has hindered their progress.

Authors presented a framework that aims to provide a fast and automated solution to the problem of identifying phishing sites. The study also covers the broader issue of malicious URLs, which include those that are designed to trick users into clicking on a link or download a gadget. One of the most popular techniques that users can use to identify phishing sites is by maintaining a blacklist. This is a list of malicious web addresses that are regularly updated by members of the community. Authors validated their framework using a real dataset, achieves 87% phishing detection accuracy in a real-time setup.

Due to the increasing number of attacks targeting individuals in the fields of diplomacy and defense, there has been a rise in the number of phishing attacks. One of the most prominent groups that has been involved in these attacks is the Kimsuky group. The Kimsuky group utilizes various attack techniques to carry out their operations. One of these is by sending out e-mails that appear to be from a legitimate source. They then trick their victims into clicking on a link in the message, which then installs a vulnerable document. This study analysed the various attack techniques used by the Kimsuky group [10]. It focused on the different types of phishing e-mails and their vulnerability use. It also performed detailed analysis of their attack methods. The study revealed that the Kimsuky group's main goal is to gather intelligence.

They mainly target Korean diplomatic and defense institutions and foreign organizations. They then use these attacks to carry out their operations. Aside from using e-mail to carry out their attacks, the researchers also suggested that mail service providers implement a countermeasure to prevent their users from getting lured into clicking on links in the messages.

This type of cyber-crime activity involves tricking users into providing their personal information, such as their passwords and credit card details. It typically involves making users believe that they are communicating with a trustworthy entity. The most common type of phishing attack is the online auction and payment web site. Authors introduced a novel method to detect and prevent the exploitation of these threats by passing the user's requested website address to the API [11]. The goal of this process is to build a parse tree with the root node of the requested URL and then validate the address of the web site that is being visited. Through the use of independent web services, this process does not require any changes in the application.

A phishing page is typically a replica of the real page, with the only difference being the address. This vulnerability allows an attacker to trick users into clicking on a link that takes them to a fake page. This paper proposes a login framework that can be used independently or with a browser extension to prevent users from being taken to a fake page. Authors proposes a semi-automated login mechanism that allows users to log into their websites without having to be alert at all times. It also allows them to distinguish between a real and fake login page.

The rapid emergence and evolution of new technologies, such as the Internet of Things and cloud computing, has created a new connotation for cyberspace. Due to the increasing number of security threats in cyberspace, traditional defense measures such as firewalls and intrusion detection systems are often not able to effectively address them. These measures often fall into a passive position, which can prevent them from taking effect when needed to respond to new attacks. The complexity and cost of an attack are increasing due to the continuous evolution of the systems' configuration characteristics. This is why the need for new strategies to counter the increasing attacks is critical. Despite the increasing number of security threats in cyberspace, many related works still lack sufficient evidence to introduce effective dynamic defense strategies. Yu Zheng et.al [12] introduce the concepts of dynamic defense and develop strategies and methods that can be used to move target defense and mimic attack behaviour. It also reviews the various implementation and evaluation procedures.

3. Automated Cyber Defense Mechanism

Cyber defense is a mechanism that aims to protect computer networks from attacks and threats. It involves identifying and preventing attacks before they can affect an organization's information and infrastructure. This is done through the detection and response of threats and attacks. Due to the increasing number of cyber-attacks and the complexity of their targets, many organizations have started to require the proper implementation of cyber defense. Through the analysis of the various factors that affect an organization's environment, cyber defense can identify and prevent attacks before they can affect its operations. It can also help in developing effective strategies to counter the threats. Various activities are also involved in the development of cyber defense.

This process can help minimize the appeal of the environment to potential attackers and prevent them from carrying out attacks. It can also help in developing effective strategies to counter the threats. Aside from analysing the environment, cyber defense also conducts technical analysis to identify the areas and paths that attackers could target. With the proper implementation of cyber defense, organizations can run their operations more efficiently and effectively. It can also help in improving the security strategy and resources by increasing the effectiveness of their security measures.

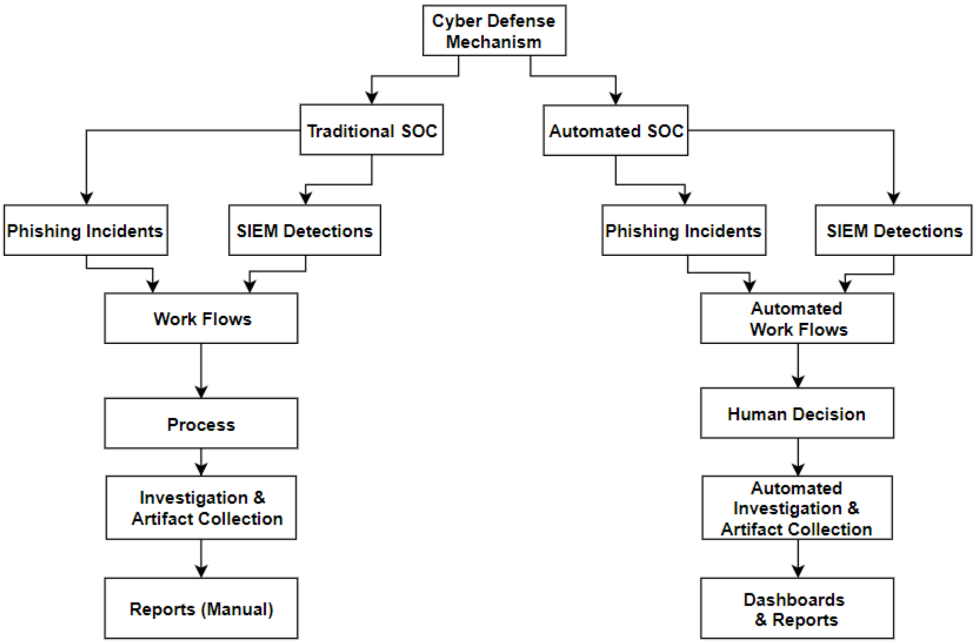


Figure – 3: Illustration about Automated Cyber Defense Mechanism

4. Proposed Method

In the proposed Automated Cyber Defense mechanism, we are collecting different data sources, which will transform from unstructured raw data to a standard structured format. In traditional methods internal phishing email analysis based on human decisions, and manually they correlate with internal data sources and external threat feeds. Here in our framework which can automate these human decisions, correlate logs using different threat hunting approaches and integrate with external threat intelligence feeds against structured data. Figure – 4, describes the architecture of proposed Automated Cyber Defense Mechanism for detecting advanced phishing and campaigns with automation and threat hunting capabilities.

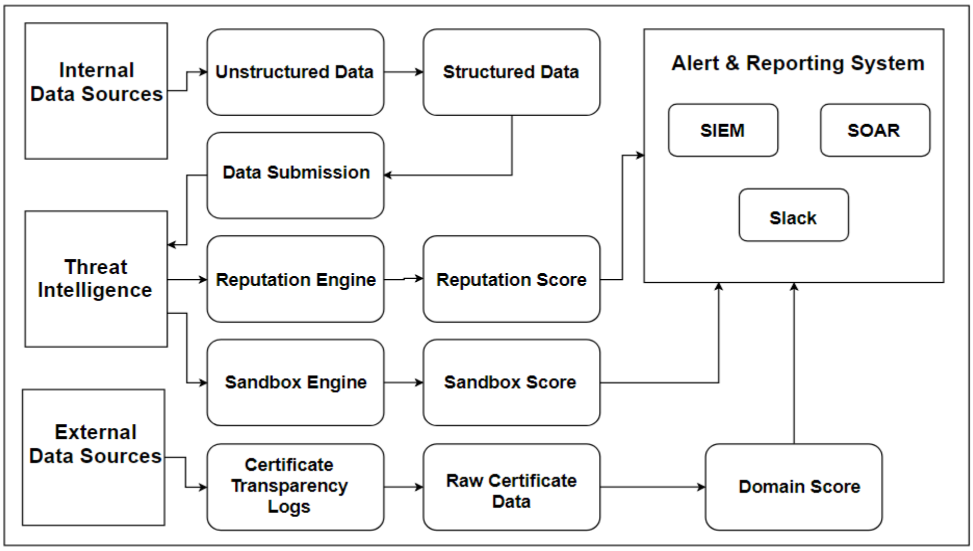


Figure – 4: Proposed Architecture for Automated Cyber Defense Mechanism

4.1 Internal Data Resources

4.1.1 Unstructured Data

Unstructured data is collected from an internal email box. This raw email data is collected from the internal employees of the organization. As per the information security policy, if they found any suspected email, it should be submitted to security teams. If contains a lot of information which can help to hunt and track down targeted advanced attacks.

4.1.2 Structured Data

Structured data is containing different elements that we can easily access anywhere. Here we are parsing the raw email data and extract the fields and transforming into a structured JSON format. We can able to extract unknown URL, Attachments, and Email headers from raw email data.

4.1.3 Data Submission

This phase is very crucial to identify the advanced threat using external threat intelligence feeds and sandbox investigation results. Here we are submitting Phishing URLs, Hashes, Malicious attachments to our Threat Intelligence Platform.

4.2.Threat Intelligence Resources

4.2.1 Reputation Engine

This engine is a core component of our detection mechanism. It was integrated with different third-party Threat intelligence APIs. It will analyse initial artifacts coming from structured data. Based on those results it will automatically trigger alerts to SIEM or SOAR solutions.

4.2.2 Sandbox Engine

It will be automatically analyzing the malicious attachments which were extracted from phishing emails. It will give detailed analysis reports with network artifacts, malicious executables, droppers, etc. Based on the impact it will give the malicious score.

4.3.External sources- Certificate Transparency Logs

These logs are assured, publicly auditable, append those certificate records stored centrally. Here we are detecting issued certificates, malicious certificates, and rogue CA certificates. After applying a few ML/Data science techniques, we can able to identify phishing domains related to the specific organization.

4.4. Alerting system

4.4.1. SIEM Engine

This tool will collect and analyse logs from the end-user's perimeter. It will then monitor for security threats in real-time and respond to them in response. It will also correlate the data from various sources.

4.4.2 Alert Integration

Alert bots are used for collaborating multiple individuals in organization wide. Here, we are using them for alerting if we get any critical incidents.

5. Implementation Process

As shown in Figure – 5, our implemented architecture for automated cyber defense mechanism coud able to identify new threat actors and IOCs (Indicator of compromise), hunting unknown threats in automated manner by using internal & external perimeter data collected by SEM. In our implementation, we included open source & enterprise security solutions, each component integrated by using SOAR (Security Orchestration Automation and Response) and Python tools. While identifying the threat actors, we introduced advanced algorithms which can give scoring for each layer of detection, based on this threat score it will automatically trigger security alerts.

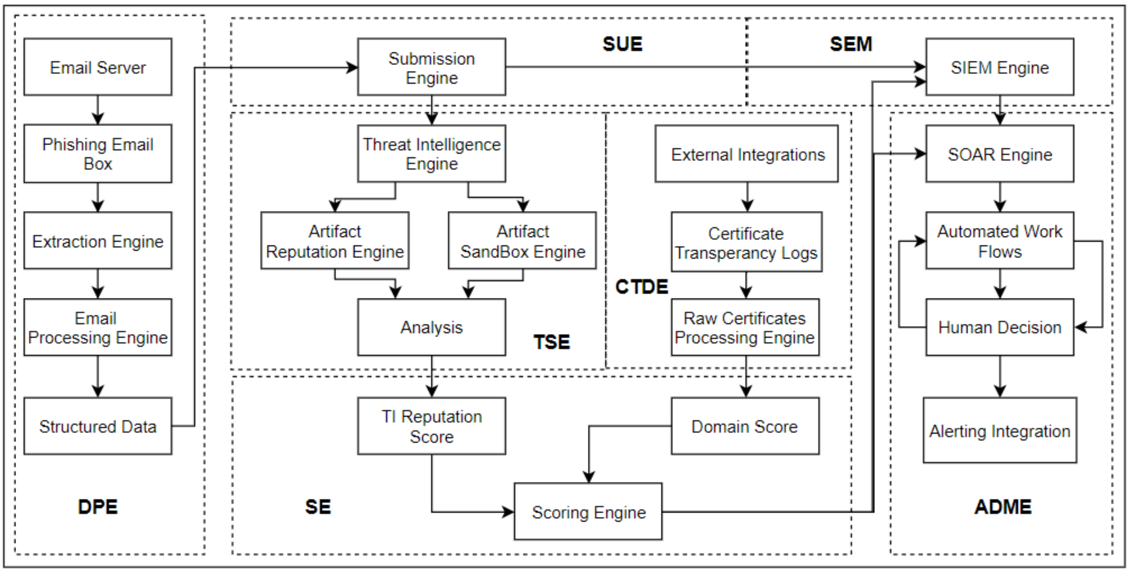


Figure – 5: Implemented Architecture for Automated Cyber Defense Mechanism

5.1 Data Processing engine (DPE)

In DPE component collects the real time internal phishing data from the targeted users and third-party resources. After collecting the phishing data, it will process and extract the artifacts from each phishing email. Finally, it will generate the structured format (JSON) where we can able to send the artifacts to different components in our Defense mechanism.

5.2 Submission & Update Engine (SUE)

In SUE component collects the structured data from DPE and sends the relevant artifacts to TSE and CTDE engines, once it's processed it will collect the response and send it to SEM and ADME engines.

5.3 Threat Intel & Sandbox Engine (TSE)

In TSE engine integrated with different third-party threat intelligence solutions to gather the intelligence and correlate on the fly over submitted artifacts like URL/domain/IP/Malicious attachments etc. Based on the detections, malicious patterns, C&C communications and sandbox environment behaviour, it will generate the different scores for each type of artifacts and send it to the SE.

5.4 Certificate Transparency Detection Engine (CTDE)

In CTDE engine crawls the real-time SSL certificate data from different open-source and commercial sources. It will be processing the raw SSL certificates information and applying on different fields based on that it will detect and tracking the compromised websites, phishing domains and APT campaigns. Once it's detected any suspicious domain it will escalated to SEM & ADME engines.

5.5 Scoring Engine (SE)

In SE mechanism defined few algorithms which they can able to detect the malicious or legit patterns based on the TSE and CTE generated appropriate artifacts score.

5.5.1 Security Event management System (SEM)

In SEM system is centralized security log collection platform for while organization. It collects & stores all endpoints, firewall, servers, network, and custom & third-party security data. Based on the ADME component instructions it will search and process the information and respond back to engine. It can able to generate different security dashboards to understand the security posture whole organization.

5.5.2 Automated decision-making engine (ADME)

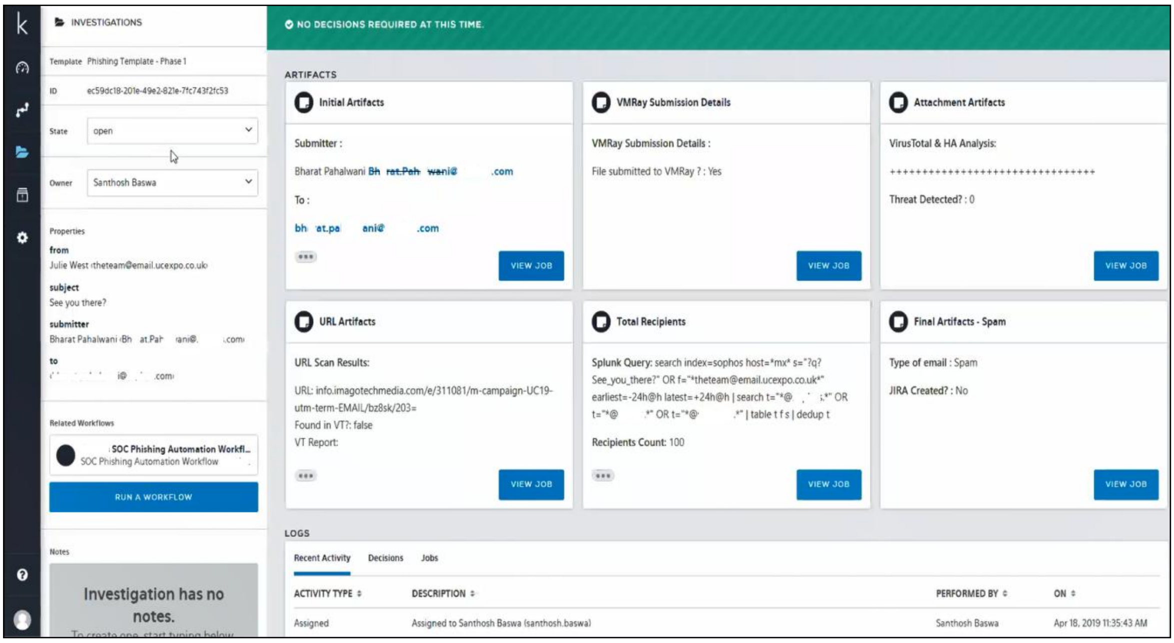
In ADME component is having different engines SOAR, Workflows Engine, Decision Engine. Each component are doing very crucial job while processing the consolidated data. Workflow engine mainly focus on the escalated incident artifacts and data sources, it will apply some rules on the incident data and do more correlation with multiple data sources and give better analyst-friendly incident overview to make human decisions. SOAR engine also known as Security Orchestration Automation Response, it will collect security incident data from different components and using workflows it will correlate & orchestrate each incident and escalated to SOC analysts to take future investigation and remediation actions. Alert Engine is escalating the critical security incidents information to analysts to 24x7 timeline. Based on the analyst responses and it takes automated decisions on SOAR workflows.

6. Results and Discussions

In Traditional security operations, we identified few gaps in investigation workflows, technical expertise, and lack of integration and manual efforts on each incident. So, each phishing incident takes average incident investigation and response time is above 30 minutes to triage and threat identification. We were able to reduce noise by using different integrations in our mechanism. In automated security operations, we fix the different manual effort problems like manual phishing analysis, threat investigations and report creation etc. In our mechanism it will automatically identify, correlates the threats and classifies and prioritize each incident based on the scoring systems. It will be able to give advanced security metrics and dashboards for management teams to understand the organization security posture. While comparing the both traditional and automated security operations incident investigation triage time, it drastically decreased. Even we were able to get automated alerting and user-friendly interface to do quick triage on any investigation.

The proposed cyber defense mechanism (CDM) having advanced hunting and detection capabilities to identify potential threats in SMB & Enterprise organizations. Mostly our internal employees are submitting suspected phishing emails to internal security teams. Then all phishing data goes to DPE engine and it will process and parse the all-phishing email data. SUE engine will submit to TSE & SE engines process the artifacts by using third party threat intelligence integration and get the score for specific artifacts and escalated to SEM or ADME to trigger alerts.

ADME contains hunting workflows, that are developed to identify potential threats depends on our hypothesis. In Workflows, it was mix-up with automated search queries/responses and analyst decision to execute the further actions, because sometimes even analyst also takes custom decisions depends on targeted threat actor. On Phishing & Certificate data, we were applying different workflows to detect threat actors and correlate with other perimeter data and enhance more overview. Figure – 6 shows the different incident overview & dashboards come up from phishing data.



Template Phishing Template - Phase 1

ID ec59dc18-201e-49e2-821e-7fc743f2fc53

State open

Owner Santhosh Baswa

Properties

from
Julie West ‹theteam@email.ucexpo.co.uk›

subject
See you there?

submitter
Bharat Pahalwani ‹Bh at.Pah ani@. .com›

to
i@ .com›

Related Workflows

SOC Phishing Automation Workfl...
SOC Phishing Automation Workflow

Notes

Investigation has no notes.
To create one, start typing below

Initial Artifacts

Submitter :

Bharat Pahalwani Bh rat.Pah wani@ .com

To :

bh at.pa ani@ .com

VMRay Submission Details

VMRay Submission Details :

File submitted to VMRay ? : Yes

Attachment Artifacts

VirusTotal & HA Analysis:

++++++++++++++++++++++++++++++

Threat Detected? : 0

URL Artifacts

URL Scan Results:

URL: info.imagotechmedia.com/e/311081/m-campaign-UC19-utm-term-EMAIL/bz8sk/203=
Found in VT?: false
VT Report:

Total Recipients

Splunk Query: search index=sophos host=*mx* s="?q? See_you_there?" OR f="*theteam@email.ucexpo.co.uk*" earliest=-24h@h latest=+24h@h | search t="*@ .*" OR t="*@ .*" OR t="*@ .*" | table t f s | dedup t

Recipients Count: 100

Final Artifacts - Spam

Type of email : Spam

JIRA Created? : No

ACTIVITY TYPE	DESCRIPTION	PERFORMED BY	ON
Assigned	Assigned to Santhosh Baswa (santhosh.baswa)	Santhosh Baswa	Apr 18, 2019 11:35:43 AM

Figure – 6: Detailed Phishing Incident Artifacts Collection

7. Conclusion

The proposed Automated Cyber Defence Mechanism (ACDM) improves the existing security detection & response and hunting capabilities to identify efficient manner. We evaluated the proposed ACDM model based on Security Detection & Response time, Analyst triage duration, Efficiency of attack detection, Track down unknown threats with existing security detection mechanism. In the future, we will use machine learning capabilities to automate threat hunting workflows. This will allow security analysts to apply corrections and improve the accuracy of the automated threat hunting tools.

8. References

1. “2022 State of the Phish Report - Stats, Trends & More | Proofpoint UK.” Available at: https://www.proofpoint.com/uk/resources/threat-reports/state-of-phish (accessed May 12, 2022).
2. Alkhalil Z, Hewage C, Nawaf L, Khan I. Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science. 2021 Mar 9;3:563060. Available at: https://doi.org/10.3389/fcomp.2021.563060
3. “What is Phishing? Avoiding Email Scams & Attacks | Fortinet.” Available at: https://www.fortinet.com/resources/cyberglossary/phishing (accessed May 12, 2022).
4. Tandale KD, Pawar SN. Different types of phishing attacks and detection techniques: A review. In2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC) 2020 Oct 30 (pp. 295-299). IEEE. Available at: https://doi.org/10.1109/ICSIDEMPC49020.2020.9299624
5. Goel D, Jain AK. Mobile phishing attacks and defence mechanisms: State of art and open research challenges. Computers & Security. 2018 Mar 1;73:519-44. Available at: https://doi.org/10.1016/j.cose.2017.12.006
6. Andrade RO, Ortiz-Garcés I, Cazares M. Cybersecurity attacks on Smart Home during Covid-19 pandemic. In2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4) 2020 Jul 27 (pp. 398-404). IEEE. Available at: https://doi.org/10.1109/WorldS450073.2020.9210363
7. Derouet E. Fighting phishing and securing data with email authentication. Computer Fraud & Security. 2016 Oct 1;2016(10):5-8. Available at: https://doi.org/10.1016/S1361-3723(16)30079-3
8. Rutherford R. The changing face of phishing. Computer Fraud & Security. 2018 Nov 1;2018(11):6-8. Available at: https://doi.org/10.1016/S1361-3723(18)30107-6

9. Sadique F, Kaul R, Badsha S, Sengupta S. An automated framework for real-time phishing url detection. In2020 10th Annual Computing and Communication Workshop and Conference (CCWC) 2020 Jan 6 (pp. 0335-0341). IEEE. Available at: https://doi.org/10.1109/CCWC47524.2020.9031269
10. Lee J, Lee Y, Lee D, Kwon H, Shin D. Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups. IEEE Access. 2021 May 31;9:80866-72. Available at: https://doi.org/10.1109/ACCESS.2021.3084897
11. Shanmughaneethi V, Abraham R, Swamynathan S. A robust defense mechanism to prevent phishing attack using parse tree validation. InInternational Conference on Advanced Computing, Networking and Security 2011 Dec 16 (pp. 551-557). Springer, Berlin, Heidelberg. Available at: https://link.springer.com/chapter/10.1007/978-3-642-29280-4_64
12. Zheng Y, Li Z, Xu X, Zhao Q. Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks. 2022 Aug 1;8(4):422-35. Available at: https://doi.org/10.1016/j.dcan.2021.07.006