Cybersecurity,
2022-2023

OSINT Tools for Risks Detection

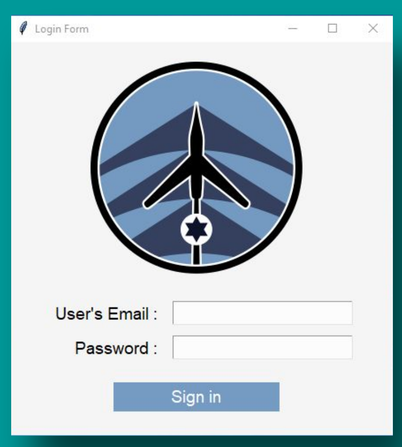
Supervisor: Mr. Roi Zimon

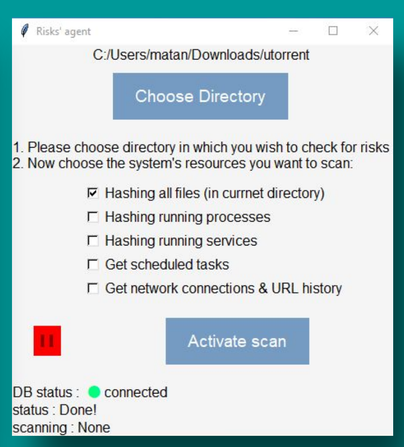
Matan Kichler, Anat Shulman, Oz Diamond

מכון טכנולוגי חולון
Holon Institute of Technology

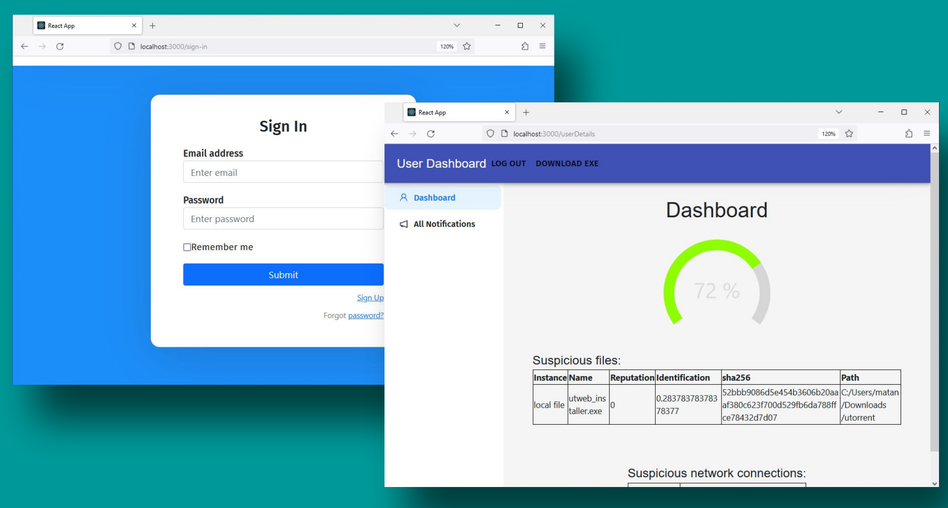
Products

Client's agnet (Executable)

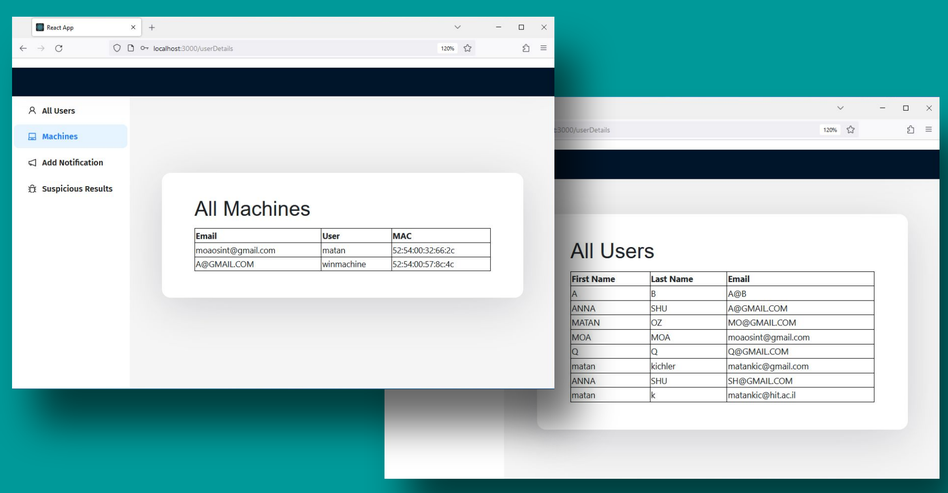




User's login and dashboard



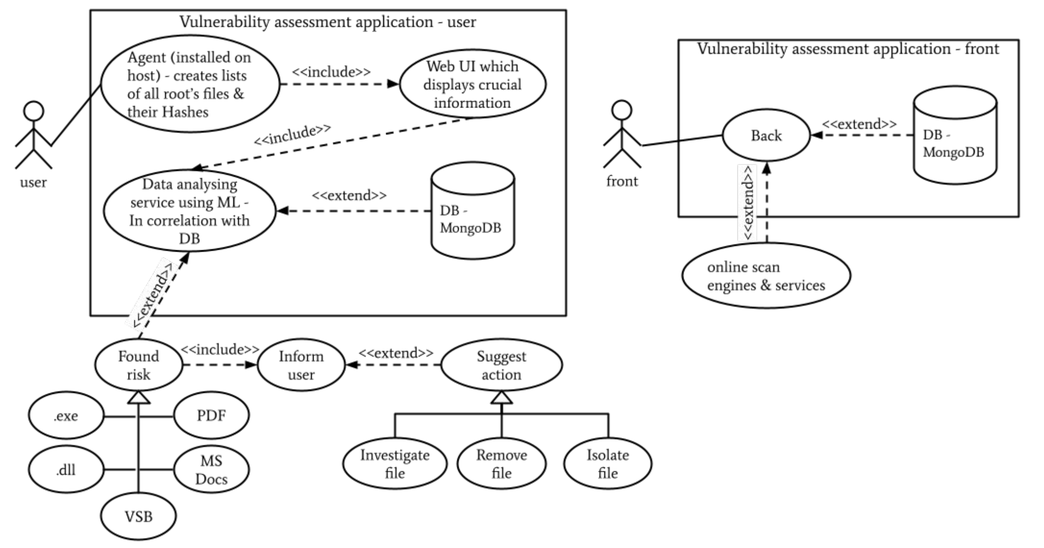
Admin's dashboard



Introduction

Our project aims to develop an advanced threat detection system that leverages machine learning and open-source intelligence (OSINT) data to protect against a wide range of cybersecurity threats. With the increasing complexity of malware attacks, our system provides timely protection by analyzing web traffic and files, detecting threats before they can cause harm. By incorporating OSINT data, we stay ahead of emerging threats and offer a powerful tool for safeguarding against malicious activities.

Use case



Disscussion

The successful implementation of our threat detection system opens up avenues for further development and expansion. Moving forward, we envision enhancing the system's capabilities by incorporating more advanced machine learning techniques and leveraging additional OSINT sources. This will enable us to tackle evolving threats and ensure comprehensive protection for our users. Additionally, we plan to explore potential collaborations and partnerships to enhance the scalability and accessibility of our system. To gain a deeper understanding of our project, please scan the QR code provided to access our video demonstration and source code repository:

Youtube

Github

Conclusions

Our project has successfully developed an advanced threat detection system that leverages machine learning and open-source intelligence (OSINT) data. We have achieved our project goals and exceeded the defined targets by delivering a highly accurate and timely protection system. The integration of OSINT data has allowed us to stay ahead of emerging threats, providing a powerful tool for safeguarding against a wide range of cybersecurity attacks. Our user-friendly interface, real-time notifications, and detailed reports contribute to an enhanced cybersecurity posture, offering an effective solution for combating the increasing complexity of malware attacks.