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

**set of logs**

**Shir Bar -   
Hen Dahan-**

**Kfir Rahamim-**

**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.**