MAST (Mitre Att&ck SIEM Tool)

By: Marcus Vidamo & Eric Mahinay **Supervisor:** Dr Thui Trang **Client:** Ruben Meneses

Reporting Interface Team Name Adding Common Field Name Interface

INTRODUCTION

MAST (Mitre Att&ck SIEM Tool) is an application that will produce common field names from attack types, to be populated into SIEM (Security information and event management). Once the SIEM is populated with the required field names, it will help a cyber security professional to monitor the systems security base on the threat model for the client's application or system.

Ensuring a system is safe from cyber-attacks is important in today's world. The existing process to set up a systems security is time consuming and unreliable for both Cyber Security Professionals and the Clients. The existing process is constant back and forth communication to discuss and figure out common field names to put into SIEM. To overcome this problem, MAST can generate the common field names based on the threat modelling which then can help populate the required fields for the SIEM.

Using MAST saves time and ensures reliability for both Cyber Security Professionals and Client. The user can ensure that they will be able to get a common field name report and can also add their own common field names relevant to Client's system.

DEVELOPMENT

MAST has been developed alongside an Iterative approach in order to ensure proper planning and milestones have been created in order to ensure MAST has been created at its full functionality as required.

Upon completion of the design phase of MAST, the project team started the development. The challenging part within the development phase is the integration between SQLite and C# but at the end all requirements was met.

After completing the development phase, testing was done for MAST. Manual testing was performed by the team. Functional testing was done using the test plan and test cases created. All the testing performed has been documented and reported on.

As the project team only consisted of two members and just enough knowledge and experience to create databases and GUI it was a lot of time and effort on learning quickly and especially finishing up the documentation.

CONCLUSION

The project was insightful and provided great experience to our current knowledge about our Majors. The development has been fruitful and full of learning experiences which has been moulded all throughout the 16 weeks creation of the project.

The activities will teach, demonstrate, and correct basic steps under Cyber Security and Networking Major.

The Project team has successfully completed the project and documents have been provided for further improvements that can be possibly done in the application. At the end of this project, the team gained a very good knowledge on different phases involved in the project.