

4 juillet - 4
septembre
2024

Mise en place d'un NEXT GEN SOC

Agence Nationale de la Cybersécurité



www.ancs.tn

Linkedin :
@ANCS – tunCERT

Sommaire

1

Introduction

p3

2

Présentation de l'entreprise &
Remerciement

p4

3

Les phases de projet

p6

4

Mes réalisations

p7

5

Bilan du stage

p10

6

Conclusion

p11

Equipe



Mariem
Mahjoub

ENCADRANTE



Aziz
Jaballah

STAGIAIRE

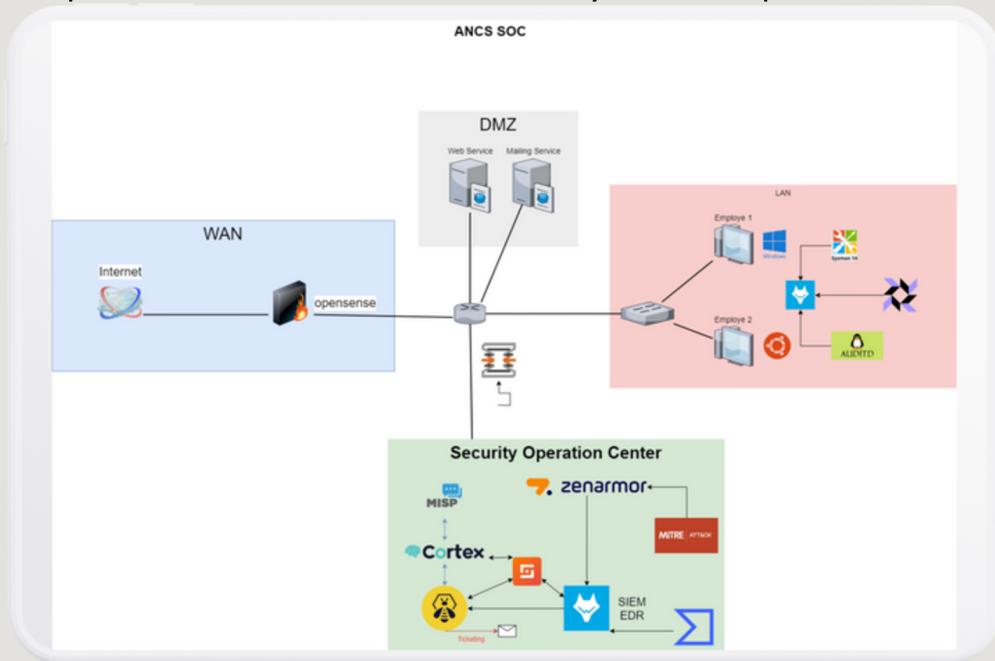
Je tiens à exprimer mes sincères remerciements à Mme Mariem Mahjoub, Ingénieur Sécurité et Chef de service supervision du Cyberspace national - ISAC, pour son encadrement et son soutien précieux tout au long de ce stage. Son expertise, ses conseils avisés et sa disponibilité constante ont grandement contribué à la réussite de ce projet, et m'ont permis de développer mes compétences dans un environnement professionnel enrichissant.

1

Introduction

Les Centres Opérationnels de Sécurité (SOC) traditionnels jouent un rôle clé dans la détection et la gestion des incidents de sécurité au sein des infrastructures d'entreprise. Cependant, ils rencontrent souvent des défis liés à la lenteur des réponses, un manque d'automatisation, et une capacité limitée à faire face à la montée en complexité et volume des menaces cyber. Ces limitations réduisent l'efficacité des SOC traditionnels dans la prévention proactive des attaques et la gestion rapide des incidents.

Face à ces défis, mon projet vise à mettre en place un SOC de nouvelle génération, intégrant des outils avancés comme Wazuh, TheHive, MISP, Cortex, OPNsense avec Zenarmor, et Shuffle SOAR. Ce SOC automatisé est capable de détecter, analyser et répondre automatiquement aux incidents de sécurité, réduisant ainsi la dépendance aux interventions manuelles. Ce projet propose une solution moderne pour améliorer la capacité de réponse aux menaces tout en augmentant la résilience face aux cyberattaques.



2

Présentation de l'entreprise

Face aux enjeux croissants de la cybersécurité, l'ANCS met en œuvre des actions concrètes pour renforcer la protection du cyberespace tunisien. Elle développe des cadres réglementaires adaptés, soutient la mise en place de mesures de sécurité robustes au sein des organisations, et encourage le partage d'informations et les bonnes pratiques entre les acteurs du secteur. L'ANCS travaille également en étroite collaboration avec les partenaires internationaux pour faire face aux défis transfrontaliers de la cybersécurité.

L'ANCS contribue à préserver la confiance dans l'économie numérique et à favoriser le développement d'un environnement numérique sûr et fiable pour la Tunisie. Son action est essentielle pour protéger les données personnelles, les infrastructures critiques et soutenir la croissance économique.

49, avenue Jean Jaurès, 1000 Tunis

www.ancs.tn

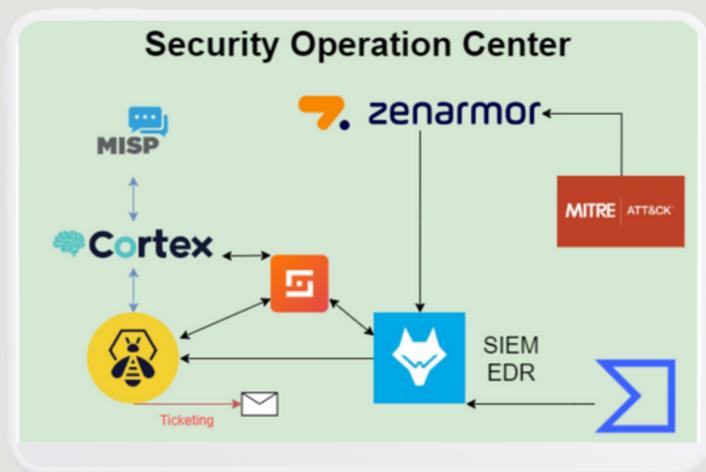
71 843 200

@Ancs -CERT

3

Les phases de projet

Nous avons divisé le projet en quatre phases pour structurer et faciliter l'implémentation progressive des différentes composantes de notre infrastructure de sécurité.



Phase 1

se concentre sur l'installation des machines et la configuration de l'infrastructure OPNsense pour établir une base réseau sécurisée.

Phase 2

Aborde l'installation et la configuration des outils SIEM et SOAR (Wazuh, Shuffle, Hive, Cortex, et MISP) pour assurer une surveillance et une réponse centralisées aux incidents.

Phase 3

Dédiée à la réponse automatisée du NIDS avec Zenarmor et Suricata, vise à renforcer la détection des intrusions réseau.

Phase 4

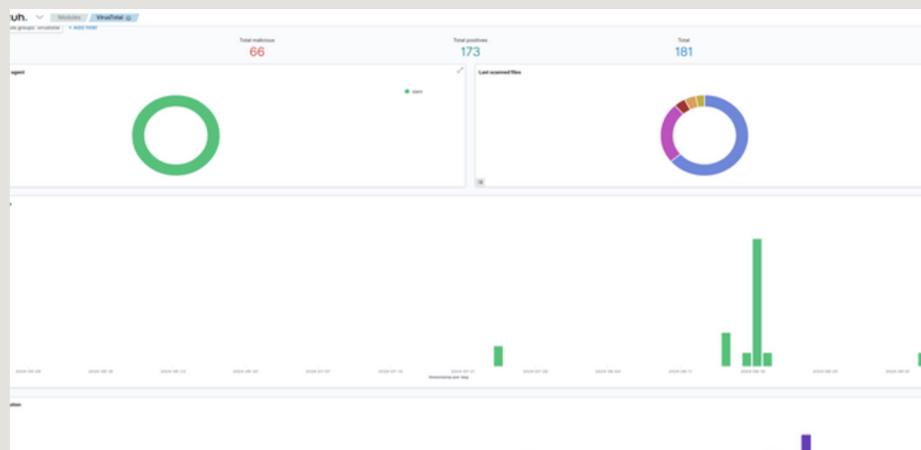
intègre des réponses automatisées au niveau HIDS, incluant des workflows avec VirusTotal et Telegram via Shuffle, pour offrir une défense complète contre les menaces internes et externes.

4

Mes réalisations

VIRUSTOTAL

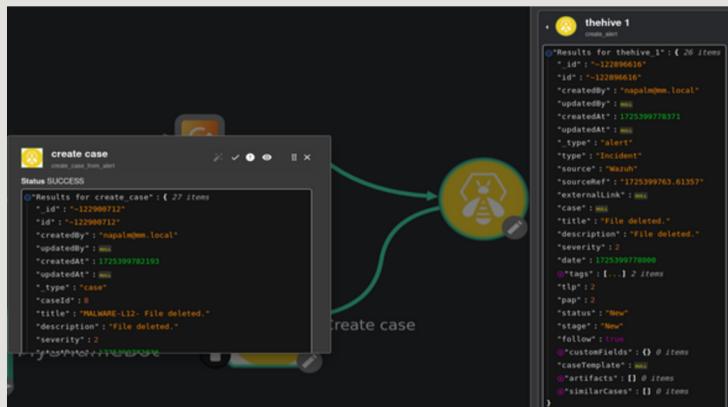
Wazuh joue un rôle clé dans la détection des malwares et des modifications non autorisées sur les fichiers critiques du système. L'ajout de VirusTotal permet d'enrichir cette fonctionnalité en vérifiant les fichiers suspects via leur hash. Si un fichier est identifié comme malveillant par VirusTotal, Wazuh déclenche une réponse active et supprime automatiquement ce fichier, ce qui évite toute propagation de la menace dans le réseau. Ce mécanisme de défense avancé renforce la sécurité en assurant une surveillance continue et une réponse proactive.



1- Vous pouvez visualiser les données d'alerte de VirusTotal dans le tableau de bord de Wazuh.

Wazuh est également configuré pour envoyer toutes les alertes de sécurité à TheHive, permettant une gestion centralisée des incidents. Lorsqu'une alerte dépasse un niveau de严重度 de 7, une intégration automatisée entre Wazuh et TheHive crée automatiquement un cas. Cela permet d'améliorer la traçabilité, l'analyse et la résolution des incidents critiques. Cette approche réduit le temps de réponse, optimise la gestion des incidents et permet aux équipes de se concentrer sur les menaces les plus sérieuses.

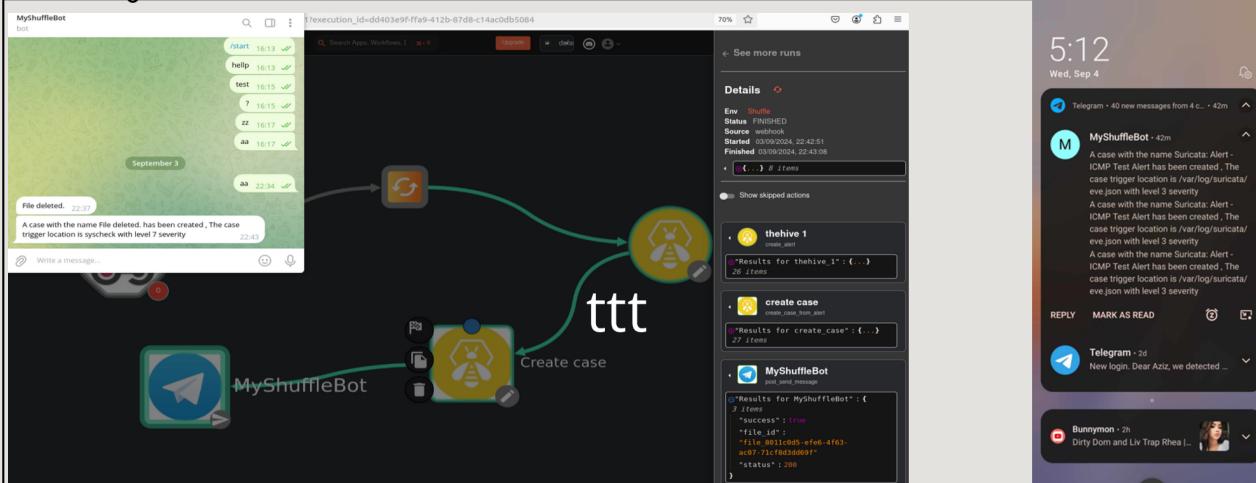
HIVE CASE GENERATION



2-L'image montre une interface Shuffle SOAR avec une alerte générée par Wazuh et un cas créé automatiquement dans TheHive. L'alerte signale une suppression de fichier, et un cas associé est créé avec succès.

Notifs via
TEI ECPAM BOT

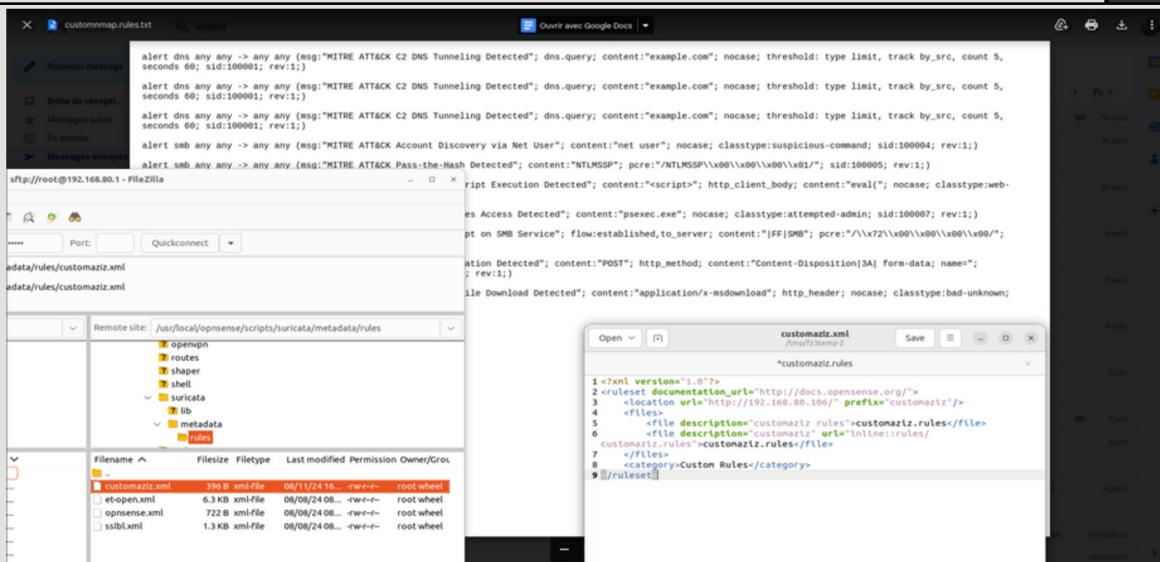
Le workflow automatisé créé avec Shuffle intègre plusieurs outils pour une gestion optimale des incidents. Lorsqu'une alerte critique est détectée par Wazuh, avec une sévérité supérieure à 7, un cas est automatiquement généré dans TheHive pour assurer un suivi rigoureux de l'incident. Cette intégration permet de centraliser la gestion des alertes et d'accélérer les réponses. De plus, une notification instantanée est envoyée via un bot Telegram, informant l'équipe en temps réel des incidents critiques. Ce processus entièrement automatisé améliore la réactivité et l'efficacité du SOC en simplifiant la gestion des alertes.



3-Ceci est le flux de travail de notification du bot Telegram qui se déclenche lors de la création d'un cas dans Hive.

L'intégration de Suricata avec les règles MITRE ATT&CK permet de renforcer la détection des menaces au sein du réseau. Suricata, en tant que NIDS, analyse le trafic réseau en temps réel pour identifier des comportements malveillants. Les règles personnalisées basées sur le framework MITRE ATT&CK fournissent un cadre structuré pour reconnaître les tactiques et techniques d'attaques connues. Cette intégration permet non seulement de détecter des tentatives d'intrusion sophistiquées, mais aussi de mieux comprendre les méthodes utilisées par les attaquants, améliorant ainsi la capacité de réponse du SOC.

SURICATA &
Mitre Att&ck



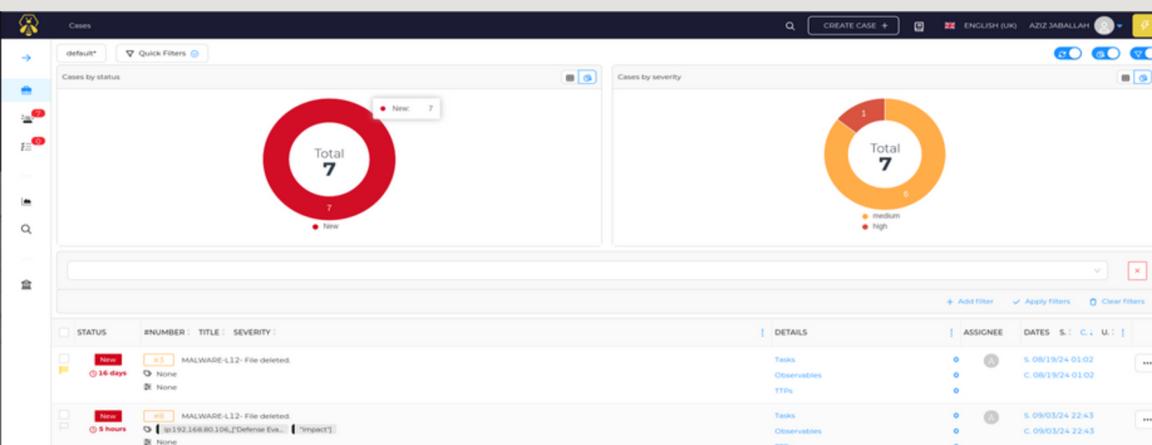
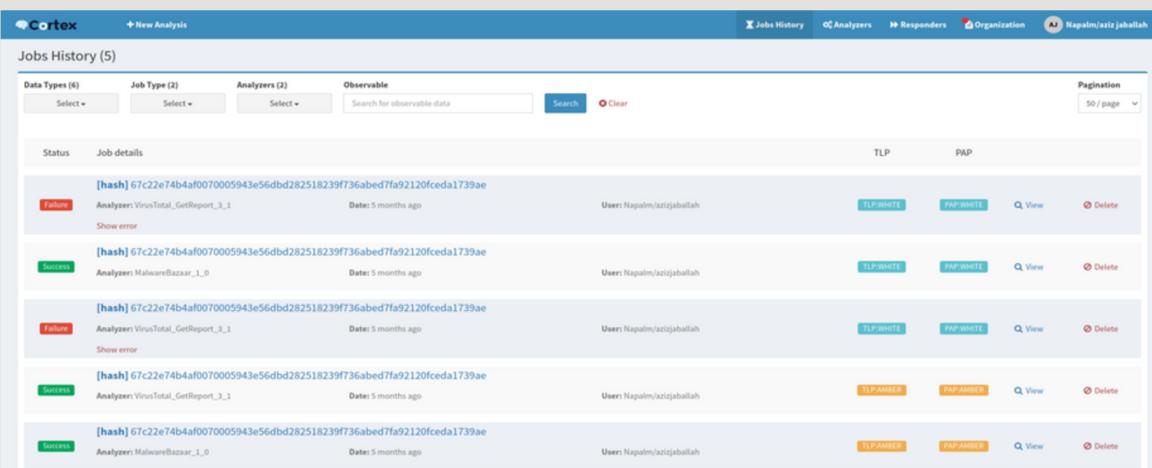
4-Rules injection via FileZilla

ZENARMOR

L'intégration de Zenarmor dans OPNsense permet une détection avancée des intrusions réseau (NIDS). Ce module analyse en temps réel le trafic réseau et identifie les activités suspectes ou malveillantes. Avec sa capacité à bloquer les menaces en temps réel, Zenarmor renforce la sécurité de l'infrastructure en agissant comme une barrière contre les attaques potentielles. L'intégration de ce module a apporté une surveillance accrue des points d'entrée réseau et a complété l'aspect protection périphérique du projet.



5-Zenarmor dashboard

6-Hive
Dashboard7-Cortex
Dashboard

5

Bilan du stage

Au terme de mon stage, j'ai acquis des compétences techniques solides dans l'intégration et la configuration de solutions de sécurité avancées, notamment avec Wazuh, TheHive, OPNsense, Suricata, et Shuffle SOAR. J'ai appris à créer une infrastructure de sécurité cohérente en intégrant des systèmes SIEM, SOAR, et des outils de détection d'intrusions, tout en développant des réponses automatisées aux menaces.

Cette expérience m'a permis de mieux comprendre les défis liés à la mise en place d'un SOC de nouvelle génération, notamment l'intégration d'outils open-source comme Wazuh, TheHive, MISP et Suricata. Parmi les problèmes techniques complexes, j'ai dû résoudre des difficultés liées à l'intégration des API entre ces différents outils pour assurer une communication fluide, ainsi que la configuration avancée des règles de détection et des workflows d'automatisation via Shuffle SOAR. Ce stage a également renforcé ma capacité à résoudre ces défis.



6

Conclusion

Pour conclure ce rapport de stage, il est important de souligner la relation étroite entre ce projet et les activités d'un CSIRT (Computer Security Incident Response Team). Le projet a permis de mettre en place une infrastructure intégrée de détection et de réponse aux incidents, alignée sur les bonnes pratiques d'un CSIRT. En intégrant des outils comme Wazuh pour la surveillance et la détection, Shuffle pour l'automatisation des réponses, et OPNsense pour la protection du réseau, nous avons créé un environnement qui renforce la capacité à réagir rapidement et efficacement aux incidents de sécurité. Ce projet illustre comment une approche coordonnée et automatisée peut améliorer les processus de réponse aux incidents, réduisant ainsi les risques et renforçant la posture de cybersécurité globale.



signature stagiaire