4 july- 4 september 2024

Next Gen SOC at ANCS

Agence Nationale de la Cybersécurité

www.ancs.tn

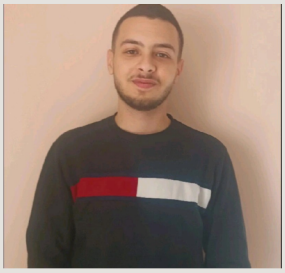
Linkedin :
@ANCS - tunCERT

Sommaire

Equipe

Mariem Mahjoub

MENTOR



Aziz Jaballah

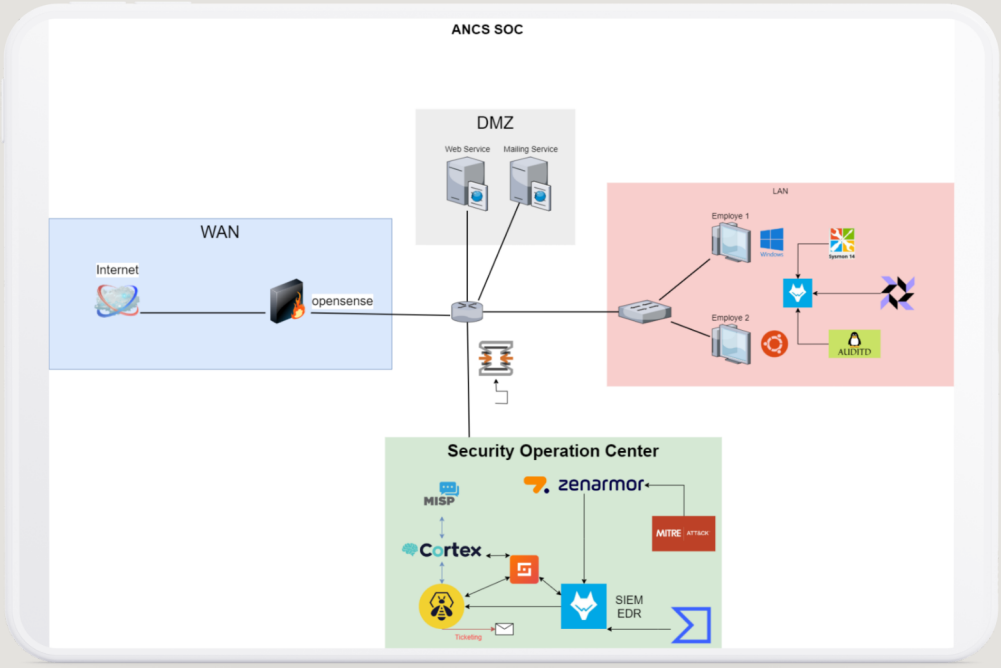
INTERN

I would like to express my sincere gratitude to Mrs. Mariem Mahjoub, Security Engineer and Head of National Cyberspace Supervision - ISAC, for her guidance and valuable support throughout this internship. Her expertise, insightful advice, and constant availability have greatly contributed to the success of this project and have allowed me to develop my skills in a rewarding professional environment.

1 Introduction

Traditional Security Operations Centers (SOCs) play a key role in detecting and managing security incidents within enterprise infrastructures. However, they often face challenges related to slow response times, a lack of automation, and a limited capacity to handle the increasing complexity and volume of cyber threats. These limitations reduce the effectiveness of traditional SOCs in proactively preventing attacks and swiftly managing incidents.

To address these challenges, my project aims to implement a next-generation SOC, integrating advanced tools such as Wazuh, TheHive, MISP, Cortex, OPNsense with Zenarmor, and Shuffle SOAR. This automated SOC is capable of detecting, analyzing, and responding to security incidents autonomously, thereby reducing reliance on manual interventions. This project offers a modern solution to enhance threat response capabilities while increasing resilience against cyberattacks.



2 Company Overview

Faced with the growing challenges of cybersecurity, ANCS implements concrete actions to strengthen the protection of Tunisia's cyberspace. It develops appropriate regulatory frameworks, supports the implementation of robust security measures within organizations, and encourages information sharing and best practices among industry stakeholders. ANCS also works closely with international partners to address cross-border cybersecurity challenges.

ANCS helps to maintain trust in the digital economy and promotes the development of a secure and reliable digital environment for Tunisia. Its role is essential in protecting personal data, securing critical infrastructures, and supporting economic growth.

49, avenue Jean Jaurès, 1000 Tunis

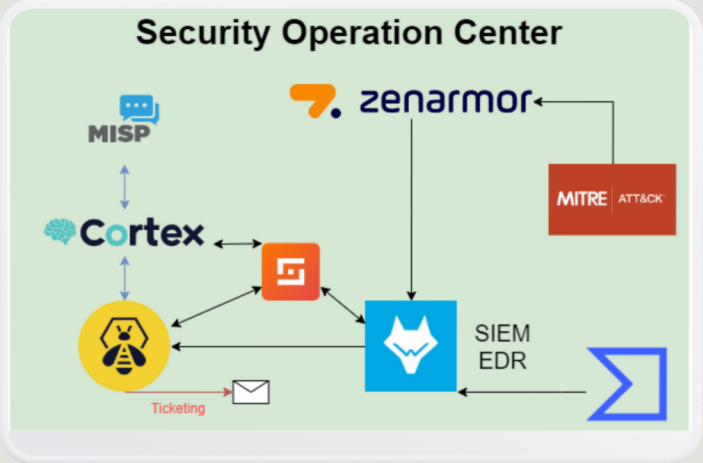
www.ancs.tn

71 843 200

@Ancs -CERT

3 Project Phases

We divided the project into four phases to structure and facilitate the gradual implementation of the various components of our security infrastructure.



Phase 1

Focuses on the installation of machines and the configuration of the OPNsense infrastructure to establish a secure network foundation.

Phase 2

Covers the installation and configuration of SIEM and SOAR tools (Wazuh, Shuffle, Hive, Cortex, and MISP) to ensure centralized monitoring and incident response.

Phase 3

Dedicated to the automated response of the NIDS with Zenarmor and Suricata, aiming to enhance network intrusion detection.

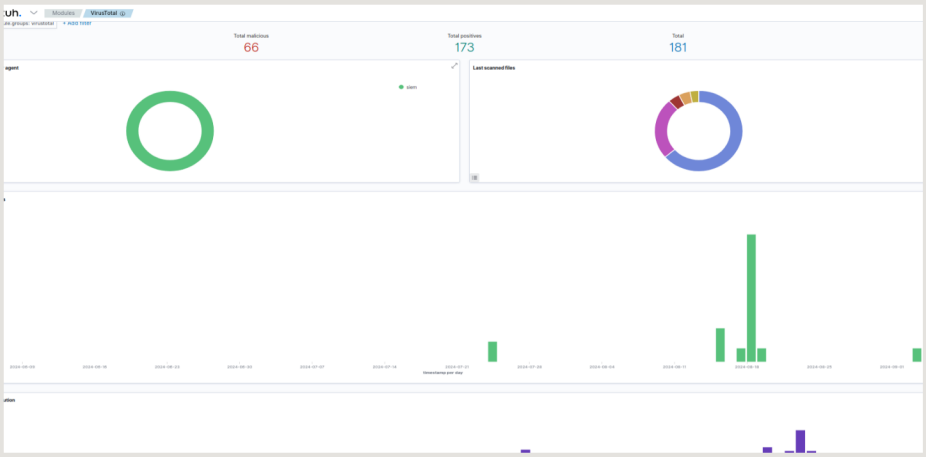
Phase 4

Integrates automated responses at the HIDS level, including workflows with VirusTotal and Telegram via Shuffle, to provide comprehensive defense against internal and external threats.

4 My Realisations

VIRUSTOTAL

Wazuh plays a key role in detecting malware and unauthorized modifications to critical system files. The integration of VirusTotal enhances this capability by verifying suspicious files through their hash. If a file is identified as malicious by VirusTotal, Wazuh triggers an active response and automatically deletes the file, preventing the threat from spreading within the network. This advanced defense mechanism strengthens security by ensuring continuous monitoring and proactive response.



1- You can view VirusTotal alert data in the Wazuh dashboard.

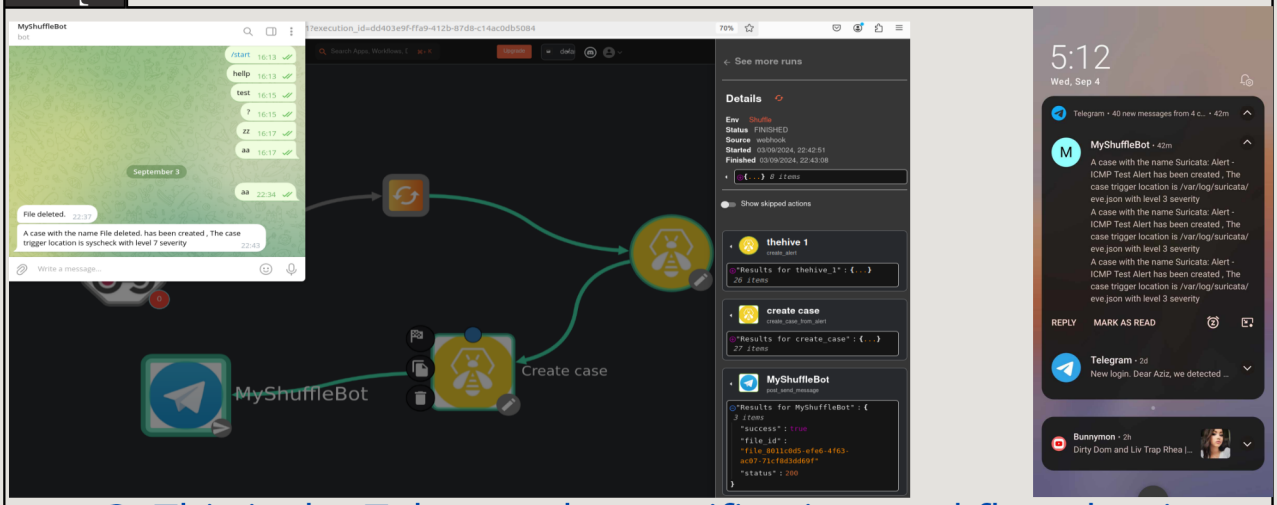
HIVE CASE GENERAATION

Wazuh is also configured to send all security alerts to TheHive, enabling centralized incident management. When an alert exceeds a severity level of 7, an automated integration between Wazuh and TheHive automatically creates a case. This enhances traceability, analysis, and resolution of critical incidents. This approach reduces response time, optimizes incident management, and allows teams to focus on the most serious threats.

2- The image shows a Shuffle SOAR interface with an alert generated by Wazuh and a case automatically created in TheHive. The alert reports a file deletion, and an associated case has been successfully created.

Notifs via TELEGRAM BOT

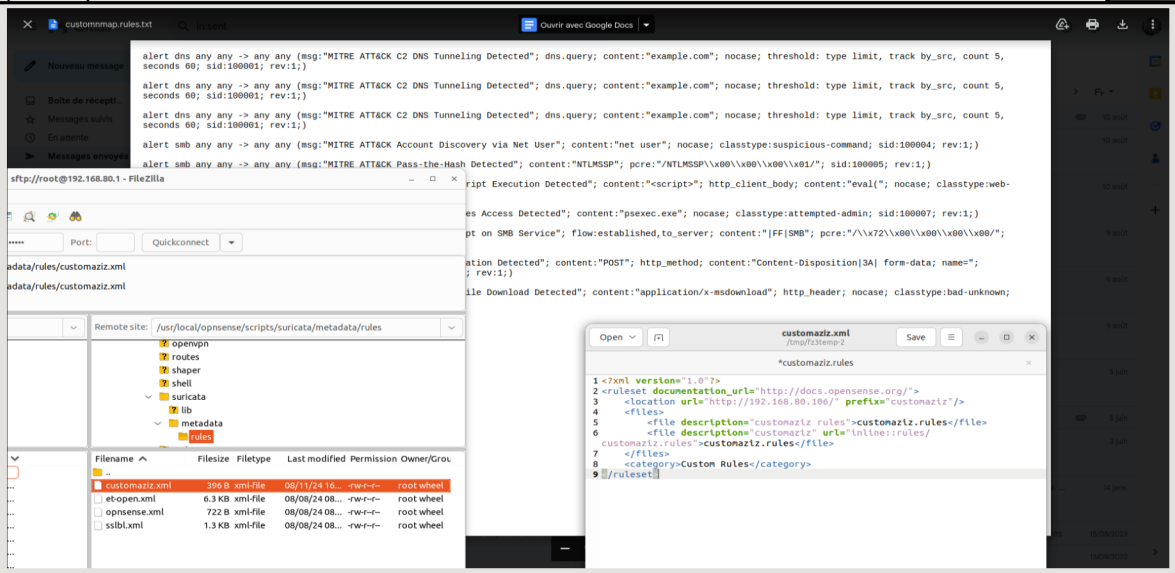
The automated workflow created with Shuffle integrates multiple tools for optimal incident management. When a critical alert is detected by Wazuh with a severity level above 7, a case is automatically generated in TheHive to ensure thorough incident tracking. This integration centralizes alert management and speeds up response times. Additionally, an instant notification is sent via a Telegram bot, informing the team in real time about critical incidents. This fully automated process enhances the SOC's responsiveness and efficiency by simplifying alert management.



3- This is the Telegram bot notification workflow that is triggered when a case is created in TheHive.

SURICATA & Mitre Att&ck

The integration of Suricata with MITRE ATT&CK rules enhances threat detection within the network. Suricata, as a NIDS, analyzes network traffic in real time to identify malicious behavior. Custom rules based on the MITRE ATT&CK framework provide a structured approach to recognizing known attack tactics and techniques. This integration not only detects sophisticated intrusion attempts but also improves the understanding of attacker methods, thereby strengthening the SOC's response capability.

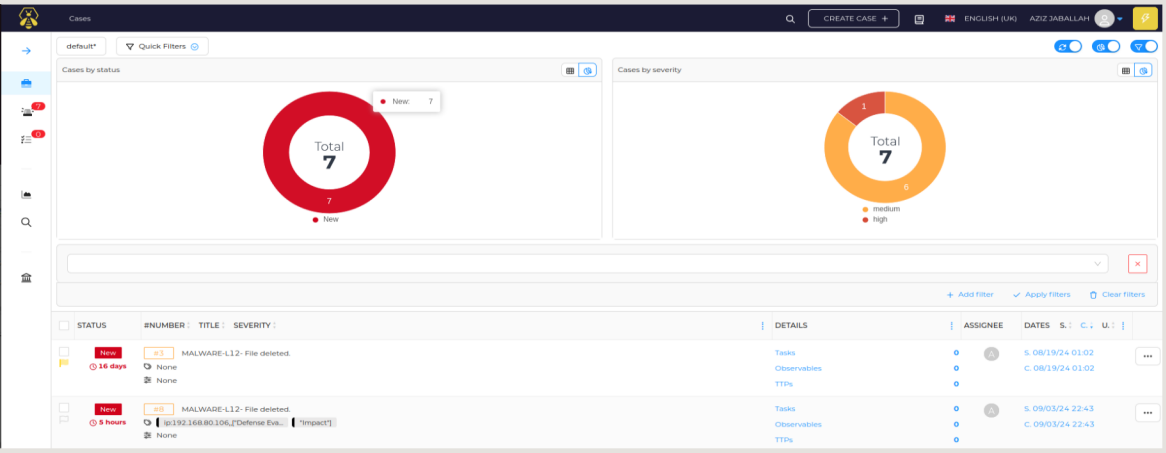


4-Rules injection via FileZilla

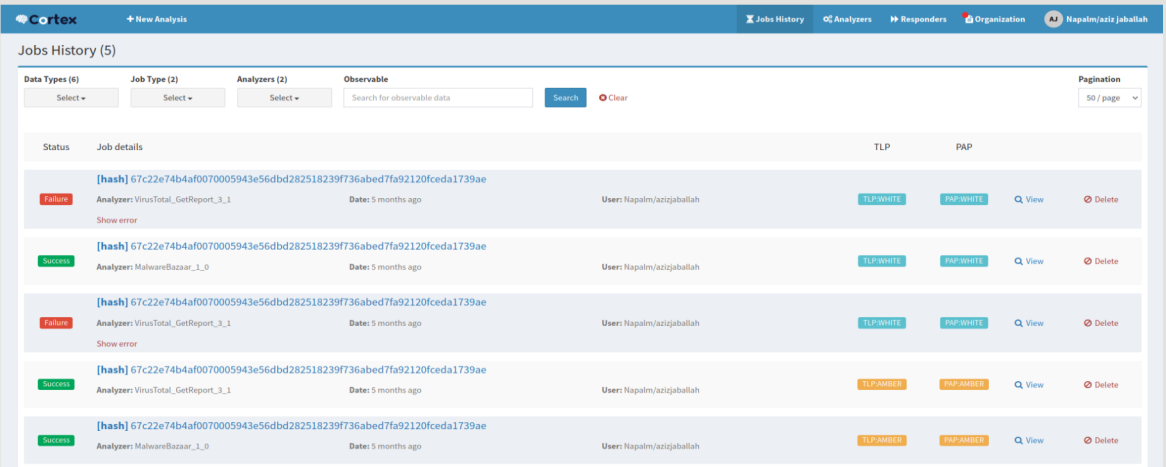
ZENARMOR

The integration of Zenarmor into OPNsense enables advanced network intrusion detection (NIDS). This module analyzes network traffic in real time and identifies suspicious or malicious activities. With its ability to block threats in real time, Zenarmor enhances infrastructure security by acting as a barrier against potential attacks. The integration of this module has provided increased monitoring of network entry points and strengthened the perimeter protection aspect of the project.

5-Zenarmor dashboard



6-Hive Dashboard



7-Cortex Dashboard

5 Internship Summary

By the end of my internship, I acquired strong technical skills in integrating and configuring advanced security solutions, particularly with Wazuh, TheHive, OPNsense, Suricata, and Shuffle SOAR. I learned how to build a cohesive security infrastructure by integrating SIEM, SOAR, and intrusion detection tools while developing automated threat responses.

This experience allowed me to better understand the challenges of implementing a next-generation SOC, especially integrating open-source tools like Wazuh, TheHive, MISP, and Suricata. Among the complex technical issues, I had to solve challenges related to API integration between these tools to ensure seamless communication, as well as the advanced configuration of detection rules and automation workflows via Shuffle SOAR. This internship also strengthened my ability to tackle these challenges effectively.

6 Conclusion

To conclude this internship report, it is important to highlight the close relationship between this project and the activities of a CSIRT (Computer Security Incident Response Team). The project established an integrated infrastructure for incident detection and response, aligned with CSIRT best practices. By integrating tools such as Wazuh for monitoring and detection, Shuffle for automated responses, and OPNsense for network protection, we created an environment that enhances the ability to respond quickly and effectively to security incidents. This project demonstrates how a coordinated and automated approach can improve incident response processes, thereby reducing risks and strengthening overall cybersecurity posture.

Intern's Signature