

جامعة جدة
University of Jeddah

University of Jeddah
College of Computer Science and Engineering
Department of Software Engineering

CCSW 223: Software Engineering

Security Service Provider

Table of Contents

Cover Page	3
Introduction	4
Lab 2 - Information Gathering	5
Lab 3 - Planning Phase 1	18
The Purpose of the Process	19
Recommendation or proposed solution	21
Cost & schedule estimates	21
Lab 4 - Planning Phase 2	22
Feasibility study	23
Project plan	27
Lab 5 - Analysis Phase 1	28
Context Diagram	29
The scope of the work	30
Context diagram	32
Lab 6 - Functional and Non-functional Requirements	34
Functional Requirements	35
Non Functional Requirements	36
Lab 7 - Analysis Phase 2	37
Use case diagram	38
List of Scenarios	39
Lab 8 - Analysis Phase 2	42
Sequence Diagram & Flow Description	43
Lab 9 - Modeling Phase	48
Class Diagram and Description	49
Recommendations	53

Security Service Provider

Prepared by:

Lena Alsinani 2210669

Boshra Alghamdi 2211385

Dania Taj 2210829

Raghad Fuad 2210302

Joud Alotaibi 2211837

Shaima Mohammed 2211268

Introduction

In light of the emerging 2030 vision, many startups and small businesses are experiencing rapid growth. However, due to budget constraints, these companies often find it challenging to establish a dedicated cybersecurity department, leading to a neglect of crucial data and information security measures. This oversight exposes them to the significant risks of data loss and hacking, ultimately jeopardizing the success of the company. Therefore, we decided to create an application that provides security for small businesses and companies to protect their data with the least cost possible, our goal is to ensure that even companies with limited resources can safeguard their sensitive information.

Security Service Provider

CCSW 223

Lab 2 Information Gathering



[C2]

Student	ID
Lena Alsinani	2210669
Boshra Alghamdi	2211385
Dania Taj	2210829
Raghad Fuad	2210302
Joud Alotaibi	2211837
Shaima Mohammed	2211268

Group Leader: Boshra Alghamdi

Editor: Lena Alsinani

a. Evaluation of a User Request

Name: Mr. Nader Alsinani

Job: IT & Digital Services Director at Saudi Downtown Company

Date: 31 January 2024

Email: nalsinani@saudidowntown.com.sa

Interviewer: Boshra Alghamdi

b. Description of the problem

I asked questions to Mr. Nader, the most important of which were:

1- What is the purpose of the department of cyber security? What are you aiming to accomplish?

First, as a company we have to meet the national regulations in Saudi Arabia. second, we have to protect the company's data and information and also to prevent the company's assets or data of being lost or hacked. We're aiming of having a safe and secure environment and also to make sure to achieve business continuity through cybersecurity so there will be no business interruption because of a hack or ransomware.

2- How do you measure the posture of cyber risk?


First, you have to make a self-assessment and from that self-assessment you create a risk register that will address all of the risks, what is the potential of exposure, what is the treatment plan and the timeline for the plan.

3- What kinds of risks do you encounter on a daily basis and find difficult to handle?

Phishing, when employees receive phishing emails they fall for it, or they fall for ransomware. Another risk is insider threat due to lack of awareness.

4- What kind of dangers did you face as a result of the employee's apathy?

Data leakage, because they don't take cybersecurity seriously and when they follow suspicious emails, they don't report it to the cybersecurity team.



5- Are there any specific types of data or information that you believe require extra protection? If so, what measures would you suggest to enhance their security?

Yes, we set something called data classification which is a tool to classify data from top confidential to public. We have to implement tools such as DLP (data loss prevention) then we set the settings as to what happens with this data

c. Analyst comments

Based on the responses that I have received I figured that a cybersecurity department is very important to have in each company due to the great amount of risks and threats that the company encounter on a daily basis that might jeopardize the company's workflow. Also I have discovered that awareness to employees is so important because if they're not aware of the risks enough the data and information will get hacked or lost.

a. Evaluation of a User Request

Name: Mrs. Safaa Khawaji

Job: Head of C&W Transformation program manager at STC

Date: 31 January 2024

Email: skhwji@stc.com.sa

Interviewer: Lena Alsinani

b. Description of the problem

I asked questions to Mrs. Safaa, the most important of which were:

1- What is the purpose of the department of cyber security? What are you aiming to accomplish?

First, in STC we don't only have a department, there is a whole sector for Cyber security, considering STC a very sensitive business that relies on data. Especially, customer data plus our services are all digital. Therefore, you have to protect this data.

We have to protect our business so it can run smoothly. Plus we have to gain the customer's trust, lastly and most importantly there are regulations on data provided from SDAIA that we have to follow.

2- How do you measure the posture of cyber risk?


To measure the risks, we have to know what are the security systems that are implemented. Also, to perform a penetration test and compliance. Plus test the maturity level by assessing and seeing at which level the company is. then, put a plan to achieve a higher maturity level.

3- What kinds of risks do you encounter on a daily basis and find difficult to handle?

Our system gets attacks through email or through external access. therefore, it's important to have a STC security system implemented in the device when opening emails or systems or working remotely

4- What kind of dangers did you face as a result of the employee's apathy?

Most employees receive phishing emails, and they fall for them due to their apathy even though our company spread awareness. It's one of the things that we focus on constantly.



5- Are there any specific types of data or information that you believe require extra protection? If so, what measures would you suggest to enhance their security?

The data that must have high protection is the customer data that have to do with payment, in STC we have the STC pay service so its important to protect the customer information considering that is bank information. To protect this information, we must have regulations that the company should follow. Also, to protect the areas containing data servers there must be restricted access for employees.

c. Analyst comments

Mrs.Safaa responses made me aware of how much a cybersecurity department or sector is important when your business relies on data and the services, you're providing are digital, also she pointed out that it's important to gain our customer's trust due to our secure systems. And even though STC focuses on spreading cyber awareness still some employees fall for the phishing emails so it's also important to provide training. Another thing to consider is when data has to do with payment we have to focus on their security even more.

a. Evaluation of a User Request

Name: Mr. Mohammed Talal

Job: Software engineer

Date: 1 February 2024

Email: muhdtalal16@gmail.com

Interviewer: Dania Taj

b. Description of the problem

I asked questions to Mr. Mohammed, the most important of which were:

1- How would you rate the current level of security in your company when it comes to protecting corporate information from hacking on a scale of 1 to 10?

I would rate the current level of security in our company as an 6 out of 10. While we have implemented robust security measures such as firewalls, encryption, and regular security audits, there is always room for improvement and the threat landscape is constantly evolving.

1- What is the CEO manager's greatest concern happens to the information?


The CEO's greatest concern is likely the potential loss or compromise of sensitive corporate information, which could result in financial loss, damage to reputation, and legal consequences.

2- What are the most critical vulnerabilities or weaknesses you have identified in your current security infrastructure?

Some critical vulnerabilities or weaknesses in our current security infrastructure include potential gaps in employee training on cybersecurity best practices, outdated software or systems that may have known vulnerabilities, and the need for better access control mechanisms to limit unauthorized access to sensitive data.

3- What kinds of risks do you encounter on a daily basis and find difficult to handle?

On a daily basis, we encounter risks such as phishing attempts, malware infections, and potential insider threats. These risks can be difficult to handle due to their evolving nature and the need for constant vigilance and proactive measures to mitigate them effectively.



5- What is the most essential feature you should look for in an app that protects your company, if you have the opportunity to download one?

The most essential feature we should look for in an app that protects our company is robust threat detection and prevention capabilities. This includes real-time monitoring for suspicious activities, advanced threat intelligence to identify emerging threats, and the ability to automatically block or mitigate security incidents before they cause harm.

c. Analyst comments

In light of Mr. Mohhamed's insights, it can be inferred that while small companies may establish a security system, it is susceptible to numerous intrusions. Consequently, our application should prioritize the proactive detection and prevention of threats before their occurrence.

a. Evaluation of a User Request

Name: Mr. Fahad Abdulwahid

Job: IT support technician

Date: 31 January 2024

Email: Fahad722@hotmail.com

Interviewer: Raghad Najmuldeen

b. Description of the problem

I asked questions to Mr. Fahad, the most important of which were:

- 1- How would you rate the current level of security in your company when it comes to protecting corporate information from hacking on a scale of 1 to 10?
6 out of 10.
- 2- What is the CEO manager's greatest concern happens to the information?
losing all of our clients' data, which would cause us to lose their trust.
- 3- What are the most critical vulnerabilities or weaknesses you have identified in your current security infrastructure?
Unknown network assets, it is unknown devices that are on network that have not been identified by our IT administrators, so it is hard for us to recognize the device and take action.
- 4- What kinds of risks do you encounter on a daily basis and find difficult to handle?
Free Wi-Fi, which make the employees connect their personal devices to the network when they could be hacked, so it will have impact in the sensitive data on our company.
- 5- What is the most essential feature you should look for in an app that protects your company, if you have the opportunity to download one?
We look for an app that can be reliable and have the ability to protect, detect and prevent our company from internal and external threats.



c. Analyst comments

According to Mr. Fahad's answers, it's evident that small companies possess a certain level of security infrastructure, but due to the fact that they are a primary target for hackers and attackers, since small companies can't afford to allocate enough resources for security. therefore, necessitating a dependable and cost-effective solution within our application to fortify their security measures

a. Evaluation of a User Request

Name: Mr. Abdullah Algamdi

Job: Web Developer

Date: 1 February 2024

Phone number: 0500469186

Interviewer: Shaima Alamoudi

b. Description of the problem

I asked questions to Mr. Abdullah, the most important of which were:

1- What are the most common types of security threats or vulnerabilities you encounter in systems?

Lack of employee awareness - Lack of a specialized department for cyber - Systems are often old, such as Windows 7, which is full of vulnerabilities - Lack of sufficient protection program.

2- When the threats occurs, what is important to do first?

Isolating the infected systems and trying to isolate the important data and also separating it from the rest of the systems and trying to extract the important data or format it.

3- Are there any specific security tools or technologies you believe would greatly enhance our program's effectiveness? If so, which ones and why?

IDS, IPS, firewall and antivirus

4- What kind of monitoring tools are in place to detect suspicious activities?

(SIEM) help detect suspicious activities, in addition to IPS and IDS, as I mentioned previously, they are systems that help detect intrusion.

5- What additional security measures or features do you think our program should have to better protect corporate information?

Updating systems periodically - educating employees against the dangers of electronic attacks



c. Analyst comments

Based on what Mr. Abdullah said, all employees must be aware in advance of the types of attacks and vulnerabilities. They are partners in making the company safe with their awareness, in addition to some important programs that help in discovering vulnerabilities or threats early to avoid damage. There must also be updates Periodicity of all systems and devices to reduce the incidence of attacks and security threats.

a. Evaluation of a User Request

Name: Dr. Hanan Nadem

Job: Professor at Jeddah university

Date: 1 February 2024

Email: hanadeem@uj.edu.sa

Interviewer: Joud Alotaibi

b. Description of the problem

I asked questions to Mr. Abdullah, the most important of which were:

1- What are the most common types of security threats or vulnerabilities you encounter in systems?

We have faced an encounter number of threats in systems. one of them is Soping. which is basically is when someone or something pretends to be something else to gain confidence, get access to the systems, steal data, steal money, or spread malware. We also witnessed another malicious attack which is man-in middle.

in this attack, the communications between two parties are intercepted, often to steal login credentials or personal information, spy on victims, sabotage communications, or corrupt data.

2- When the threats occur, what is important to do first? prevent or detect

First, taking control back. When a threat occurs is essential for minimizing damage, preventing escalation, restoring normal operations, protecting sensitive information, complying with legal requirements, and rebuilding trust. It is a proactive approach to cybersecurity that focuses on swift and effective response to mitigate the impact of the threat.

3- Are there any specific security tools or technologies you believe would greatly enhance our program's effectiveness? If so, which ones and why?

We have proxies that provide security by hiding the internal network from the internet. Also, firewall to prevents unauthorized access to the computer by blocking ports and programs.

4- What kind of monitoring tools are in place to detect suspicious activities?

For example, Intrusion detection system. It monitors network traffic and searches for known threats and suspicious or malicious activity.



5- What additional security measures or features do you think our program should have to better protect corporate information?

Simply, starting with verifying the authentication for people. For example, two factor of passwords, Credential, Also the regulations that you implemented.

6- What are the industry standards and regulations that should be implemented at any app that provide security to the organization?

First you have to know the vulnerability to each system that up to date, so you can implement and provide best services

c. Analyst comments

As professor Hanan, a cyber security expert, it's critical to stay updated on any potential threats or weaknesses in order to effectively apply security measures and safeguard confidential information. Furthermore, the significance of taking back control to prevent the attacker from seriously harming the system.

Security Service Provider

CCSW 223

Lab 3 Planning Phase 1



[C2]

Student	ID	Task
Lena Alsinani	2210669	Recommendations and cost
Boshra Alghamdi	2211385	Recommendations and cost
Dania Taj	2210829	The problem and Findings
Raghad Fuad	2210302	Consideration
Joud Alotaibi	2211837	Goals
Shaima Mohammed	2211268	Motivation and Consideration

Group Leader: Boshra Alghamdi

Editor: Lena Alsinani

The purpose of the project

a. The User Business or Background of the Project Effort

Content

With the escalating threats of cyber-attacks, data breaches, and ransomware, small companies often overlook their cybersecurity posture. In response, a comprehensive cybersecurity application has been developed. This application empowers businesses to assess and fortify their digital defenses, ultimately safeguarding their sensitive information and preserving their reputation.

Motivation

In the era of progress and development and the presence of security risks and cyber attacks on individuals or startup companies, the necessary protection must be provided to prevent their occurrence.

Considerations

The problem we aim to address with our cybersecurity application is significant. Many startup companies encounter challenges in establishing an integrated cybersecurity department due to limited resources or expertise. As a result, they struggle to provide protection for their sensitive data and assets. Our solution provides an alternative by offering a comprehensive application or system designed to safeguard against cyber threats efficiently and affordably.

b. Goals of the Project

We developed this application because some startup companies can't provide a cybersecurity department. Also, to address the limitations faced by small companies in securing their data effectively. By offering affordable pricing, our application caters to the needs of these entities. It installs on employees' devices, safeguarding both company and personal data from various cyber threats. This approach ensures that even companies with limited resources can benefit from the protection we're providing.

c. Preliminary report

The problem

The current system faces numerous security challenges, putting the company's software at risk of hacking. These issues include slow software updates, making it vulnerable to known attacks, weak controls on who can access what, making it easier for unauthorized people to get in, and reliance on outdated software, which can be exploited by attackers. If we were to establish a dedicated cybersecurity department to address these problems, it would require a substantial investment in terms of hiring skilled professionals, implementing advanced security technologies, and conducting regular audits and assessments. Such an investment would impose a significant financial burden on the company, highlighting the urgent need for improved protection measures to safeguard the company's software assets.

Findings

- **Lack of Employee Training:** Without proper training, employees may not understand the importance of cybersecurity or recognize potential threats. They may inadvertently click on malicious links in phishing emails, share sensitive information, or neglect security best practices, leaving the company vulnerable to cyberattacks.
- **Lack of Security of Sensitive Data:** Failing to adequately secure sensitive data puts the company at risk of data breaches, which can lead to financial loss, and damage to reputation.
- **Weak Access Control:** Weak access controls make it easier for unauthorized users to gain access to sensitive systems and information. Without proper authentication mechanisms, strong password policies, and role-based access controls, malicious actors could exploit these vulnerabilities to infiltrate the network, steal data, or disrupt operations.
- **Lack of Intrusion Detection:** Without robust intrusion detection mechanisms, the organization may not be able to detect and respond to unauthorized access attempts or suspicious activities in a timely manner.

Recommendation or proposed solution

- **Firewalls:** Firewalls and network security appliances help monitor and control incoming and outgoing network traffic to prevent unauthorized access and protect against cyber threats.
- **Antivirus and Antimalware:** These tools help detect and remove malicious software, such as viruses, worms, and spyware, from computers and networks.
- **Data Encryption Tools:** Encryption tools encrypts sensitive data to protect it from unauthorized access, both at rest and in transit. This helps ensure the confidentiality and integrity of client data.
- **Identity and Access Management (IAM) Solutions:** IAM tools help manage user identities, access rights, and authentication methods to prevent unauthorized access to systems and data.
- **Intrusion Detection:** Deploy intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic for signs of unauthorized access or malicious activity.
- **Employee Training:** Implement regular cybersecurity training programs for all employees to educate them about the importance of cybersecurity, common threats, and best practices for protecting sensitive information.

Cost & schedule estimates

The project will approximately cost 150,000 SAR and the estimated duration is 33 weeks

Tasks	Estimated cost	Estimated duration
Project Planning	13,000SAR	2 weeks
Project Analysis	15,000SAR	3 weeks
Design	35,000SAR	6 weeks
Implementation	50,000SAR	16 weeks
Testing	20,000SAR	4 weeks
Maintenance	20,000SAR	2 weeks
Total	153,000SAR	33 weeks

Security Service Provider

CCSW 223

Lab 4 Planning Phase 2



[C2]

Student	ID	Task
Lena Alsinani	2210669	Cost and benefits - Recommended alternative
Boshra Alghamdi	2211385	Alternative solutions
Dania Taj	2210829	Software impacts
Raghad Fuad	2210302	Potential changes
Joud Alotaibi	2211837	Problem definition
Shaima Mohammed	2211268	Scope objectives

Group Leader: Boshra Alghamdi

Editor: Lena Alsinani

Feasibility study

Problem Definition

The main problem is that small companies that are unable to provide a dedicated cyber security department are more vulnerable to attacks and the risk of hacking, which leads to easy access for unauthorized people, insecurity of sensitive data of the company and employees, and the company's exposure to financial risks. This problem may branch out into other problems such as the ease of access of malware to the company, the disruption of the company's work, the non-disclosure of intrusion, and poor access control. To impose a dedicated cybersecurity section will require a significant financial burden on the company.

Scope Objectives of “new system”

“**Security Service Provider**” is an application designed to strengthen the digital defenses of individuals and companies, offering complete security against cyberattacks. It also provides many defense programs that deter and reduce cyber attacks and risks to protect users' devices from intrusions. Furthermore, it can identify questionable activities and dangerous connections that might result in device hacking and immediately remove them directly to ensure that no breach happens as a result of a user or employee ignorance.

What distinguishes Security Service Provider from other applications:

- Cost-Effectiveness for Startups
- User-Friendly Interface and Ease of Use
- Advanced Threat Detection and Response Capabilities
- Scalability and Adaptability to Growth

Alternative Solutions

1- Implement Cloud-Based Security:

- Cloud service providers offer built-in security features that can help protect startup companies' infrastructure and data. Utilizing cloud security services can enhance security.

2- Regular Security Updates and Patch Management:

- Ensuring that software and systems are regularly updated with the latest security patches and updates can help protect against known vulnerabilities. Startups should implement robust patch management processes to address security vulnerabilities promptly.

3- Invest in Employee Training and Awareness:

- Startups can educate their employees about cybersecurity best practices, phishing awareness, and data protection measures to reduce the risk of human error.

4- Conduct Regular Security Risk Assessments:

- Regularly conducting comprehensive security risk assessments can help startups identify and prioritize cybersecurity risks based on their potential impact and likelihood. Risk assessments can inform decision-making and resource allocation for cybersecurity initiatives.

Cost and benefits of Alternatives

Alternatives	Cost	Benefits	Drawbacks
Implement Cloud-Based Security	100,000SAR	scalability, cost-effectiveness, and accessibility	data privacy concerns, dependency on internet connectivity, and security risks
Regular Security Updates and Patch Management	150,000SAR	vulnerability mitigation, and improved security	operational disruptions, resource intensiveness, and the risk of patching errors
Invest in Employee Training and Awareness	20,000SAR	risk reduction, improved security culture	resource intensiveness and resistance to training
Conduct Regular Security Risk Assessments	15,000SAR	identifying vulnerabilities and prioritizing security	resource intensiveness, complexity, and subjectivity

Software impacts

Several considerations need to be taken into account, including additions and modifications to existing software and supporting systems:

1. **Real-time Monitoring:** Enhance existing monitoring systems to integrate with the app, allowing real-time monitoring of software activities for anomalies or suspicious behavior.
2. **Automated Patch Management:** Integrate automated patch management functionality to ensure timely updates and patches for software vulnerabilities across the organization's systems.
3. **Access Control Mechanisms:** Enhance existing access control mechanisms to enforce least privilege access and ensure only authorized personnel can interact with critical software systems.
4. **Incident Response Integration:** Modify existing incident response protocols to seamlessly integrate with the app, allowing for rapid response and mitigation of software-related incidents.
5. **Integration with Security Information and Event Management (SIEM):** Integrate the app with existing SIEM systems to aggregate and correlate security events across the organization's software environment for comprehensive threat analysis.
6. **Background Process Management:** Implement background process management capabilities to prioritize critical tasks and prevent memory-intensive processes from impacting system performance.

Potential Changes in the Organization

the changes and variations this application will implement in the system to enhance cybersecurity measures include:

1. awareness: Our cybersecurity platform offers valuable insights and best practices for enhancing digital security awareness. You'll have access to resources and educational materials to better understand cybersecurity risks and preventive measures, assisting you to make informed decisions to safeguard your digital assets.
2. Seamless collaboration : You can easily share your cybersecurity assessment results with IT professionals and stakeholders through our app. This streamlined communication enables prompt evaluation and collaboration to address security gaps and strengthen your digital defenses effectively.
3. alerts: Our application ensures you receive timely reminders for cybersecurity assessments. These notifications keep you informed about the importance of regular security checks, empowering you to stay ahead of emerging threats and maintain a resilient cybersecurity framework.
4. threat detection: By utilizing our application for regular cybersecurity checks, you can promptly detect any anomalies or potential threats. The app's analysis can flag issues such as malware intrusions, network vulnerabilities, or other security breaches, allowing for proactive mitigation measures.

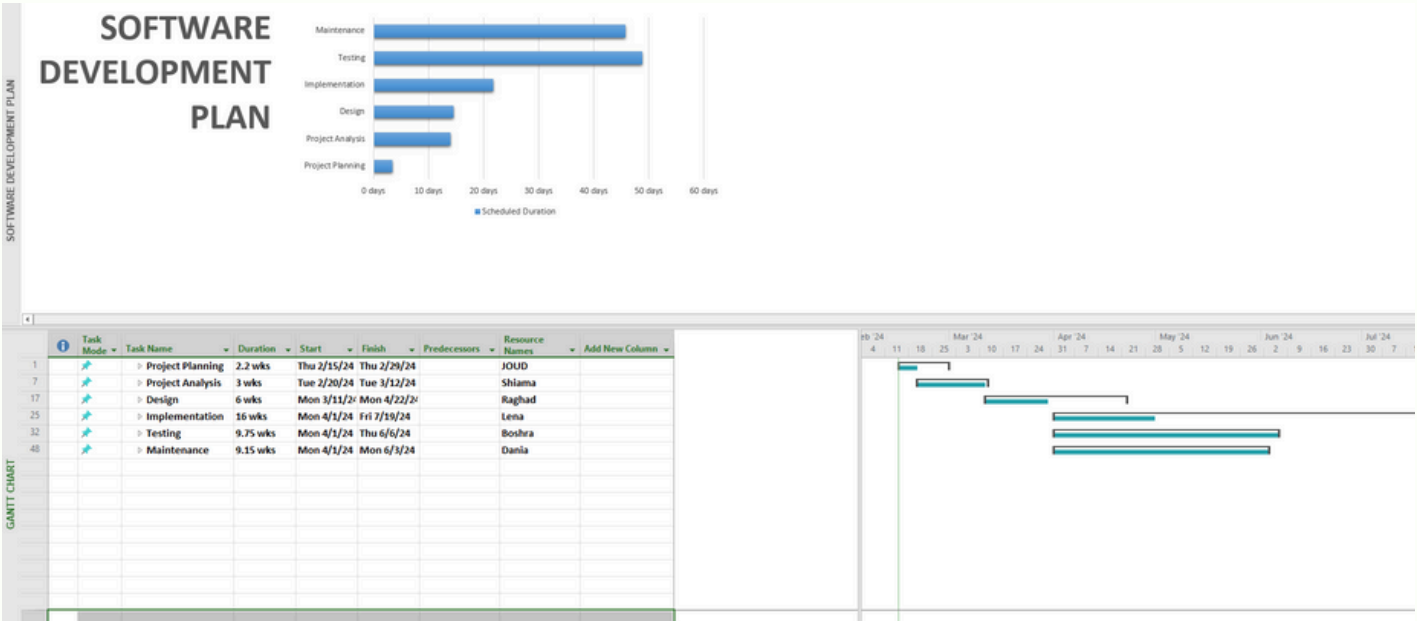
In summary, our cybersecurity application provides a comprehensive solution for proactive threat management and defense. By utilizing our platform, businesses can efficiently monitor their cybersecurity posture, detect threats early, and take effective measures to safeguard their digital assets.

Recommended Alternative of the course of Action

Given the difficulties and costs associated with a cybersecurity department, we recommend that Conducting Regular Security Risk Assessments is the best alternative.

Conducting regular security risk assessments is the best alternative for organizations seeking to maintain a strong cybersecurity posture. It enables proactive identification of vulnerabilities, tailored risk mitigation strategies, compliance adherence, informed decision-making, continuous improvement, and a holistic approach to security. By prioritizing regular risk assessments, organizations can effectively manage cybersecurity risks and protect their assets, reputation, and stakeholders from potential cyber threats.

Project plan



Security Service Provider

CCSW 223

Lab 5 Analysis Phase 1



[C2]

Student	ID	Task
Lena Alsinani	2210669	Content and Motivation
Boshra Alghamdi	2211385	Diagram
Dania Taj	2210829	Business Event list
Raghad Fuad	2210302	Content
Joud Alotaibi	2211837	Client and Customer
Shaima Mohammed	2211268	Other Stakeholder and Motivation

Group Leader: Boshra Alghamdi

Editor: Lena Alsinani

Context Diagram

Stockholder definition

The Client

Individuals with security inclinations including managers, employees, programmers and the National Cybersecurity Authority.

The Customer

Individuals who are interested in protecting their information or small companies that lack a security department are considered customers.

Other Stakeholder

Hospitals, Ministry of education, banks, telecommunications companies (STC), Ministry of Health, Ministry of Finance.

The scope of the work

a. The Current Situation

Content

The current system lacks security measures, so there are many vulnerabilities that invite harmful incidents. Without robust defenses, the system becomes an easy target for malicious actors seeking to exploit its weaknesses. Hackers take advantage of the lack of protection to access important data and disrupt operations. Malicious software spreads freely and causes problems across networks. When the system's defenses fail, it leads to serious breaches, resulting in the exposure of confidential information and destroy trust among users and stakeholders.

Motivation

In our application, we will need all the tools and programs that will provide the necessary protection for the user and companies such as vulnerability detection systems, intrusion detection, anti-virus programs and other programs that will enhance protection and reduce the chances of risks associated with cyberattacks.



b. The Context of the Work

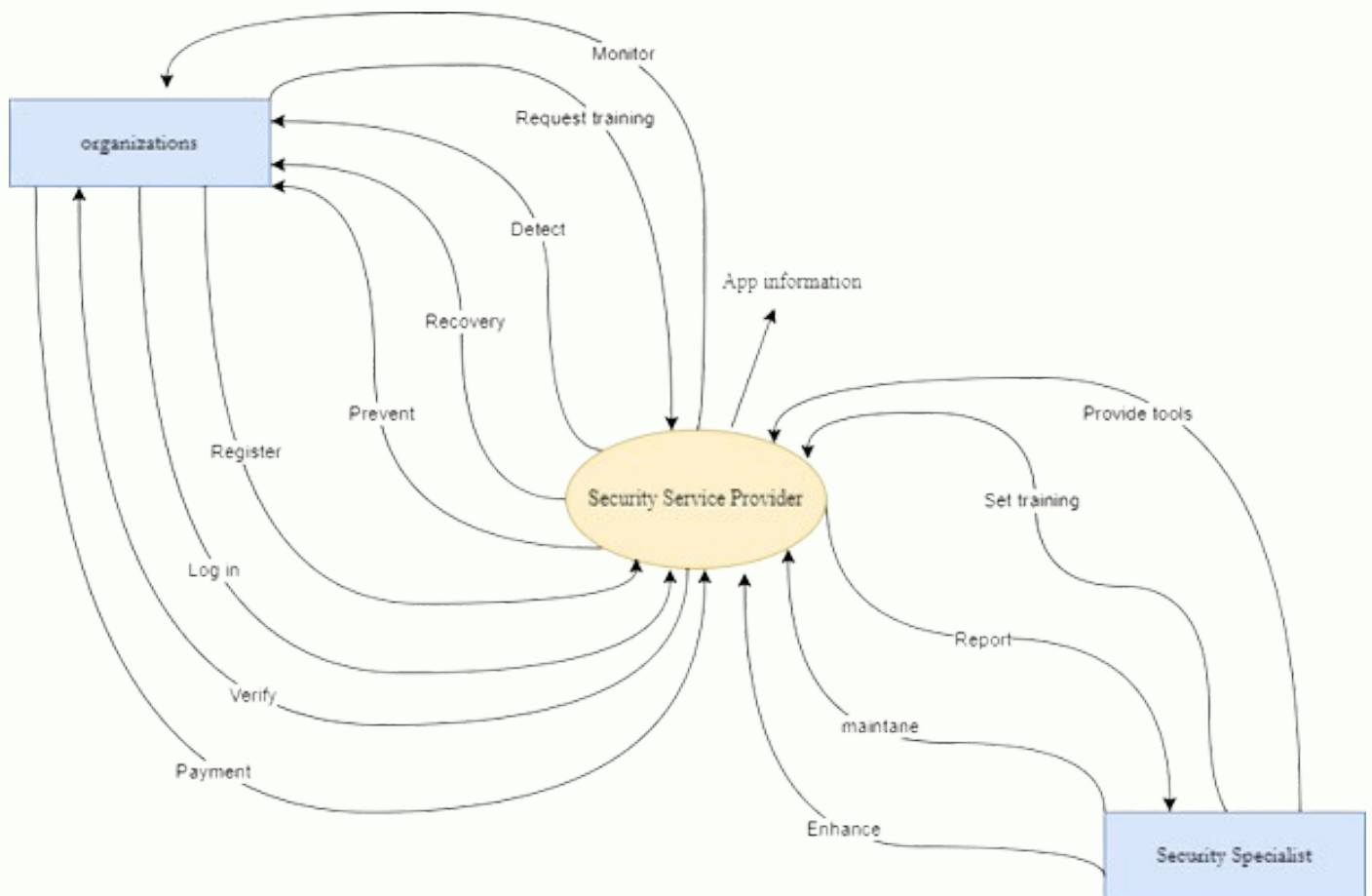
Content

Our cybersecurity application provides a robust response to the escalating landscape of cyber threats, offering advanced technology solutions at a competitive price. By utilizing our platform, businesses can comprehensively evaluate and strengthen their digital defenses. This proactive approach not only protects sensitive information but also ensures scalability and flexibility in maintaining a robust cybersecurity posture. Companies can effectively mitigate the risks associated with cyber-attacks, adapting their defenses to evolving threats and ensuring a resilient cybersecurity infrastructure.

Motivation

In the future, our app will provide hardware protection through features such as device encryption, remote wipe capabilities, and secure boot processes. Additionally, we'll implement tamper detection mechanisms and firmware integrity checks to safeguard against unauthorized access and tampering. With these advanced security measures in place, users can trust that their devices are shielded from potential threats, ensuring peace of mind and reliable operation.

Context diagram



Event Name	Input and Output	Summary
1. Request training	Request training (in)	Organizations can request training for employees through the application
2. Detect	Detect (out)	The application detects vulnerabilities and attacks
3. Monitor	Monitor (out)	The application monitors the data of the organizations.
4. Recovery	Recovery (out)	The application helps the system recover after any kind of attacks
5. Register	Register (in)	The organization enters the data required to register in the application
6. Login	Login (in)	employees of the organizations access the application through login credentials.
7. Prevent	Prevent (out)	The application prevents attacks that happen to the system
8. Verify	Verify (out)	the application confirms the identity of the individual
9. Payment	Payment (in)	The organization pays for the application services
10. Provide tools	Provide tools (in)	The security specialist supplies security tools to the application
11. Set training	Set training (in)	The security specialist choose training sessions for the application to enable its sale to organizations.
12. Report	Report (out)	the application provides reports about the organization to the security specialist
13. Maintain	Maintain (in)	The security specialist oversees maintenance of the application
14. Enhance	Enhance (in)	The security specialist improves the application
15. App information	App information (out)	The client will get the application information

Security Service Provider

CCSW 223

Lab 6

[C2]

Student	ID	Task
Lena Alsinani	2210669	Functional Requirements
Boshra Alghamdi	2211385	Functional Requirements
Dania Taj	2210829	Non Functional Requirements
Raghad Fuad	2210302	Non Functional Requirements
Joud Alotaibi	2211837	Functional Requirements
Shaima Mohammed	2211268	Functional Requirements

Group Leader: Boshra Alghamdi

Editor: Lena Alsinani

Functional Requirements

ID	Requirement Definition
FR1	Create an account
FR1.1	The user shall be able to create an account using their email.
FR2	Login
FR2.1	the user shall be able to login using their username and password.
FR3	Password verification
FR3.1	The user shall receive a password verification message on their email.
FR4	Detect threats
FR4.1	The system shall provide tools to detect threats to the user.
FR5	Prevent attacks
FR5.1	The system shall provide software to prevent attacks targeting the user.
FR6	Report incidents
FR6.1	The user should be able to report incidents if occurred.
FR7	Track Security System
FR7.1	The system will keep track of the security posture.
FR8	Report company status
FR8.1	The system shall record the company status and provide it to the user.
FR9	Training plan
FR9.1	A training plan will be provided when requested to be followed by the user.
FR10	Payment
FR10.1	The system shall allow the user to pay for the services.

Non Functional Requirements

ID	Requirement Definition
NFR1	User Interface
NFR1.1	The UI should be intuitive and user-friendly, ensuring that users can easily navigate through the application without extensive training.
NFR1.2	Provide clear error messages and guidance to users in case of input errors or system failures
NFR2	Hardware Interface
NFR2.1	Ensure compatibility with various hardware devices commonly used within the organization
NFR2.2	Design the application to scale efficiently with the hardware infrastructure, accommodating growth in the number of protected software assets and increasing workloads.
NFR3	Software Interface
NFR3.1	Integrate seamlessly with existing software systems and tools used within the organization, such as identity management systems, SIEM solutions, and vulnerability scanners.
NFR3.2	Ensure interoperability with different operating systems, databases, and middleware platforms to support heterogeneous IT environments
NFR4	Security
NFR4.1	Implement strong authentication mechanisms, such as multi-factor authentication (MFA), and granular authorization controls to ensure that only authorized users can access sensitive functions and data.
NFR4.2	Log all user activities, system events, and security-related incidents for auditing and forensic analysis purposes.
NFR4.3	Establish incident response procedures and protocols to effectively respond to security incidents, minimize their impact, and restore normal operations promptly.

Security Service Provider

CCSW 223

Lab 7 Analysis Phase 2



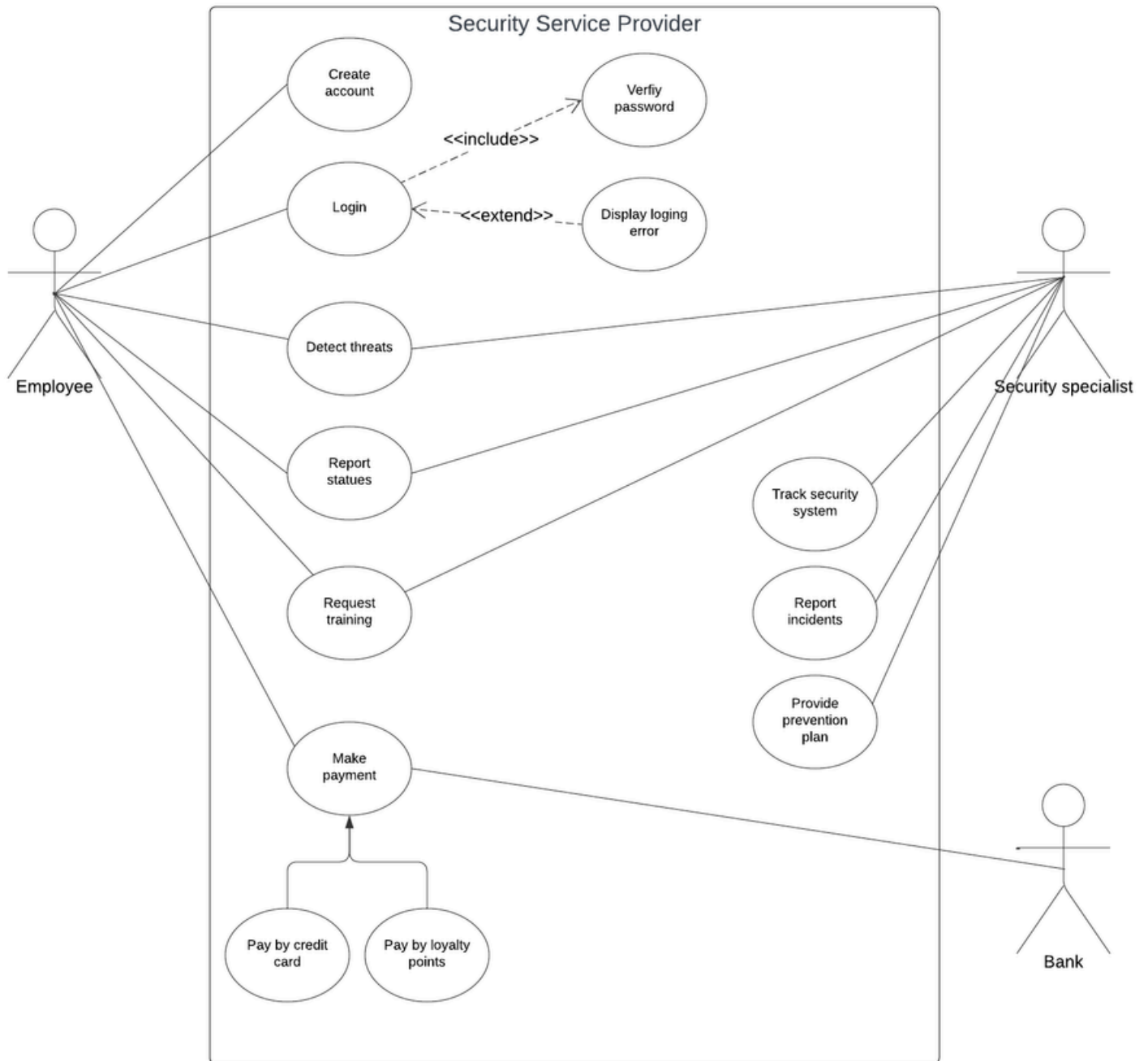
[C2]

Student	ID	Task
Lena Alsinani	2210669	Scenario
Boshra Alghamdi	2211385	Use case - Scenario
Dania Taj	2210829	Scenario
Raghad Fuad	2210302	Scenario
Joud Alotaibi	2211837	Scenario
Shaima Mohammed	2211268	Scenario

Group Leader: Boshra Alghamdi

Editor: Lena Alsinani

Use case diagram



List of Scenarios

Name	Detect threats
ID	UC1
Actors	Employee - Security specialist
Path	<p>1-When an employee accesses a suspicious website or a hacked search engine</p> <p>2-The system starts activating the intrusion detection (IDS) tool</p> <p>3-The network traffic is continuously monitored, analyzing attributes such as IP addresses, ports, protocols, and packet payloads.</p> <p>4-The IDS examines the network traffic for patterns, anomalies, and known attack signatures.</p> <p>5-If a network packet matches a known attack signature, the IDS raises an alert.</p> <p>6-The IDS sends the alerts to security specialist for further investigation and response.</p> <p>7- The IDS operates as an ongoing process, continuously monitoring network traffic and adapting to emerging threats through regular updates.</p>

Name	Report Status
ID	UC2
Actors	Employee - Security specialist
Path	<p>1- The user requests a report on the current status of the company.</p> <p>2- The system collects data about the company to provide an accurate report on the current situation.</p> <p>3- The collected data is processed.</p> <p>4-Specialists analyze the data collected to provide a clear vision of the company's general situation.</p> <p>5- The status report is delivered to the user.</p> <p>6- In the event of threats or risks, the system sends critical alerts to draw attention and take the necessary measures.</p> <p>7- The system updates the company's status periodically so that the user can obtain accurate information about his company.</p>

List of Scenarios

Name	Training plan
ID	UC3
Actors	Employee - Security specialist
Path	<p>1- The security specialist assesses the current knowledge and skill gaps among the employees.</p> <p>2- Based on the identified needs, the security specialist develops a training curriculum for the employees.</p> <p>3- Security specialist conducts interactive training sessions for employees, utilizing workshops, and hands-on exercises.</p> <p>4- Employees engage in hands-on practice to apply their newly acquired knowledge and skills in realistic scenarios.</p> <p>5- Security specialists continuously evaluate the effectiveness of the training program through assessments and feedback.</p>

Name	Report incidents
ID	UC4
Actors	Security specialist
Path	<p>1-The system detects and identifies suspicious activity or security breach when the employee accesses the suspicious website or search engine.</p> <p>2- The system generates an alert or flags the incident</p> <p>3-The generated alert is sent to security specialist</p> <p>4-The security specialist initiates the incident triage and investigation process, assessing the severity and potential impact of the incident.</p> <p>5 The security specialist formulates an appropriate response plan, which may involve blocking access, isolating affected systems, or resetting compromised credentials.</p> <p>6- A comprehensive report is generated after resolving the incident</p>

List of Scenarios

Name	Prevent attacks
ID	UC5
Actors	Security specialist
Path	<p>1- The security specialist conducts a comprehensive assessment of potential threats and vulnerabilities.</p> <p>2- Based on the threat assessment, the security specialist develops a risk mitigation strategy to prevent identified threats.</p> <p>3- Intrusion Prevention Systems (IPS) tools are deployed to monitor and prevent suspicious activities.</p> <p>4- Firewalls are configured by the security specialist to filter incoming and outgoing traffic.</p> <p>5- Access control policies are enforced by the security specialist to restrict access to sensitive data and critical systems.</p> <p>6- The security specialist continuously monitors the application's environment for signs of potential security threats.</p>

Name	Track security system
ID	UC6
Actors	Security specialist
Path	<p>1- When the system is turned on, the security tracking system is immediately triggered.</p> <p>2- The system gathers data from security systems, including antivirus, firewall programs, IDS and others</p> <p>3- Experts examine this information to look for odd trends and possible security breaches.</p> <p>4- Based on these findings, the system creates a comprehensive security plan to prevent these security issues.</p> <p>5- The system produces thorough reports outlining these occurrences, the dangers involved, and the steps done.</p>

Security Service Provider

CCSW 223

Lab 8 Analysis Phase 2



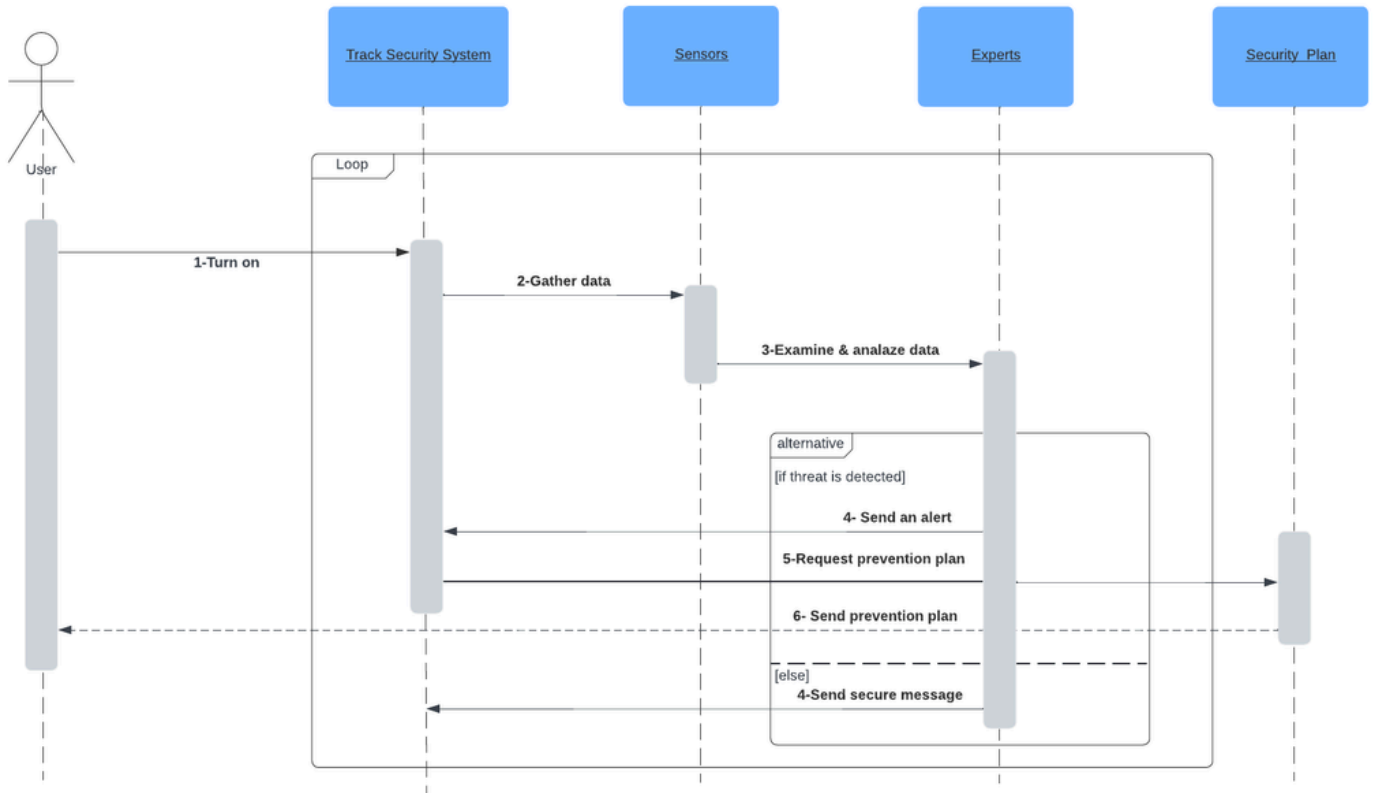
[C2]

Student	ID	Task
Lena Alsinani	2210669	Create Track security system sequence diagram
Boshra Alghamdi	2211385	Create Track security system sequence diagram
Dania Taj	2210829	Create Request training sequence diagram
Raghad Fuad	2210302	Create Detect threats sequence diagram
Joud Alotaibi	2211837	Create Report incident sequence diagram
Shaima Mohammed	2211268	Create Report status sequence diagram

Group Leader: Boshra Alghamdi

Editor: Lena Alsinani

Track Security System:



1- Employee Interaction: The sequence starts with an employee (User) turning on the track security system.

2 - Data Gathering: Once activated, the system triggers the Track Security System, which proceeds to gather data from various sources, including sensors.

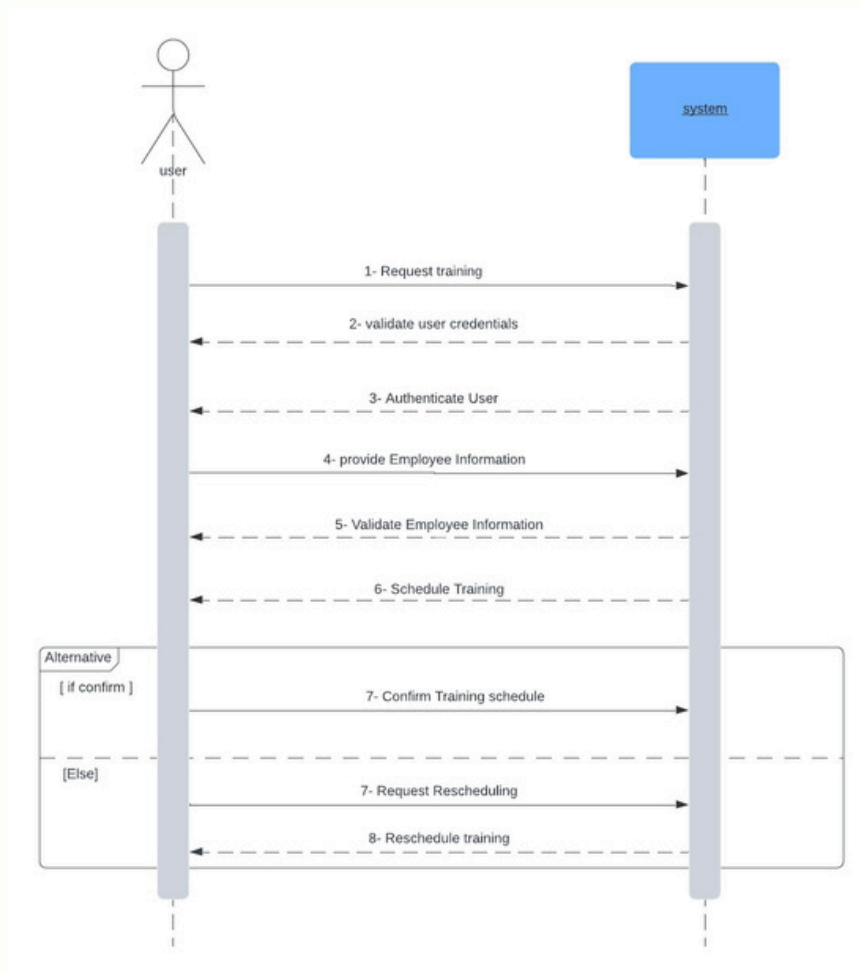
3 - Data Analysis: The gathered data is then examined and analyzed by experts to identify any potential threats or security breaches.

4 - Security Plan Creation: Based on the analysis, if a threat is detected, the system sends an alert and requests a prevention plan.

5 - Prevention Plan Execution: The system then sends the prevention plan to mitigate the identified threat.

6 - System Secure Message: If no threat is detected during the data analysis phase, the system sends a message indicating that the system is secure.

Request Training:



1- User requests training: The user initiates the process by requesting training for their employee through the app.

2- Validate User Credentials: The system validates the user's credentials to ensure they have the authority to request training.

3- Authenticate User: Once validated, the system authenticates the user's identity.

4- Provide Employee Information: The user provides information about the employee who needs training.

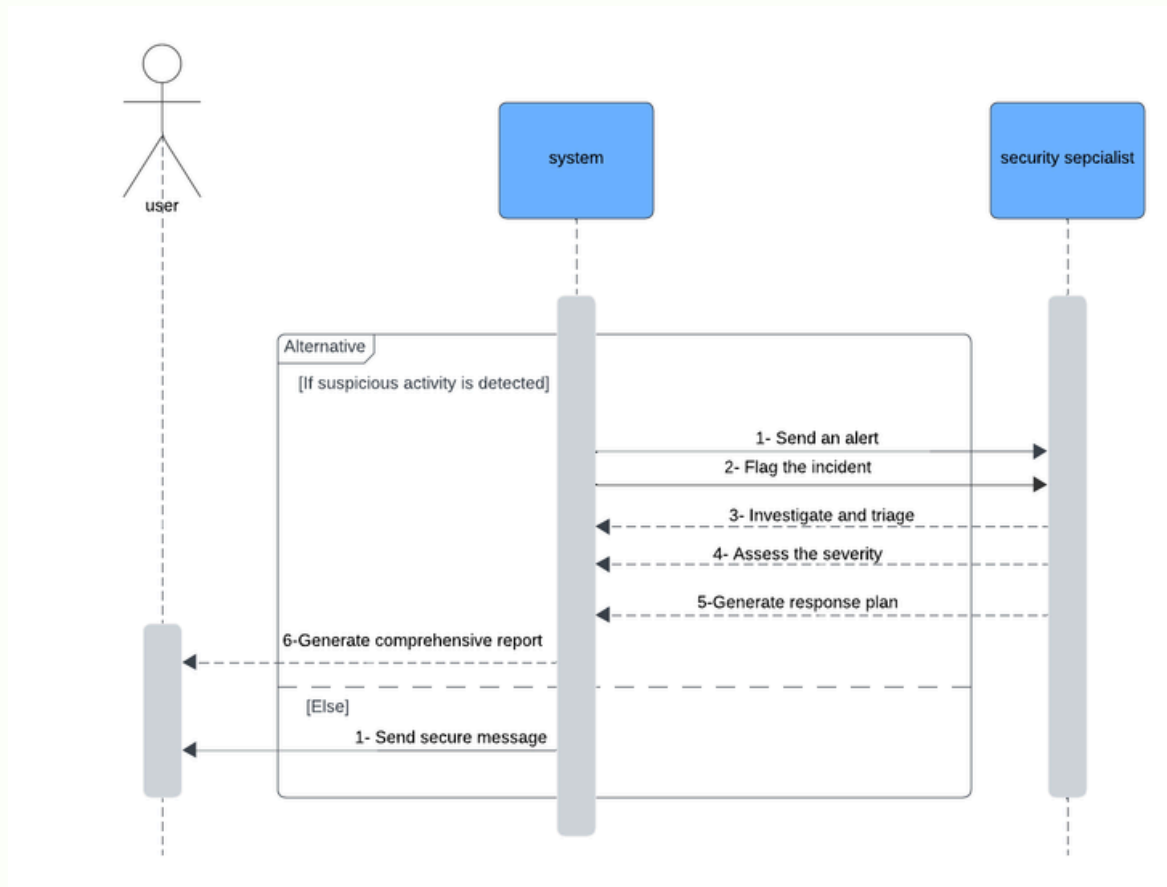
5- Validate Employee Information: The system validates the provided employee information.

6- Schedule Training: The system schedules the training session.

7- If Confirm, confirm training schedule: Confirmation of the training schedule is sent by the user. Else, request rescheduling: the user request a reschedule for the training

8- Reschedule: response to the user request and send a new schedule

Detect threats:



1- System Activation: The System begins the process by activating the IDS tool.

2- Traffic Monitoring: The IDS Tool monitors the network traffic for any anomalies by sending a request to the network traffic tool.

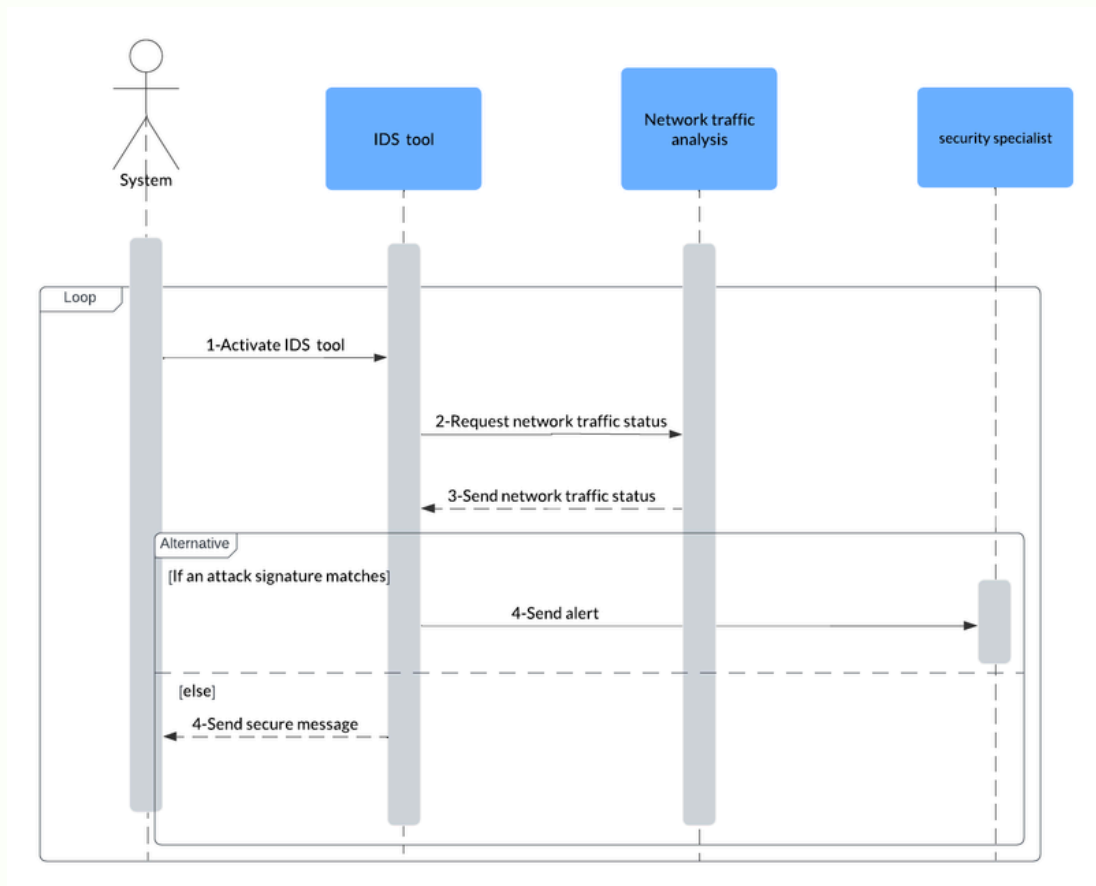
3- Status Response: the network traffic tool provides the IDS tool the network traffic status.

4- Threat Detection: If an attack signature is detected, the IDS Tool initiates an Alert to the Security Specialist.

5- Secure Message: If no threats are detected, the IDS Tool sends a Secure Message indicating safety.

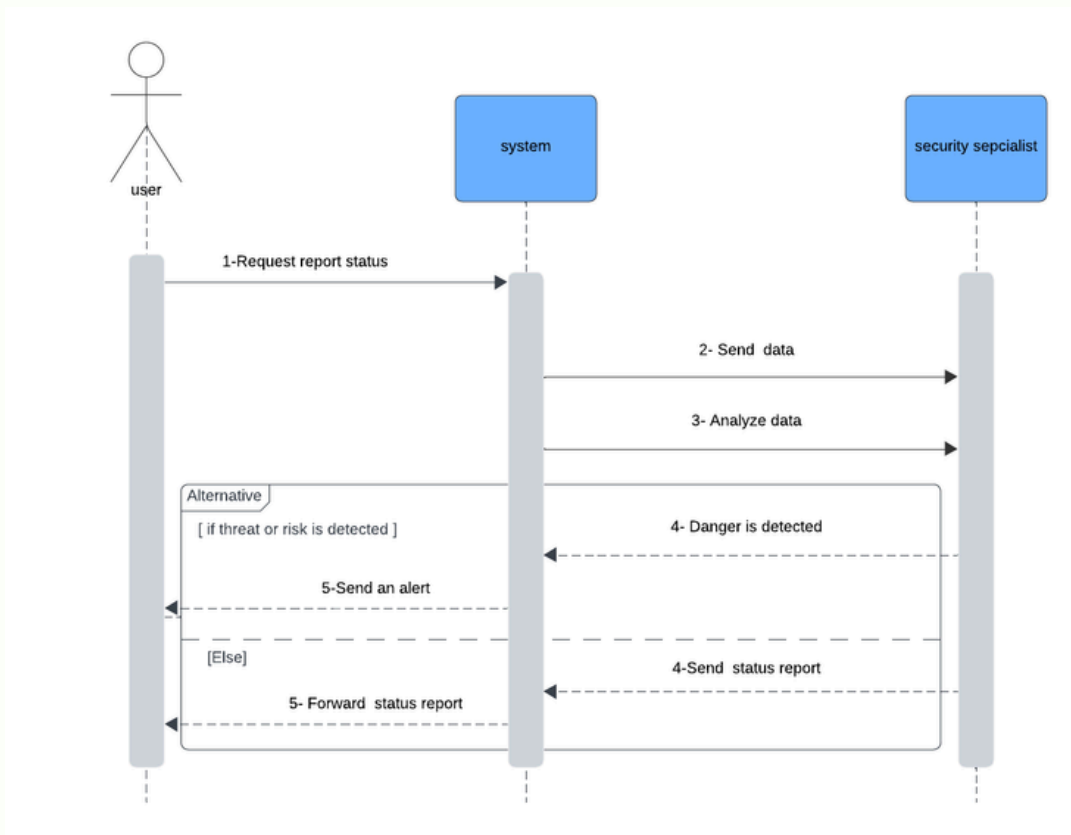
6- Specialist Response: Upon receiving an alert, the Security Specialist takes appropriate action to address the potential security threat.

Report Incidents:



- 1- If the system detects and identifies suspicious activity or security breaches.
- 2- The system generates an alert and flags the incident to indicate the presence of a security issue.
- 3- The security specialist receives the alert and initiates the incident triage and investigation process.
- 4- The security specialist assesses the severity and potential impact of the incident.
- 5- Based on the assessment, the security specialist formulates an appropriate response plan, which may involve actions such as blocking access, isolating affected systems, or resetting compromised credentials.
- 6- The security specialist communicates with the system to execute the response plan, instructing it to perform necessary actions such as blocking access or isolating systems.
- 7- Once the incident is resolved, the system generates a comprehensive report summarizing the details of the incident, including the actions taken and their outcomes.
- 8- If no suspicious activities occur the system will send a message indicating that the system is secure

Report Status:



1- Request report:The user begins the process by sending a request to evaluate the situation (the level of security of the user or company)

2- Send data: The system then sends the collected data to specialists so that they can quickly examine and evaluate it

3- If status good: If the specialists do not find any danger or threat of vulnerabilities or security risks, the system will send the report.

Else : the system will send critical alert signals to the user to warn of the presence of risks.

Security Service Provider

CCSW 223

Lab 9 Modeling Phase

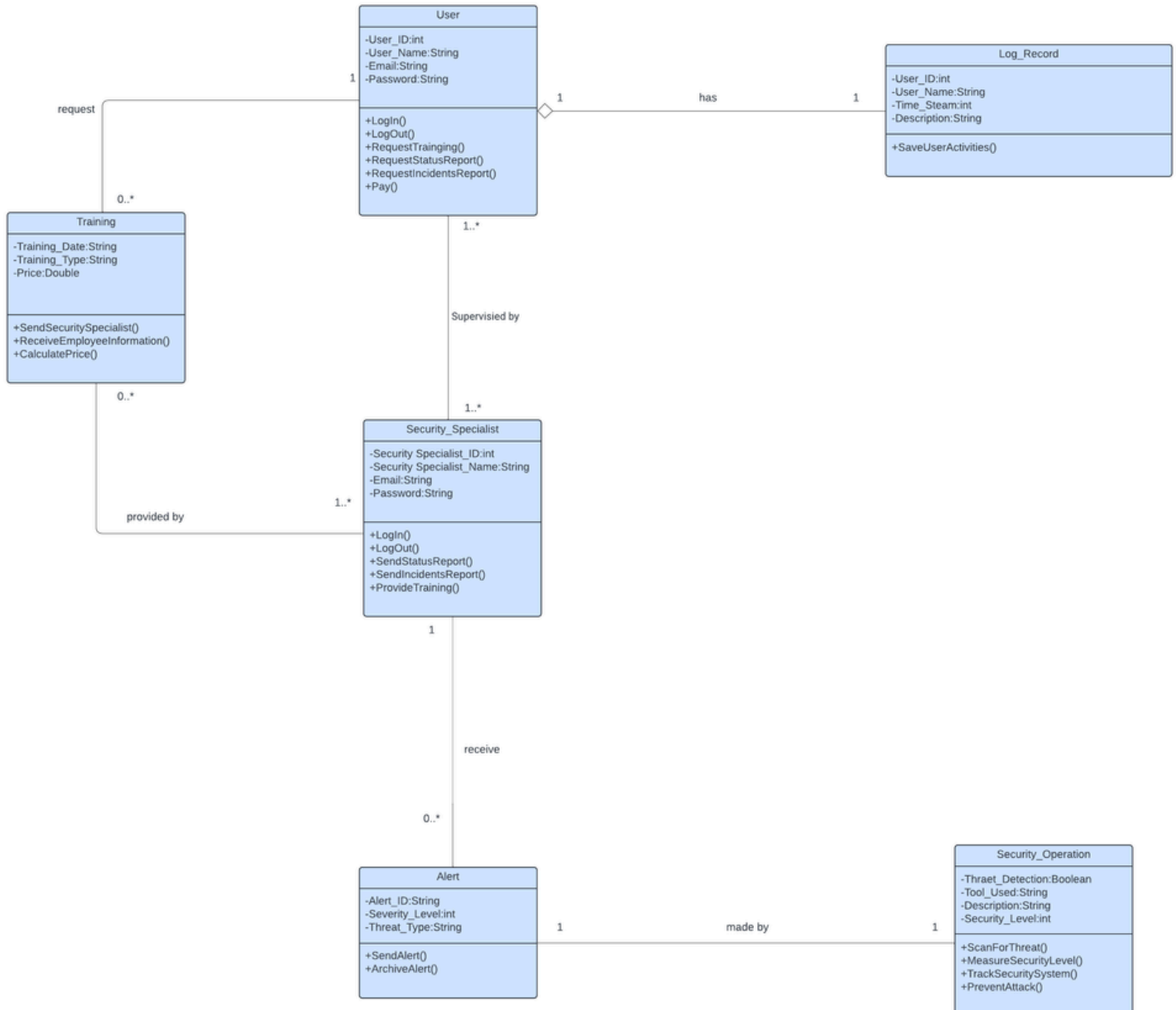
[C2]

Student	ID	Task
Lena Alsinani	2210669	Class Diagram
Boshra Alghamdi	2211385	Class Diagram
Dania Taj	2210829	Class Diagram
Raghad Fuad	2210302	Class Diagram
Joud Alotaibi	2211837	Class Diagram
Shaima Mohammed	2211268	Class Diagram

Group Leader: Boshra Alghamdi

Editor: Lena Alsinani

Class Diagram



Class Diagram description:

The User class

Attributes:

- User ID: int - A unique identifier for the user.
- User Name: String - Username for the user.
- Email: String - Email address of the user.
- Password: String – password of the user

Methods:

- Login(): This method verifies the user credentials and allows the user to login to the system.
- Logout(): This method terminates the user's session and logs them out of the system.
- RequestTraining(): This method allows the user to request training.
- RequestStatusReport(): This method allows the user to request a report on the status of the system
- RequestIncidentReport(): This method allows the user to request a report on security incidents.
- Pay(): This method allows the user to pay for the service.

Log Record class:

Attributes:

- User ID: int - A foreign key that references the User class. This creates a link between a log record and the user it belongs to.
- User Name: String - Username for the user.
- Time Stamp: int - The amount of time that the user spent on the system.
- Description: String - A description of the user activity that was logged.

Methods:

- SaveUserActivities(): This method saves the user's activities that was done in the system.

Class Diagram description:

Training Class

Attributes:

- TrainingDate: String - Date of the training.
- TrainingType: String - Type of training offered.
- Price: Double - Cost of the training.

Methods:

- SendSecuritySpecialist(): This method initiates a request to a Security Specialist to provide training.
- ReceiveEmployeeInformation(): This method fetches the information of the employee to be trained.
- CalculatePrice(): This method calculates the cost of the training.

Security_Specialist Class

Attributes:

- SecuritySpecialist_ID: int - Unique identifier for the security specialist.
- SecuritySpecialist_Name: String - Name of the security specialist.
- Email: String - Email address of the security specialist.
- Password: String - password of the Security Specialist

Methods:

- Login(): This method verifies the security specialist credentials and allows them to login to the system.
- Logout(): This method terminates the security specialist's session and logs them out of the system.
- SendStatusReport(): This method allows the security specialist to send the report status to the user.
- ProvideTraining(): This method sends a Security Specialist to Provide Training.
- SendIncidentReport(): This method allows the security specialist to send incident reports to the user.

Class Diagram description:

Alert class

Attributes:

- AlertID: String - A unique identifier for the alert.
- SeverityLevel: int - A number representing the severity level of the alert.
- ThreatType: String - describing the type of threat detected.

Methods:

- SendAlert() - This method sends the alert to the Security specialist.
- ArchiveAlert(): This method stores the alert in an archive.

Security_Operation class

Attributes:

- Threat_Detection: Boolean - detecting threats.
- Tool_Used: String - specifies the name of the tool used for threat detection.
- Description: String - provides a description of the threat that was detected.
- Security_Level: Int - A number representing the security level of the system.

Methods:

- ScanForThreat() - This method initiates a scan to search for security threats in the system.
- MeasureSecurityLevel() - This method calculates a security level metric based on the current state of the system.
- TrackSecuritySystem() - This method monitors the security system for any suspicious activity.
- PreventAttack() - This method prevents the detected attack.



Recommendations

We are enthusiastic about the prospect of further expansion and development as after we started this first phase of our project. The application is built to grow and develop with small businesses. Furthermore, we're dedicated to advancing continuously and staying ahead of new cybersecurity threats. Our roadmap for upcoming improvements demonstrates our commitment to provide our users the greatest protection available. Our ultimate objective is to empower small businesses to concentrate on their core competencies rather than always worrying about cyberattacks. Our comprehensive, reasonably priced, and easily accessible cybersecurity solution helps entrepreneurs prosper in the current digital environment. Additionally, we urge small businesses to be proactive in safeguarding their data and to have faith in the safety of their business operations.

Our project represents just the initial phase of our ambitious vision. We're excited about the prospect of expanding its capabilities to mobile devices, such as smartphones, ensuring users can stay informed and protected wherever they go. Through downloadable mobile applications, we aim to provide timely alerts and notifications, keeping users vigilant against emerging threats and potential hacks across various online platforms.

Moreover, our commitment extends to the safety of our youngest users. By tailoring our project for children's devices like tablets and iPads, we strive to create a secure digital environment, shielding them from any websites or activities that pose a risk of hacking.

In essence, our endeavor is not only about reacting to threats but also about proactively preventing them. By empowering users with real-time alerts and comprehensive safeguards, we aim to redefine cybersecurity, making it accessible, intuitive, and indispensable in today's digital landscape.