MINISTERUL EDUCAȚIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susținere

Șef departament:

Fiodorov Ion, dr., conf. univ.

____

„ ___ ” _______________ 2024

Platformă de monitorizare centralizată a atacurilor cibernetice
Platform for centralized monitoring of cyberattacks

Proiect de master

Student: Obuh Dmitrii, SI – 221M

Coordonator: Bolun Ion, prof. univ., dr. hab.

Consultant: Bulai Rodica, asist. univ.

Chișinău 2024

ADNOTARE

la teza de master cu tema „Platformă de monitorizare centralizată a atacurilor cibernetice” a studentului Obuh Dmitrii, gr. SI-221M

Teza de master include studiul tehnicilor și metodelor de monitorizare și gestionare centralizată a atacurilor cibernetice, precum și dezvoltarea unei platforme adecvate, cu un accent deosebit pe utilizare, securitate și eficiență. Platforma utilizează tehnologii precum Spring Framework, React și OSSEC pentru a oferi o soluție cuprinzătoare pentru monitorizarea și răspunsul la amenințările cibernetice.

Obiectivul principal al acestei teze este de a crea o platformă ușor de utilizat și ușor, cu o infrastructură backend extrem de sigură. Platforma va permite utilizatorilor să își creeze un Cont personal, să acceseze instrumente de monitorizare centralizate și să răspundă la atacuri cibernetice în timp util. Caracteristicile sale de bază includ detectarea atacurilor în timp real, analiza și răspunsul la incidente.

Semnificația acestui proiect rezultă din importanța tot mai mare a securității cibernetice în fața amenințărilor cibernetice în creștere. Pe măsură ce apar noi companii IT în țara noastră, există o nevoie urgentă de a gestiona și proteja eficient datele sensibile. Capacitatea platformei de a asigura monitorizarea centralizată a atacurilor cibernetice va economisi timp și resurse pentru aceste afaceri emergente, reducând obstacolele birocratice asociate cu asigurarea securității informațiilor. Unul dintre obiective este crearea unei platforme scalabile la nivel de stat, care să ofere o oportunitate de a monitoriza securitatea tuturor instituțiilor statului dintr-o singură interfață și de a răspunde rapid la amenințările emergente.

Această teză conține o introducere, cinci capitole cuprinzătoare care acoperă diferite aspecte ale dezvoltării platformei, funcționalitatea acesteia, o concluzie care rezumă constatările, o bibliografie care detaliază sursele la care se face referire și aplicația web reală.

Ca stivă de tehnologie, am folosit Java și Spring Framework pentru a dezvolta backend performant, scalabil și ușor de înțeles, PostgreSQL pentru stocarea rapidă, convenabilă și fiabilă a datelor. Pe frontend, JavaScript și React sunt folosite pentru a crea o interfață de utilizator intuitivă și receptivă.

Cuvinte cheie: atac cibernetic, monitorizare, amenințare, vulnerabilitate, securitate, Spring Framework, Java, React, JavaScript, OSSEC, PostgreSQL.

ANNOTATION

to the master’s thesis on the topic “Platform for centralized monitoring of cyberattacks” of student Obuh Dmitrii, gr. SI-221M

This master's thesis includes the study of techniques and methods of centralized monitoring and management of cyberattacks, as well as the development of an appropriate platform, with a particular focus on usability, security and efficiency. The platform leverages technologies such as the Spring Framework, React and OSSEC to provide a comprehensive solution for monitoring and responding to cyber threats.

The primary objective of this thesis is to create a user-friendly and lightweight platform with a highly secure backend infrastructure. The platform will enable users to set up a personal account, access centralized monitoring tools, and respond to cyberattacks in a timely manner. Its core features include real-time attack detection, analysis and incident response.

The significance of this project arises from the growing importance of cybersecurity in the face of increasing cyber threats. As new IT companies emerge in our country, there is a pressing need to efficiently manage and protect sensitive data. The platform's ability to provide centralized monitoring of cyberattacks will save time and resources for these emerging businesses, reducing the bureaucratic hurdles associated with ensuring information security. One of the goals is to create a platform that is scalable to the state level, which will provide an opportunity to monitor the security of all state institutions from one interface and quickly respond to emerging threats.

This thesis contains of an introduction, five comprehensive chapters covering various aspects of the platform's development, its functionality, a conclusion summarizing the findings, a bibliography detailing the referenced sources, and the actual web application.

As a technology stack, Java and Spring Framework were used to develop performant, scalable and understandable backend, PostgreSQL for fast, convenient and reliable data storage. On the frontend, JavaScript and React are employed to create an intuitive and responsive user interface.

Keywords: Cyberattack, monitoring, threat, vulnerability, security, Spring Framework, Java, React, JavaScript, OSSEC, PostgreSQL.

CONTENTS

INTRODUCTION...7

1 DOMAIN ANALYSIS……………………………………………………………………………9

1.1 Description of the subject area ………………………………………………………………9

1.2 Review of existing analogues………………………………………………………………10

1.3 Choosing a platform for the implementation of the system…………………………………15

1.4 Application areas……………………………………………………………………………16

2 SYSTEM MODELING AND DESIGN………………………………………………………...17

2.1 Context diagrams in IDEF0 notation………………………………………………………..17

2.2 Decomposition diagram in IDEF3 notation…………………………………………………21

2.3 Decomposition diagram in DFD notation…………………………………………………...22

2.4 System use cases……………………………………………………………………………23

2.5 Database design……………………………………………………………………………..25

3 IMPLEMENTATION OF THE SYSTEM………………………………………………………26

3.1 Description of the main purposes of the system……………………………………………26

3.2 Used technologies…………………………………………………………………………...29

4 SYSTEM DOCUMENTATION………………………………………………………………..47

4.1 Login and registration………………………………………………………………………47

4.2 Department management……………………………………………………………………48

4.3 Workstation management…………………………………………………………………...50

4.4 Agent installation……………………………………………………………………………51

4.5 Alert table…………………………………………………………………………………...52

4.6 Notifications…………………………………………………………………………………53

5 PROJECT EVALUATION……………………………………………………………………….54

5.1 Risk analysis based on the OWASP methodology…………………………………………….54

5.2 Valuation………………………………………………………………………………………63

5.3 Impact analysis………………………………………………………………………………...65

CONCLUSION…………………………………………………………………………………....68

BIBLIOGRAPHY…………………………………………………………………………………69

INTRODUCTION

In our modern world, everything seems to have gone digital. It's like a giant web connecting us all, making our lives more convenient. Think about your day. Maybe you wake up to an alarm on your smartphone. You check your emails on your computer, order breakfast through an app, and then get a ride to work using another app. At work, you use a computer for your tasks and maybe even have a video meeting with colleagues from all over the world. When you're done, you shop online, watch movies on streaming platforms, and chat with friends on social media. Even when you're not working or socializing, you might use a fitness tracker or smart home devices like thermostats and lights. And that’s not all. Everything is more dependent on information technology than it may seem at first glance. Every modern person, small business, huge organization counts on free and access to their sensitive information at any time, while having confidence that the data will remain protected and unharmed. States store the most important information about their citizens in digital form. Many domestic and international processes critically depend on compliance with the CIA triad. This abbreviation stands for confidentiality, integrity and availability - the three key principles of information security. We should always remember that this digital world also has a dark side. There are people out there who want to break into our digital lives, steal our information, and cause all sorts of trouble. These troublemakers are known as cyberattackers, and they're a big problem.

Imagine what could happen if our digital world was suddenly under attack. Hackers could steal your personal information, like your passwords and bank details. They could shut down power grids, causing blackouts across entire cities. They could even tamper with medical devices or disrupt emergency services, putting people's lives at risk. The more we rely on technology, the more we have to lose if something goes wrong. That's why the topic of centralized management of cyberattacks is incredibly important and relevant. It's like having a team of experts who watch over our digital world and keep us safe. Without this, we're vulnerable to all sorts of digital disasters.

To make our digital world a little bit safer, a platform is going to be created, which is like a powerful tool, to help monitor, manage, react to and consequently stop ongoing cyberattacks. The tool will do several important things:

- Monitoring

  Just like security cameras watch over a building, this platform will watch over our digital systems. It will keep an eye out for any unusual activity that might signal a cyberattack.

- Detection

  When something suspicious happens, the platform will use its detective skills to figure out if it's a real threat or just a false alarm. This helps us focus on what's important.

- Response

  If a cyberattack is happening, the platform will act quickly to stop it. It's like calling the police when there's trouble.

- Coordination

  Our digital world is big, and many organizations and people are part of it. This platform will help coordinate efforts to stop cyberattacks.

- Learning

  Just like we learn from our experiences, this platform will learn from cyberattacks. It will become smarter and better at protecting us over time.

In general, there are several main goals to be achieved within the framework of this master's thesis:

- various mechanisms and techniques for detecting cyberattacks will be studied, as well as ways to monitor them;
- as it is mentioned above, the plan is to create a platform for centralized monitoring of cyberattacks;
- to share valuable insights gained while working on the thesis;
- to raise awareness about the importance of centralized cyber threat management and the potential benefits it offers.

The thesis consists of an annotation, content, introduction, five main chapters (domain analysis, system modeling and design, implementation of the system, system documentation, project evaluation), conclusion, list of sources used and appendices. Domain analysis explores the background and context of the research domain, reviews relevant literature and existing research to establish a foundation for the study. System modeling and design describes the theoretical framework, models used in the development process, contains diagrams which represent solutions and discusses the design choices. Implementation of the system details the actual development and implementation of the proposed system, provides insights into the technologies and tools. System documentation offers comprehensive documentation for the developed system and provides information to facilitate understanding, maintenance and potential future enhancements. Project evaluation estimates costs, discusses the outcomes, benefits and limitations of the project.

BIBLIOGRAPHY

1. I. H. Sarker, “Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview,” SECURITY AND PRIVACY, vol. 6, no. 5, p. e295, 2023, doi: 10.1002/spy2.295.
2. “Malware Attacks,” CyberArk. Accessed: Sep. 06, 2023. [Online]. Available: https://www.cyberark.com/what-is/malware/
3. “Password Attack - Definition, Types and Prevention.” Crashtest Security. Accessed: Sep. 10, 2023. [Online]. Available: https://crashtest-security.com/password-attack/
4. “What Is a Man-in-the-Middle Attack? Prevention Tips and Guide,” UpGuard. Accessed: Sep. 15, 2023. [Online]. Available: https://www.upguard.com/blog/man-in-the-middle-attack
5. A. Falor, M. Hirani, H. Vedant, P. Mehta, and D. Krishnan, “A Deep Learning Approach for Detection of SQL Injection Attacks Using Convolutional Neural Networks,” in Proceedings of Data Analytics and Management, D. Gupta, Z. Polkowski, A. Khanna, S. Bhattacharyya, and O. Castillo, Eds., in Lecture Notes on Data Engineering and Communications Technologies. Singapore: Springer, 2022, pp. 293–304. doi: 10.1007/978-981-16-6285-0_24.
6. “What is a denial of service attack (DoS)?” Palo Alto Networks. Accessed: Sep. 17, 2023. [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
7. “Malwarebytes for business,” Malwarebytes. Accessed: Sep. 21, 2023. [Online]. Available: https://www.malwarebytes.com/business
8. “ESET Endpoint Security,” ESET. Accessed: Sep. 21, 2023. [Online]. Available: https://www.eset.com/md-ru/business/download/endpoint-security-windows/
9. “Endpoint Protection & Business Antivirus Software,” Webroot. Accessed: Sep. 23, 2023. [Online]. Available: https://www.webroot.com/us/en/business/products/endpoint-protection
10. “The CrowdStrike Falcon,” CrowdStrike. Accessed: Sep. 23, 2023. [Online]. Available: https://www.crowdstrike.com/falcon-platform/
11. “Bitdefender GravityZone,” Bitdefender. Accessed: Sep. 23, 2023. [Online]. Available: https://www.bitdefender.co.th/resources/GravityZoneEnterprise/Current/Documentation/en_US/Bitdefender_GravityZone_InstallationGuide_7_enUS.pdf
12. “Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution.” Zabbix. Accessed: Sep. 24, 2023. [Online]. Available: https://www.zabbix.com/

13. P. Stegeby, “Intrusion Detection systems : A comparison in configuration and implementation between OSSEC and Snort”, Dissertation, 2023.
14. “Lesson 2: Introduction to Spring IoC container,” Spring Projects. Accessed: Oct. 01, 2023. [Online]. Available: https://spring-projects.ru/guides/lessons/lesson-2/
15. “How is PostgreSQL better than other open source SQL databases. Part 1,” Habr. Accessed: Oct. 10, 2023. [Online]. Available: https://habr.com/ru/articles/282764/
16. “Styled Components — perfect styling of the React application,” Tproger. Accessed: Oct. 22, 2023. [Online]. Available: https://tproger.ru/articles/styled-components-idealnaja-stilizacija-react-prilozhenija/
17. “Advantages of PostgreSQL,” Bitnine Global Inc. Accessed: Nov. 03, 2023. [Online]. Available: https://bitnine.net/blog-postgresql/advantages-of-postgresql/
18. “Why use Spring?” Stack Overflow. Accessed: Nov. 11, 2023. [Online]. Available: https://ru.stackoverflow.com/questions/428719/Зачем-использовать-spring
19. “Java Spring Pros and Cons,” Javatpoint. Accessed: Nov. 14, 2023. [Online]. Available: https://www.javatpoint.com/java-spring-pros-and-cons
20. “What is SWOT analysis and why a business needs it,” Unisender. Accessed: Nov. 17, 2023. [Online]. Available: https://www.unisender.com/ru/glossary/shto-takoe-swot-analiz/
21. R. W. Puyt, F. B. Lie, and C. P. M. Wilderom, “The origins of SWOT analysis,” Long Range Planning, vol. 56, no. 3, p. 102304, Jun. 2023, doi: 10.1016/j.lrp.2023.102304.