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

[1]Mr. Santhosh Baswa, [2]Dr. G Rajendra Kumar [3]Dr. J Bala Bhaskara Rao
[1] M.Tech student, Department of Computer Science and Engineering, [2]Professor,
Department of Computer Science and Engineering, [3]Professor, Department of Mechanical
Engineering, Sri Sivani College of Engineering, Chilakapalem, Srikakulam– A.P.
[1]santhosh.nuz@gmail.com, [2]rajendragk@rediffmail.com, [3]drjbbrao@gmail.com

Abstract— **We are in the new era of cyber security; Now a day's 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 the simple way of sending an email or something similar and hoping you get information from the user. 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 that can conduct an in-depth analysis of phishing emails, integrating with Security Orchestration Automation Response (SOAR), Security Information Event Management tools and Automated Threat Intel detection using Internal & External feeds. Here, we combine both Automated workflows and Human Investigation to identify advanced persistent attacks. In this way, we can identify 80-90% of threats against any organization and generate accurate metrics & reports.**

Keywords— Threat Hunting, SOAR, Automation, Threat Intelligence, SIEM

I. INTRODUCTION

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. In this case, threat hunting needs internal and external log data resources and threat intel 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.

II. RELATED WORK

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. Reference [3] validates results with advanced detection within less response time, that mechanism will give in-detail analysis and correlated with existing logs and gives high-level insights on specific threats with advanced reporting.

III. ILLUSTRATIONS

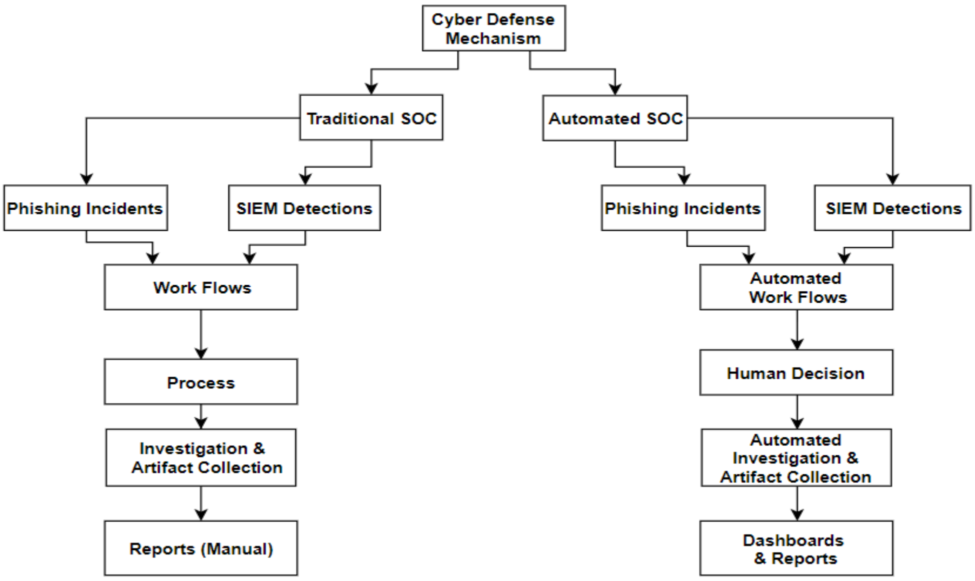


Fig. 1. Illustration about Cyber Defense Mechanism

IV. THE PROPOSED METHOD

The Fig.2. describes the architecture of proposed cyber defense mechanism for detecting advanced phishing and campaigns with automation and threat hunting capabilities.

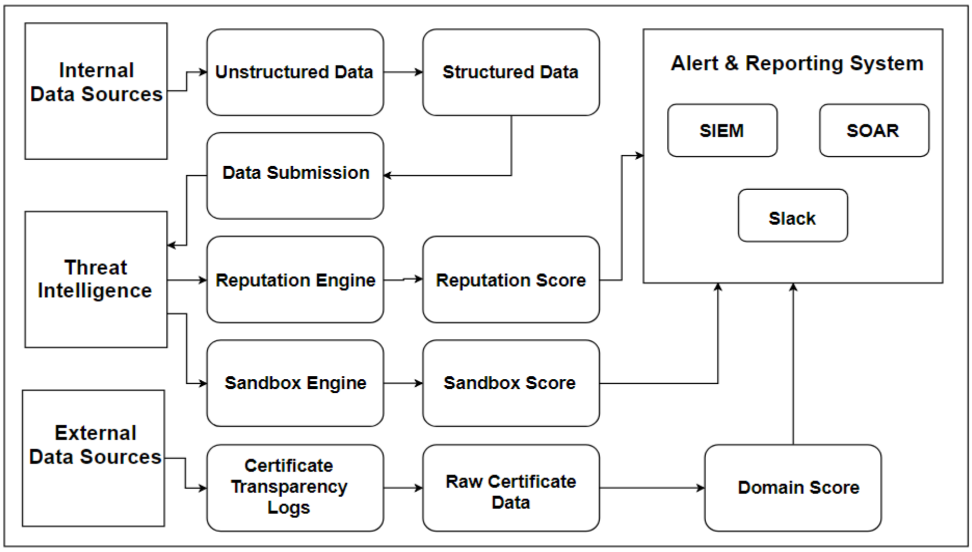


Fig. 2. Proposed Architecture for Automated Cyber Defense Mechanism

V. AUTOMATED CYBER DEFENSE MECHANISM

In our proposed 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.

VI. INTERNAL DATA RESOURCES

A. *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.

B. *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, Email headers from raw email data.

C. *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.

VII. THREAT INTELLIGENCE RESOURCES

D. 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.

E. 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.

VIII. EXTERNAL SOURCES

F. 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.

IX. ALERTING SYSTEM

G. SIEM Engine

It will collect, store and analyse logs from perimeter to end-user. It monitors for security threats in real-time for quick attack detection, containment and response with security reporting & compliance. Here we are using for correlating our structured data with other log sources.

H. Alert Integration

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

X. IMPLEMENTATION PROCESS

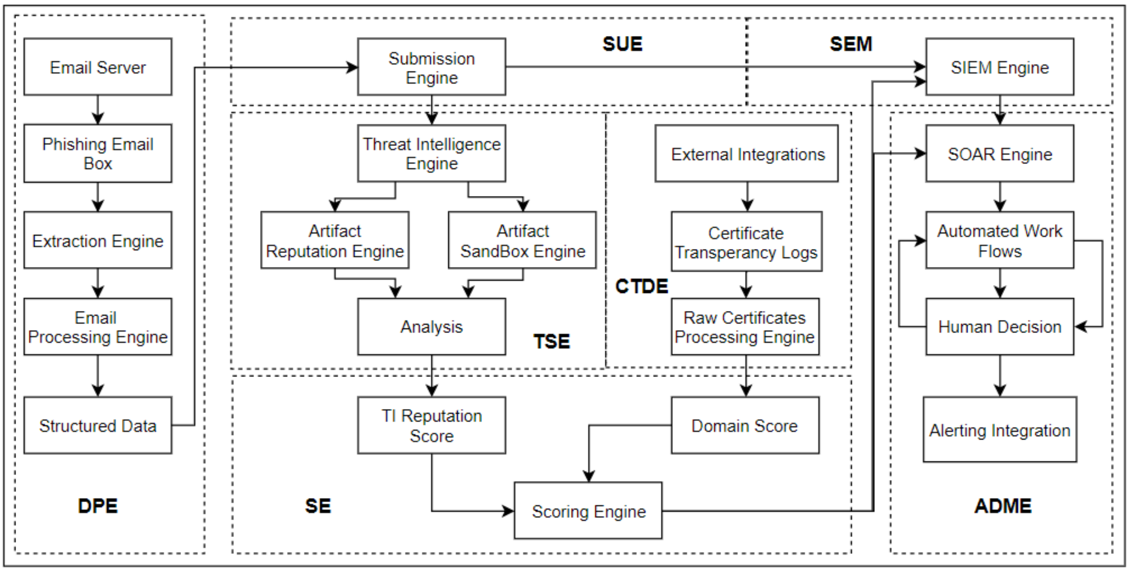


Fig. 3. Implemented Architecture for Automated Cyber Defense Mechanism

Using our implemented architecture for automated cyber defense mechanism can 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.

I. 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.

J. 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.

K. 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.

L. 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.

M. 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.

G. Security Event management System (SEM)

In SEM system is centralized security log collection platform for while organization. It collect & stores all endpoints, firewall, servers, network, 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.

N. Automated decision-making engine (ADME)

In ADME component is having different engines SOAR, Workflows Engine, Decision Engine. Each component 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 as an input and take automated decisions on SOAR workflows.

Tools: SIEM Engine (Splunk), SOAR Engine (Komand/Resilient), Python Development, Alert Integration (Slack)

XI. RESULT

In Traditional security operations we identified few gaps in investigation workflows, technical expertise, 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.

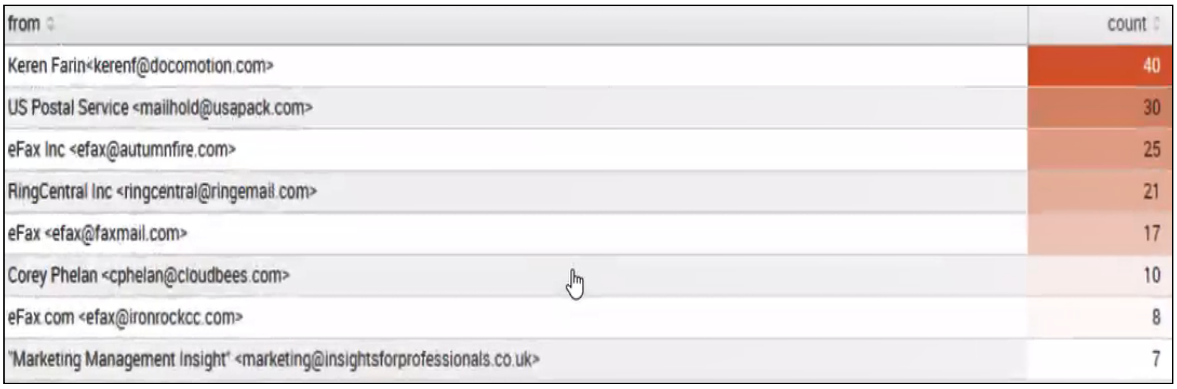
In Automated security operations, we fix the different manual effort problems like manual phishing analysis, threat investigations and report creation etc. In our mechanism it will automatically identify, correlates the threats and classifies and prioritize each incident based on the scoring systems. It can able to give advanced security metrics and dashboards for management teams to understand the organization security posture. While compare 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.

Our Cyber Defense Mechanism 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 is 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 take 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.

Here are the different incident metrics & dashboards come up from phishing data.



from	count
Keren Farin<kerenf@docomotion.com>	40
US Postal Service <mailhold@usapack.com>	30
eFax Inc <efax@autumnfire.com>	25
RingCentral Inc <ringcentral@ringemail.com>	21
eFax <efax@faxmail.com>	17
Corey Phelan <cphelan@cloudbees.com>	10
eFax.com <efax@ironrockcc.com>	8
"Marketing Management Insight" <marketing@insightsforprofessionals.co.uk>	7

Fig. 4. Top targeted phishing email senders

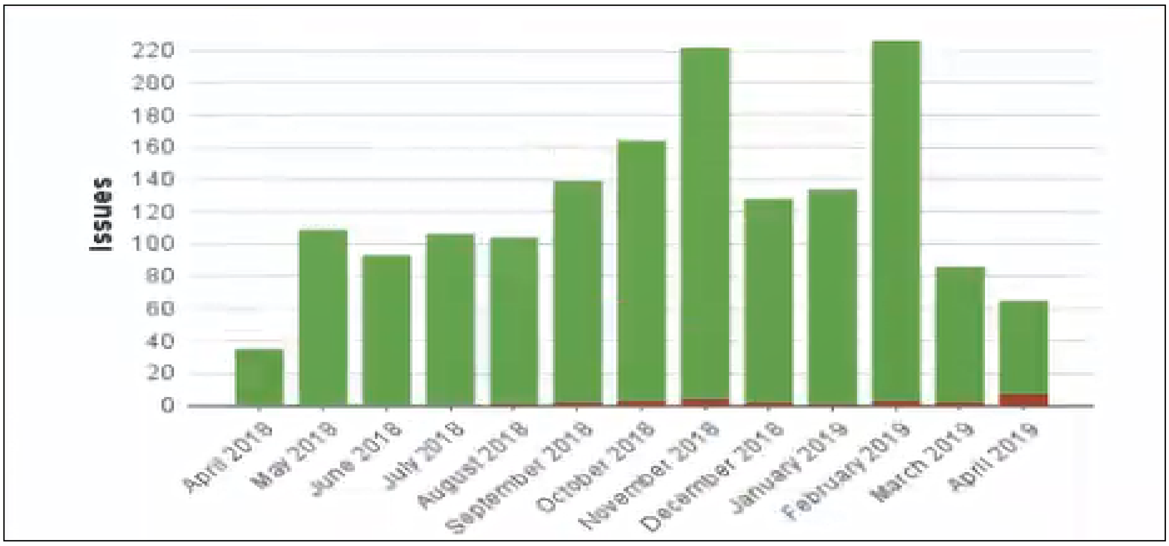


Fig. 5. Phishing incident metrics by month

XII. CONCLUSIONS

We tried to achieve few things, where we can improve our existing security detection & response and hunting capabilities to identify efficient manner. Here we evaluated based on Security Detection & Response time, Analyst triage duration, Efficiency of attack detection, Track down unknown threats with existing security detection mechanism. In future we are trying to implement threat hunting workflows with machine learning capabilities where you can train the software to accept and apply corrections and refinements from security analysts, so that the automated threat hunting becomes increasingly fast and accurate over time.

REFERENCES

[1]. Diego Fernandez, Oscar Pastor Acosta, Christopher Spirito: *Conceptual framework for cyber defense information sharing within trust relationships,* 2012 4th International Conference on Cyber Conflict – (CYCON 2012).

[2]. Hongchao Hu, Jiangxing Wu, Zhenpeng Wang, Guozhen Cheng: *Mimic defense: A designed-in cybersecurity defense framework*. IET Information Security (Volume:12, Issue: 3, 5 2018)

[3]. Y.B. Luo, B.S. Wang, G.L. Cai, *"Effectiveness of port hopping as a moving target defense"*, 2014 7th Int. Conf. Security Technology (SecTech), pp. 7-10, 2014.

[4]. R. Zhuang, S.A. DeLoach, X. Ou*, "Towards a theory of moving target defense",* Proc. First ACM Workshop on Moving Target Defense. ACM, pp. 31-40, 2014.

[5]. F. Cohen, *"Operating system protection through program evolution", Comput. Secur.*, vol. 12, no. 6, pp. 565-584, 1993.

[6]. W. Peng, F. Li, C.T. Huang et al., *"A moving-target defense strategy for cloud-based services with heterogeneous and dynamic attack surfaces",* 2014 IEEE Int. Conf. Communications (ICC), pp. 804-809, 2014.

[7]. B. Choudhury, T. S. Choudhary, A. Pranmanik, W. Arif, J. Mehedi, *"Design and implementation of an SMS based home security system",* IEEE International Conference on Electrical Computer and Communication Technologies [ICECCT], pp. 1-7, 2015.

[8]. Supreeta Venkatesan, A. Jawahar, S. Varsha, N. Roshane, *"Design and Implementation of an automated security system using Twilio messaging services"*, 2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS).

[9]. Zhaoqing Peng, Takumi Kato, Hideyuki Takahashi, Tetsuo Kinoshita, *"Intelligent Home Security System Using Agent-based IoT Devices",* IEEE 4th Global Conference on Consumer Electronics [GCCE], pp. 313-314, 2015.

[10]. Ravi Kishore Kodali, Vishal Jain, Suvadeep Bose, Lakshmi Boppana, *"IoT Based Smart Security and Home Automation",* International Conference on Computing Communication and Automation [ICCCA 2016]", pp. 1286-1289.

[11]. Vasileios Mavroeidis and Siri Bromander, *"Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence".* In Proceedings of the European Intelligence and Security Informatics Conference. IEEE, 2017.

[12]. Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka, "*Guide to Cyber Threat Information Sharing*"**.** NIST Special Publication, 800:150, 2016.

[13]. Ju An Wang, Minzhe Guo, *"OVM: an ontology for vulnerability management"***,** Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, April 13-15, 2009, Oak Ridge, Tennessee, USA [doi>10.1145/1558607.1558646]