Intelligent-based SIEM security email alert

1st Chyun Horng Chi
Faculty of Information Science and Technology
Multimedia University
Melaka, Malaysia
chunhong479@gmail.com

2nd Shih Yin Ooi
Faculty of Information Science and Technology
Multimedia University
Melaka, Malaysia
0000-0002-3024-1011

3rd Evita Herawaty Binti Othman *Product & Innovations*
TM One
Kuala Lumpur, Malaysia
evita.othman@tm.com.my

4th Ying Han Pang
Faculty of Information Science and Technology
Multimedia University
Melaka, Malaysia
0000-0002-8381-4071

5th Mohd Khir Bin Abu Yan
Security Operation Center
TM One
Kuala Lumpur, Malaysia
mkhir@tm.com.my

6th Khairul Idzwan Bin Sidin
Security Operation Center
TM One
Kuala Lumpur, Malaysia
idzwan.sidin@tm.com.my

2023 11th International Conference on Information and Communication Technology (ICoICT) | 979-8-3503-2198-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICoICT58202.2023.10262562

***Abstract*—SIEM, or Security Information and Event Management, can be considered the latest cybersecurity technology in the security strategy that was taken and utilized mostly by professional cybersecurity teams. Whether it's from a large enterprise to a medium-small size company, it is used as a tool to monitor their IT environment to protect the company's digital assets, security incident prevention, and in addition, protect the company's reputation. Due to its reliability, it is fair to say that SIEM plays a vital role in the current cybersecurity trends since it can provide all these features through just a platform or web console compared to an antivirus. Even though SIEM includes many advanced security features. However, some pre-installed features contain limitations that may not suit a security team's needs when it comes to their operation manuals. For instance, the SOC (Security Operations Center) team is often required to review the reports generated by SIEM and send the info to their clients with the company's customized email templates. This feature is not provided by most of the SIEM software. Thus, this paper aims to develop a system that can overcome the lack of email customization and SOC team-to-customers email sending-related issues in the SIEM that the SOC teams currently face in their daily operation.**

Keywords*—*SIEM, security information, event management, cybersecurity, soc team, email customization

I. INTRODUCTION

A security event or incident usually refers to any occurrence in an IT environment with the possibility of causing a vulnerability, exploitation in the environment, or simply a false positive. Such events could consist of unauthorized user access, changes in system configuration, suspicious user activity, or notable user activity.

Compared with antivirus software, a SIEM could do more than detect and eliminate malicious viruses. It helps SOC (Security Operations Center) team members to ease the task of standard security operation by allowing them to monitor their virtual security environment of the company, detecting any unwanted events or activities, reporting any occurrence of security incidents, investigating security events, and most importantly, alerting both SOC team members and respective clients. As such, SIEM becomes the favorable and necessary tool for SOC teams to operate to protect and serve their organization.

SOC teams always entrust the reliability of the operation of their IT systems to this kind of automated security technology, which can report any issues that may occur. Though SIEM alerts are one of the most popular tools in the security experts' field, one of the difficulties with checking SIEM data for values is that there is no standardized or customized format for the information in these messages. Security alert email received from SIEM is not formatted and raw, resulting in SOC needing to manually format and add additional relevant data from other sources before sending the alert to the clients.

Often, when the client's site has requested an email alert report from the corresponding IT company, SOC teams will be the crucial department responsible for analyzing the specific log generated by the SIEM software. Filtering out the necessary content that needs to be included in the email and sending it back to the client's site. However, the limitation of the email-sending feature and content customization feature available in the SIEM software causes most SOC teams to manually customize their email content by referring to or copy-pasting the information methods from various sources. Furthermore, the provided default email template with a predefined format prevents SOC teams from customizing it to their company's preferred format before sending it to respective customers.

Furthermore, all these problems mentioned above will not only cause the SOC team members to have a tedious and tiring experience in manually customizing email problems, but it could sometimes also cause a time-critical situation where clients have serious threats in their network and need email alert reports immediately.

Thus, this paper aims to develop a system that can overcome the problems of lacking log content and email template editing ability of SIEM software. For instance, the user can customize their email template to include necessary information inside the email and forward it to the customer automatically or manually. This can reduce the time-consuming process of manual formatting and the risk of human errors. In addition, a content filter feature allows the users to choose the information and data they think must include in the email. This can help SOC teams greatly when they do not require to review one by one and the data from the detailed report generated by SIEM tools.

II. STUDY ON EXISTING SIEMS

A. Characteristics of a SIEM

Security Information and Event Management[1], also recognized as "SIEM". It is a professional security tool often used by large corporates and enterprises for real-time system monitoring, analysis, and alerts of suspicious security-related activities and events.

SIEM has become an important security strategy for most enterprises today as SIEM techniques include the two most commonly used security technology, which is the security information management (SIM) which collects log file data or reports on security threats, and security event management (SEM) that performs system network real-time monitoring, notifications about essential issues and establishes correlations between security events [2]. Simply put, it has both security management and event management capabilities.

Many organizations prefer using SIEM because it helps the company handle its cybersecurity environment by filtering out a large amount of raw data and notifying network security specialists with security alerts generated by the software. Besides that, it also satisfies the requirements by spontaneously creating reports from the corresponding logged security events, which allows specialists to store and analyze them effectively. With the SIEM as a cybersecurity tool, the corporation will not have to collect log data and compose reports manually.

SIEM tools normally operate in several steps. Usually, the SIEM tools will first perform data gathering from the possible sources of network security information by which collecting log data or events that generated by the system host, software, or devices, such as antivirus software or firewalls system, across a company's network environment, then gathering those data altogether to put it into a centralized platform. Afterward, the SIEM will analyze and classify each data into a category, such as successful or failed logins, suspicious activity, and other risky events. Then, SIEM tools will generate security alerts upon detection of any unwanted security issues for the company to prefer those alerts to a lower or higher priority through predefined rules [3][4].

In sum, the SIEM delivers two main purposes, which are:

1)To provide reports on any cybersecurity incidents, events, or activities. For example, successful and failed logins, suspicious activity, and other possible risk events.

2)Send alerts and inform SOC teams if any analysis shows that an activity or event runs over the predetermined rulesets set by the organizations and indicates a potential security issue.

Without any SIEM tools, it’s difficult, especially for security teams, to pinpoint which events should be considered and which data can be ignored. Thus, when SIEM has been implemented, security teams can get a better understanding of their security environment as there could be false threats, multiple incidents may be occurring that have not yet affected performance, or even unseen malicious events that might cause massive damage to the company in the future [5][6].

B. Analysis of current SIEM models

Based on the extensive study and research on various SIEM brands, Table I below shows the data comparison between the latest type of SIEM models and the basic SIEM features that they provide in their system and for their users[7][8][9][10].

This analysis includes most SIEM models with the standard SIEM feature, such as real-time monitoring, compliance reporting, and notification alert features. However, we can see that the IBM Security QRadar, LogRhythm NextGen SIEM, and Rapid7 InsightIDR are not up to par when it comes to email customization-related features, which might cause any companies that are implemented this SIEM software to have to look for an alternative solution to counter the limitation and lacking email customization functions. Even though the other rest of the SIEM models do provide will either fully or partially customizable email alerts, the pre-provided email template may not match well with certain companies’ needs as well as the possibility of violating a SOC team’s operation manuals and thus leading the problems back to the email customizing issues.

TABLE I. COMPARISON BETWEEN CURRENT SIEM BRANDS

SIEM Model	**SIEM Feature**			
	Real-time Monitoring	***Compliance Reporting***	***Alerts Notification Type***	***Customizable Email Alerts***
IBM Security QRadar	Capable	Not Capable	Email, MS Team, SMS, Telegram	Not Capable
SolarWinds Security Event Manager	Capable	Capable	Email	Capable
Splunk Enterprise Security	Capable	Capable	Email	Capable
ArcSight Enterprise Security Manager	Capable	Capable	Not Capable	Capable
LogRhythm NextGen SIEM	Capable	Capable	Email, SMS	Not Capable
Exabeam Fusion SIEM	Not Capable	Capable	Email, Security Dashboard	Capable
Rapid7 InsightIDR	Capable	Not Capable	Email	Not Capable

III. Proposed Scheme

A. System flow Implementation

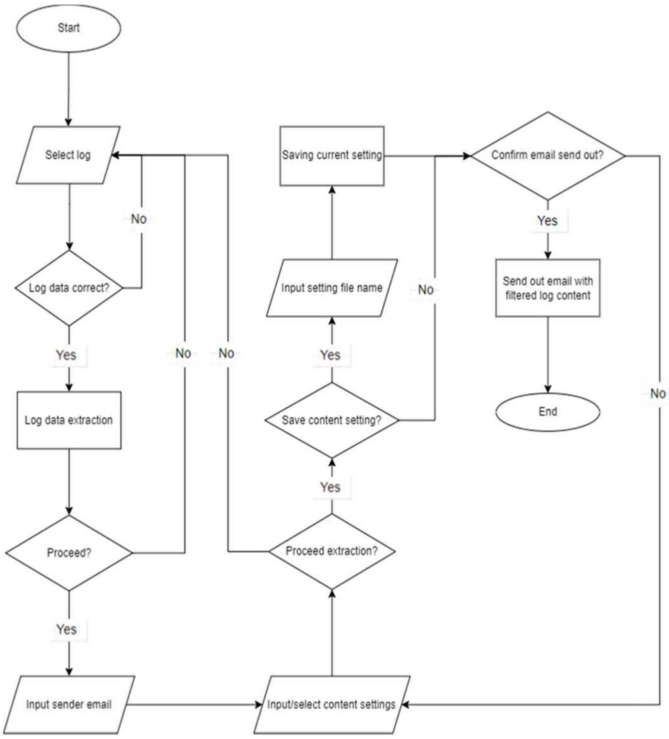


Fig. 1. Flowchart indicating the general system flows

Step 1 – When the user first approaches the system, the initial action must be to select the log file that needs to be included in the output email.

Once done, the user can choose to extract the data from the log file and proceed to the next page or refresh the page and choose a new log file. These actions can be done by interacting with the few UI elements provided on the first screen of the system, such as:

- Button "Choose File" – When the user clicks on this button, the file dialog will show up, allowing the user to select the log data that must be extracted.

- Button "Extraction" – The system will extract the info from the selected log data once the user clicks it.

- Button "Cancel" – This element functions as a refresh to clear the screen for the user to reselect new log data

Besides that, an element labeled "Extracted Data" will display the selected log file in the middle of the screen after using the "Choose File" button.

Step 2 – After the user has completed step 1, the system will direct the user to the next page, the email content settings page, which requires most user input. The first thing the user needs to do is fill up the receiver or client's email address information. From there, the user is provided 2 types of email sending:

- Emails for "TO" – This allowed the email content to be sent to the client as a direct response or action.

- Emails for "CC" – This is an acknowledgment to keep the receiver or client in the loop but is not addressed directly.

Step 3 – Besides the email addresses, the user must also fill in all the necessary information that will be included in the email content under the "Dropdown Settings" and "Filling Information" before proceeding to the next page.

Step 4 – After the user has done filling up all the information for the entire page, the user can select the "Confirm" button to allow the system to capture the filled info and insert it into the email content or click "Return to report" button to redirect back to the first page which is the log file selection section.

- The "Confirm" button also included an option for the user to save the entire information that the user has filled in as a setting file that allows the user to use it as a shortcut instead of filling the entire inputs again. If the user decides to do so, the setting file will be stored in the user's local device directory, while choosing "No" will save nothing and proceed to the next page.

Step 5 – Once the user has completed Step 1 (log data selection) till Step 4 (email content settings), the user will be brought to the "Confirmation" page. At this point, the system should be able to detect all the necessary information, including raw data from log data selection and the inputs from the user for both email content and send-out addresses. The system will then perform data conversion by automatically including and rearranging those raw data and inputs from users into their respective position inside the email template based on the provided user's or company's client email format. Once done, the system will display the generated email with filtered log content as a preview for the user to confirm whether the content inside the email is correct and accurate. If the user is satisfied with the results, the user can click on any space of the preview and select "Submit" to send out the email. Otherwise, if the user is unsatisfied or needs to make some changes from the previous page, the user can select the "Cancel" button, where the system will redirect the back user to the "Email Settings" page to make some adjustments or fix some mistakes.

Step 6 – Once the user has confirmed the send-out from Step 5 (Confirmation page). The screen will display a message as an indicator of the success of the sending result.

B. Programming language implementation requirement

- HTML – Will be used mainly as the main programming language for constructing the base structure of the whole web page system.

- CSS – Used to design the presentation style of the system web pages, including page colors, text size, display layout, positions, and the overall UI.

- JavaScript – Create interactive elements such as buttons, selective options, or dropdown menus. Besides that, it is also used as algorithm implementation to ensure the features work as intended, such as content filtration, email validation, web session storage, and load data from local devices.

- PHP – Responsible for generating a directory on a local device for storing software data, including settings content on the local device. Besides that, one of the code libraries, the PHPMailer, will be used for sending emails securely and effectively from a web server.

C. Algorithms of the system's core functionality

To further evidence our proposed framework, the two primary pseudocode are disclosed in this section to provide a logical understanding and visualization of the proposed framework.

Algorithm I:
Pseudocode of log file data extraction and validation function

```
START
IF input file's type NOT application/vnd.openxmlformats-officedocument.spreadsheetml.sheet THEN

   TRIGGER POPUP "Only .xlsx or .xls file format are allowed"
   SET extractedDataLabel display style TO none
   SET extractedData innerHTML TO ''

ELSE

   BefEmailHeader ← input file's name
   SET extractedDataLabel display style TO inline

   reader ← FileReader
   USING reader's function that read input file as array buffer

   WHEN reader has been loaded

    data ← Uint8Array FOR reader's result
    work_book ← XLSX's function that read input file's data in array format
sheet_name ← work_book's Sheet Names
sheet_data ← XLSX's function that convert sheet_name to JSON

   IF sheet_data's length is larger than 0 THEN
        table_output ← Create table

        FOR row = 0 TO sheet_data's length
          table_output ← table_output + 'table row'

          IF row is larger than 0 THEN
    table_output ← table_output + ' table data + row '
          ELSE
          table_output ← table_output + ' table header + "No" '
          END IF

          FOR cell = 0 TO sheet_data[row]'s length
            IF row is larger than 0 THEN
                         table_output ← table_output + ' table data + sheet_data's current row's cell '
                  ELSE
                  table_output ← table_output + ' table header + sheet_data's current row's cell '
                  END IF
          NEXT
                 table_output ← table_output + table row
         NEXT
    END IF
                 table_output ← table_output + ' end of table creation and align table to center position'
                 SET extractedData's innerHTML TO table_output
END IF
END
```

The Algorithm I above represent one of the main core functions of the system and the main feature of the first web page. It is mainly responsible for performing data validation on the selected file type of the log data file by the user, creating and displaying the log data table on the screen based on the extracted data from the selected log data file, and transferring all the necessary extracted data that has been stored in a temporary array to local session storage for passing data.

Algorithm II:
Pseudocode of generate email output with extracted log data and email send-out function

```
START
   Using PHPMailer
   Using PHPMailer Exception
   Load Exception.php that locates in C > xampp > php > PHPMailer > src folder
   Load PHPMailer.php that locates in C > xampp > php > PHPMailer > src folder
   Load SMTP.php that locates in C > xampp > php > PHPMailer > src folder

   receiverList ← received form data 'Receiver'
   receiverItem ← split receiverList into array elements by using "," as separator
   ccEmailList ← received form data 'CCEmails'
   ccEmailItem ← split ccEmailList into array elements by using "," as separator
   mail ← PHPMailer

   SET mail isSMTP ← true
   SET SMTPSecure ← 'tls'
   SET mail SMTPAuth ← true
   SET mail Host ← 'smtp.gmail.com'
   SET mail Port ← 587
   SET mail Username ← 'pr0JectPurpos3@gmail.com'
   SET mail Password ← 'wmgpmahddrtackqy'
   SET mail From ← 'pr0JectPurpos3@gmail.com'
   SET mail FromName ← '1171103091_ChiChyunHorng_ST'

   FOREACH receiverItem emailAdd do
      SET mail addAddress ← emailAdd
   END

   FOREACH ccEmailItem ccEmailAdd do
      SET mail AddCC ← ccEmailAdd)
   END

   SET mail Subject ← received form data 'EmailHeader'
   SET mail Body ← received form data 'EmailValue'
   SET mail AddEmbeddedImage ← 'C:/xampp/htdocs/FYP2-1171103091_ChiChyunHorng_ST/Design/Image/Head.png','Head'
   SET mail AddEmbeddedImage ← 'C:/xampp/htdocs/FYP2-1171103091_ChiChyunHorng_ST/Design/Image/DigitalImage.png','DigitalImage'
   SET mail AddEmbeddedImage ← 'C:/xampp/htdocs/FYP2-1171103091_ChiChyunHorng_ST/Design/Image/Footer.png','Footer'
   SET mail IsHTML ← true

   IF mail not send THEN
    OUTPUT START OF HTML
    OUTPUT applied CSS link
    OUTPUT header "EMAIL SENDING STATUS"
    OUTPUT paragraph "Dear user, the emails can't be sent out due to" + mail's ErrorInfo that aligns to center
    OUTPUT END of HTML
  ELSE
    OUTPUT START OF HTML
OUTPUT applied CSS link
OUTPUT header "EMAIL SENDING STATUS"
    OUTPUT paragraph "Dear user, the emails had been sent out" that aligns to center
    OUTPUT button "Return to Report" that aligns to center
    OUTPUT script that only be trigger when user click on "Return to Report"
          REDIRECT TO 'http://localhost/FYP2-1171103091_ChiChyunHorng_ST/Website/Reportpage.html'
    OUTPUT END OF HTML
  END IF
END
```

Algorithm II above represents another main core function of the system and the main feature of the third web page of the system. It mainly handles displaying the final output of the generated email by the system which its content is included with all the necessary extracted log data. It also serves as a confirmation for the user to check the output's integrity and to ensure that the generated email is sent to the corresponding client's email address.

IV. Development Results and Experiments Showcase

This section will discuss the various showcases of the system development and experiment results that were conducted based on various combinations across different web browser types, log data types, and the receiver's email platform types to ensure the developed system is compatible with the tested factors and all the features inside the system will be working as intended.

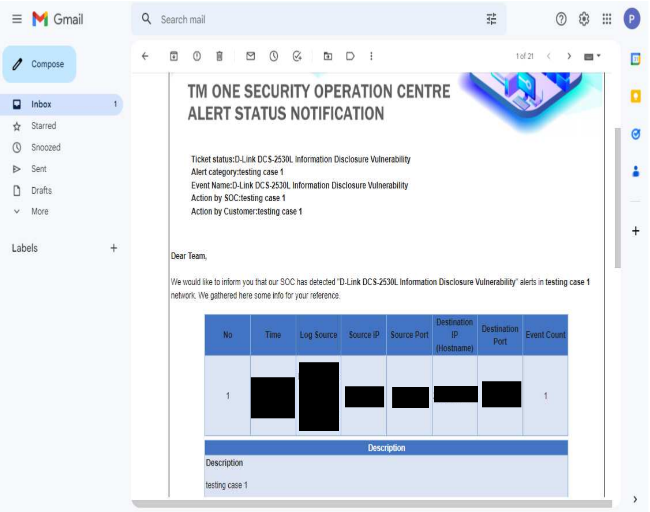
A. *Testing cases of system compatibility*

1) Testing case 1

Browser type: Google Chrome

Log data type: D-Link DCS-2530L Information Disclosure Vulnerability

Receiver email platform: Gmail



TM ONE SECURITY OPERATION CENTRE
ALERT STATUS NOTIFICATION

Ticket status:D-Link DCS-2530L Information Disclosure Vulnerability
Alert category:testing case 1
Event Name:D-Link DCS-2530L Information Disclosure Vulnerability
Action by SOC:testing case 1
Action by Customer:testing case 1

Dear Team,

We would like to inform you that our SOC has detected "D-Link DCS-2530L Information Disclosure Vulnerability" alerts in testing case 1 network. We gathered here some info for your reference.

No	Time	Log Source	Source IP	Source Port	Destination IP (Hostname)	Destination Port	Event Count
1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1

Description
Description
testing case 1

Fig. 2. Sample experimental result of the system tested on testing case 1

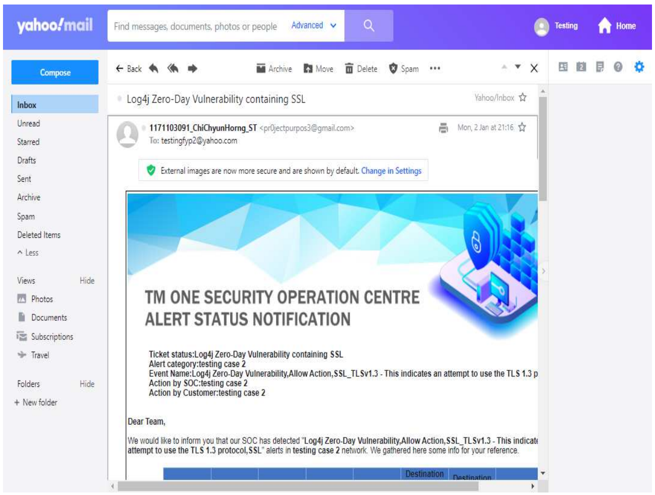
As the first testing case result, the sample image from the above indicates that the proposed system is compatible well with the web browser type, Google Chrome, and it is able to extract and convert the raw data into the generated email from the selected log data type, D-Link DCS-2530L Information Disclosure Vulnerability. Furthermore, with the tested email platform type, Gmail, it is also proven that the proposed system can successfully send out the generated email that includes all the extracted log data to the corresponding email platform by using the "Submit" function from the Intelligent-based SIEM security email alert system.

2) Testing case 2

Browser type: Firefox

Log data type: Log4j Zero-Day Vulnerability containing SSL

Receiver email platform: Yahoo mail



Log4j Zero-Day Vulnerability containing SSL

1171103091_ChiChyunHorng_ST <pr0jectpurpos3@gmail.com>
To: testingfyp2@yahoo.com
Mon, 2 Jan at 21:16

External images are now more secure and are shown by default. Change in Settings

TM ONE SECURITY OPERATION CENTRE
ALERT STATUS NOTIFICATION

Ticket status:Log4j Zero-Day Vulnerability containing SSL
Alert category:testing case 2
Event Name:Log4j Zero-Day Vulnerability,Allow Action,SSL_TLSv1.3 - This indicates an attempt to use the TLS 1.3 p
Action by SOC:testing case 2
Action by Customer:testing case 2

Dear Team,

We would like to inform you that our SOC has detected "Log4j Zero-Day Vulnerability,Allow Action,SSL_TLSv1.3 - This indicate attempt to use the TLS 1.3 protocol,SSL" alerts in testing case 2 network. We gathered here some info for your reference.

Destination Destination

Fig. 3. Sample experimental result of the system tested on testing case 2

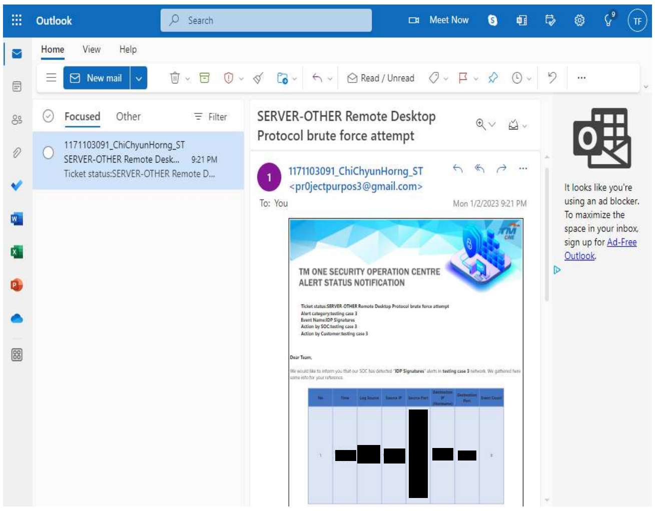
Through the second testing case, the result above showcases that the proposed system can function as well as the first testing case through the web browser type, Firefox, and can perform the log data extraction function that includes the raw data into the generated email based on the selected log data type, Log4j Zero-Day Vulnerability containing SSL. Other than that, it also shows that the Intelligent-based SIEM security email alert system successfully sends out the generated email to the email platform type, Yahoo Mail, without any function error or missing data.

3) Testing case 3

Browser type: Microsoft Edge

Log data type: SERVER-OTHER Remote Desktop Protocol brute force attempt

Receiver email platform: Microsoft Outlook



1171103091_ChiChyunHorng_ST
SERVER-OTHER Remote Desk... 9:21 PM
Ticket status:SERVER-OTHER Remote D...

SERVER-OTHER Remote Desktop Protocol brute force attempt

1171103091_ChiChyunHorng_ST <pr0jectpurpos3@gmail.com>
To: You
Mon 1/2/2023 9:21 PM

TM ONE SECURITY OPERATION CENTRE
ALERT STATUS NOTIFICATION

Ticket status:SERVER-OTHER Remote Desktop Protocol brute force attempt
Alert category:testing case 3
Event Name:IDP Signatures
Action by SOC:testing case 3
Action by Customer:testing case 3

Dear Team,

We would like to inform you that our SOC has detected "IDP Signatures" alerts in testing case 3 network. We gathered here some info for your reference.

No	Time	Log Source	Source IP	Source Port	Destination IP (Hostname)	Destination Port	Event Count
1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1

It looks like you're using an ad blocker. To maximize the space in your inbox, sign up for Ad-Free Outlook.

Fig. 4. Sample experimental result of the system tested on testing case 3

Based on the third result above, the web browser type, Microsoft Edge, enables the proposed system to perform well on the log data extraction function that involves extracting and converting raw data into a filtered generated email based on the selected log data type, SERVER-OTHER Remote Desktop Protocol brute force attempt. Moreover, the Intelligent-based SIEM security email alert system has also shown us that the generated email sent out to the email platform type, Microsoft Outlook, is successful because the email platform site can receive all the necessary information and extracted log data together in one generated email.

V. CONCLUSION

Through tons of effort and studies on the flaws of most common SIEM, especially issues related to limiting and lacking email functionality. A proper solution and a series of evidence regarding the Intelligent-based SIEM security email alert system's tested results have been recorded and showcased under the few crucial sections in this paper. In addition, a completed system prototype of this paper has been tested and experimented with by one of Malaysia's largest government-linked telecommunications companies, TM One.

With all the extensive and problem-solving features implemented inside the Intelligent-based SIEM security system, it is reasonable to say that not only the proposed idea would able to enhance the existing SIEM software to another level, but it could also bring huge benefits to the SOC team members or professional cybersecurity users in producing a better result whether it is for their own daily work operation or personal usage, along the help of the system.

As an intelligent-based SIEM security email alert system, operating through web pages will allow the system to pair well with any SIEM tools since most SIEM is also operated on a web browser. Besides that, the feature's ability to save all the previously filled-in information on a local device can significantly reduce the user's operating time and human error by loading again these setting files when required to fill in the same information. Finally, the custom company's email format can benefit a SOC team in dealing with emergency time rather than manually performing copy-pasting, which is more time-consuming and tedious.

Unfortunately, the current Intelligent-based SIEM security email alert system can only perform all these features. The system is only available on a web browser platform instead of independent software, not to mention the system can only accept log data files with `xslx` or `xls` file format such as an excel file format for the data extraction process. However, the Intelligent-based SIEM security email alert system does achieve the main objectives of this paper: solve the lack of email customization problems encountered by most SOC team and SIEM software users, provides flexibility in customizing the contents of the email, and last but not least, having an intelligent system feature that enables the automated conversion from a raw log data generated by SIEM software into a piece of well-filtered information that able to fit well into the predefined email template based on the email format provided by the user. Thus, for all that reasons, I believe the Intelligent-based SIEM security email alert system still has many possibilities for further improvement.

REFERENCES

[1] M.K. Pratt, "What is SIEM software? How it works and how to choose the right tool | CSO Online," Nov. 28, 2017. https://www.csoonline.com/article/2124604/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html (accessed Feb. 11, 2022).

[2] K. Gast, "What is SIEM? And how does it work? - LogRhythm," Mar. 12, 2021. https://logrhythm.com/what-is-siem/ (accessed Feb. 11, 2022).

[3] L. Rosencrance, "What is SIEM and why is it important?," 2020. https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM (accessed Feb. 11, 2022).

[4] O. Podzins and A. Romanovs, "Why SIEM is irreplaceable in a secure IT environment?," *2019 Open Conference of Electrical, Electronic and Information Sciences, eStream 2019 - Proceedings*, Apr. 2019, doi: 10.1109/ESTREAM.2019.8732173.

[5] B. Alsabbagh and S. Kowalski, "A framework and prototype for a socio-technical security information and event management system (ST-SIEM)," *Proceedings - 2016 European Intelligence and Security Informatics Conference, EISIC 2016*, pp. 192–195, Mar. 2017, doi: 10.1109/EISIC.2016.049.

[6] Coresecurity, "What is SIEM? Meaning, function, and benefits | Core Security." https://www.coresecurity.com/siem (accessed Feb. 11, 2022).

[7] S.S. Sekharan and K. Kandasamy, "Profiling SIEM tools and correlation engines for security analytics," *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017*, vol. 2018-January, pp. 717–721, Feb. 2018, doi: 10.1109/WISPNET.2017.8299855.

[8] C. Smith, "SolarWinds security event manager reviews 2022: details, pricing, & features | G2." https://www.g2.com/products/solarwinds-security-event-manager/reviews (accessed Feb. 13, 2022).

[9] Riversafe, "Maximising the value of Exabeam Fusion SIEM with RiverSafe - RiverSafe," 2021. https://riversafe.co.uk/news/maximising-the-value-of-exabeam-fusion-siem-with-riversafe/ (accessed Mar. 05, 2022).

[10] S. Ingalls, "Rapid7 InsightIDR review: features & benefits | eSecurity Planet," 2021. https://www.esecurityplanet.com/products/rapid7-insightidr-review/ (accessed Mar. 06, 2022).