École Nationale des Sciences Appliquées de Marrakech

Filière : Cybersécurité

Cyber Chaos Arena

SOC intelligent avec IA locale, visualisation et remédiation automatisée

Réalisé par :

Halima

Ikram

Oussama

Asma

Sayf

Encadré par :

Omar Achbarou

Année universitaire : 2025–2026

Dédicaces

Nous dédions ce travail à nos familles, à nos enseignants et à toutes les personnes qui nous ont encouragés durant la réalisation de ce projet. Ce travail est le résultat d'un effort collectif, d'une persévérance technique et d'une volonté de comprendre concrètement les mécanismes d'un SOC moderne.

Remerciements

Nous remercions notre encadrant Monsieur Omar Achbarou pour son accompagnement, ses orientations et ses remarques constructives. Nous remercions également l'ensemble des enseignants de la filière Cybersécurité de l'ENSA Marrakech pour les connaissances transmises dans les domaines des réseaux, des systèmes, de la sécurité défensive et de la supervision.

Résumé

Ce rapport présente la conception et la réalisation de *Cyber Chaos Arena*, une solution SOC expérimentale intégrant la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation automatisée. Les logs provenant d'une passerelle login et d'un honeypot sont centralisés dans Splunk, analysés par Ollama, transmis vers Grafana via Logstash et exploités par une interface Flask de remédiation. La contribution principale est une blacklist dynamique NGINX permettant de rediriger les IP malveillantes vers un honeypot au lieu de bloquer simplement le trafic. Cette approche protège le service réel tout en maintenant une observation active de l'attaquant.

Mots-clés : SOC, SIEM, SOAR, Splunk, Grafana, Logstash, Ollama, Honeypot, NGINX, blacklist dynamique, remédiation, MITRE ATT&CK.

Abstract

This report presents the design and implementation of *Cyber Chaos Arena*, an experimental SOC solution integrating log collection, local AI analysis, visualization and automated remediation. Logs from a login gateway and a honeypot are centralized in Splunk, analyzed by Ollama, forwarded to Grafana through Logstash and used by a Flask remediation interface. The main contribution is a dynamic NGINX blacklist that redirects malicious IP addresses to a honeypot instead of simply dropping the traffic. This protects the real service while preserving attacker visibility.

Mots-clés

SOC, SIEM, SOAR, Splunk, Grafana, Logstash, Ollama, IA locale, Honeypot, NGINX, Reverse proxy, Blacklist dynamique, Remédiation automatisée, MITRE ATT&CK, Webhook, JSON.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

SOC	Security Operations Center
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
IA	Intelligence Artificielle
NGINX	Reverse proxy et serveur web
WAF	Web Application Firewall
VPN	Virtual Private Network
JSON	JavaScript Object Notation
MITRE ATT&CK	Base de connaissances des tactiques et techniques adverses

Introduction générale

La cybersécurité moderne exige des solutions capables de détecter rapidement les attaques, de comprendre leur impact et de réagir de manière adaptée. Dans un SOC, les analystes doivent traiter des volumes importants de journaux provenant de plusieurs sources. Ce projet propose une chaîne complète de sécurité défensive : collecte des logs, analyse par IA locale, visualisation et remédiation contrôlée. L'objectif n'est pas uniquement d'afficher des alertes, mais de transformer chaque événement important en décision opérationnelle. La solution conçue s'appuie sur Splunk, Ollama, NGINX, Grafana, Logstash et Flask. Elle introduit une stratégie de déception : les adresses IP considérées comme malveillantes peuvent être redirigées automatiquement vers un honeypot afin de protéger le service réel tout en continuant à observer l'attaquant.

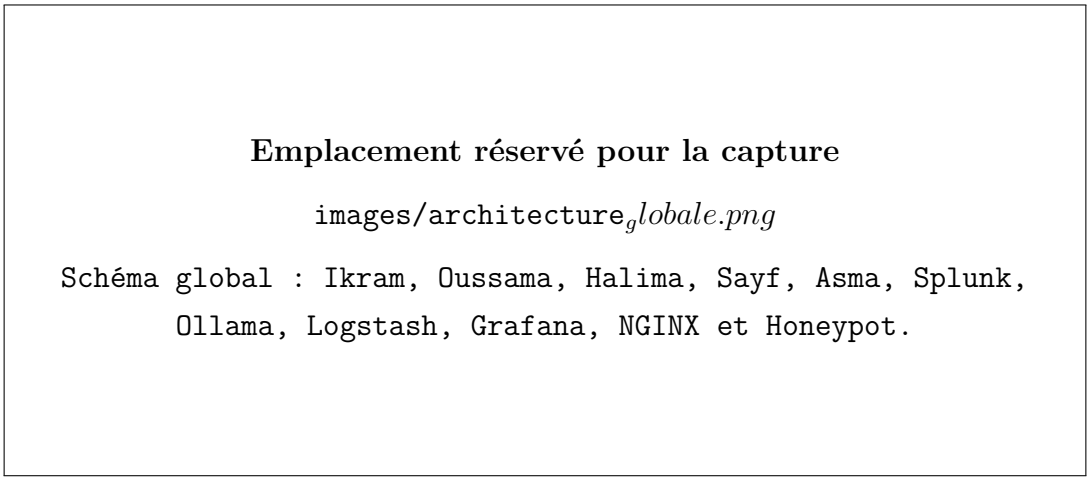

FIGURE 1 – Architecture globale de Cyber Chaos Arena

Chapitre 1

Contexte général du projet

1.1 Présentation du cadre général

Cette partie présente l'élément extbfPrésentation du cadre général dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

1.2 Présentation du projet

Cette partie présente l'élément extbfPrésentation du projet dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

1.3 Motivation du projet

Cette partie présente l'élément extbfMotivation du projet dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

1.4 Enjeux du domaine

Cette partie présente l'élément extbfEnjeux du domaine dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

1.5 Présentation de l'équipe et répartition fonctionnelle

Cette partie présente l'élément extbfPrésentation de l'équipe et répartition fonctionnelle dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises

vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Table 1.1 – Répartition fonctionnelle de l'équipe

Membre	**Rôle principal**
Ikram	Passerelle login, génération d'attaques web, logs d'authentification.
Oussama	Honeypot, logs de terminal, commandes suspectes et événements runtime.
Halima	Splunk, Ollama, interface de remédiation, blacklist dynamique et intégration.
Asma	Visualisation Grafana et réception des rapports IA via Logstash.
Sayf	Analyse IA, recommandations et logique de décision.

1.6 Vision globale de la solution proposée

Cette partie présente l'élément extbfVision globale de la solution proposée dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

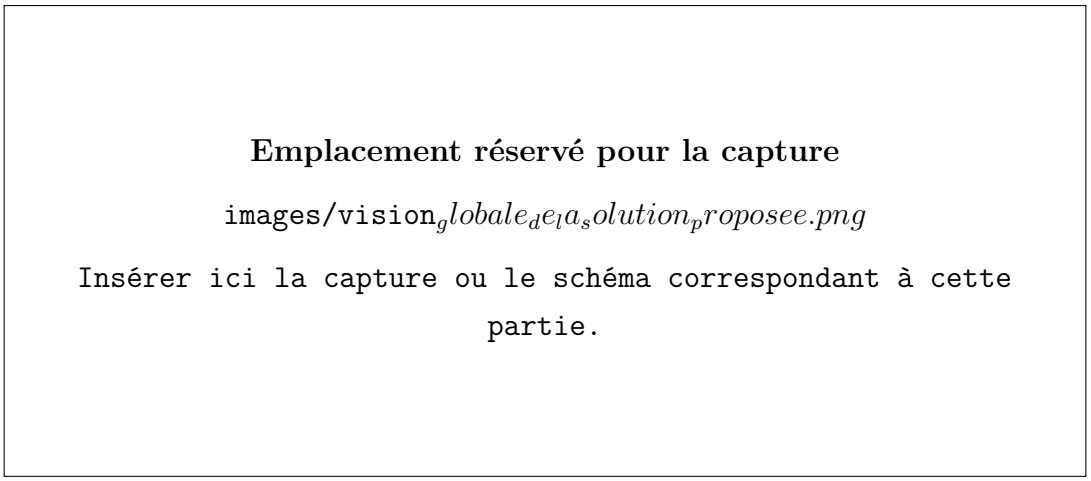

FIGURE 1.1 – Vision globale de la solution proposée

1.7 Organisation du rapport

Cette partie présente l'élément extbfOrganisation du rapport dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Chapitre 2

Problématique et objectifs

2.1 Contexte de la problématique

Cette partie présente l'élément extbfContexte de la problématique dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

2.2 Problématique principale

Cette partie présente l'élément extbfProblématique principale dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

2.3 Limites des approches existantes

Cette partie présente l'élément extbfLimites des approches existantes dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

2.4 Objectif général du projet

Cette partie présente l'élément extbfObjectif général du projet dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

2.5 Objectifs spécifiques

Cette partie présente l'élément extbfObjectifs spécifiques dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une

blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

2.6 Contributions principales du projet

Cette partie présente l'élément extbfContributions principales du projet dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

2.7 Résultats attendus

Cette partie présente l'élément extbfRésultats attendus dans le cadre du projet extit-Cyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Chapitre 3

Étude théorique et état de l'art

3.1 Security Operations Center

Cette partie présente l'élément extbfSecurity Operations Center dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

3.2 Supervision et analyse des événements de sécurité

Cette partie présente l'élément extbfSupervision et analyse des événements de sécurité dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu

du service réel.

3.3 SIEM et centralisation des logs

Cette partie présente l'élément extbfSIEM et centralisation des logs dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

3.4 SOAR et automatisation de la réponse aux incidents

Cette partie présente l'élément extbfSOAR et automatisation de la réponse aux incidents dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

3.5 Honeypot et mécanismes de déception

Cette partie présente l'élément extbfHoneypot et mécanismes de déception dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

3.6 Reverse proxy et filtrage du trafic

Cette partie présente l'élément extbfReverse proxy et filtrage du trafic dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

3.7 Blacklist dynamique

Cette partie présente l'élément extbfBlacklist dynamique dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

La blacklist dynamique est un élément central de la remédiation. Elle ne se limite pas à bloquer l'adresse IP, mais applique une stratégie de déception : l'adresse jugée malveillante est dirigée vers un honeypot. Cette approche permet de protéger le vrai service tout en maintenant une visibilité sur le comportement de l'attaquant.

Listing 3.1 – Exemple d'entrée dans la blacklist NGINX

```
10.79.241.251 1;
```

3.8 Intelligence artificielle locale

Cette partie présente l'élément extbfIntelligence artificielle locale dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Le webhook local reçoit les alertes Splunk au format JSON et les transmet vers Ollama. L'intérêt d'Ollama est de conserver l'analyse localement tout en produisant un résultat lisible par les autres modules. Le rapport IA contient notamment le type d'attaque, la sévérité, le score de confiance, l'explication et les actions recommandées.

Listing 3.2 – Exemple de sortie IA simplifiée

```
{
  "attack_type": "SQL Injection",
  "severity": "high",
  "confidence": 98,
  "recommended_action": ["alert_soc", "block_ip", "
     investigate_host"]
}
```

3.9 MITRE ATTCK

Cette partie présente l'élément extbfMITRE ATTCK dans le cadre du projet extit-Cyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises

vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

3.10 Visualisation des événements de sécurité

Cette partie présente l'élément extbfVisualisation des événements de sécurité dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

FIGURE 3.1 – Visualisation des événements de sécurité

3.11 Comparaison des approches existantes

Cette partie présente l'élément extbfComparaison des approches existantes dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

3.12 Synthèse de l'étude théorique

Cette partie présente l'élément extbfSynthèse de l'étude théorique dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Chapitre 4

Analyse des besoins

4.1 Présentation des acteurs du système

Cette partie présente l'élément extbfPrésentation des acteurs du système dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

4.2 Besoins fonctionnels

Cette partie présente l'élément extbfBesoins fonctionnels dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

4.3 Besoins non fonctionnels

Cette partie présente l'élément extbfBesoins non fonctionnels dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

4.4 Besoins de sécurité

Cette partie présente l'élément extbfBesoins de sécurité dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

4.5 Besoins de supervision

Cette partie présente l'élément extbfBesoins de supervision dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une

blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

4.6 Besoins liés à la remédiation

Cette partie présente l'élément extbfBesoins liés à la remédiation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

4.7 Contraintes techniques

Cette partie présente l'élément extbfContraintes techniques dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

4.8 Contraintes réseau

Cette partie présente l'élément extbfContraintes réseau dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

4.9 Contraintes d'intégration

Cette partie présente l'élément extbfContraintes d'intégration dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

4.10 Synthèse des besoins

Cette partie présente l'élément extbfSynthèse des besoins dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Chapitre 5

Analyse et conception

5.1 Méthodologie de conception adoptée

Cette partie présente l'élément extbfMéthodologie de conception adoptée dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

5.2 Diagramme de cas d'utilisation

Cette partie présente l'élément extbfDiagramme de cas d'utilisation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

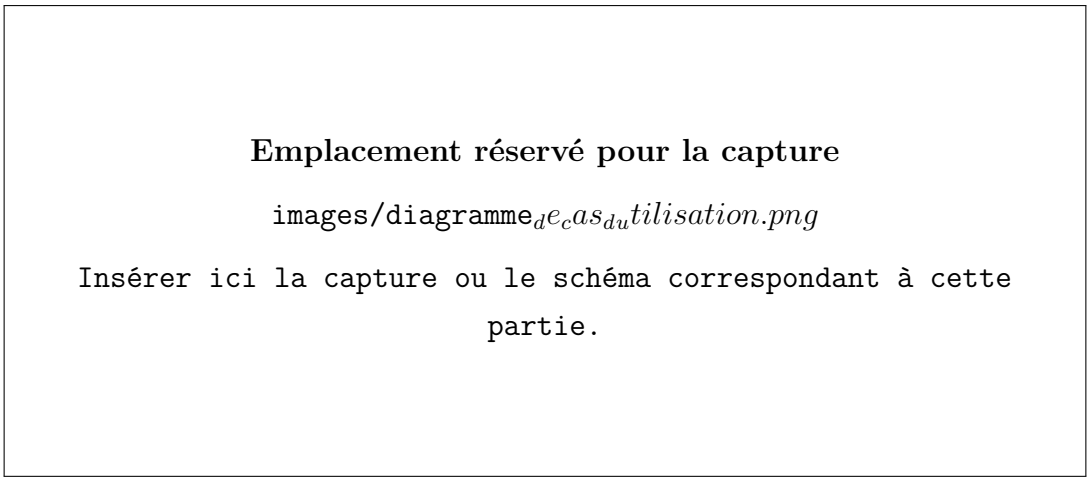

FIGURE 5.1 – Diagramme de cas d'utilisation

5.3 Description des cas d'utilisation

Cette partie présente l'élément extbfDescription des cas d'utilisation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

5.4 Diagramme d'activité du processus global

Cette partie présente l'élément extbfDiagramme d'activité du processus global dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu

du service réel.

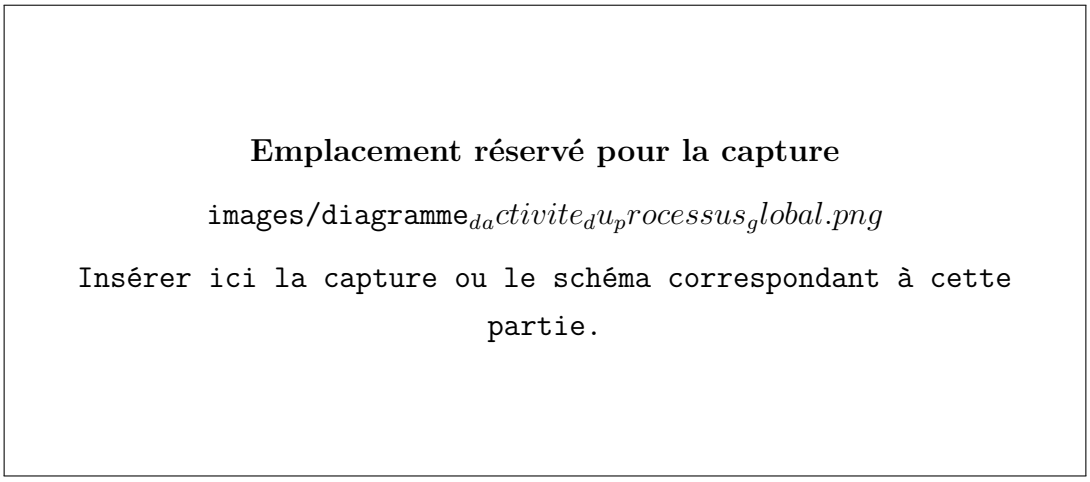

FIGURE 5.2 – Diagramme d'activité du processus global

5.5 Modèle de décision

Cette partie présente l'élément extbfModèle de décision dans le cadre du projet extit-Cyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

5.6 Modèle de données des incidents

Cette partie présente l'élément extbfModèle de données des incidents dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une

blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

5.7 Diagramme conceptuel de la solution

Cette partie présente l'élément extbfDiagramme conceptuel de la solution dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

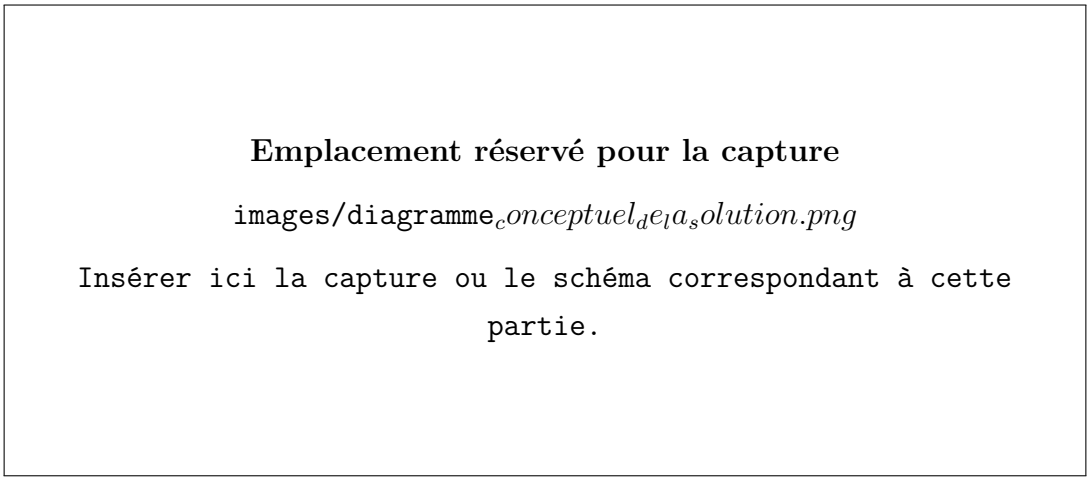

FIGURE 5.3 – Diagramme conceptuel de la solution

5.8 Règles de décision appliquées

Cette partie présente l'élément extbfRègles de décision appliquées dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une

explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

5.9 Scénarios de fonctionnement

Cette partie présente l'élément extbfScénarios de fonctionnement dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

5.10 Synthèse de la conception

Cette partie présente l'élément extbfSynthèse de la conception dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Chapitre 6

Choix technologiques

6.1 Critères de choix des technologies

Cette partie présente l'élément extbfCritères de choix des technologies dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

6.2 Choix du système de collecte des logs

Cette partie présente l'élément extbfChoix du système de collecte des logs dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

6.3 Choix de la plateforme de visualisation

Cette partie présente l'élément extbfChoix de la plateforme de visualisation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

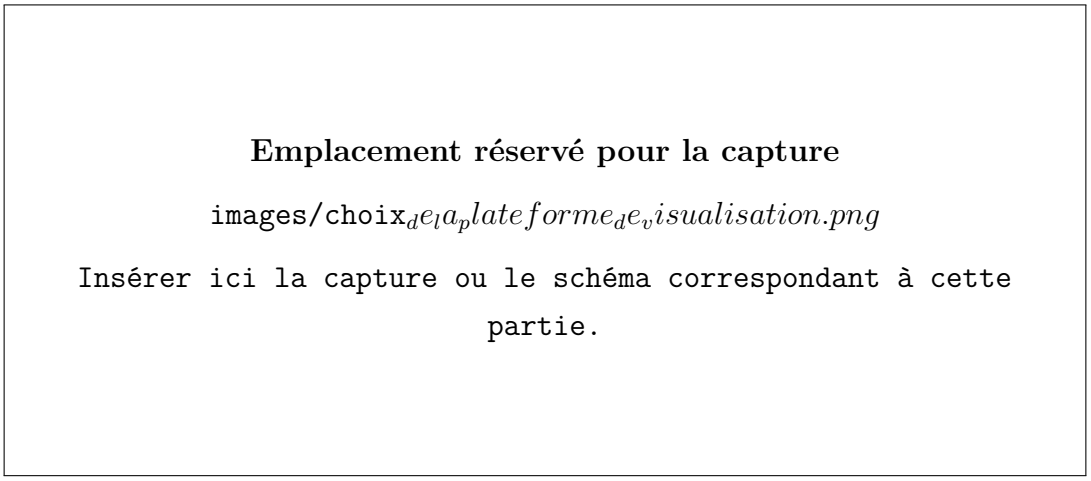

FIGURE 6.1 – Choix de la plateforme de visualisation

6.4 Choix du moteur d'intelligence artificielle locale

Cette partie présente l'élément extbfChoix du moteur d'intelligence artificielle locale dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Le webhook local reçoit les alertes Splunk au format JSON et les transmet vers Ollama. L'intérêt d'Ollama est de conserver l'analyse localement tout en produisant un résultat lisible par les autres modules. Le rapport IA contient notamment le type d'attaque, la sévérité, le score de confiance, l'explication et les actions recommandées.

Listing 6.1 – Exemple de sortie IA simplifiée

```
{
  "attack_type": "SQL Injection",
  "severity": "high",
  "confidence": 98,
  "recommended_action": ["alert_soc", "block_ip", "
     investigate_host"]
}
```

6.5 Choix du langage d'automatisation

Cette partie présente l'élément extbfChoix du langage d'automatisation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

6.6 Choix du reverse proxy

Cette partie présente l'élément extbfChoix du reverse proxy dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une

blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

6.7 Choix de la blacklist dynamique

Cette partie présente l'élément extbfChoix de la blacklist dynamique dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

La blacklist dynamique est un élément central de la remédiation. Elle ne se limite pas à bloquer l'adresse IP, mais applique une stratégie de déception : l'adresse jugée malveillante est dirigée vers un honeypot. Cette approche permet de protéger le vrai service tout en maintenant une visibilité sur le comportement de l'attaquant.

Listing 6.2 – Exemple d'entrée dans la blacklist NGINX

```
1 10.79.241.251 1;
```

6.8 Choix du webhook local

Cette partie présente l'élément extbfChoix du webhook local dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Le webhook local reçoit les alertes Splunk au format JSON et les transmet vers Ollama. L'intérêt d'Ollama est de conserver l'analyse localement tout en produisant un résultat

lisible par les autres modules. Le rapport IA contient notamment le type d'attaque, la sévérité, le score de confiance, l'explication et les actions recommandées.

Listing 6.3 – Exemple de sortie IA simplifiée

```
{
  "attack_type": "SQL Injection",
  "severity": "high",
  "confidence": 98,
  "recommended_action": ["alert_soc", "block_ip", "
     investigate_host"]
}
```

6.9 Comparaison avec d'autres solutions possibles

Cette partie présente l'élément extbfComparaison avec d'autres solutions possibles dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

6.10 Synthèse des choix technologiques

Cette partie présente l'élément extbfSynthèse des choix technologiques dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Chapitre 7

Architecture détaillée de la solution

7.1 Architecture globale du projet

Cette partie présente l'élément extbfArchitecture globale du projet dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

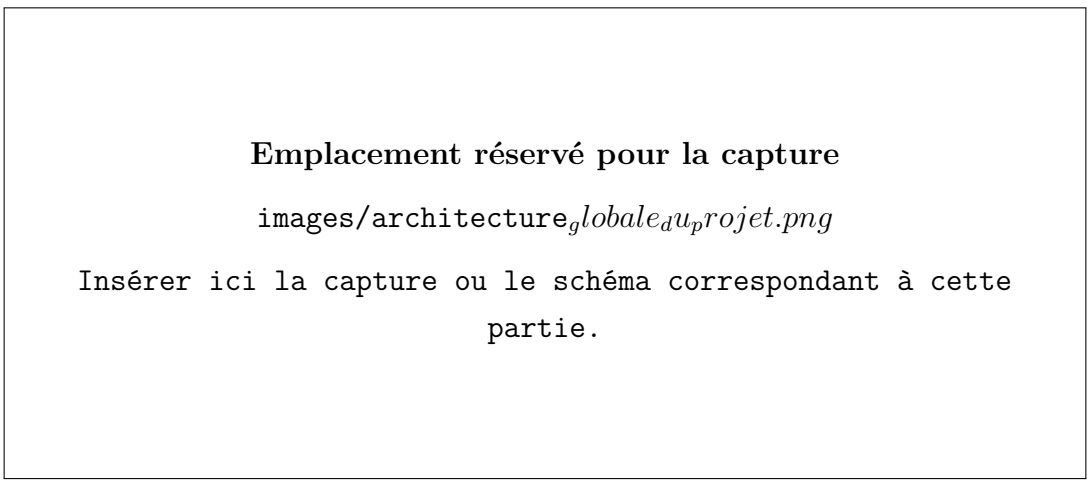

FIGURE 7.1 – Architecture globale du projet

7.2 Architecture logique

Cette partie présente l'élément extbfArchitecture logique dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

FIGURE 7.2 – Architecture logique

7.3 Architecture physique

Cette partie présente l'élément extbfArchitecture physique dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Emplacement réservé pour la capture

`images/architecture_physique.png`

`Insérer ici la capture ou le schéma correspondant à cette partie.`

FIGURE 7.3 – Architecture physique

7.4 Description des composants principaux

Cette partie présente l'élément extbfDescription des composants principaux dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

7.5 Flux complet des données

Cette partie présente l'élément extbfFlux complet des données dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu

du service réel.

7.6 Chaîne de détection

Cette partie présente l'élément extbfChaîne de détection dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

7.7 Chaîne d'analyse

Cette partie présente l'élément extbfChaîne d'analyse dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

7.8 Chaîne de remédiation

Cette partie présente l'élément extbfChaîne de remédiation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises

vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

7.9 Communication entre les composants

Cette partie présente l'élément extbfCommunication entre les composants dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

7.10 Format des événements traités

Cette partie présente l'élément extbfFormat des événements traités dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

7.11 Format des données envoyées à la visualisation

Cette partie présente l'élément extbfFormat des données envoyées à la visualisation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste

SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

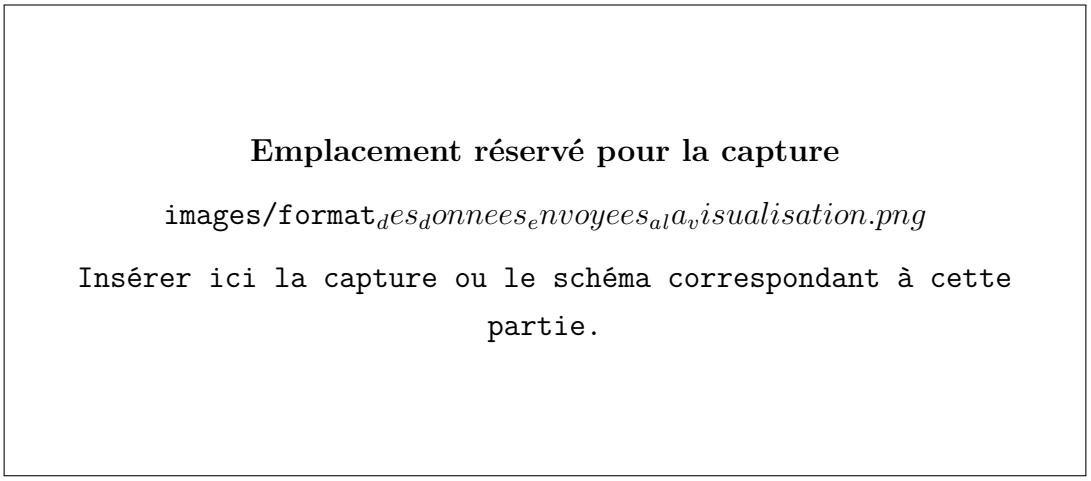

FIGURE 7.4 – Format des données envoyées à la visualisation

7.12 Gestion des erreurs

Cette partie présente l'élément extbfGestion des erreurs dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

7.13 Sécurisation de l'architecture

Cette partie présente l'élément extbfSécurisation de l'architecture dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements

de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

7.14 Synthèse de l'architecture

Cette partie présente l'élément extbfSynthèse de l'architecture dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Chapitre 8

Planification et gestion du projet

8.1 Méthodologie de travail adoptée

Cette partie présente l'élément extbfMéthodologie de travail adoptée dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

8.2 Découpage du projet en phases

Cette partie présente l'élément extbfDécoupage du projet en phases dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

8.3 Répartition des tâches

Cette partie présente l'élément extbfRépartition des tâches dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Table 8.1 – Répartition fonctionnelle de l'équipe

Membre	**Rôle principal**
Ikram	Passerelle login, génération d'attaques web, logs d'authentification.
Oussama	Honeypot, logs de terminal, commandes suspectes et événements runtime.
Halima	Splunk, Ollama, interface de remédiation, blacklist dynamique et intégration.
Asma	Visualisation Grafana et réception des rapports IA via Logstash.
Sayf	Analyse IA, recommandations et logique de décision.

8.4 Planning de réalisation

Cette partie présente l'élément extbfPlanning de réalisation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

8.5 Livrables du projet

Cette partie présente l'élément extbfLivrables du projet dans le cadre du projet extit-Cyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

8.6 Suivi d'avancement

Cette partie présente l'élément extbfSuivi d'avancement dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

8.7 Gestion des risques projet

Cette partie présente l'élément extbfGestion des risques projet dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une

blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

8.8 Difficultés prévues et mesures d'atténuation

Cette partie présente l'élément extbfDifficultés prévues et mesures d'atténuation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

8.9 Synthèse de la planification

Cette partie présente l'élément extbfSynthèse de la planification dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Chapitre 9

Réalisation et implémentation

9.1 Préparation de l'environnement de travail

Cette partie présente l'élément extbfPréparation de l'environnement de travail dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

9.2 Installation et configuration des outils

Cette partie présente l'élément extbfInstallation et configuration des outils dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

9.3 Mise en place de la collecte des logs

Cette partie présente l'élément extbfMise en place de la collecte des logs dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

9.4 Développement du module de traitement des alertes

Cette partie présente l'élément extbfDéveloppement du module de traitement des alertes dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

9.5 Mise en place du webhook local

Cette partie présente l'élément extbfMise en place du webhook local dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une

blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Le webhook local reçoit les alertes Splunk au format JSON et les transmet vers Ollama. L'intérêt d'Ollama est de conserver l'analyse localement tout en produisant un résultat lisible par les autres modules. Le rapport IA contient notamment le type d'attaque, la sévérité, le score de confiance, l'explication et les actions recommandées.

Listing 9.1 – Exemple de sortie IA simplifiée

```
{
  "attack_type": "SQL Injection",
  "severity": "high",
  "confidence": 98,
  "recommended_action": ["alert_soc", "block_ip", "
     investigate_host"]
}
```

9.6 Intégration de l'intelligence artificielle locale

Cette partie présente l'élément extbfIntégration de l'intelligence artificielle locale dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Le webhook local reçoit les alertes Splunk au format JSON et les transmet vers Ollama. L'intérêt d'Ollama est de conserver l'analyse localement tout en produisant un résultat lisible par les autres modules. Le rapport IA contient notamment le type d'attaque, la sévérité, le score de confiance, l'explication et les actions recommandées.

Listing 9.2 – Exemple de sortie IA simplifiée

```
{
  "attack_type": "SQL Injection",
  "severity": "high",
  "confidence": 98,
```

```
  "recommended_action": ["alert_soc", "block_ip", "
     investigate_host"]
}
```

9.7 Développement du module de décision

Cette partie présente l'élément extbfDéveloppement du module de décision dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

9.8 Génération des actions de remédiation

Cette partie présente l'élément extbfGénération des actions de remédiation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

9.9 Mise en place de l'interface de remédiation

Cette partie présente l'élément extbfMise en place de l'interface de remédiation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste

SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

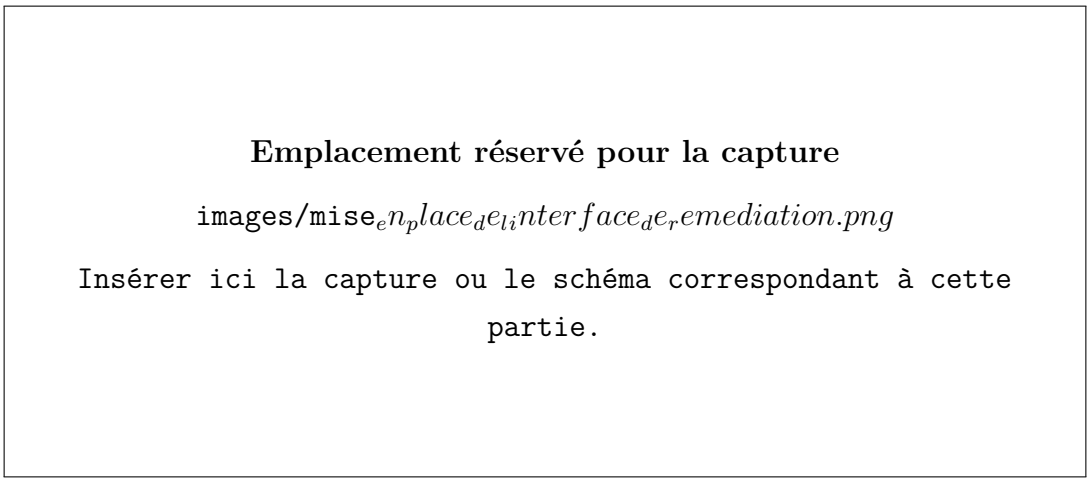

FIGURE 9.1 – Mise en place de l'interface de remédiation

9.10 Configuration de la blacklist dynamique

Cette partie présente l'élément extbfConfiguration de la blacklist dynamique dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

La blacklist dynamique est un élément central de la remédiation. Elle ne se limite pas à bloquer l'adresse IP, mais applique une stratégie de déception : l'adresse jugée malveillante est dirigée vers un honeypot. Cette approche permet de protéger le vrai service tout en maintenant une visibilité sur le comportement de l'attaquant.

Listing 9.3 – Exemple d'entrée dans la blacklist NGINX

```
10.79.241.251 1;
```

9.11 Intégration avec la plateforme de visualisation

Cette partie présente l'élément extbfIntégration avec la plateforme de visualisation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Emplacement réservé pour la capture

`images/integration`$_a vec_l a_p late forme_d e_v isualisation.png$

`Insérer ici la capture ou le schéma correspondant à cette partie.`

FIGURE 9.2 – Intégration avec la plateforme de visualisation

9.12 Journalisation des actions effectuées

Cette partie présente l'élément extbfJournalisation des actions effectuées dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises

vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

9.13 Intégration globale des composants

Cette partie présente l'élément extbfIntégration globale des composants dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

9.14 Validation du fonctionnement complet

Cette partie présente l'élément extbfValidation du fonctionnement complet dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Chapitre 10

Sécurité, fiabilité et qualité

10.1 Politique de sécurité appliquée

Cette partie présente l'élément extbfPolitique de sécurité appliquée dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

10.2 Protection contre les blocages accidentels

Cette partie présente l'élément extbfProtection contre les blocages accidentels dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

10.3 Whitelist des adresses internes

Cette partie présente l'élément extbfWhitelist des adresses internes dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

10.4 Exclusion des adresses critiques

Cette partie présente l'élément extbfExclusion des adresses critiques dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

10.5 Validation des adresses IP avant remédiation

Cette partie présente l'élément extbfValidation des adresses IP avant remédiation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une

blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

10.6 Mécanisme de rollback

Cette partie présente l'élément extbfMécanisme de rollback dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

10.7 Traçabilité des actions

Cette partie présente l'élément extbfTraçabilité des actions dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

10.8 Gestion des erreurs

Cette partie présente l'élément extbfGestion des erreurs dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

10.9 Fiabilité du processus de remédiation

Cette partie présente l'élément extbfFiabilité du processus de remédiation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

10.10 Qualité logicielle du code

Cette partie présente l'élément extbfQualité logicielle du code dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

10.11 Bonnes pratiques appliquées

Cette partie présente l'élément extbfBonnes pratiques appliquées dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements

de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

10.12 Synthèse sécurité et qualité

Cette partie présente l'élément extbfSynthèse sécurité et qualité dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Chapitre 11

Tests et validation

11.1 Stratégie de test adoptée

Cette partie présente l'élément extbfStratégie de test adoptée dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

11.2 Environnement de test

Cette partie présente l'élément extbfEnvironnement de test dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

11.3 Tests de connectivité

Cette partie présente l'élément extbfTests de connectivité dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

11.4 Tests de collecte des logs

Cette partie présente l'élément extbfTests de collecte des logs dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

11.5 Tests du webhook local

Cette partie présente l'élément extbfTests du webhook local dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une

blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Le webhook local reçoit les alertes Splunk au format JSON et les transmet vers Ollama. L'intérêt d'Ollama est de conserver l'analyse localement tout en produisant un résultat lisible par les autres modules. Le rapport IA contient notamment le type d'attaque, la sévérité, le score de confiance, l'explication et les actions recommandées.

Listing 11.1 – Exemple de sortie IA simplifiée

```
{
  "attack_type": "SQL Injection",
  "severity": "high",
  "confidence": 98,
  "recommended_action": ["alert_soc", "block_ip", "
     investigate_host"]
}
```

11.6 Tests du module de traitement

Cette partie présente l'élément extbfTests du module de traitement dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

11.7 Tests de l'analyse par intelligence artificielle

Cette partie présente l'élément extbfTests de l'analyse par intelligence artificielle dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises

vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Le webhook local reçoit les alertes Splunk au format JSON et les transmet vers Ollama. L'intérêt d'Ollama est de conserver l'analyse localement tout en produisant un résultat lisible par les autres modules. Le rapport IA contient notamment le type d'attaque, la sévérité, le score de confiance, l'explication et les actions recommandées.

Listing 11.2 – Exemple de sortie IA simplifiée

```
{
  "attack_type": "SQL Injection",
  "severity": "high",
  "confidence": 98,
  "recommended_action": ["alert_soc", "block_ip", "
     investigate_host"]
}
```

11.8 Tests du module de décision

Cette partie présente l'élément extbfTests du module de décision dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

11.9 Tests de la blacklist dynamique

Cette partie présente l'élément extbfTests de la blacklist dynamique dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

La blacklist dynamique est un élément central de la remédiation. Elle ne se limite pas à bloquer l'adresse IP, mais applique une stratégie de déception : l'adresse jugée malveillante est dirigée vers un honeypot. Cette approche permet de protéger le vrai service tout en maintenant une visibilité sur le comportement de l'attaquant.

Listing 11.3 – Exemple d'entrée dans la blacklist NGINX

```
10.79.241.251 1;
```

11.10 Tests de remédiation

Cette partie présente l'élément extbfTests de remédiation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

11.11 Tests de rollback

Cette partie présente l'élément extbfTests de rollback dans le cadre du projet extit-Cyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une

blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

11.12 Tests de visualisation

Cette partie présente l'élément extbfTests de visualisation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

FIGURE 11.1 – Tests de visualisation

11.13 Résultats attendus et résultats obtenus

Cette partie présente l'élément extbfRésultats attendus et résultats obtenus dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une

explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

11.14 Validation finale de la solution

Cette partie présente l'élément extbfValidation finale de la solution dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Chapitre 12

Résultats obtenus

12.1 Résultats fonctionnels

Cette partie présente l'élément extbfRésultats fonctionnels dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

12.2 Résultats techniques

Cette partie présente l'élément extbfRésultats techniques dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

12.3 Résultats de supervision

Cette partie présente l'élément extbfRésultats de supervision dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

12.4 Résultats de remédiation

Cette partie présente l'élément extbfRésultats de remédiation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

12.5 Résultats liés à la visualisation

Cette partie présente l'élément extbfRésultats liés à la visualisation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une

blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

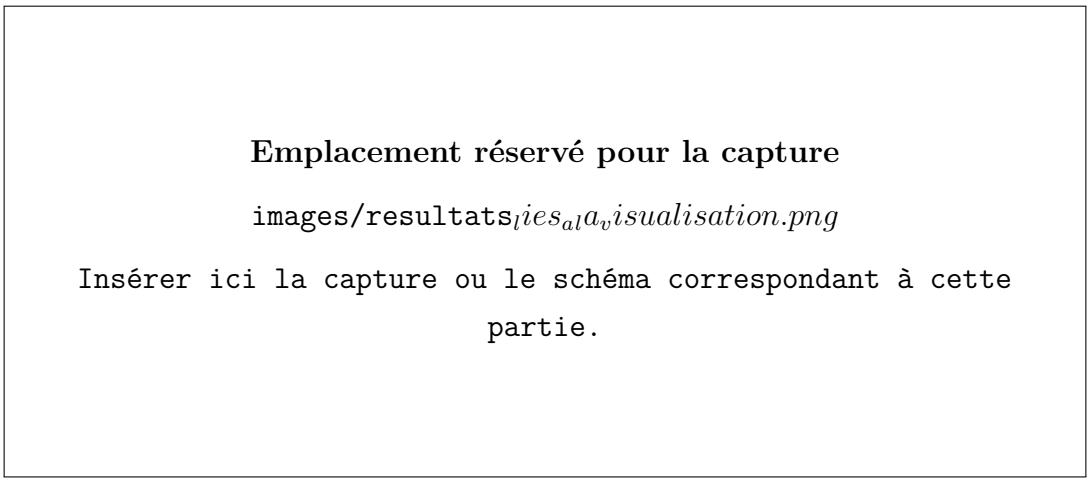

FIGURE 12.1 – Résultats liés à la visualisation

12.6 Exemple d'incident traité

Cette partie présente l'élément extbfExemple d'incident traité dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

12.7 Tableau récapitulatif des fonctionnalités réalisées

Cette partie présente l'élément extbfTableau récapitulatif des fonctionnalités réalisées dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du

honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

12.8 Comparaison entre objectifs initiaux et résultats obtenus

Cette partie présente l'élément extbfComparaison entre objectifs initiaux et résultats obtenus dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

12.9 Apport du projet pour l'équipe

Cette partie présente l'élément extbfApport du projet pour l'équipe dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Table 12.1 – Répartition fonctionnelle de l'équipe

Membre	**Rôle principal**
Ikram	Passerelle login, génération d'attaques web, logs d'authentification.
Oussama	Honeypot, logs de terminal, commandes suspectes et événements runtime.
Halima	Splunk, Ollama, interface de remédiation, blacklist dynamique et intégration.
Asma	Visualisation Grafana et réception des rapports IA via Logstash.
Sayf	Analyse IA, recommandations et logique de décision.

12.10 Synthèse des résultats

Cette partie présente l'élément extbfSynthèse des résultats dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Chapitre 13

Analyse et discussion

13.1 Analyse technique de la solution

Cette partie présente l'élément extbfAnalyse technique de la solution dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

13.2 Analyse du flux de détection

Cette partie présente l'élément extbfAnalyse du flux de détection dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

13.3 Analyse du flux de remédiation

Cette partie présente l'élément extbfAnalyse du flux de remédiation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

13.4 Valeur ajoutée de l'intelligence artificielle locale

Cette partie présente l'élément extbfValeur ajoutée de l'intelligence artificielle locale dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Le webhook local reçoit les alertes Splunk au format JSON et les transmet vers Ollama. L'intérêt d'Ollama est de conserver l'analyse localement tout en produisant un résultat lisible par les autres modules. Le rapport IA contient notamment le type d'attaque, la sévérité, le score de confiance, l'explication et les actions recommandées.

Listing 13.1 – Exemple de sortie IA simplifiée

```
{
  "attack_type": "SQL Injection",
  "severity": "high",
  "confidence": 98,
  "recommended_action": ["alert_soc", "block_ip", "
     investigate_host"]
}
```

13.5 Apport de l'automatisation

Cette partie présente l'élément extbfApport de l'automatisation dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

13.6 Points forts de la solution

Cette partie présente l'élément extbfPoints forts de la solution dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

13.7 Points faibles de la solution

Cette partie présente l'élément extbfPoints faibles de la solution dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

13.8 Analyse de la scalabilité

Cette partie présente l'élément extbfAnalyse de la scalabilité dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

13.9 Analyse de la fiabilité

Cette partie présente l'élément extbfAnalyse de la fiabilité dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

13.10 Impact du projet

Cette partie présente l'élément extbfImpact du projet dans le cadre du projet extitCyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité

bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

13.11 Synthèse critique

Cette partie présente l'élément extbfSynthèse critique dans le cadre du projet extit-Cyber Chaos Arena. La solution réalisée vise à transformer des événements de sécurité bruts en décisions opérationnelles exploitables par un analyste SOC. Elle combine la collecte des logs, l'analyse par intelligence artificielle locale, la visualisation et la remédiation dynamique.

Dans notre implémentation, les événements issus de la passerelle login d'Ikram et du honeypot d'Oussama sont centralisés dans Splunk. Les alertes sont ensuite transmises vers Ollama afin d'obtenir une classification, une sévérité, un score de confiance, une explication et une recommandation. La remédiation peut ajouter une adresse IP à une blacklist NGINX afin de rediriger automatiquement l'attaquant vers un honeypot au lieu du service réel.

Difficultés rencontrées

Les principales difficultés ont concerné la connectivité entre les machines, les délais de réponse d'Ollama, la synchronisation horaire, les permissions sudo, la configuration NGINX, la gestion de la blacklist dynamique et l'affichage correct des statuts dans l'interface de remédiation. Ces problèmes ont été résolus par des tests progressifs, l'augmentation des timeouts, la validation des fichiers de configuration, l'ajout de règles sudoers contrôlées et la vérification directe du contenu du fichier blacklist.

Limites du projet

Le projet reste une plateforme académique. Il ne remplace pas un SOC industriel complet. Les scénarios d'attaque sont limités, les décisions IA doivent être contrôlées et la remédiation automatique doit rester encadrée par une whitelist et des mécanismes de rollback.

Perspectives et améliorations futures

Les améliorations possibles incluent l'ajout d'un système de tickets, l'intégration de notifications, l'authentification de l'interface, l'enrichissement GeoIP, l'orchestration multi-hôtes, l'ajout de playbooks SOAR et l'intégration plus avancée des techniques MITRE ATT&CK.

Conclusion générale

Le projet *Cyber Chaos Arena* a permis de concevoir une solution SOC complète reliant détection, analyse, visualisation et remédiation. La solution démontre l'intérêt d'une intelligence artificielle locale pour enrichir les alertes, ainsi que l'intérêt d'une remédiation par déception reposant sur une blacklist dynamique NGINX. Au lieu de bloquer simplement un attaquant, le système le redirige vers un honeypot, ce qui protège le service réel tout en maintenant une visibilité opérationnelle. Le projet constitue ainsi une base solide pour une architecture SOC plus avancée.

Bibliographie

1. Stallings, W. *Network Security Essentials*. Pearson.
2. Scarfone, K. et Mell, P. *Guide to Intrusion Detection and Prevention Systems*. NIST.
3. Chuvakin, A. *Security Information and Event Management Implementation*.

Webographie

1. Documentation Splunk : https://docs.splunk.com
2. Documentation Grafana : https://grafana.com/docs
3. Documentation NGINX : https://nginx.org/en/docs
4. Documentation Ollama : https://ollama.com
5. MITRE ATT&CK : https://attack.mitre.org
6. Documentation Flask : https://flask.palletsprojects.com

Annexe A

Commandes principales utilisées

```
python3 splunk_to_ollama.py
python3 realtime_poller.py
python3 forward_to_asma_logstash.py
python app.py
sudo -n /usr/local/bin/cyberchaos-blacklist-add 10.79.241.251
sudo -n /usr/local/bin/cyberchaos-blacklist-remove 10.79.241.251
```

Annexe B

Scripts principaux

— splunk_to_ollama.py

— realtime_poller.py

— forward_to_asma_logstash.py

— app.py

— cyberchaos-blacklist-add

— cyberchaos-blacklist-remove

Annexe C

Fichiers de configuration

— /etc/nginx/conf.d/cyberchaos_blacklist.conf

— /etc/nginx/blacklist.d/blacklist_ips.conf

— /etc/sudoers.d/cyberchaos-blacklist

Annexe D

Format des logs traités

```
1 {"source_ip":"10.79.241.63","event":"sql_injection","severity":"
     critical","source_module":"ikram_login_gateway"}
```

Annexe E

Format des actions de remédiation

```
1 {"action":"blacklist_redirect_to_honeypot","source_ip
    ":"10.79.241.251","status":"redirected_to_honeypot","rollback
    ":"sudo -n /usr/local/bin/cyberchaos-blacklist-remove
    10.79.241.251"}
```

Annexe F

Extrait de configuration du reverse proxy

```
1 geo $is_blacklisted { default 0; include /etc/nginx/blacklist.d/
    blacklist_ips.conf; }
2 server { listen 80; location / { error_page 418 = @honeypot; if (
    $is_blacklisted) { return 418; } proxy_pass http://real_backend
    ; } location @honeypot { proxy_pass http://honeypot_backend; }
    }
```

Annexe G

Extrait de configuration de la blacklist

```
10.79.241.251 1;
```

Annexe H

Captures complémentaires

Emplacement réservé pour la capture

`images/capture`$_{s}plunk.png$

`Insérer la capture du dashboard Splunk.`

FIGURE H.1 – Capture Splunk

Emplacement réservé pour la capture

`images/capture`$_{g}rafana.png$

`Insérer la capture Grafana.`

FIGURE H.2 – Capture Grafana

Emplacement réservé pour la capture

`images/capture`$_{interface_remediation.png}$

`Insérer la capture de l'interface finale.`

FIGURE H.3 – Capture interface remédiation

Emplacement réservé pour la capture

`images/capture`$_{blacklist.png}$

`Insérer la capture de la blacklist.`

FIGURE H.4 – Capture blacklist NGINX

Annexe I

Manuel de démonstration

1. Lancer Splunk, Ollama, le webhook et le poller.
2. Générer une attaque.
3. Vérifier l'alerte dans Splunk.
4. Vérifier l'analyse Ollama.
5. Vérifier l'envoi à Grafana.
6. Appliquer la redirection vers honeypot.
7. Vérifier la blacklist.
8. Tester le rollback avec Remove.

Annexe J

Liens utiles

- https://docs.splunk.com
- https://grafana.com/docs
- https://ollama.com
- https://nginx.org
- https://attack.mitre.org