Design and Implementation of a Chatbot for the Supervision of Security Events (SIEM)

Deussom Djomadji Eric Michel
College of Technology
University of Buea
Department of Electrical and Electronic Engineering

Tonye Emmanuel
National Advanced School of Engineering University of Yaoundé I.
Department of Electrical and Telecommunications

Bama Si Franck Arnold Franck
National Advanced School of Engineering
University of Yaoundé I.
Department of Electrical and Telecommunications

Binele Abana Alphonse
National Advanced School of Engineering University of Yaoundé I.
Department of Electrical and Telecommunications

ABSTRACT
Companies around the world are the first targets of cybercriminals, because the end product of their attacks is much more lucrative than that of targeted attacks against individuals. As a result, businesses have much greater and more stringent cyber security needs. Moreover, losses in cases of compromise can be evaluated in terms of tens of millions of CFA francs, which makes it a prime target for cybercriminals. Generally, in companies, all the intervention capacities are put into play through an Information System Security team in order to meet the maximum-security needs of its information system. This team is often responsible for the SOC (Security Operation Centre), i.e., the supervision of the security of the information system of a structure through tools of collection, correlation of events and remote intervention. The main mission of the SOC is to identify, analyse and ameliorate cyber security incidents. To assist this team in the continuous management of security and to improve the response time to various security incidents, we designed and implemented a conversational agent for security event monitoring using the ELK Stack SIEM tool. As a result, we obtained a conversational agent that is able to identify and analyse security incidents and events of the company's information system, centralize and have a global view of the security status of all monitored devices, create personalized and adequate rules that can detect flaws in the system, provide reports on security incidents and events through voice exchanges. This will allow the SOC to fulfil the first two terms of its main mission, i.e. the identification and analysis of incidents in order to be able to react more quickly and efficiently to them, thus fulfilling the third and last term of its main mission, remediation.

General Terms
Supervision of security events

Keywords
Cybersecurity, information systems security, security event monitoring, conversational agent, SIEM.

1. INTRODUCTION
The multiplication and proliferation of new information and communication technologies and the Internet has led to a marked improvement in all aspects of human life. There are currently very few areas that do not benefit from this boom in new technologies. Medicine, agriculture, education, transportation and many other fields have experienced glaring advances since the arrival and popularization of new information and communication technologies for the greatest pleasure of man [1]. However, what we tend to neglect is that with all these advantages, there are also risks and threats to which the users of these technologies are exposed to. These risks and threats are as great as the benefits we get from them in our daily lives.

Individually, we are all subject to potential attacks, but companies are all the more targeted by attackers because of the huge capital managed by most of them [2]. Losses in the millions are at stake if an attack succeeds. In 2021, more than 6.9 billion dollars of losses due to cybercrime in the United States according to the FBI ICR (Federal Bureau of Investigation Internet Crime Report [3].

Cameroon is also affected by these risks, because according to data published by ANTIC, 27,052 vulnerabilities have been identified in the computer security systems of public and private structures, i.e., ministries, telecommunication operators, banks and public administrative institutions. Cybercrime caused financial losses of 12.2 billion CFA francs to the Cameroonian economy in 2021. That is, double the losses reported for the 2019 fiscal year [4].

To counter this exponential proliferation of cybercrime, companies are adopting multiple security measures, from the installation of security equipment to the implementation of procedures, including increased monitoring of their information systems.

An optimal supervision of the security events is necessary within any company, not only to supervise and avoid to the maximum any compromise of the information system, but also to know how to react to minimize the losses in the worst case, because there is no zero risk in cyber security [5].

This article proposes the implementation of a conversational agent for the supervision of security events within a company. This would help the company's cybersecurity teams to have instant access to crucial information about cybersecurity incidents to ensure maximum security of its information system.

This article presents the principles of security event monitoring using SIEM tools, describes the process used to carry out this

work within an enterprise, presents the results obtained, the analysis of these results, our various comments and the main recommendations made to solve each problem encountered.

1.1 Problem statement

The information system of a company is the basis of the services offered by this company; it handles important and sensitive information that is essential to the survival of the company. Hackers multiply every day, the strategies to attack these information systems with the aim of compromising their security; hence the importance of meeting all the security needs of its information system. This mission of utmost importance has been entrusted to an Information System Security team that is carrying out several actions to this end.

The deployment of a Security Operations Centre (SOC) is an important solution to the rapid detection of security events in a network. The SOC is a team dedicated to monitoring the security of the information system and its main mission is to identify, analyse and remediate cyber security incidents.

When monitoring a company's network, it is necessary to collect logs to understand and identify events on the network and to do this the SOC uses its main tool which is the SIEM (Security Information Event Management). The limits of this system are that the optimal use and handling of these tools requires months of training, practice and experience usually not held by the engineers in charge of the security of the information system.

As a result, some companies outsource the supervision of their security or call on consultants, which represents very high costs in the tens of millions of CFA francs. However, with a digitization of the SOC system, we could facilitate the work of the engineers in charge of the security of the information system of any structure with an information system in general.

Even more, now that the Covid-19 pandemic has hit the world and companies are forced to limit human relationships as much as possible, it would be interesting and important for a company to be able to have this SIEM expertise without having to call upon a physical person to ensure the analysis of security events on a continuous basis.

From the above, we are therefore entitled to ask the following research questions that will guide our study:

- What solution can we build to dematerialize or digitize a SOC?
- How can we simplify the analysis of IS security events while facilitating the reporting of information to the SOC?
- How can we reduce the costs of outsourcing security?
- What additional functionalities can we give to this solution?

1.2 Objectives

The different objectives to be reached in the realization of this work are:
- Identify and analyze the security incidents and events of the information system.
- Centralize and have a global view of the security status of all the monitored equipment.
- Create personalized and adequate rules that can detect and block vulnerabilities in the system.
- Provide reports on security incidents and events through voice exchanges.
- Establish a report of the automatic conversation.

The rest of the paper is organized as follow, in section 2 we have the context which is related to the supervision of security events, section 3 present the method followed by the results in section 4 and finally we have a conclusion.

2. SUPERVISION OF SECURITY EVENTS

2.1. The SOC (Security Operation Center)

The SOC or Security Operation Center is a team dedicated to the supervision of the security of an organization's information system through the use of tools for collecting, correlating and remotely intervening in events. Its main mission is to identify, analyze and remediate cybersecurity incidents. Figure 1 shows the components of a modern SOC.

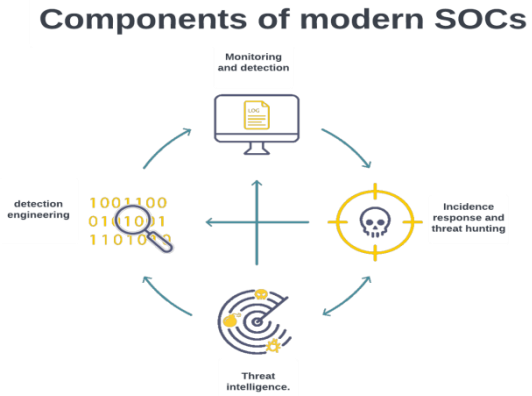

Figure 1: Components of modern SOC's.

2.2. SIEM tools

The SIEM (Security Information and Event Management) is the main tool of the SOC since it manages the events of an IS. SIEM should not be confused with SIM (Security Information Management) and SEM (Security Event Management). Indeed, these last two notions complement each other and are not identical elements (figure 2).

- **The SIM (Security Information Management)** monitors, collects and analyzes the data coming from the different computers of a company and more precisely from the firewalls, proxy servers, anti-virus that compose them. This data is analyzed and then translated into graphs or other forms. They allow the person in charge of monitoring the SIM to monitor in real time any possible intrusion in the systems.
- **SEM (Security Event Management**) is present in companies that use SQL databases. The main purpose and function of a SEM is to provide a stronger real-time data processing and thus find the cause faster than a SIM. One of the main disadvantages is that it has a low compression capacity that does not allow it to be able to store on the long term. [5]

It allows security teams to quickly detect and respond to internal and external attacks to simplify threat management while minimizing risk and protecting the enterprise.
SIEM tools are therefore used for network monitoring, information systems security, and in particular for reporting alerts on activities that could pose a threat to data security (detect and respond to attacks), compliance with standards and regulations, and logging for maintenance and troubleshooting.

They also allow for reporting for auditing purposes. Figure 2 presents the meaning and components of the word SIEM while figure 3 presents the principle of SIEM operations.

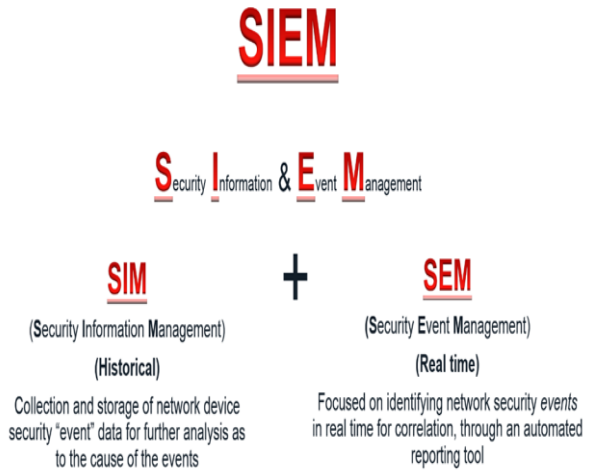

Figure 2: SIEM= SIM + SEM [5]

2.3. How a SIEM works

SIEM collects and summarizes log data generated throughout your information system, from applications to network and security devices, such as firewalls and antimalware detectors. It then identifies and categorizes incidents and events, and analyzes them. Figure 2 illustrates how a SIEM tool works from log collection to the use of information generated by operational security teams.
The SIEM serves two main purposes:

- **Provide reports on security-related incidents and events:** Successful and failed logins, malware activity, and other possible malicious activity,
- **Send alerts** if analysis shows that activity is running on predetermined rule sets, such as malware execution, and thus indicates a potential security problem. [6]

When monitoring an organization's network, it is necessary to perform log collection to **understand and identify events on the network**. This centralization is essential in maintaining the operational status of the information system.
A log is a file that records events that occur on an operating system or any other computer equipment, router, switch, server. For example, the screenshot below shows us Syslog logs from a Linux server. Logs are also called log files.
The management of your log collection will consist in setting up logging and centralization. **Logging** is the implementation of a system allowing the automatic reporting of logs. Sending your logs to a central point describes **centralization,** which will give you a global view of the events in the information system [6]. This log management has several objectives:

- **Obtain a general state of the IS** and identify abnormal events,
- **Detect intrusions**, for example by means of IPS/IDS solutions or SIEM rules,
- **Trace the history** and actions of an attacker as part of a forensic investigation,
- **Visualize IS actions**, define statistics and identify weak signals. [6]

The first step in monitoring security is to identify logs of interest that allow for the detection of suspicious events. For example, if you receive a log of a connection to the Active Directory server outside working hours, this may be an abnormal behaviour that should be reacted to. The role of monitoring is to identify this type of event.

- ✓ The list below proposes logs of interest to be monitored as part of IS security monitoring.
- ✓ Authentication.
- ✓ Account and rights management.
- ✓ Access to resources.
- ✓ Modification of security policies.
- ✓ Process activity.
- ✓ System activity [6]

The SOC [7] is a team dedicated to monitoring the security of the information system and its main mission is to identify, analyze and remediate cybersecurity incidents. When monitoring a company's network, it is necessary to collect logs to understand and identify events on the network and to do this the SOC uses its main tool which is the SIEM (Security Information Event Management). The SIEM [8] [9] tools allow managing the security events of an IS and some of them are already used by the mobile Operator namely IBM Qradar, and Elastic.

2.4 Chatbots

A chatbot or conversational agent is a computer program capable of simulating a conversation with one or more humans by voice exchange. It is a **computer program** set up **to accomplish a precise task, delivering a pre-recorded response at a given moment**, **T**. It is capable of interacting in natural language and in real time, answering questions, proposing solutions and services adapted to the requests made to it. There are two types of chatbots:

- **Simple or basic bots:** the discussion is guided by the "conversational agent" who draws from a library of pre-formatted and pre-recorded questions/answers. It delivers them according to a pre-established scenario that we call WorkFlow in the jargon and in the original version. However, interaction can quickly become limited.
- **Intelligent or advanced bots:** integrate natural language processing (NLP) technology, allowing them to deliver relevant and precise content. This type of bot gives the user the feeling of a live conversation with an operator via a platform. [10].

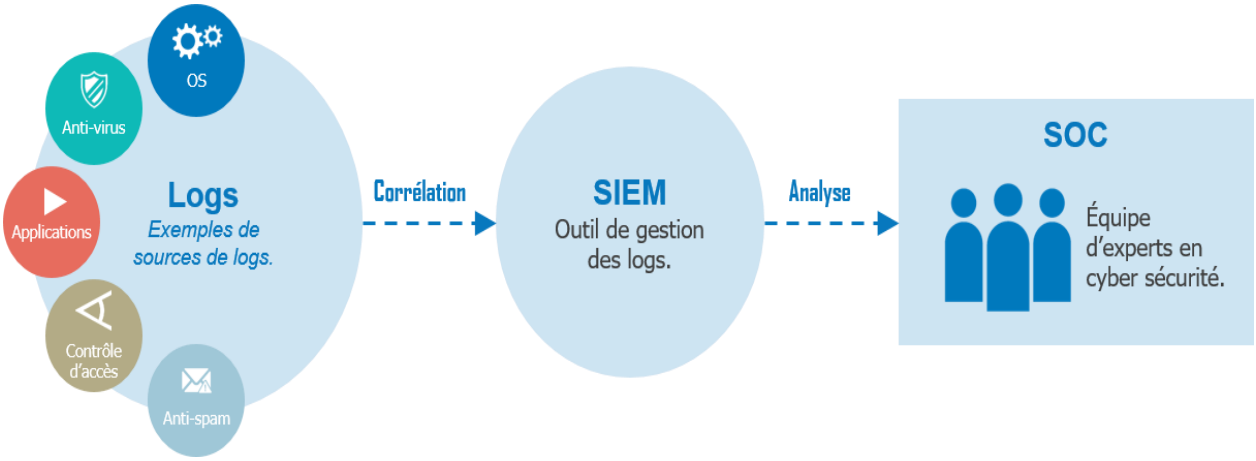

Figure 3: Principles of SEIM operation [11].

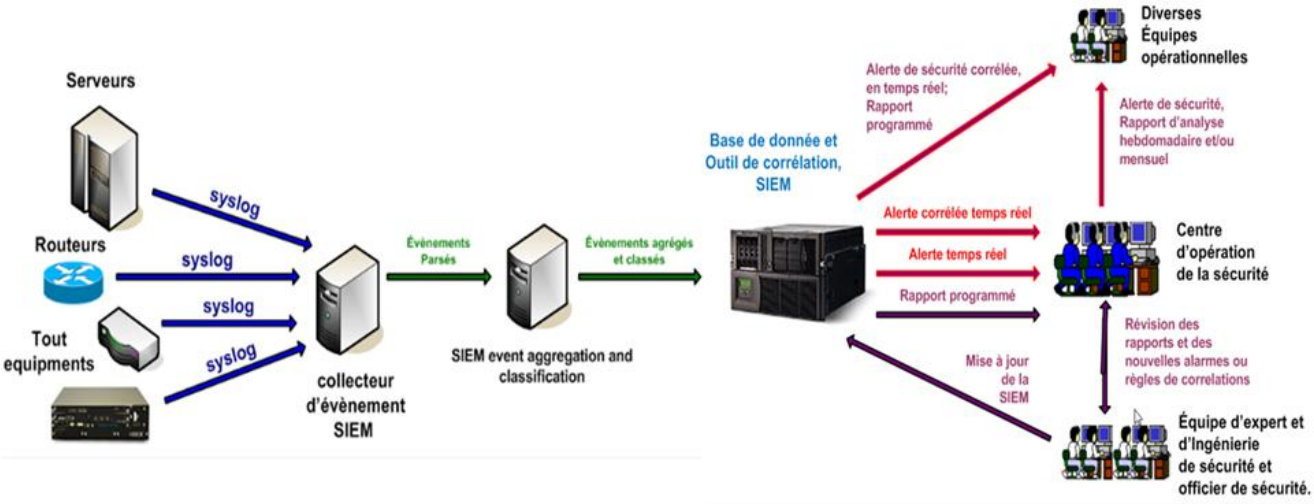

Figure 4: Principle of SEIM operation.

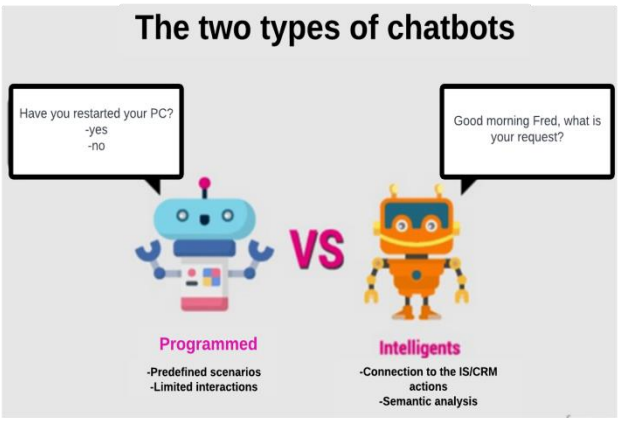

Figure 5: The two types of chatbots. [11]

Figure 4 above is an illustration of the types of chatbots presented.

2.5 Overview of some chatbots usaged

Many authors have worked on the usage of chatbox for different purposes; some have proposed the utilization of chatbox for educational purpose, maintenance one or security [12] [13].

Suha K. Assayed et Al in [14] worked A Chatbot Intent Classifier for Supporting High School Students, in their work the used chatbox for educational purpose.

Santana, R et Al in [15] worked on A "Chatbot to Support Basic Students Questions", where chatbox is used to assist the teachers to ask basic questions to students.

Zahour, O et Al in [16] worked on "Towards a Chatbot for educational and vocational guidance in Morocco: Chatbot E-Orientation", this to show the importance of chatbox to solve problems for specific context, here it was the case of Morocco.

Fryer, L. K., Nakao, K., & Thompson, in [17] worked on "Chatbot learning partners: connecting learning experiences, interest and competence".

Abbas, N et Al in [18] worked on "Online chat and chatbots to enhance mature student engagement in higher education."

Hamad, S. and Yeferny, T in [19] worked on "A chatbot for information security", in this case the chatbox is used for the management of information system security. In the same way we can used chatbox for maintenance by using artificial intelligence, this has been proposed by author in [20]; The authors used The device that they called MAAI (Maintenance Assisted by Artificial Intelligence) which allows them to obtain real-time information on the state of network equipment, automatically alert engineers and technicians in the event of a problem and even prevent possible network failures, and remedy them. These functionalities are performed through the combination of ZABBIX' relevance,

and the innovative nature of voice chatbots. In the same way, authors in [21] has proposed a solution of intrusion Detection aided by Artificial Intelligence (IDAI).

IDAI solution proposed by these authors provided a tool which was able to do the following actions:

(1) Retrieving the user's voice command from the Raspberry PI board;

(2) Automatic voice recognition and sending the text command to the NLP engine;

(3) Sending the command in a new data format to the conversational engine (neural network);

(4) Mapping user intent to business functions;

(5) Sending the user's command to the application server via the REST API;

(6) Interaction with network infrastructure and security stack;

(7) Sending the result of the execution of the command;

(8) Speech synthesis and sending of the final voice response (plus text) to the user.

Their operational prototype was a set of tools including the conversational agent which will accompany the monitoring and intrusion detection solutions. It was composed as follows [21]:

- A Raspberry PI 4 card in which runs the voice assistant shown in Figure 9;
- The application server (presented in the telematics network datacenter) which contains the trained neural network model and which acts as a conversational engine and NLP processing;
- A software client that can be installed on a Raspberry PI 4B nano computer or on Windows/Linux workstations to interact with the infrastructure via the conversation agent;

Through all what was presented so far, we can see that AI and precisely machine learning methods can help for education, fraud detection in mobile network operator [22] [23], maintenance of mobile and optical networks [24] [25] and security of information systems [26][27][28].

3. DESIGN APPROACH

3.1. Choice of the type of conversational agent

The artificial intelligence conversational agent is a virtual assistant in the form of software that uses new technologies combined with language; illustration is presented in figure 5.

Based on recent technological developments such as machine learning, learning algorithms and artificial neural system, the conversational robot can act in a way that is very close to human behaviors such as:

- Ensuring the reception of all incoming requests
- Understand the subject for which it is solicited and confirm it with the person in question
- Provide answers to the most common questions
- Learn from its experiences to improve its performance.

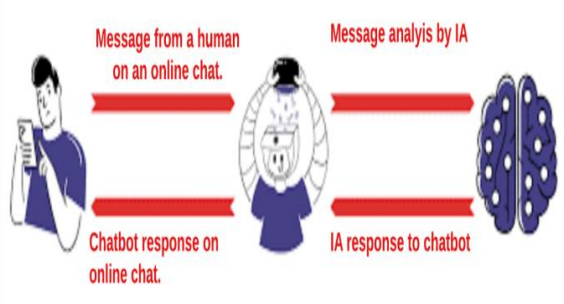

Figure 6: Intelligent chatbot.

3.2. Choice of SIEM tool: ELK Stack

ELK Stack is an open source suite with 4 main components that not only analyze logs to detect problems, but also monitor system usage and identify improvement opportunities. Figure 6 presents the ELT stack components.

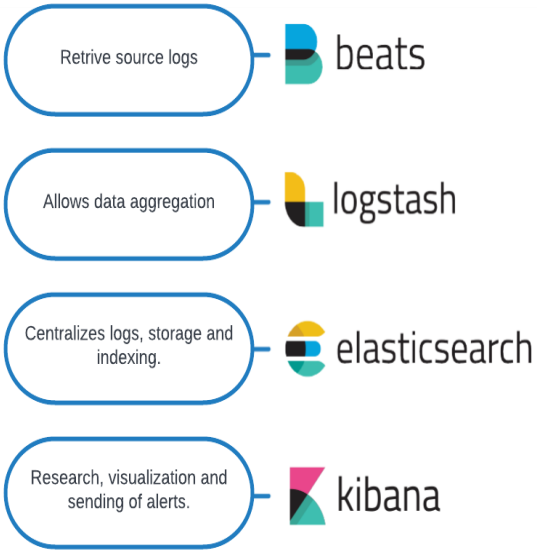

Figure 7: ELK stack.

- Advantages
- Event log records
- Interface customization possible
- Disadvantages

- Elasticsearch tool is insufficient in terms of correlation
- Does not provide alerts

➢ **Beats**

It is a set of tools allowing the sending of logs. These tools must be installed on the machines you want to monitor.

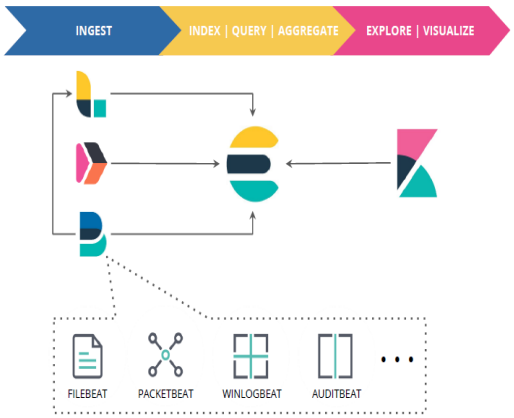

Figure 8: Beats tools for sending logs.

They will act as agents that collect event logs (see figure 7 as an illustration). There are several of them such as:

- Filebeat: ingestion of log files.
- Packetbeat: ingestion of network capture files.
- Auditbeat: ingestion of audit files.
- Heartbeat: check if a service is available or not.
- Functionbeat: monitoring of cloud environments.
- Journalbeat: ingestion of system logs.
- Metricbeat: collection of metrics from different systems.
- Winlogbeat: collection of Windows logs.

For our study, we will focus on Filebeat, Packetbeat, Winlogbeat and Auditbeat, which are the only beats used in the context of security event management.

➢ ***Logstash***

Logstash allows for the data to be easily aggregated and formatted to be sent to Elasticsearch. Logstash will therefore allow you to send different types of data other than logs.

➢ ***Elasticsearch***

ElasticSearch is the main engine of the ELK stack: it is the one that will store the data and make it accessible. It can be used for several purposes, but its main functionality is indexing or listing data streams. In our case, this functionality allows the centralized storage of logs, such as logs or network packets, for example. It is therefore very useful for our security monitoring.

Elasticsearch stores data in JSON format. This data is contained in indexes which are databases.

➢ ***Kibana***

Kibana will allow you to visualize Elasticsearch data in real time. This tool offers preconfigured dashboards to analyze the logs that are sent to you. It is also possible to view and explore your data in the Discover section. This is very useful to visualize your logs and understand what they contain. This will allow you to implement your SIEM rules more easily because a picture is better than 1000 lines of logs.

3.3. Designing the Artificial Intelligence program for the conversational agent

❖ ***Identification of the objectives***

The objectives of the realization of our conversational agent have already been defined previously, but we are going to remind them anyway.

- Identify and analyze the security incidents and events of the information system.
- Centralize and have a global view of the security status of all the monitored equipment.
- Create personalized and adequate rules that can detect and block vulnerabilities in the system.
- Provide reports on security incidents and events through voice exchanges.
- Establish a report of the automatic conversation.

❖ ***Establishment of conversational scenarios***

Based on the previously stated objectives, we will define the different conversational scenarios based on the engineer's "intentions".

These conversational scenarios depend on the objectives and the five main functionalities of our conversational agent tool:

- Events on the hosts: questions can be asked about the number of successful and failed authentications, host connections to the network, open files and the geographical location of the monitored hosts.
- Network events: the engineer can ask questions about the source and destination addresses of exchanges in the network, IP address scans.
- Detection of anomalies in the system.
- Creation of customized rules: allows creating rules specific to the the mobile Operator information system.
- Conversation report: to have a written record of the conversation, i.e. the questions asked by the engineer and the answers given by the conversational agent.

a. Setting up language recognition and processing engines and Machine Learning (ML)

Associate the answers that the conversational agent will have to give to the conversational scenarios. These responses will be of two kinds:

- A simple predefined answer

Example: To the question "Hello, how are you?" the conversational agent will automatically answer "Hello, I'm fine and you" without using the functionalities of our SIEM tool.

- An answer from the ELK Stack database (JSON file).

b. Development

In the field of speech recognition, we had two choices. The first one is to program ourselves a system that will understand what the user says and the second one is to base ourselves on an already existing and performing system. We chose to program a system ourselves because the implementation of the functionalities of our ELK Stack SIEM tool will be more controlled and have more flexibility. We will use Python because it is a programming language that is particularly suited to speech recognition. We can easily set up systems that will understand what the user is going to say and thus react to his requests.

- **Installation of the libraries**

- PyAudio is a library that allows python to communicate with the audio ports of your machine. This library allows to play and record audio.
- SpeechRecognition allows to launch speech recognition operations. This library supports several recognition systems and is easy to use.
- Jsonify
- Pyttsx3

The program captures what the user says and transcribes it into writing. Once this logic is implemented, it is easy to create conditions to react to certain voice commands. Table 1 presenta summary of some libraries used.

Table 1: Summary of the libraries used for the development of our AI program.

Procedures	**Commands**
Voice recognition	pip install jsonify
Voice synthesis Voice recognition and synthesis	pip install speech recognition pip install py audio
Analysis and interpretation	pip install pyttsx3

3.4. The RASPBERRY PI 4

The Raspberry Pi is a credit-card sized single-board ARM nano computer designed by professors at the University of Cambridge's Computer Science Department as part of the Raspberry Pi Foundation 3.

Modelling of the solution

- ***Functional architecture of the device.***

The conversational agent has three functional entities:

- The engineer who speaks to the conversational agent embedded in the Raspberry Pi to harvest information about security events.
- The assembled Raspberry Pi module inside which there is the code of our artificial intelligence program, the ELK Stack and its database in which log files are stored in JSON format.
- The last entity of the solution is the mobile operator information system monitored in real time by the proposed ELK Stack tool.

- ***Use case diagrams***

Figure 9 presents the sequence diagram used during the design of the proposed tool, while figure 10 presents the flowchart of the different steps of methodology to build the prototype. Figure 12 presents the Raspberry pi hardware used during the implementation and testing of the proposed solution. Figure 11 shows the functional diagram of the proposed solution and finally figure 13 presents functional architecture for the proposed solution. The next step after all these is the presentation of the results obtained after the implementation of the proposed methodology and after all testing.

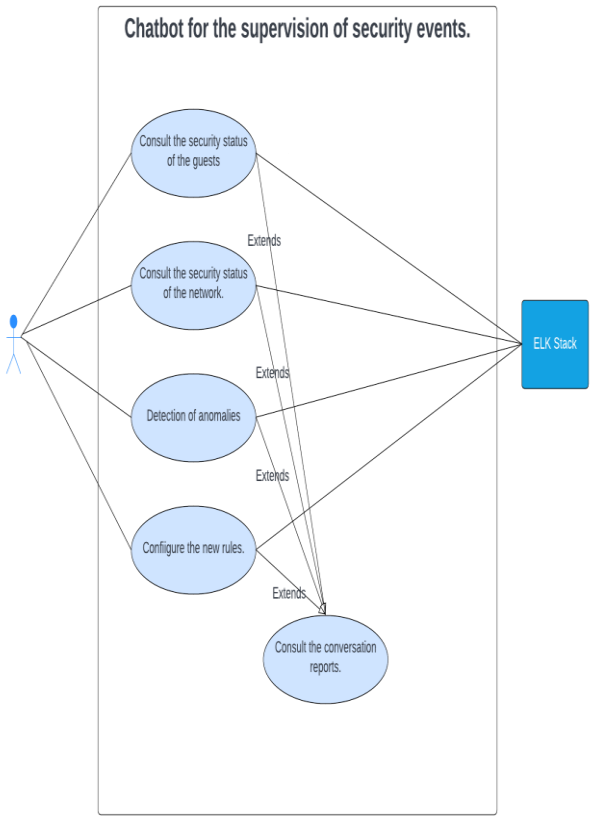

Figure 9: Sequence diagram

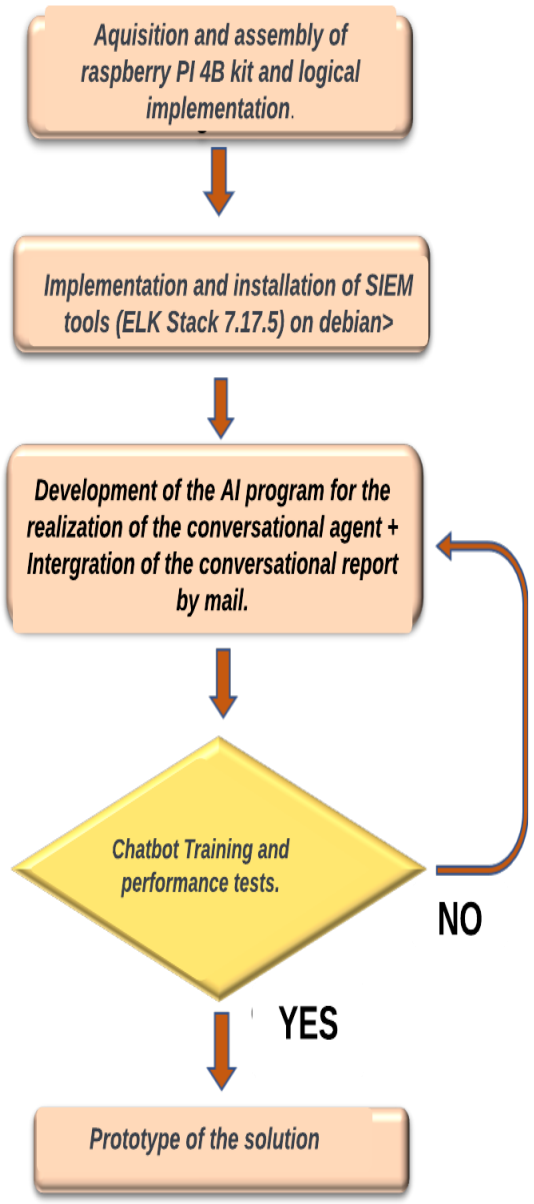

Figure 10: Flowchart of the different steps of methodology

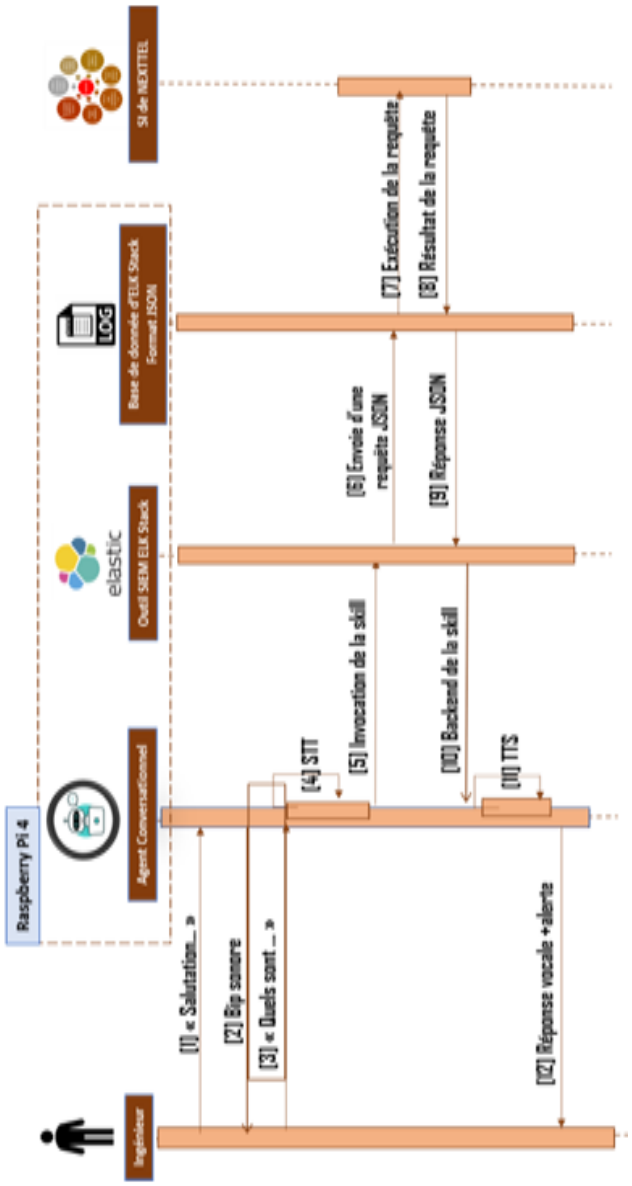

Figure 11: Sequence diagram.

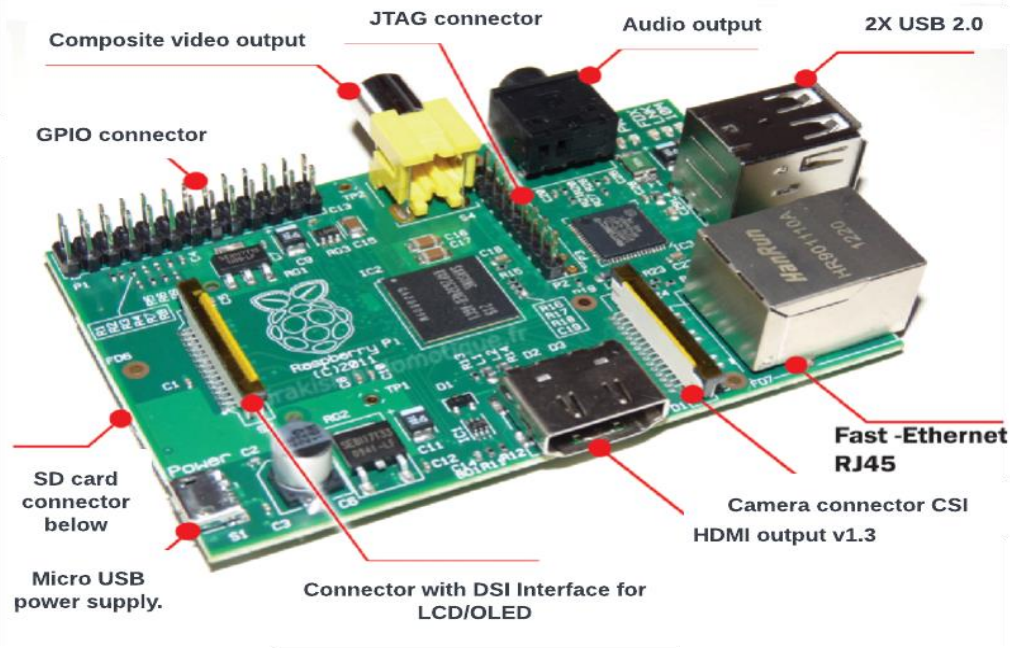

Figure 12: Raspberry pi.

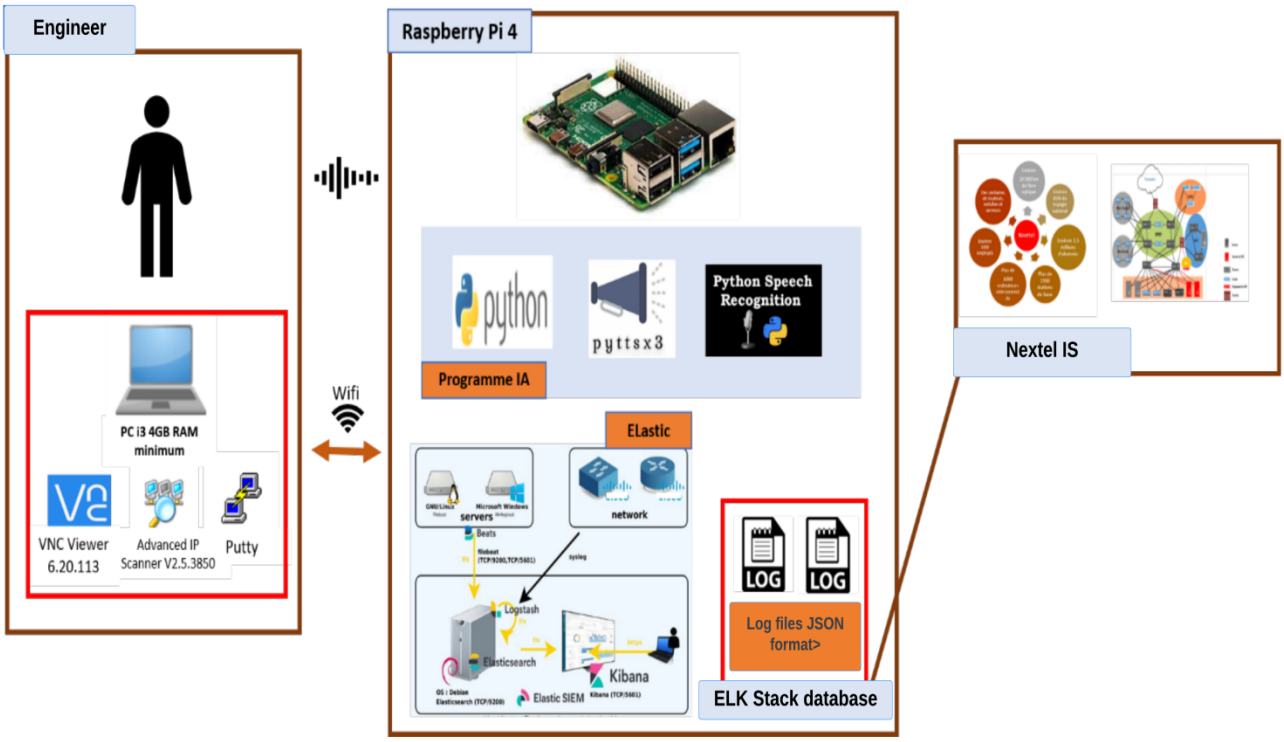

Figure 13: Functional Architecture.

4. RESULTS

One of the essential steps in the deployment of the proposed solution is the implementation and installation of ELK, which involves the installation and configuration of each of the elements that constitute it. The installation steps are following:

- Installing and configuring ElasticSearch
- Installation and configuration of Kibana
- Installation and configuration of beats: Winlogbeat, Packetbeat, Filebeat, Auditbeat.
- Anomaly detection settings
- Creation of personalized rules specific to the operator information system
- Allocation of access (Authentication)

Figure 14 below shows us that after executing the ***systemctl status kibana*** and systemctl ***status elasticsearch*** commands, we can see that the two services are operational.

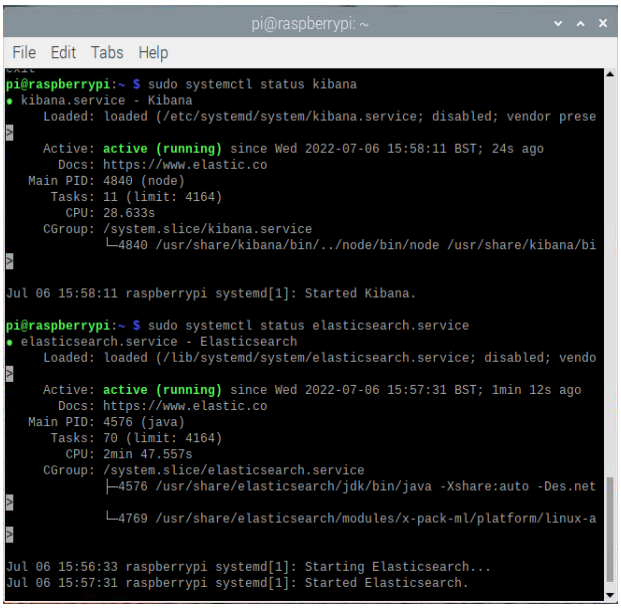

Figure 14: Elasticsearch and Kibana status verification

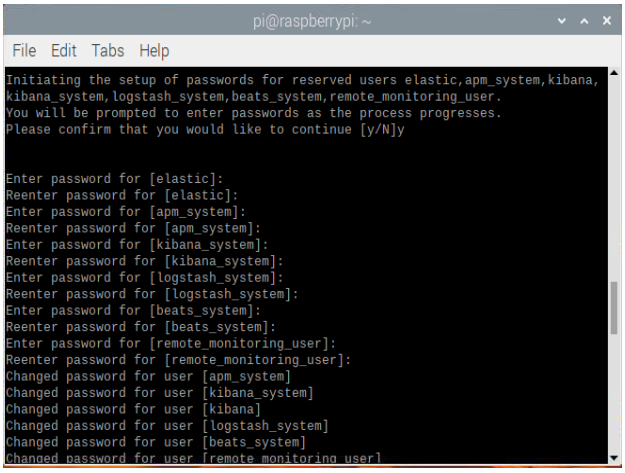

Figure 15: authentication parameters

Then, it was also a question of defining all the security and authentication parameters within ELK Stack. This is presented in figure 15.

The conversation with our chatbot connected to a company's network gave us the following results:

In Figure 16, we have an overview of all security events that occurred on our two monitored elements.

We see that the events related to the hosts come from three sources, namely ***auditbeat***, ***filebeat*** and ***winlogbeat***. And those concerning the network come from the network logs recorded by ***packetbeat***.

Figure 17 allows us to observe the host part of our interface on kibana. On top there is the number of hosts, the number of user authentications and the source and destination IP addresses with which our hosts interacted.
We see that the events related to the hosts come from three sources, namely ***auditbeat***, ***filebeat*** and ***winlogbeat***. And those concerning the network come from the network logs recorded by ***packetbeat***.

After the previous steps, the development of an AI program for the realization of the conversational agent need to be done and this is possible through the following steps:

- Installation of python3-pyaudio
- Installation of telegram for alerts
- Installation of espeak
- Installation of telebot

Figure 16, figure 17 and figure 18 present captures obtained after the installation of telebot, the other captures are not presented intentionally. This is to show that the solution is working well.

In figure 16, under the host events tab we can see the events on host and under the network events tab, we can see the network events. Figure 17 allows us to observe the host part of the interface on kibana. On it are the number of hosts, the number of user authentications and the source and destination IP addresses with which the hosts have interacted.
After all this deployment, the solution proposed can work normally and the chatbot is operational.

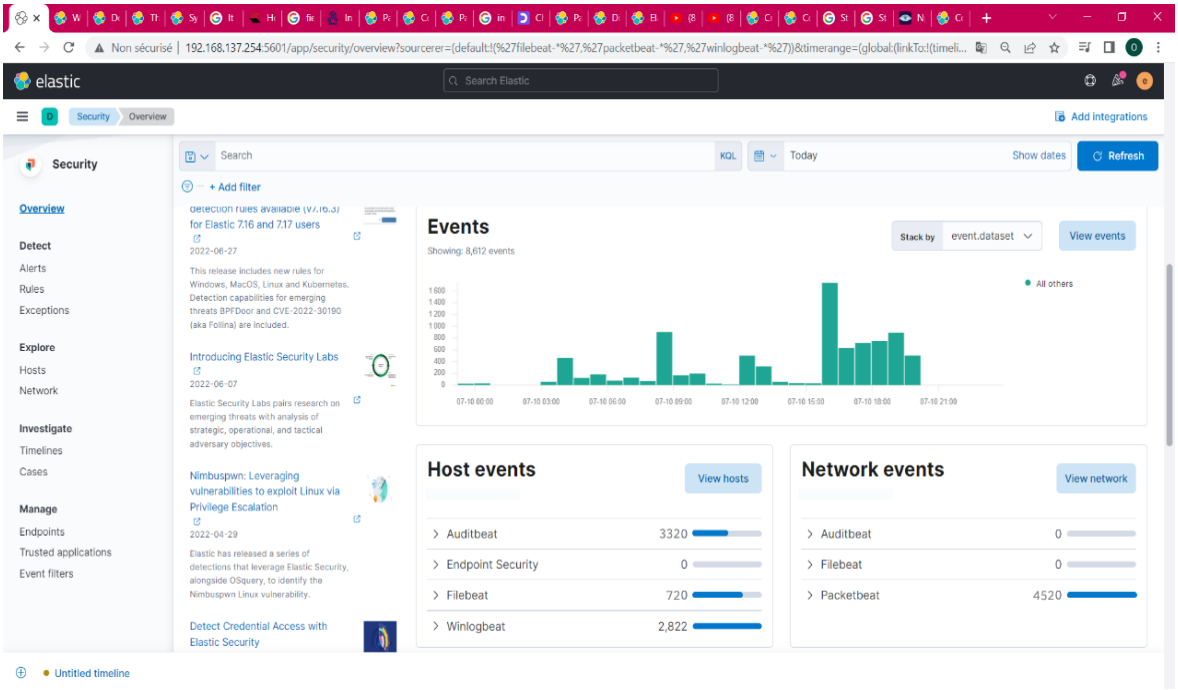

Figure 16: Security overview.

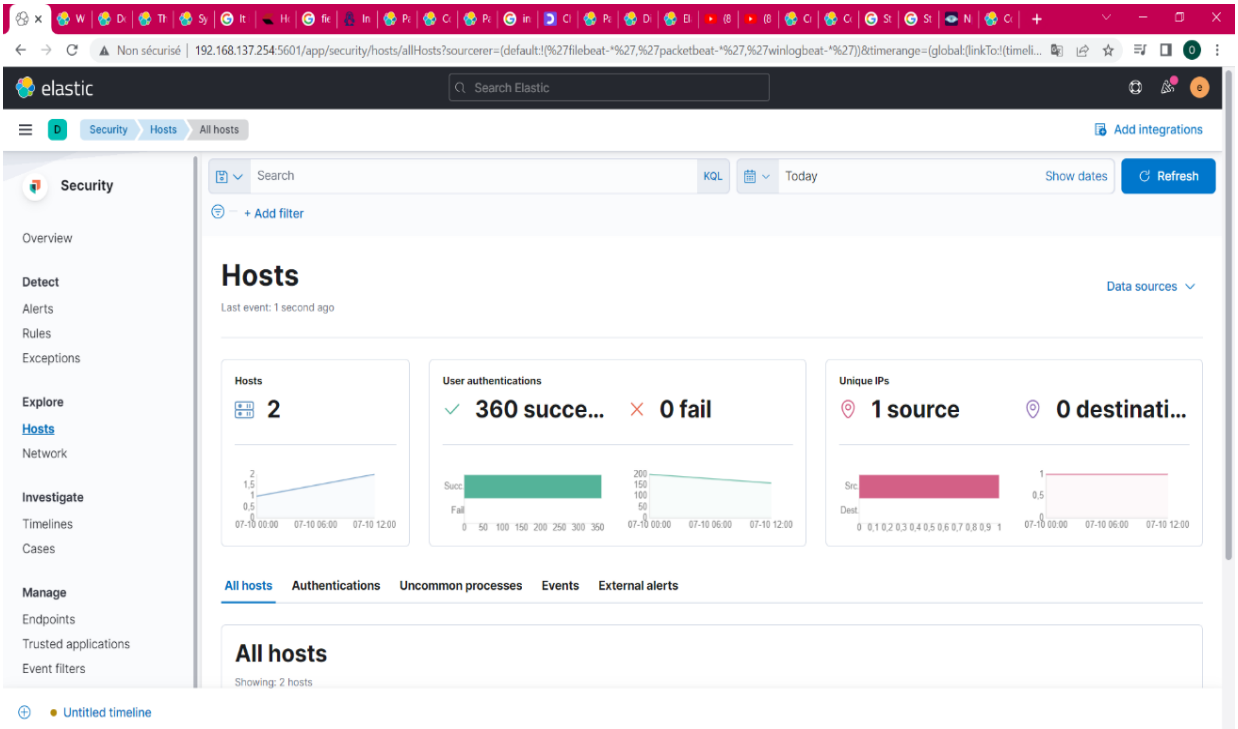

Figure 17: Events listed at the host level.

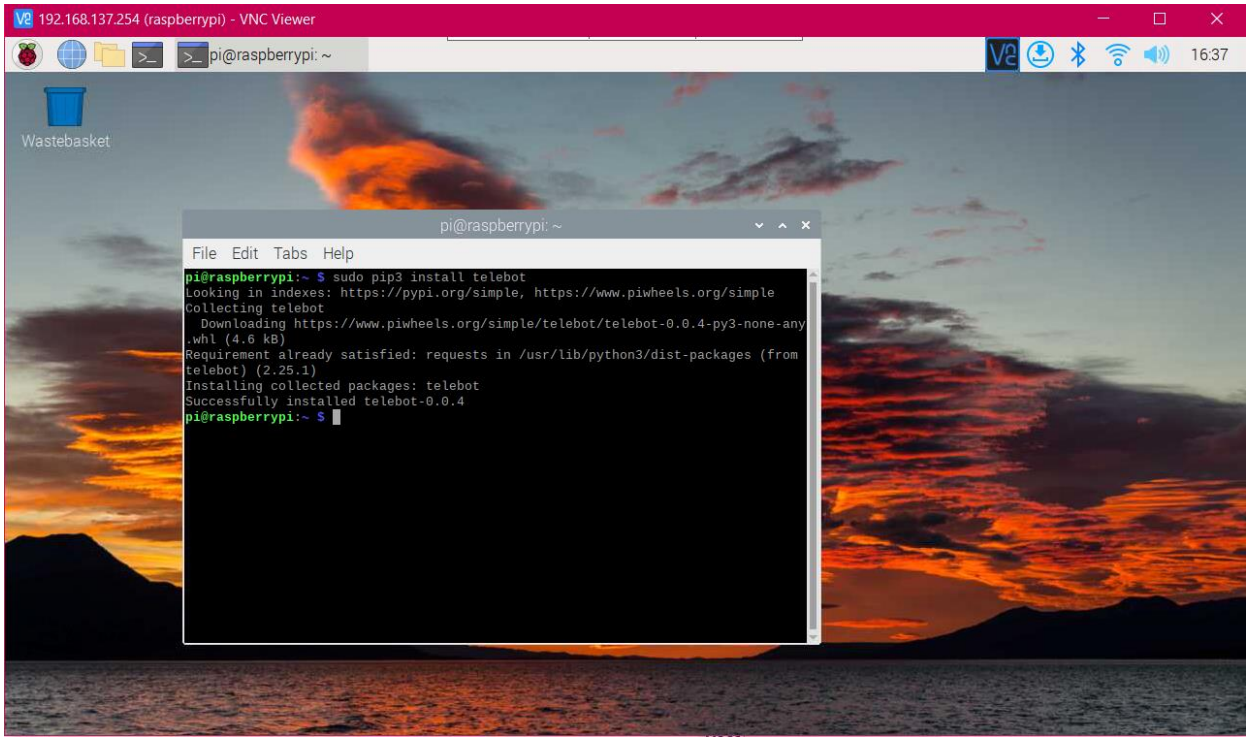

Figure 18 : Teleboot installation presentation

5. CONCLUSION

The objective of this work was to create a conversational agent for the supervision of security events using SIEM tools in order to identify and analyze security incidents and events in a mobile network operator information system, centralize and have a global view of the security status of all monitored equipment, create personalized and adequate rules that can detect flaws in the system, provide reports on incidents and events related to security through exchanges vocals.

To carry out this work, a study was initially made for the understanding of the concepts related to the supervision of the security events of the information systems, we presented in a general way the stakes, methods and tools of supervision which exist and are currently in use. In a second step, it was spread all the methodology of realization of a conversational agent. Finally, the results of these various works were presented and recommendations were made among which the most important are:

- The use of a paid and license based SIEM tool with more features than the existing Solar Winds platform used,
- Further training of our agent's artificial intelligence program.
- Set up an automatic SMS alert system that works without internet.

At the end of this work, we propose a solution which can now serve as a tool for monitoring the security of an information system. It can identify and analyze information system security incidents and events, centralize and have a global view of the security status of all monitored equipment monitored equipment, provide reports on incidents and events related to security through voice exchanges. The proposed conversational agent can also provide reports of conversations maintained automatically to always have a trace of what has been exchanged.

6. REFERENCES

[1] Mathieu Pierre, Sylvain Loizeau, The impact of new information and communication technologies. (accessed on 30/02/2022)

[2] Myriam QUEMENER (October 2008), Cyber threats, companies and Internet users (consulted on 30/02/2022)

[3] Federal Bureau of Investigation (2021), Internet Crime Report. (Accessed on 19/03/2022)

[4] Monday, October 25, 2021 https://web.antic.cm/antic.cm/index.php/fr/news/blog-items-by-tags/itemlist/date/2021/10/25 (Accessed 02/30/2022)

[5] NGANE Noelle (2021), *Mise ne place d'un système de gestion d'événements dans un réseau distant*. Mémoire de fin d'études, ENSPY, UY1, Cameroun.

[6] Openclassroom, Optimize IT security with monitoring https://openclassrooms.com/fr/courses/ (Accessed on 08/06/2022)

[7] Fortinet (2019), *SOC Analyst Bases Online Course* (consulté le 18/04/2022)

[8] H. Shah et al. Can machines talk? Comparison of Eliza with modern dialogue systems Computers in Human Behavior. (2016).

[9] Elastic SIEM Fundamentals elastic.co/training (Accessed on 20/06/2022)

[10] *Les deux types de chatbots*, https://mbamci.com/un-chatbot-pour-mes-clients-pourquoi-comment/ (Consulté le 20/03/2022)

[11] *Agent conversationnel intelligent*, https://www.citizencall.fr/agent-conversationnel-intelligence-artificielle/ (Consulté le 17/06/2022)

[12] J. Hill et al. Real conversations with artificial intelligence: A comparison between human–human online conversations and human–chatbot conversations. Computers in Human Behavior. (2015)

[13] Alphorm (2020), *Fonctionnement de base d'un SIEM* (consulté le 10/03/2022)

[14] Assayed SK, Shaalan K, Alkhatib M. A Chatbot Intent Classifier for Supporting High School Students. EAI Endorsed Scal Inf Syst [Internet]. 2022 Dec. 21 [cited 2023 Apr. 27];10(3):e1. Available from: https://publications.eai.eu/index.php/sis/article/view/2948

[15] Santana, R., Ferreira, S., Rolim, V., de Miranda, P. B., Nascimento, A. C., & Mello, R. F. (2021). A Chatbot to Support Basic Students Questions. In LALA (pp. 58-67).

[16] Zahour, O., El Habib Benlahmar, A. E., Ouchra, H., & Hourrane, O. (2020). Towards a Chatbot for educational and vocational guidance in Morocco: Chatbot E-Orientation. International Journal, 9(2).

[17] Fryer, L. K., Nakao, K., & Thompson, A. (2019). Chatbot learning partners: connecting learning experiences, interest and competence. Computers in Human Behavior, 93, 279–289. https://doi.org/10.1016/j.chb.2018.12.023

[18] Abbas, N., Whitfield, J., Atwell, E., Bowman, H., Pickard, T., & Walker, A. (2022). Online chat and chatbots to enhance mature student engagement in higher education. International Journal of Lifelong Education, 1-19.

[19] Hamad, S., & Yeferny, T. (2020). A chatbot for information security. arXiv preprint arXiv:2012.00826.

[20] Cecile L. NLEMBA, Emmanuel TONYE, Alphonse BINELE ABANA; Maintenance Assisted by Artificial Intelligence (MAAI); London Journal of Research in Computer Science and Technology, volume 22, issue 1, compilation 1.0; 2022.

[21] Jean MELI TAMWA, Emmanuel TONYE, Alphonse BINELE ABANA, Chantal MVEH; Intrusion Detection aided by Artificial Intelligence (IDAI); American Journal of Engineering Research (AJER); volume-11, Issue-03, pp99-106; march 2022.

[22] DEUSSOM Eric, MATEMTSAP MBOU B., TCHAGNA KOUANOU A., Michael EKONDE SONE, & BAYONBOG Parfait, Machine learning-based approach for designing and implementing a collaborative fraud detection model through CDR and traffic analysis. Transactions on Machine Learning and Artificial Intelligence, Yaoundé, 2022.

[23] Deussom Djomadji Eric Michel, Kabiena Ivan Basile, Tchapga Tchito Christian, Kouam Djoko Ferr V. and Michael Ekonde Sone. (2023)Machine Learning-Based Approach for Identification of SIM Box Bypass Fraud ina Telecom Network Based on CDR Analysis:Case of a Fixed and Mobile Operator in Cameroon. Journal of Computer and Communications , 11, 142-157. https://doi.org/10.4236/jcc.2023.112010

[24] BATCHAKUI Bernabe, DEUSSOM DJOMADJI Eric Michel, CHANA Anne, MAMA TSIMI Serge Fabrice, (2022) Comparing Machine Learn-ing Algorithms for Improving the Maintenance of LTE Networks Based on Alarms Analysis. Journal of Computer and Communications, 10, 125-137. https://doi.org/10.4236/jcc.2022.1012010.

[25] DEUSSOM DJOMADJI, E. M., Takembo, T.C., Tchapga Tchito, C., Mamadou, A.and Michael Ekonde Sone. (2023) Machine Learning-Based Alarms Classification and Correlation in an SDH/WDM Optical Network to Improve Network Maintenance. Journal of Computer and Communications, 11,122-141. https://doi.org/10.4236/jcc.2023.112009

[26] Qingchuan Meng, Youzi Zhang, Fengzhi Wu, Xiaoming Chen, Network Intrusion Detection Model Based on Artificial Intelligence, Journal of Physics Conference Series, August 2020.

[27] Anitha A, SV Revathi, S Jeevanantham, E Eliza Godwin, Intrusion Detection System based on Artificial Intelligence, International Journal of Technology, January 2017.

[28] ANDELA OLINGA Yvette Ophélie, Conception et réalisation d'un chatbot pour la supervision des évènements de sécurité (SIEM) Mémoire de fin d'étude en vue de l'obtention du diplôme d'ingénieur de conception Option Génie des Télécommunications à l'ENSP, UYI, Juillet 2022.