**A system to evaluate the implementation of MITRE ATT&CK framework using a given**

**set of logs**

**Shir Bar -   
Hen Dahan - 312585953**

**Kfir Ram - 203426721**

**A brief description:**

The proposed system offers a method to evaluate the value of a source data set when being used with the MITRE ATT&CK for IT and ICS for the purpose of detecting cyber-attack techniques.  
This system will allow organizations to measure how the data that is being collected into their SIEM system can be used to detect events that correspond to the result of their risk management and threat intelligence.

**Project Charter / Business plan**

**Quality Objectives:**

* This system will allow organizations to measure how the data that is being collected into their SIEM system can be used to detect events that correspond to the result of their risk management and threat intelligence.
* The system will allow a method to denote what logs are being collected and from which systems. The logs will be correlated with the MITRE ATT&CK data and will output the list of ATT&CK techniques that can be identified using the logs.
* The system will contain the latest data and knowledge that consists of MITRE ATT&CK for IT and ICS.
* The system will clearly state what logs can be interpreted and identified
* The system will allow the compilation of cyber security attacks based on threat intelligence and using ATT&CK IDs.

**Project Stakeholders:**

Our stakeholders are any organization that works with logs collection systems (SIM and SIEM systems) and provide cyber security services.

Our main stakeholder is Efi Kaufman, Head of Big Data & Analytics, Cyber Security Center, Ministry of Energy under Dell company.

**Stakeholders Analysis:**

Effie's ability to influence and get involved in the project will be relatively high.

The project will be developed according to his requirements.

Beyond that Effie will accompany us at the professional level throughout the year.

**Business Process Management:**

Our business process management life cycle is:

* **Market Survey**:  
  Exploring the options currently available on the market and investigation into the sources of information that will help us during the project.
* **Design:**

System analysis and design.

The design process will include setting requirements and coordinating expectations with the customer before we move on to the next step.

* **Modeling**:

At this point we will create a model of the system and its processes that constructed by graphically representing.

In this part we will alsofocus on analyzing system users, permissions, and dashboards.

* **Establish of work environment**
* **Execution:**Start system development according to the requirements and modeling performed previously.
* **Code test and optimization:**

We will make improvements and repairs following to the test results and feedback from the customer.

* **Send prototype product to the customer**
* **Receiving ideas and suggestions for improving the process from the client**
* **Send the final version of the system to the customer.**

**We updated this file starting here --- (part 2)**

**Reports**Our system reports will provide relevant relationship between the Logs and MITRE ATT&CK:

* **Results –** Possible attack techniques based on the logs of the input to the system.
* **Logs description** – display a log list with an explanation of the meaning and the purpose of each log received by the system.
* **MITRE ATT&CK Enterprise Tactics** – display the tactics available of the adversary with a description.

**Main Processes**

|  |  |
| --- | --- |
| Process Name | Process Description |
| Main Process Screen |  |
|  |  |
|  |  |
|  |  |
|  |  |
| Result Report | This action comes after clicking on |
| Log Description Report | This action comes after selecting Reports in the main screen. The action will display the logs description of the input. |
| MITRE ATT&CK Tactics Report | This action comes after selecting Reports in the main screen. The action will display the main MITRE ATT&CK Tactics. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**General characteristics**The project was done in collaboration with DEL EMC in order to develop a product (software) that will help them better analyze their network and thus increase their security on the network.

The project will be related to cyber and security and will help prevent attacks on the network.

The software will function as stand-alone software that will not actually be connected to the network or any other software,

And will serve as a "black box".

The software will function as a "black box" which will receive as input a name of an attack that is suspected as an attack that occurs in the system and in real time the "black box" will return a list of logs with which company employees can locate the attack or verify it does not exist.

**User interface**  
  
The app will function as a "black box" which will be used to find relevant logs to detect attacks.

The user interface will be - The user must enter a name of the attack that he suspects exists in the system and in response to the black box will return to him a list of relevant logs with the help of which the requested attack can be detected.

**Glossary of Terms**

* BLACK BOX - black box is a device, system or object which can be viewed in terms of its inputs and outputs, without any knowledge of its internal workings. Its implementation is "opaque" (black).
* STAND ALONE PROGRAM - A stand-alone program, also known as a freestanding program, is a computer program that does not load any external module, library function or program and that is designed to boot with the bootstrap procedure of the target processor – it runs on bare metal.
* ATT&CK - A cyber-attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. A cyber-attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks.
* MITRE ATT&CK - A MITRE ATT&CK is a framework is a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk.
* LOG - A log file is a file that records either [events](https://en.wikipedia.org/wiki/Event_(computing)) that occur in an [operating system](https://en.wikipedia.org/wiki/Operating_system) or other [software](https://en.wikipedia.org/wiki/Software) runs, or messages between different users of a [communication software](https://en.wikipedia.org/wiki/Internet_chat). Logging is the act of keeping a [log](https://en.wiktionary.org/wiki/log#Etymology_2). In the simplest case, messages are written to a single log file.

**information security**The system functioning as a 'black box' therefore it does not hold any private information of the users of the system, through logs obtained by the user the system will run and return a list of tactics and techniques connected to the logs and display them to the relevant user.  
furthermore, the system is locally used without the need of internet connection therefore the information security is less likely to be damaged.

**Architecture and external interfaces**

The software architecture will be as a stand-alone "black box".

The software will be used as a "black box" so that all end users who cannot see what is happening inside these only the input and output of the software.

The software will be stand-alone software, meaning the software will be able to work on its own without any dependence on other software or network connection.

The "black box" will stand alone and therefore will contain the DB it needs to perform the job, in addition it will contain all the tools needed to perform the job.

**פרק 2 – לשאול לגבי:**

**תיחום חיצוני – משתמשים ?actors**

**תהיליכים**

**אבטחת מידע**

**נפחים, עומסים וביצועים?**

**ארכיטקטורה וממשקים חיצוניים**

**this picture is just for us to remember what are the main tactics.**

**Each of the tactics has many Techniques to it.**

**We need to decide what we are focusing on.**