CYBER SECURITY LONG-TERM INTERNSHIP

Smart Internz

Technology Stack: Cyber security with IBM QRadar

Project Title: Leveraging real-time security intelligence for enhanced defence.

Team ID : LTVIP2024TMID14828

Team Size : 4

Team Leader : Mahalakshmi Talabakthula

Team member : Palepu Divya

Register number : SBAP0014840

MY TASK

INTRODUCTION TO REAL-TIME SECURITY INTELLIGENCE

Security intelligence refers to the practice of collecting, standardizing and analysing data that is generated by networks, applications, and other IT infrastructure in real-time, and the use of that information to assess and improve an organization's security posture. Real-time security monitoring is continuously overseeing and analysing the data traffic and activities in an organization's network to detect, alert, and respond to potential security threats as they happen.

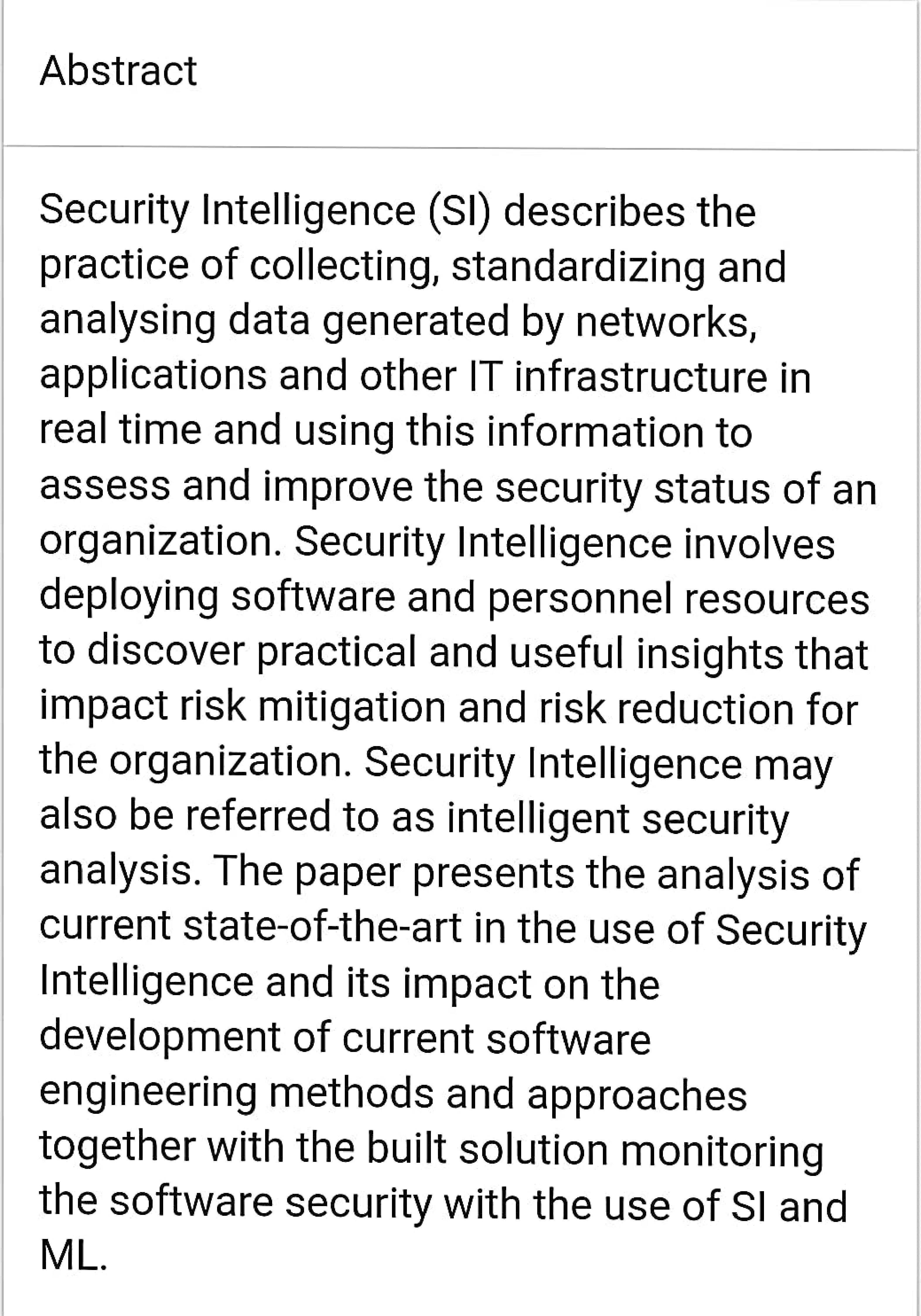
With Security Intelligence solutions, organizations can identify and mitigate those inside threats and many more, by detecting the following: Unauthorized application access or usage. Data loss such as sensitive data being transmitted to unauthorized destinations.

There are a few key principles that define security intelligence:

- Real-Time Analysis
- Pre-Exploit Analysis
- Collection, Normalization, And Analysis
- Actionable Insight
- Scalable
- Adjustable Size And Cost

Security intelligence refers to the practice of collecting, standardizing and analyzing data that is generated by networks, applications, and other IT infrastructure in real-time, and the use of that information to assess and improve an organization's security posture.

... **Security Intelligence** for **Real** - **Time** Security Monitoring Software updates 1 Aneta Poniszewska - Marańdal ( ) Radoslaw Grela1 , and Natalia Kryvinska2 İD ... **Security Intelligence** for **Real**- **Time** Security Monitoring Software 1 **Introduction**.



Abstract

Security Intelligence (SI) describes the practice of collecting, standardizing and analysing data generated by networks, applications and other IT infrastructure in real time and using this information to assess and improve the security status of an organization. Security Intelligence involves deploying software and personnel resources to discover practical and useful insights that impact risk mitigation and risk reduction for the organization. Security Intelligence may also be referred to as intelligent security analysis. The paper presents the analysis of current state-of-the-art in the use of Security Intelligence and its impact on the development of current software engineering methods and approaches together with the built solution monitoring the software security with the use of SI and ML.

Conclusion

Real-time intelligence is a rapidly growing field with significant potential for various industries and applications. Organizations can analyze vast amounts of data in real-time and make informed decisions by leveraging technologies such as machine learning, AI, IoT, edge computing, and predictive analytics.Cyber security is one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, so it is crucial to learn how to defend from them and teach others how to do it too.