2019 International Conference on Advancements in Computing (ICAC)
December 5-6, 2019. Malabe, Sri Lanka

INTELLIGENT SOC CHATBOT FOR SECURITY OPERATION CENTER

Vihanga Heshan Perera, Amila Nuwan Senarathne, Lakmal Rupasinghe
Faculty of Graduate Studies and Research, Sri Lanka Institute of Information Technology
Malabe, Sri Lanka
ms18902112@my.sliit.lk, amila.n@sliit.lk, lakmal.r@sliit.lk

Abstract— **Information security analysts currently face many challenges: both hidden and visible in the face of unique attack records. The rapid increase patterns of security monitoring and investigation tools (as an average of 20 security solutions have been used per company) leads to frequent changing between screens, alert fatigue, disjointed record keeping, and increased investigation time. This chatbot can suggest the flow of investigation and the relevant commands that will help to obtain the results which need to be resolved the incident. Automate the incident ticket creation is one of major achievement of this research. Security analysts also receive messages of security alerts of the AWS hosted instances. Security analysts are also continuing to work on their sub tasks, quite overloaded with their main tasks to engage in collaborative investigations and knowledge sharing. Chat-Ops help to vanquish and meet those challenges. Processes, automated workflows, the chatbot, security tools, and humans exist in the same chat window feeding data and commands in a worthy cycle. It will lead to huge changes in everything from remediation times and investigation depth to future learning and knowledge administration. Different analysts will drive the investigation in different ways. Most of the time, analysts will miss most important parts and techniques, but those parts could be very valuable for the result. The investigation flow and commands will suggest based on past investigations and commands that previous analysts were used. This chatbot will help in many ways of current analyst who work in a security operation center.**

Keywords— ***ChatOps, SIEM, SOC, IPS, IDS, Cryptography***

I. INTRODUCTION

A chatbot also referred as chatterbot, is a program that simulates the "chatter" or conversation of a human being using voice or text interactions. Visual assistants with chatbots are gradually being used to get simple searching and look-up tasks done in both B2B (Business-to-Business) and B2C (Business-to-Consumer) environments. Chatbots assist with not only reducing overall cost by creating better use of employee's time and it permits organizations to provide a higher level of customer (stakeholders) services. These chatbots have various levels of complications and will be functioning as state-full or state-less. A state-less chatbot will approach every conversation as it is interacting with a new user. A stateful chatbot will be able to analyze previous interactions and create response in context [1]. Chatbots are important in many different ways. Efficient task completion and time saving are the most valuable features. Addition to that, AI (Artificial Intelligence) chatbots are answering and conversing re-occurrence user questions to enhance their services and provide the user with better experience. It can be enabled information security roles to answer quicker, work more collaboratively, and deliver/ share new knowledge in more effective way. And yet, it is where companies are struggling the most.

The chat below (even though grammatically corrected and sanitized), is proverbial in PC game known as "Counter Strike: Global Offensive" private chat, as groups of game players playing for pleasure [2].

Player1: "Site 1, they're going to take Site 1! Plz split up and spread out. They just got me."

GamingChatBot: "I'm going for it. How many have still left?"

Player1: "Two. Use cross-hair 5 and turn bullet tracers on."

GamingChatBot: "Got it. And catch them all!"

+$600: Award for neutralizing an enemy with the MAC-10.
+$600: Award for neutralizing an enemy with the MAC-10.
+$3250: Team award for eliminating the enemy team.
DEAD da si znaqt ;] : uzi 1 round ?
DEAD da si znaqt ;] : uzi 1 round ?
DEAD b0k0™ : ?!
da si znaqt ;] : uzi 1 roundd?
InMarius : watch replay
b0k0™ : cmon dude
Saul Goodman : its legit ;]
InMarius : you will learn some csgo
Thunder*!*EX @ Outside Long [RADIO]: Flashbang Out!
da si znaqt ;] : stfu

Fig. 1. All players know what is ongoing on the war field through chatbot on the left bottom [2]

Following objectives are achieved by this research:

- Analyze incidents precisely.
- Minimize and contain damage.
- Automate incident ticket creation.

This research paper is organized in following manner:
First section discusses about the introduction and provides the brief idea for the readers, what is a Chatbot? Section II deals with previous researches in chatbots and related security tools which can integrate with the chatbot. Section III discusses current issues of Security Operation Centers. Section IV discusses workflow of the SOC chatbot and define priority of the incident. Section V, and VI, include functionality of the SOC chatbot with obtained results and the conclusion. Section VII contains future work and VIII includes references.

II. RELATED WORK

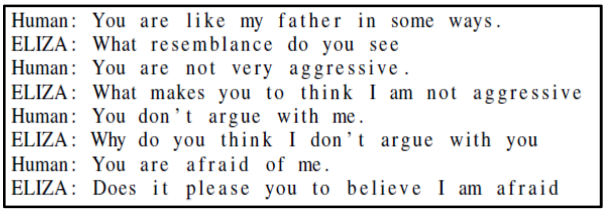
A Chat-bot also known as IM Bot, interactive agent, artificial conversational object which uses AI or a computer program which is conducting a conversation through textual or

978-1-7281-4170-1/19/$31.00 ©2019 IEEE

auditory methods. The word “Chatter Bot” was used by Michael Mauldin who developed the ‘Verbot’ in 1994 [3]. Nowadays, most chat bots are accessed through virtual assistants such Amazon Alexa and Google Assistant for messaging applications like ‘WeChat’ or ‘Facebook Messenger’. Apart from above stated chat bots, “Conversational Artificial Intelligence” is referring to the requirements of based assistant, and communication automation for messaging apps.

A. Turing Bot

Alan Turing proposed in 1950, a criterion of the ability of a computer application impersonating human being in a real time conversation in written [4]. There were many historical chatbots developed in between 1960 to 1975. Especially, the chatbot developed in 1966 which was “ELIZA” and in 1972 “PARRY”. These programs were simulated in typed conversations. PARRY and ELIZA applications were used to exclusively simulated in typed discussions. Different chatbots are currently included with practical features like web searching and gaming capabilities [5].



Human: You are like my father in some ways.
ELIZA: What resemblance do you see
Human: You are not very aggressive.
ELIZA: What makes you to think I am not aggressive
Human: You don't argue with me.
ELIZA: Why do you think I don't argue with you
Human: You are afraid of me.
ELIZA: Does it please you to believe I am afraid

Fig. 2. A specimen conversation with application ELIZA

The above chatbot did not understand what it was saying. It responded back to the user as coded by guidelines. For these situations, there were controls which were connecting to mother of chats and families. Then it needed to generate a solution which would wish the user to deliver from another question with expecting a keyword**.** One applicable field of artificial intelligence research is NLP (Natural Language Processing). For an example, A.L.I.C.E bot used a specialized markup language named AIML which was precise as a conversational agent [6]. Most of the organizations in the world, run chatbots on simply via SMS (Short Message Service) or messaging apps. Facebook messenger application permitted other developers to create chatbot on their local platforms in 2016. In first six months, there were 40,000 bots created using Facebook Messenger and raised it up to 200,000 by October 2017 [7].

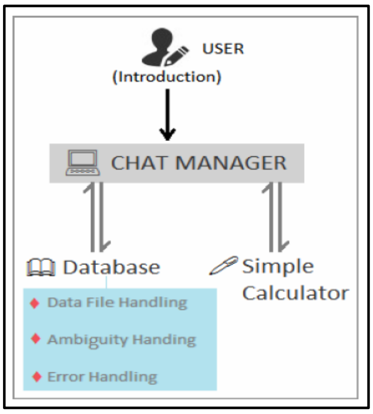


Fig. 3. Various modules for interactions

Chatbot is one of the most popular and elementary sample of HCI (Human Computer Interaction). In artificial intelligence, it always comes with an intelligent system. The system can be divided into many levels based on the intelligence; it would be partially intelligent system or completely intelligent system [8]. Any program, system or machine exhibits several factors but not all are listed fundamentals of intelligence in partially intelligent system. Some chatbots use for reasoning & logic, name comparison, and memory & heuristics learning. Chatbots do not use for whole end-to-end processes. Most of the time it uses for above stated purposes. Therefore, it is concluded that these chatbot systems are partially intelligent systems. These bots are becoming more popular and productive when applications such as dictionaries, calculators or even a small game are embedded in it.

B. FUTURE Bot

According to the FUTURE bot research group [9], if the chatbot user requests calculator application for their requirement, chatbot itself has a small calculator program with the basic mathematical arithmetic operations. Other than that, user can create notes, memos and open applications on user’s mobile phone or computer on demand. It does contain ambiguity handling part, when the user asks a question which does not contain any clue in the database, there is a special function for handling such ambiguities and it fits for wide range of unexpected questions. And, it supports data handlings and error handling parts. FUTURE chatbot team inferred that using artificial intelligence markup language with dedicated applications in artificial intelligence field were boosted in many times of speed of implementing the project. As stated above, the first chatbot suggested by Turing, had large number of problems. Turing test was not a better measure to obtain if a chatbot/ machine is wise enough to complete the given task. But there was no fool-proof procedure to test if the entity was intelligent enough or not. But even in the real-world people experienced unintelligent behavior in intelligent beings. In the same time, unintelligence machines/ applications might be performed several tasks more accurately and intelligently than wise human being. In Turing test, it had its own challenges as listed below [8]:

1. Short purview
2. Unproductive developments
3. Limitedness
4. Disillusionment of Goals

C. SIEM and other security tools in SOC

SIEM combines Security Event Management [10] (SEM) and Security Information Management [10] (SIM). The primary focus is reporting, analyzing of long-term storage and log data while the next focuses on notifications and real-time monitoring. Security Incidents & Event Management joins with these parts and includes real time analysis and correlation. Security Incidents & Event Management is also emphasizing the effect of the technology on the entire system, even though the main focus is on information security. Many researchers would rather express of ‘SIEOM’, [10] addition of the ‘O’ is for “opportunity”. Since the alerts and reports of a Security Incidents & Event Management environment provides opportunities to improve on the information security of the system. While the market for SIEMs have been growing for some time, a structured methodology is still making a little headway [11]. The SIEM systems are accountable for examining security related information occurrence in real-time for external and internal threats/ risks management, collect, store, analyze, and report on logged information for forensics, regulatory compliance, and incident response. This analyzes day-to-day security incidents which are reported through switches, firewalls, Intrusion Detection System (IDS), routers, and Intrusion Prevention system (IPS) etc. Through the solution provided, it is possible to decrease the cost of security operation process in majority of the organizations as well as help to rise the effectiveness of analysis. Also, the suggested system can eliminate false-positives or the reporting of incorrect weaknesses (vulnerabilities) by learning about the security operation center infrastructure and organization environment. Leading companies are trying to do more than enough tasks to improve on their current state. Companies are looking for enlarge their efforts, take braver steps to battle against cyber threats, rather than waiting for the threats & attacks to come to their premises. These companies are ranking on efforts that improve visibility of the attacks and allow a proactive response through analytics, prompt detection, and monitoring. Companies might not be able to take full control when information security incidents occur, but they could control how they respond to those. Increasing of detection abilities is the key place to initiate for proper response against cyber threats.

III. Methodology

A. *Current issues of soc*

Present SOCs have large number of incident handlings approaches. But the general gripe from security engineers/ analysts is the time it will take effectively answer and close incidents. This low speed stems are due to different reasons: the different types of alerts marsh analysts into submission, interchange between numerous security products and leaves them in a confusion & working in silos deprives them of each other's expertise. When incidents are adding up, it feels like participating a marathon with heavy boots. There are few reasons for slowness of the investigation process.

Conversations and discussions take all over the place: When a security analyst get stuck during prioritized incident response procedure and require more help, the analysts generally ask assistance through online (web) or from colleagues. These discussions will get stored on mail threads, ticketing chains, on the internet, slack channels or simply lost due to SLA (Service Level Agreement) time exceeded. Further, valuable time will be wasted while collecting all resources for compliance and audit logs. While analyzing and investigating, security analysts frequently require getting use of multiple security tools at their disposal. This might be useful for collecting data, executing actions, running queries or mixture of all three tasks. To deal with all these security tools, security analysts need to have many tabs opened on their web browsers and monitored multiple screens, changing to different product console screens to accomplish that product's action. This makes unfortunate dwell time, during lengthy investigations which required to use of 20-25 security products. It will be a reason for the increased of possible human errors as security analysts are anticipated to perform copy & paste the outcomes onto main console, monotonous tasks and keeping a track of the outcome of which information came from each security product. These downsides exasperate and rise analyst anxiety, alert fatigue and unnecessarily extend investigations to put service level agreement at risk. There are few incident handling goals available in SOC [12].

- Capture incidents fast.
- Analyze incidents precisely.
- Minimize and contain damage.
- Reinstate affected systems.
- Identify root causes.
- Implement developments to prevent reoccurrence of same incidents.
- Reporting and Documenting.

B. *Work flow of SOC ChatBot*

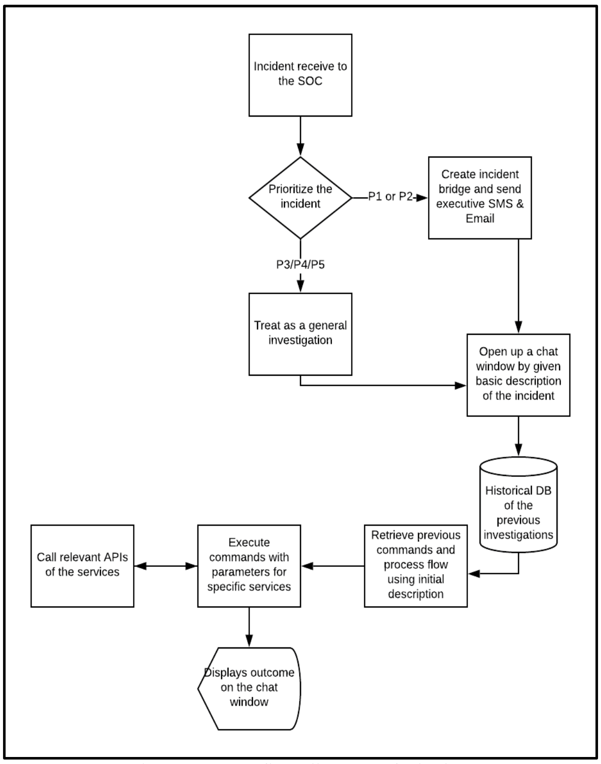

Incident receive to the SOC
Prioritize the incident
P1 or P2
Create incident bridge and send executive SMS & Email
P3/P4/P5
Treat as a general investigation
Open up a chat window by given basic description of the incident
Historical DB of the previous investigations
Retrieve previous commands and process flow using initial description
Execute commands with parameters for specific services
Call relevant APIs of the services
Displays outcome on the chat window

Fig. 4. Process flow diagram of Chatbot

As shown in Figure 4, the process flow is defined. The process starts, when an incident is received to the SOC. Incident will be received through an email, a ticket, a phone call, a self-observed or walk-in (person comes to the SOC area and log the incident). Every incident will be created a ticket. After the incident logged, it will be uniquely identified by that ticket number (E.g.: INCXXXXX). Once the incident ticket is created, then it needs to determine the priority level of the incident. According to ITIL (Information Technology Infrastructure Library) framework, it is defined five levels of priorities. Namely (P1, P2, P3, P4 and P5). P1 and P2 incidents are classified as high priority incidents.

It should engage a bridge call with an IM (Incident Manager). P3 also can be considered as a high priority incident, but it will depend on the situation. High priority incidents are classified based on below conditions [13].

- The system/ business service damage is caused by the incident which surge quickly.
- Work/jobs that cannot be fulfilled by employees and stakeholders are highly time sensitive.
- Few users who are with C-level or VIP are affected.
- A minor incident will be able to mitigate from becoming a major incident by responding quickly.

If it is a P1 or P2 incident, then it needs to be treated as a high priority incident. Then initial executive SMS and email need to be sent. Otherwise treat as a general incident and start the investigation. Every incident that needs further investigation, should start a new chat window on the Chatbot. This specific chat window requires incident number, description and investigation leader. That is how incident keep track of the commands that execute by other security analysts. When opens a new Chatbot channel, it will predict the relevant/ supportive command and investigation flow based previous similar investigation with machine learning techniques. Either using suggested commands or using different commands available in the Chatbot database, analysts can proceed with the investigation. Every command execution will be recorded by Chatbot and store in the database. Since supported tools are integrated within the Chatbot, it will be used API calls to communicate with the relevant tools.

C. Basic algorithm is stated in the below

Step 1: Issue the command with the parameter: vtip ["parameter"]. (E.g: vtip 39.25.45.68)
Step 2: Invoke related alias in the Stackstorm platform. (E.g: vtip.py and vtip.yaml files)
Step 3: Gets the parameter and connects to the security tool using API call.
Step 4: Returns the results to the Stackstorm platform.
Step 5: Re-format the output according to the requirement.
Step 6: Displays the output.
Step 7: If the SIEM triggered an alert, it will create a ticket in ticketing system.
Step 8: If there is high CPU utilization detected in the AWS account, Slack chatbot will be informed, dropped email to the SOC email address, and sent an SMS to SOC members.

IV. CONVERSATION-DRIVEN CHAT WINDOW

Since there are 20-25 security tools used in a SOC, will lead to more complex processes. Collaborating with all the available tools and at the same time, respond to the incidents as well as follow the run books make life harder. When the SOC manager asks to execute some tasks on a security product or outcomes of an investigation, manager might require evidences and a report of what actions have taken for the investigations. Because it was a black box process for the SOC manager. The Chatbot will solve the main problem of lack-box approach. Responding to the incidents might be different from analyst to analyst. Different approaches are taken by different analysts. That leads to fail provide important facts of the investigation as well as the effort of the security analyst. When reviewing KPIs (Key Point Indicators) of the analyst, there will be high possibility that the effort of the analyst will not consider. A single window will eliminate the requirement to interchange between screens. This chat-based program window inspires security analysts to share/ deliver knowledge and work as a group in combined investigations. It directly leads to a decrease in alert volume in the queue of SOC. Even one second of the system down-time after large cyber-attack might lead financial crisis to the company.

If the security operation center has a Chatbot tool enabled, security analyst can have conversations/ discussions with other team members/ SOC lead/ SOC manager or other collaborative staffs on that window to remove the requirement of several association sources. Chatbot application can integrate with several other messaging/ chatting platforms such as Slack or HipChat. It will mirror discussions across different screens and avoid boring copy & paste tasks. If there are any kind of tickets, freestyle notes or even straggling comments (left as emails) will be able to upload to the Chatbot as a central repository of security analysts' comments and suggestions. Other benefit of the Chatbot is executing security commands among various products. It does not have to login through remote connections, use different product screens and transporting outcomes or results send back to central platform. ChatOps permits security analysts to execute commands in real-time from one chat window through CLI (Command Line Interface). This tool has "Go-To" option to named products then run the given commands and provide the results back to the main investigation window which will be able to observe by all analysts. This will lead to surge of investigation accuracy and reduce human errors. There will be few value additions to the SOC through conversation-driven Chatbot [14].

- Better-quality evidence to customers/users on aspects of service excellence.
- Better-quality evidence on the consistency of the equipment.
- Certainty that incidents logged will be addressed and not forgotten.
- Decrease of the influence of incidents on the business/organization.
- Better-quality monitoring and capability to interpret the reports, which will help to identify incidents before they have an impact.
- Policy upgrading to limit reoccurrence.

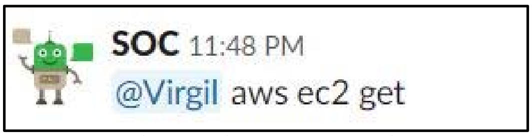
V. SOC CHATBOTS RESULTS

A. IP health checking from the Chatbot

Basically, 3 types of services are added to the SOC Chatops. VirusTotal, AWS and Google service. SOC analyst can type below command to get health status of given IP address. As an example, SOC analyst can issue the command "@Virgil soc vtip 8.8.8.8". Virgil is the Chatbot name. "soc vtip" is the command name to get health report of given IP address using VirusTotal.com. Figure 6 shows the output results of the requested report. This process has taken only 7 seconds to complete and provided details that are relevant for current investigation. SOC member does not need to go for a different site to observe this output (P.S: This output is the raw output and did not format in anyway). Most importantly, all SOC members will aware with the output that one SOC member obtained (No more black-box type investigation). It includes network, autonomous number, signature algorithm, public key etc. Those details will help for the security analyst use in the ongoing investigations. Whois look-up also include in the outcome result which will assist for the investigation.

B. Request EC2 instance details from Chatbot

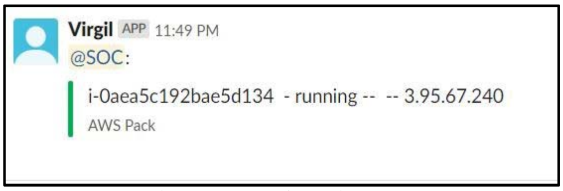
Further, when SOC Chatbot is connected to the AWS account in the company, analyst will be able to manage the AWS resources and obtain health records of instances.



SOC 11:48 PM

@Virgil aws ec2 get

Fig. 5. Issuing AWS commands



Virgil APP 11:49 PM

@SOC:

i-0aea5c192bae5d134 - running -- -- 3.95.67.240

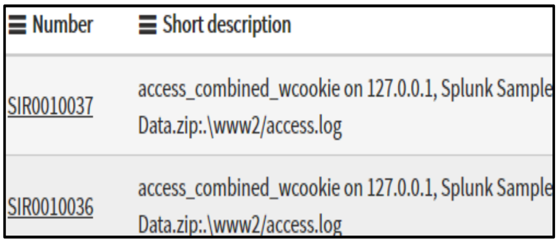
AWS Pack

Fig. 6. Report of EC2 instances

As shown in the Figure5 & Figure 6, SOC analyst can be able to observe EC2 (Elastic Cloud Compute) details as well. It shows command issue time and result output time as well. It is observed within 10-20 seconds. Therefore, SOC members do not want to manually log into the organization's AWS account and observe EC2 instance details. With this approach, higher efficient level can be expected. It has been taken only 30 seconds to complete this command. Stack-storm [15] platform will perform all the intermediate execution and act as a connection between Slack [16] and the third party or internal security tools.

C. Automated the creating ticket in Service-Now

SIEM is scanning for different alerts in real-time. Malware alert is the only configured alert in this research. When there is specified parameter met in the log, the alert will be triggered. Generally, SOC analyst will be informed through an email by SIEM. Then SOC analyst prioritize this task, because it can be a severe incident.

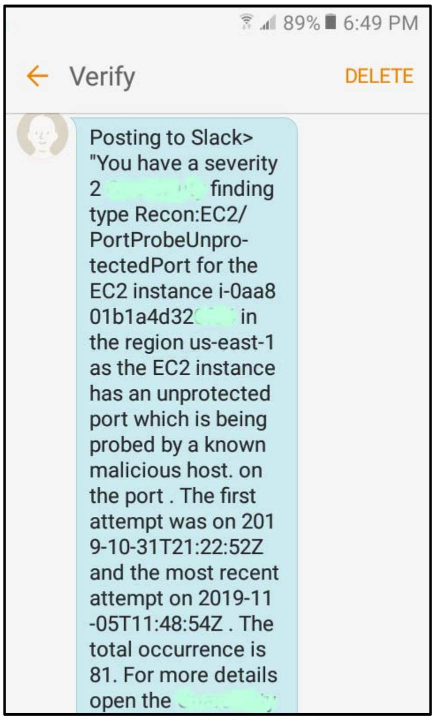


☰ Number	☰ Short description
SIR0010037	access_combined_wcookie on 127.0.0.1, Splunk Sample Data.zip:.\www2/access.log
SIR0010036	access_combined_wcookie on 127.0.0.1, Splunk Sample Data.zip:.\www2/access.log

Fig. 7. Ticket is created in Service-Now system

When the specified alert is triggered, ticket with relevant details will be created in the ticketing system which is Service-Now (Figure 7). The process is now automated. SOC members do not have to manually create the ticket (It takes 2-3 minutes to manually create the Service-Now ticket). SIEM plugins and the Service-Now API used to develop this functionality.

D. Reporting AWS security alerts to mobile



89% 6:49 PM

Verify DELETE

Posting to Slack> "You have a severity 2 [redacted] finding type Recon:EC2/PortProbeUnprotectedPort for the EC2 instance i-0aa801b1a4d32[redacted] in the region us-east-1 as the EC2 instance has an unprotected port which is being probed by a known malicious host. on the port . The first attempt was on 2019-10-31T21:22:52Z and the most recent attempt on 2019-11-05T11:48:54Z . The total occurrence is 81. For more details open the [redacted]

Fig. 8. SMS detail of the security alert

There are several pre-defined attack types mentioned in the AWS Guard duty service. If those alerts are triggered, SOC members and C-level people will receive an SMS alert, email alert, and chatbot post in the Slack application. It acts as a better monitoring system for EC2 instances. The message mentioned attack type, severity level, instance name, AWS region, date & time, and number of occurrences. This is free tool for monitor AWS instances. SOC member already received important details of the attack. It increases the efficient of the SOC.

VI. CONCLUSION

In present time, number of cyber-attacks are getting bigger. The knowledge and tools to detect and analyze those attacks need much effort. Organizations will be well equipped with security tools with knowledgeable security engineers/ analysts. But still due to a slight security hole, large damage can happen to the organization. In order to clusters information security incidents, organizations set up a SOC (Security Operation Center). SOC contains highly skill people with advance security tools. With large number of employees, products, and different geo-graphical area will increase the complexity of the attack and the investigation. In the same time, chatbots are again coming to the field as a very interesting topic. Especially in customer care and getting user details for an occasion, chatbot will play important task in these days. Since it is user friendly, the bot, and the security tools get to gather. It will be making perfect team. Bot is acting like another person (virtual) in the SOC. Analysts can ask questions, command certain tasks and share knowledge with other members of the SOC. These chatbots are now becoming next generation intelligence virtual humans with help of AI (Artificial Intelligent). SOC chatbot will help SOC analysts to effectively do their work with least authorization level. It does not have to switch within multiple systems to proceed for security investigations.

VII. Future work

There are unlimited ideas hidden inside this SOC chatbot. Few areas can be developed in the chatbot to detect the incident, intelligently analyze the evidence with suitable security tools and resolve itself or escalate to the relevant authority. But this will reduce human interaction and this human effort and valuable time can provide to the research areas. Similarly, this chatbot only works with SOC members only. But if it needs to enhance the people involvement with different departments in the organization, there will be a confidentiality issue. Because investigations may contain sensitive information. According the department and the job position it needs to hide several information. That will be led to another research area. If the current integrated security tools are not enough for the investigation, chatbot should be smart enough to get help of trustworthy security tools on the Internet. How it finds those security tools and properly authenticate with third party tools? It makes another research area. Every area in this ChatOps will make advanced and effective tools for the security professionals.

VIII. Acknowledgment

Vihanga Perera likes to express honest appreciation towards Mr. Amila Senarathne and Dr. Lakmal Rupasinghe, faculty of graduated studies and research, Sri Lanka Institute of Information Technology, who guided me throughout this research.

IX. References

[1] R. Margaret, "Chatbot," Searchcrm, January 2019. [Online]. Available: https://searchcrm.techtarget.com/definition/chatbot. [Accessed August 2019].

[2] Demisto Inc., "ChatOps: The Perfect Tool To Help Security Analysts Counter-Strike," Demisto, 18 November 2017. [Online]. Available: https://blog.demisto.com/chatops-the-perfect-tool-to-help-security-analysts-counter-strike. [Accessed 13 August 2019].

[3] D. Orf, "Google Assistant Is a Mega AI Bot That Wants To Be Absoutely Everywhere," Gizmodo, 18 May 2016. [Online]. Available: https://gizmodo.com/google-assistant-is-a-mega-chatbot-that-wants-to-be-abs-1777351140. [Accessed 12 March 2019].

[4] R. Margaret , "Turing test," Searchenterpriseai, December 2017. [Online]. Available: https://searchenterpriseai.techtarget.com/definition/Turing-test. [Accessed 12 March 2019].

[5] S. Franchi and G. Güzeldere, "Constructions of the Mind," *Dialogues with colorful personalities of early AI,* vol. 4, no. 2, 1995.

[6] V. Cerf, "PARRY Encounters the DOCTOR," *Network Working Group,* vol. 439, no. 13771, 1973.

[7] K. Johnson, "Facebook Messenger hits 200,000 bots," Venture Beat, 18 April 2017. [Online]. Available: https://venturebeat.com/2017/04/18/facebook-messenger-hits-100000-bots/. [Accessed 13 March 2019].

[8] A. Khanna, B. Pandey, P. Bhale and K. Kalia, "A Study of Today's A.I. through Chatbots and Rediscovery of Machine Intelligence," *Research Gate,* no. 10, p. 9, 2015.

[9] A. Khanna, B. Pandey, K. Vashishta, K. Kalia and T. Das, "A Study of Today's A.I. through Chatbots and Rediscovery of Machine Intelligence," *International Journal of u- and e-Service, Science and Technology,* vol. 8, no. 7, pp. 277-284, July 2016.

[10] M. Nicolett , "How to Implement SIEM Technology," *Gartner,* vol. 2, p. November, 2009.

[11] G. Sadowski, T. Bussa and K. Kavanagh, "Magic Quadrant for Security Information and Event Management," *Gartner,* vol. 4, p. December, 2018.

[12] M. Bromiley, "SANS Institute: Reading Room - Incident Handling," SANS, 20 March 2019. [Online]. Available: https://www.sans.org/reading-room/whitepapers/incident/. [Accessed 28 March 2019].

[13] D. Topalovic, "All about Incident Classification," Advisera, February 2018. [Online]. Available: https://advisera.com/20000academy/knowledgebase/incident-classification/. [Accessed March 2019].

[14] P. Bharathi and D. Berg, "Managing information systems for service quality: a study from the other side," *Emerald Insight,* vol. 16, no. 2, p. 9, 2014.

[15] Spinx Theme, "StackStorm Overview," Stack Storm, November 2018. [Online]. Available: https://docs.stackstorm.com/overview.html. [Accessed 29 August 2019].

[16] Slack Community, "The collaboration software that moves work forward," Slack, 2015. [Online]. Available: https://slack.com/intl/en-lk/features. [Accessed 18 September 2019].