École Supérieure Privée d'Ingénierie et De Technologies

TIC DEPARTEMENT

Next Generation Soc Project Report

Design and Development of a Next Generation Security Operations Centre

Developed by :

Amairi Hajer
Kahloul Aziz
Safi Aymen
Gesmi Raed
Ondo Melchor
El Hamed Brahime
El Houdhaiffoudine Ben Sidi

Encadré par :
Mme Berrahal Sarra
École Supérieure Privée d'Ingénierie et De Technologies

Année Universitaire: 2022/2023

DEDICATIONS

The end result of this project required valuable advice and assistance from many people. Everything we have done is thanks to their invaluable guidance and support and I will not forget to thank them.

To our dear parents,

Who have never ceased to support and support us in achieving our goals, your prayers and blessings have been of great help to us in carrying out our studies.

To those with whom our success is very important, with whom we share the highlights of our lives, a big thank you for your help and advice during all the trials of our lives.

.

To our dear friends and classmates,

With whom we shared unforgettable moments.

APPRECIATION

After giving thanks to GOD who is the origin of all success in our life.

Our sincere thanks go to our supervisor, Mrs Berrahal Sarra, who has taken charge of this project. Her interest in this work, her benevolence, her scientific rigor, her high human qualities, have been invaluable in helping us to complete this work.

At the same time, I would like to thank Mr Ghahbich Mohamed Habib, Founder of Itc, for his welcome and guidance.

I would also like to thank all my teachers and the entire NIDS family for their efforts in guiding us and enriching our work throughout our university studies.

Our thanks also go to all those who participated, from near or far, in the development of this graduation project and especially to our families and friends.

Finally, we would like to thank the jury members for taking the time to review and evaluate our work.

Content Table

Liste of Figures

Liste of Tables

Liste of Acronyms

SOC Security Operations Center

General Introduction

The next generation Security Operations Center, often referred to as SOC 2.0 or SOC of the future, represents an evolved approach to security monitoring, detection, and response within organizations. Building upon the foundations of traditional Security Operations Centers, next-generation SOCs aim to address the ever-evolving threat landscape and the increasing complexity of cyber threats.

The key characteristics of a next-generation SOC include:

1. Advanced Threat Intelligence: Next-generation SOCs leverage a wide range of intelligence sources, including threat feeds, dark web monitoring, machine learning algorithms, and data analytics, to proactively identify and respond to emerging threats.

2. Automation and Orchestration: Next-generation SOCs emphasize the use of automation and orchestration tools to streamline routine tasks, accelerate incident response, and improve overall efficiency. Automated processes help SOC analysts focus on more complex and critical security issues.

3. Artificial Intelligence and Machine Learning: These technologies play a significant role in next-generation SOCs. AI and machine learning algorithms are employed to analyze large volumes of security data, detect patterns, and identify anomalies, enabling faster and more accurate threat detection.

4. Threat Hunting: Next-generation SOCs actively engage in proactive threat hunting activities. This involves conducting in-depth investigations, searching for potential threats or signs of compromise within the network, and using various tools and techniques to identify and mitigate potential risks.

5. Collaboration and Integration: Next-generation SOCs foster collaboration between different teams within the organization, including IT, network operations, incident response, and external stakeholders such as law enforcement or industry peers. Integration with external threat intelligence providers and security platforms enhances the SOC's capabilities and strengthens overall defense.

6. Continuous Monitoring and Response: Next-generation SOCs emphasize the need for continuous monitoring of network traffic, systems, and applications. They implement real-time detection and response mechanisms to quickly identify and mitigate threats as they occur.

7. Data-driven Decision Making: Next-generation SOCs leverage data analytics to gain insights into security incidents, identify trends, and improve decision-making processes. They use metrics and key performance indicators (KPIs) to measure the effectiveness of security operations and drive continuous improvement.

The goal of a next-generation SOC is to enhance an organization's ability to detect and respond to security incidents rapidly, effectively mitigating risks and minimizing the impact of potential breaches. By combining advanced technologies, automation, and human expertise, these SOCs strive to stay one step ahead of cyber threats in an increasingly dynamic and challenging cybersecurity landscape.

Chapitre 1: Project Description

1.1 Introduction

The project aims to implement a proof of concept for a next-generation security operation center (SOC) solution for the banking sector provided by ITC.

The solution should include vulnerability management, automated incident response, investigations coordination, automated compliance reporting, comprehensive integration, security analytics integration, and automated asset security testing.

In a world invaded by hackers, banks must protect themselves against ransomware, denial of service attacks and the TOP 10 OWASP vulnerabilities in order to protect themselves against the loss of confidential data, the loss of reputation, the loss of clients.

1.2 Project Overview

Realizing a next-generation Security Operations Center (SOC) involves the process of designing, implementing, and optimizing an advanced security infrastructure to effectively monitor, detect, and respond to cyber threats.

The steps involved in realizing a next-generation SOC:

1. Assessment and Planning: The first step is to conduct a thorough assessment of the organization's current security capabilities, including existing SOC infrastructure, tools, processes, and personnel. This assessment helps identify gaps and challenges that need to be addressed in the next-generation SOC. Based on the assessment, a strategic plan is developed, outlining the goals, objectives, and roadmap for implementing the next-generation SOC.

2. Technology Selection: Next, the appropriate technologies and tools are selected to support the next-generation SOC's capabilities. This may include advanced threat intelligence platforms, security analytics tools, automation and orchestration solutions, artificial intelligence/machine learning systems, and data visualization platforms. The technology selection process should align with the organization's specific security requirements and objectives.

3. Infrastructure Design and Deployment: Once the technology is selected, the next step is to design the infrastructure for the next-generation SOC. This involves determining the hardware and software requirements, network architecture, data storage and management systems, and integration with existing security systems. The deployment plan includes setting up the necessary hardware, configuring the software, and establishing connectivity with relevant systems and data sources.

4. Process and Workflow Development: Next-generation SOCs require well-defined processes and workflows to ensure efficient and effective security operations. This includes defining incident response procedures, escalation protocols, threat hunting methodologies, and standard operating procedures (SOPs) for security analysts. Clear roles and responsibilities should be established, and regular training and skill development programs should be implemented to empower SOC personnel.

5. Automation and Orchestration Implementation: Automation and orchestration play a crucial role in next-generation SOCs. Security processes that can be automated, such as alert triage, data enrichment, and response actions, should be identified and implemented using appropriate tools and technologies. Orchestration helps streamline and integrate various security tools and workflows, enabling faster and more coordinated incident response.

6. Integration and Collaboration: A next-generation SOC should be integrated with various internal and external systems to enhance its capabilities. This includes integrating with threat intelligence feeds, security information and event management (SIEM) systems, endpoint detection and response (EDR) solutions, and other security controls. Collaboration with internal teams, external partners, and industry peers should also be fostered to share threat intelligence and best practices.

7. Continuous Improvement and Optimization: Realizing a next-generation SOC is an iterative process that requires ongoing monitoring, analysis, and optimization. Regular review of SOC performance metrics, incident response effectiveness, and feedback from analysts helps identify areas for improvement. Continuous training and skill development programs should be implemented to keep SOC personnel up to date with the latest threats, technologies, and techniques.

1.3 Project Objectives

The project objectives are as follows:

1. Enhance Threat Intelligence Capabilities: The objective is to improve the organization's ability to gather, analyze, and utilize threat intelligence data to proactively identify and mitigate potential cyber threats.

2. Improve Incident Detection and Response Times: The goal is to enhance the organization's incident detection and response capabilities by implementing advanced technologies and automation, enabling swift identification, containment, and remediation of security incidents.

3. Streamline Security Processes through Automation and Orchestration: The objective is to automate routine security tasks, streamline workflows, and integrate security tools and systems for efficient security operations and incident management.

4. Foster Collaboration and Information Sharing: The goal is to establish a collaborative environment that promotes effective communication and information sharing among internal teams, external stakeholders, and industry partners to improve overall threat awareness and response.

5. Continuously Improve SOC Performance: The objective is to regularly monitor and optimize the SOC's performance through metrics analysis, performance tuning, and process refinement, ensuring the SOC remains effective and aligned with industry best practices.

6. Strengthen Security Posture: The goal is to enhance the organization's overall security posture by implementing a comprehensive security infrastructure that effectively safeguards critical assets, mitigates risks, and protects against evolving cyber threats.

1.4 Technical Requirements

Requirements	Technical constraints	Technologies	Products	Final Product
- Secure the bank's IT infrastructure with the implementation of IDS/IPS technologies -Web Application Firewall (WAF) to ensure the security of the web server. - Control inbound and outbound traffic by implementing a firewall - Managing/Correlating Data with threat intelligence - Monitoring threats - Guarantee the integrity, authenticity, confidentiality, availability of transactions and system components - Security events and alert extraction - Providing platform for incident analysis - Provide real-time alerts through IPS/IDS - Centralizing automation and orchestration tools on a dashboard - Follow the regulatory guidelines - Resist internal and external threats - Monitoring physical access by using CCTV cameras	- Compliance with security regulations and standards such as **PCI-DSS**, **ISO 2700x**, **NIST** Cybersecurity Framework, **GDPR**, **SWIFT**, **SOX** - Data privacy and protection of sensitive information & loss through breaches/leaks - Vulnerability management that correlates log data with threat intelligence to identify vulnerable elements in the infrastructure - Deployment tools integration (ex. Jenkins) - Availability of resources for real-time API integration - Dashboard designing and integrating - Properly ingest and analyze data using DL and ML - Constant guideline update - Constant update of attacks and threats -Verifying integrity of files system - Ensure the availability of the bank system.	- Security Information and Event Management (SIEM) systems. Network and endpoint security solutions - SOAR (Security Orchestration, Automation and Response) - Threat Intelligence Platforms. Cloud Security Solutions - Vulnerability and Risk Management tools - Automated incident response systems - Endpoint detection and response (EDR) - User and entity behavior analytics (UEBA) - Data Loss Prevention (DLP) Solutions - Antivirus - Backup solution	- Elastic search - RSA Archer SOC -Open source Microsoft product -Alien vault OSSIM - Open source Cisco solution -Snort -Ossec -TheHive -Cortex -MISP -Shuffle -NAXSI -ClamAV -Pfsense -Opensense -EXDR -Elastic XDR -NGINX -reNgine -Zabbix -AIDE - Bacula	-ELK stack(elasticsearch, logstash,kibana) -Snort -Wazuh -Crowdsec -Zabbix -Sysmon -TheHive -Cortex -MISP -Shuffle -NAXSI -ClamAV -Pfsense -Opensense -EXDR -Elastic XDR -NGINX -reNgine

-Backup solution to ensure that there's no data loss.		-Modsecurity	-Radius (AAA)	

Table 1-4. *Requirements Table*

1.5 Conclusion

Experienced professional dedicated to the realization of a next-generation Security Operations Center (SOC) that establishes an advanced security infrastructure to proactively monitor, detect, and respond to evolving cyber threats.

With a focus on leveraging advanced technologies, automation, and collaboration, the project aims to address the complexities of the threat landscape. Requirements include assessing current security capabilities, selecting appropriate technologies, designing and deploying infrastructure, implementing automation, and fostering collaboration. Objectives encompass enhancing threat intelligence, improving incident response, streamlining processes, and optimizing SOC performance. By achieving these goals, the organization strengthens its security posture, safeguards critical assets, and aligns with industry best practices.

Chapitre 2: Project Solution

2.1 Introduction

2.2 Proposed Solutions

Figure 2-2. *Our Solution*

The implemented Security Operations Center (SOC) solution is a comprehensive and advanced security infrastructure designed to protect banking organizations from evolving cyber threats. Leveraging a range of powerful tools and technologies, the SOC incorporates cutting-edge capabilities to monitor, detect, and respond to security incidents proactively.

The SOC utilizes Sysmon, ZABBIX, and Wazuh agents, along with an Elastic search engine, to collect and analyze system activity logs, network data, and security events. This wealth of information is seamlessly aggregated, managed, and visualized using the ELK Stack (Elasticsearch, Logstash, Kibana), providing real-time insights into potential threats.

To bolster network security, Snort, a robust network intrusion detection and prevention system, continuously monitors network traffic, identifying and blocking malicious activities. Crowdsec further enhances the SOC's threat detection capabilities by analyzing behavior patterns and promptly blocking suspicious IP addresses based on community-driven intelligence.

Incident response and collaboration are facilitated through integrated tools such as TheHive and Cortex. TheHive serves as an incident response platform, enabling efficient case management, collaboration, and tracking of security incidents. Cortex, a security orchestration and automation platform, automates routine tasks, allowing analysts to focus on critical issues and accelerate incident response processes.

The SOC leverages MISP, a powerful threat intelligence platform, to store, share, and analyze threat intelligence information. This integration enhances the SOC's ability to detect and respond to emerging threats effectively.

Furthermore, the SOC solution incorporates additional security measures. NAXSI acts as a web application firewall (WAF) for NGINX, providing robust protection against web-based attacks. ClamAV, an open-source antivirus engine, detects and eliminates malware from files and email attachments, fortifying the SOC's defenses.

Network connectivity is facilitated through the utilization of a Cisco router, enabling seamless communication and data transfer between the various components of the SOC. Cables, carefully deployed to interconnect the eight machines, establish a reliable and secure network infrastructure.

Overall, this SOC solution combines the power of multiple tools and technologies, providing a holistic approach to security operations. By leveraging advanced monitoring, detection, and response capabilities, the SOC enables proactive threat mitigation, efficient incident handling, and collaborative analysis. This comprehensive SOC solution helps banking organizations stay ahead of cyber threats, safeguard critical assets, and maintain a robust security posture in an ever-evolving threat landscape.

2.3 Physical Architecture

Figure 2-3. *Physical Architecture*

The physical architecture of the Next Generation Security Operations Center (SOC), designed specifically for banking organizations, adheres to the rigorous requirements outlined by the National Institute of Standards and Technology (NIST) standards. It encompasses three distinct zones: LAN, SOC, and DMZ.

Within the LAN zone, various agents such as Sysmon, ZABBIX, and WAZUH, along with an Elastic search engine, operate on workstations running Kali, Windows, and Ubuntu operating systems. The LAN is connected via a switch and is protected by the OpenSense firewall, ensuring compliance with NIST security guidelines.

The SOC zone, connected to the LAN through the same NIST-compliant OpenSense firewall, incorporates an Endpoint Detection and Response (EDR) system called WAZUH and a Network Detection and Response (NDR) system. To facilitate efficient security operations, the SOC also integrates multiple NIST-compliant security tools, including MISP, ELK, Cortex, and TheHive, forming a comprehensive Security Orchestration, Automation, and Response (SOAR) system.

Similarly, the DMZ zone, also connected to the NIST-compliant OpenSense firewall, provides a secure environment for external-facing services, such as DNS, HTTP, and MAIL. It is designed to isolate and protect these services from the rest of the network, in alignment with NIST guidelines.

Moreover, the architecture incorporates a honeypot, connected to another NIST-compliant firewall called Pfsense. The Pfsense firewall, in turn, connects to a router that facilitates internet connectivity while adhering to NIST standards.

In conclusion, this meticulously designed architecture for banking organizations follows NIST standards requirements, ensuring robust security measures across the LAN, SOC, and DMZ zones. By combining NIST-compliant security tools and techniques, it provides comprehensive protection against potential threats, in accordance with industry best practices.

2.4 Logical Architecture

Figure 2-4. *Physical Architecture*

The logical architecture designed for this project is aimed at creating a secure and efficient system for the next-generation Security Operations Center (SOC). The logical architecture encompasses the arrangement and integration of various components and technologies to ensure effective threat monitoring, incident detection, and response.

At the core of the logical architecture is the SOC, which serves as the central hub for security operations. The SOC consists of different layers and components that work together seamlessly.

The first layer includes the data sources, which provide the necessary information for threat monitoring and analysis. These data sources can include logs from network devices, endpoints, applications, and external threat intelligence feeds.

The next layer involves the ingestion and processing of the collected data. This layer includes components such as log collectors, data parsers, and normalization tools. They collect and transform the data into a standardized format for further analysis.

The third layer focuses on threat detection and analysis. It includes components such as SIEM (Security Information and Event Management) systems, intrusion detection systems (IDS), and machine learning algorithms. These components analyze the collected data, identify patterns, detect anomalies, and generate alerts for potential security incidents.

The fourth layer involves incident response and management. It includes tools for case management, workflow automation, and ticketing systems. These components streamline the incident response process, enabling security teams to investigate and mitigate security incidents efficiently.

The final layer encompasses reporting and visualization. This includes components such as dashboards, reporting tools, and analytics platforms. These components provide visual representations of security data, enabling security teams to gain insights, track performance metrics, and make informed decisions.

2.5 Technology Used

2.5.1 Sysmon

Figure 2-5.1. *Sysmon*

A system monitoring tool used to collect and analyze system activity logs for threat detection and incident response.

2.5.2 Zabbix

Figure 2-5.2. *Zabbix*

A monitoring and alerting system that provides real-time monitoring of network devices, servers, and applications to ensure their availability and performance.

2.5.3 Wazuh

Figure 2-5.3. Wazuh

An open-source security platform that combines intrusion detection, log analysis, file integrity monitoring, and active response capabilities.

2.5.4 Crowdsec

Figure 2-5.4. Crowdsec

An open-source, behavior-based threat detection system that identifies and blocks malicious IP addresses based on community-driven intelligence.

2.5.5 ELK Stack (Elasticsearch, Logstash, Kibana)

Figure 2-5.5. ELK Stack

A powerful combination of open-source tools for log management, log aggregation, and data visualization.

2.5.6 Snort

Figure 2-5.1. Snort

An open-source network intrusion detection and prevention system (NIDS/NIPS) that analyzes network traffic for malicious activity.

2.5.7 TheHive

Figure 2-5.7. TheHive

An open-source incident response platform that facilitates collaboration, case management, and tracking of security incidents.

2.5.8 Cortex

Figure 2-5.8. Cortex

An open-source security orchestration and automation platform that integrates with various tools to automate incident response processes.

2.5.9 MISP

Figure 2-5.9. MISP

An open-source threat intelligence platform that enables the sharing, storage, and analysis of threat intelligence information.

2.5.10 Shuffle

Figure 2-5.10. *Shuffle*

A tool for capturing and analyzing network traffic, allowing for the identification of network-based threats and vulnerabilities.

2.5.11 NAXSI

Figure 2-5.11. *NAXSI*

A web application firewall (WAF) for NGINX that provides protection against common web application attacks.

2.5.12 Pfsense

Figure 2-5.12. *Pfsense*

An open-source firewall and routing platform that provides network security and access control.

2.5.13 Opensense

Figure 2-5.13. Opensense

An open-source firewall solution that offers network security features and traffic filtering capabilities.

2.5.14 EXDR (Elastic XDR)

Figure 2-5.14. EXDR

A comprehensive extended detection and response solution that combines endpoint security, network security, and threat intelligence.

2.5.15 NGINX

Figure 2-5.15. NGINX

A popular open-source web server and reverse proxy server that provides high-performance HTTP and proxy services.

2.5.16 reNgine

Figure 2-5.16. reNgine

A reconnaissance framework that automates the process of gathering information about target systems and vulnerabilities.

2.5.17 ClamAV

Figure 2-5.17. ClamAV

An open-source antivirus engine designed for detecting and removing malware from files and email attachments.

2.6 Machines and IPS

In the realization of this project, we leveraged a total of eight machines to implement the diverse range of technologies and tools. These machines served as the foundation for the comprehensive security infrastructure.

To support the project's requirements, significant resources were allocated, including computing power, storage capacity, and network connectivity. Interconnecting

these machines was accomplished through the utilization of a Cisco router and appropriate cables.

This networking setup ensured seamless communication and data flow between the various components of the system, enabling efficient collaboration and integration of the implemented technologies. By carefully deploying these resources and employing robust networking infrastructure, we were able to establish a solid foundation for the next-generation Security Operations Center (SOC) in alignment with the project's objectives.

2.7 Conclusion

The implemented next-generation Security Operations Center (SOC) has bolstered the security capabilities of banking organizations through the integration of advanced technologies and tools.

These include Sysmon, ZABBIX, Wazuh, ELK Stack, Snort, TheHive, Cortex, MISP, NAXSI, and ClamAV. The SOC solution, interconnected by a Cisco router and cables, enables proactive threat monitoring, efficient incident response, and collaborative analysis. By leveraging this comprehensive SOC solution, banking organizations can effectively mitigate risks, protect critical assets, and navigate the evolving cyber threat landscape with confidence.

Chapitre 3: Deployment

3.1 Introduction

In this section, we will discuss the development of our Next Generation SOC, which is designed to address the growing need for advanced security in modern systems.

With the increase in cyber threats and the spread of smart devices, a secure SOC solution is becoming more and more
important.

In addition to the SOC, we have developed a complementary framework called SOAR (Security Orchestration, Automation, and Response) that provides a comprehensive security solution for the SOC.

The SOAR is designed to work with our SOC, providing a wide range of security capabilities including threat detection and response, incident management, and vulnerability scanning.

3.2 SOC

Our SOC includes a variety of security tools that work together to provide comprehensive protection for our network. Here are the tools and their roles in our SOC:

Figure 3-2. *SOC*

- Wazuh: Our SOC uses the Wazuh EDR (Endpoint Detection and Response) system to monitor our endpoints in real-time.
  Wazuh helps us detect and respond to threats quickly by providing features such as file integrity monitoring, log analysis, and threat detection.

- MISP: Our SOC uses MISP to share threat intelligence with other organizations, allowing us to collaborate and stay informed about the latest threats and vulnerabilities

- SIEM: We used ELK (Elasticsearch, Logstash, and Kibana) as our SIEM to provide centralized logging and analysis of security events

- Cortex: Cortex is used in our SOC for automation and orchestration of our security operations

- TheHive: For our incident response platform, we got TheHive which is the most efficient way to manage and respond to security incidents in real-time

- IPS: We use CrowdSec as an IPS for detecting any brute-force attacks, port-scanning, DoS attacks, and more

- Zabbix: It helps us provides real-time monitoring of servers, applications, and network devices in all the network

3.3 SOAR

Our next generation SOC uses a variety of security tools to ensure comprehensive protection of your network.
TheHive, Cortex, and MISP are the three main components of our SOAR (Security Orchestration, Automation, and Response) system.

Figure 3-3. *SOAR*

- TheHive: TheHive is our incident response platform. It provides a centralized location for our security team to manage and respond to security incidents. When a security event is detected, TheHive automatically creates a case and assigns it to the appropriate analyst for investigation. The analyst can then use TheHive to track the progress of the investigation, document findings, and communicate with other team members.

- Cortex: Cortex is our automation and orchestration tool. It enables us to automate our incident response workflows and integrate our various security tools. When an incident is detected in TheHive, Cortex can automatically trigger a response, such as running a malware analysis tool or blocking traffic from a malicious IP address. Cortex also provides a way to enrich our security data by integrating with third-party threat intelligence feeds.

- MISP: Is our threat intelligence platform. It enables us to share threat intelligence with other organizations and stay informed about the latest threats and vulnerabilities. With MISP, we can quickly identify and respond to emerging threats and take proactive measures to prevent potential security incidents.
- In addition to these tools, we use CrowdSec as our IPS for detecting and preventing a wide range of attacks, including brute-force attacks, port scanning, and DoS attacks.

- Zabbix: Provides real-time monitoring of our servers, applications, and network devices, giving us full visibility into our network and enabling us to identify potential issues before they can cause problems.

3.4 Services

As the threat landscape continues to evolve, having a strong cybersecurity infrastructure is crucial. We take a proactive approach to protecting your network from a variety of threats through several security services that work together to create defense-in-depth mechanisms. Our firewall system, which utilizes Snort, pfSense, and OpenSense: Has been customized to meet our banking SOC needs. This section provides

details on how we implemented and optimized our firewall system to ensure the highest level of protection for the banking organizations.

We implemented a robust security infrastructure for our organization's network using a combination of Snort, pfSense, and OpenSense as firewalls. These tools were selected based on their proven track record of effectiveness and flexibility as open-source solutions.

Figure 3-4. *Services*

Snort: An intrusion detection and prevention system, was used to analyze network traffic and detect suspicious activities. We configured Snort to create custom rules tailored to the specific needs of our organization, allowing us to detect and prevent specific types of attacks. This provided us with real-time visibility into network traffic, allowing us to quickly identify and respond to security incidents.

PfSense and OpenSense: Were used to create a secure perimeter around our network and protect against unauthorized access and malicious traffic. These firewalls were customized to enforce strict access controls and network segmentation, reducing the attack surface and preventing lateral movement within our network. We also leveraged their advanced capabilities such as VPN tunnels and IDS/IPS features to further enhance our security posture.

3.5 Conclusion

In this section, we talked about the development of our Next Generation SOC, which is designed to address the growing need for advanced security in modern systems. With the increase in cyber threats and the spread of smart devices, a secure SOC solution is becoming more and more important. Alongside the SOC, we have developed a complementary framework called SOAR (Security Orchestration, Automation, and Response), providing a comprehensive security solution. The integration of TheHive,

Cortex, and MISP within the SOAR system empowers us to swiftly and efficiently respond to potential security incidents. Through regular monitoring, tuning, and firewall policy updates, we ensured optimal operation and the highest level of protection for our network, keeping up with the latest threats and vulnerabilities.

Chapitre 4: Implementation

4.1 Introduction

The implementation of a comprehensive security solution involves key design phases, including Security Architecture Deployment, Deployment of SOAR's components,

and Review and Audit of the Deployed Solution. The Security Architecture Deployment phase focuses on designing and implementing a robust security architecture tailored to the organization's needs.

The Deployment of SOAR's components involves integrating components like TheHive, Cortex, and MISP to enhance incident response capabilities. The Review and Audit phase assesses the deployed solution for effectiveness, efficiency, and adherence to security standards.

These implementation phases ensure a proactive and adaptive security posture to effectively protect critical assets and maintain overall security.

4.2 Implementation Phases

4.2.1 Design

During the design phase of the project, key aspects were addressed to ensure successful implementation. This included analyzing the problematic description, defining functional requirements, presenting the project objectives, conducting a comparative study of security and network services, designing the physical architecture, and assigning tasks to team members.

The design phase provided a clear roadmap for building an advanced security infrastructure that effectively monitors, detects, and responds to cyber threats. By integrating cutting-edge technologies and allocating responsibilities appropriately, the project team ensured a well-planned and coordinated approach to realizing the next-generation Security Operations Center.

4.2.2 Security Architecture Deployment

In the security architecture deployment phase, we implemented a range of security tools, including firewalls, EDR, honeynet, DLP, NDR, Sysmon, and SIEM.

PfSense and OpenSense were used to create a secure perimeter around our network, enforcing strict access controls and network segmentation to reduce the attack surface and

prevent lateral movement within our network. Snort provided real-time traffic analysis, packet logging, and threat detection, alerting us to potential security
threats in real-time.

In addition to our firewall solution, we also implemented an EDR solution to provide real-time monitoring and protection against advanced threats. Our honeynet, DLP, NDR, Sysmon, and SIEM solutions were also deployed and configured to provide comprehensive protection for our network.

Finally, we configured the communication and networking services according to the best practices and standards outlined in the National Institute of Standards and Technology (NIST) cybersecurity framework. This ensured that the services were deployed and properly configured in a secure and efficient manner. We also ensured that all the services were integrated with each other to provide comprehensive protection for our network.

4.2.3 Deployment of SOAR's components

In the deployment of SOAR components phase, we did the SOAR integration with the various security tools mentioned above.

Our SOAR platform is based on Shuffle to create custom workflows that automated our incident response processes.

For example, when a security incident occurred, the workflow sent alerts to TheHive, which triaged the incident, then to Cortex, which enriched the incident with additional data, and finally to the SIEM, which produced an alert.

The workflows were designed to ensure that our incident response was as efficient and effective as possible. They enabled us to respond to security incidents in real-time, minimizing the damage and reducing the risk of data loss or system downtime.

4.2.4 Review and Audit the Deployed Solution

After deploying and integrating all the necessary security tools and components, we conducted a thorough review and audit of the final solution to ensure its effectiveness and identify any potential vulnerabilities.

To perform the audit, we had a group assigned to us which we would pentest on and vice-versa. We used Nessus and other tools such as Burp Suite to identify vulnerabilities in the systems and generate a detailed report using pwndocs.

During the audit, we found several vulnerabilities in the systems, including outdated library versions, misconfigurations in TLS communication, and other issues. We shared our findings with the other groups, and they also identified vulnerabilities in our system that we promptly fixed.

4.3 Conclusion

In conclusion, the implementation phases of Security Architecture Deployment, Deployment of SOAR's components, and Review and Audit of the Deployed Solution are essential in establishing a comprehensive and effective security infrastructure.

By carefully designing and deploying a robust security architecture, organizations can address their specific security needs and ensure a solid foundation for threat monitoring and risk mitigation.

The integration of SOAR components enhances incident response capabilities, streamlines security operations, and improves overall efficiency. Regular reviews and audits of the deployed solution allow organizations to identify areas for improvement, address vulnerabilities, and optimize performance..

General Conclusion

In conclusion, this project has focused on the realization of a next-generation Security Operations Center (SOC) to address the growing need for advanced security in

modern systems. The project involved several crucial steps, including project overview, project requirements, and project objectives, which provided a clear roadmap for the implementation process. The project overview emphasized the importance of leveraging advanced technologies, automation, and collaboration to stay ahead of potential breaches and minimize their impact. The project requirements encompassed various aspects such as assessing the organization's current security capabilities, selecting appropriate technologies, and developing robust processes and workflows. The project objectives aimed at enhancing threat intelligence capabilities, improving incident detection and response times, and fostering collaboration and information sharing.

The successful implementation of the SOC involved the integration of a wide range of technologies and tools such as ELK stack, Snort, Wazuh, Zabbix, Sysmon, TheHive, Cortex, MISP, Shuffle, NAXSI, ClamAV, Pfsense, Opensense, EXDR, Elastic XDR, NGINX, and reNgine. These components formed a comprehensive security infrastructure, enabling proactive threat monitoring, efficient incident response, and collaboration among stakeholders.

Throughout the project, a strong emphasis was placed on following industry best practices and adhering to NIST standards to ensure a robust and secure SOC solution. The project also involved the deployment of complementary frameworks such as SOAR (Security Orchestration, Automation, and Response) to enhance incident management, automate routine tasks, and improve overall security operations.

By implementing these steps and leveraging advanced technologies, the project successfully established a next-generation SOC that enables banking organizations to effectively monitor, detect, and respond to cyber threats in a proactive and efficient manner. The project's outcomes include an enhanced security posture, protection of critical assets and data, and continuous improvement through regular monitoring and optimization.

To conclude, this project serves as a strategic initiative to align security operations with industry standards and best practices, ensuring that organizations are well-equipped to mitigate the risks posed by evolving cyber threats. By following the established roadmap and incorporating cutting-edge technologies, organizations can establish a robust security infrastructure capable of effectively safeguarding their digital assets.