

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Centre de Recherche sur l'Information

Scientifique & Technique

Département Formation et Audiovisuel

Service de la Formation Continue et de Télé-enseignement

Filiale : Post Graduation spécialisée en Sécurité Informatique

Promotion 2019/2020

Mémoire pour l'obtention du diplôme de Post graduation
spécialisée en Sécurité Informatique

THÈME

Outils de Gestion de l'Information et des Évènements de Sécurité (SIEM)

Réalisé par :

BOUTEFARA Abdeldjalil

NEKROUF Mohamad

Encadré par :

Promoteur : DJEDJIG Nabil

Co-Promoteur : AMIRA Abdelouahab

Alger le 01/02/2022

Dédicace

Amon cher père « rahimaho ELLAH » رحمه الله

Ama très chère mère

Quoi que je fasse ou que je dise,

Je ne saurai point te remercier comme il se doit

À ma chère femme et mes chers enfants

À mes frères Mohamad et Fateh, Houssèm et sa femme

Ames sœurs, ses maries et ses enfants

À tous ceux que j'aime et ceux qui m'aiment.

Abdeldjalil

Dédicace

Je dédie ce modeste travail

À mes chers parents.

À ma chère femme et mes chers enfants.

À mes frères, mes sœurs et ma famille.

*À mes amis et tous ceux qui m'ont
soutenu et encouragé.*

MOHAMMED



Remerciement

Nous remercions Dieu tout puissant de nous avoir permis de mener à terme ce projet qui est pour le point de départ d'une merveilleuse aventure, celle de la recherche, source de remise en cause permanent et de Perfectionnement perpétuel.

*Nous voulons exprimer toute notre reconnaissance et toute notre considération à Monsieur, **DJEDJIG Nabil** notre Promoteur au CERIST, pour avoir bien voulu nous encadrer, pour tout le temps qu'il nous a octroyé et pour tous les conseils qu'ils nous a prodigués. Qu'il trouve ici l'expression de notre profonde gratitude.*

*Il nous est très agréable d'exprimer notre gratitude ainsi que notre profonde reconnaissance à Monsieur **AMIRA Abdelouahab** notre Co-promoteur au CERIST pour son soutien constant, son aide précieuse et ses conseils attentifs durant tout le projet.*

Nous adressons nos honorables respects :

*Au responsable chargé de la formation PGS en Sécurité Informatique et à tous les enseignants du CERIST,
Aux membres de jury et à tous ceux qui ont bien voulu accepter d'examiner et d'évaluer ce travail.*

Table des matières

Liste des figures :.....	7
Introduction générale.....	9
1. Chapitre 01 : SIEM, Définition et Fonctionnement.....	12
1.1 Introduction.....	13
1.2 Définition.....	13
1.3 Fonctionnement.....	13
1.3.1 Collecte de données.....	14
1.3.2 Normalisation de l'information.....	15
1.3.3 Agrégation des évènements.....	17
1.3.4 Corrélation des évènements.....	18
1.3.5 Gestion des alertes.....	19
1.3.6 Les tableaux de bord.....	20
1.4 Cas pratiques d'utilisation des outils SIEM.....	20
1.4.1 Sécurité à des fins de détection et d'enquête.....	21
1.4.2 Conformité aux réglementations et aux stratégies.....	21
1.4.3 Fonctionnement normal et dépannage de l'exploitation au niveau du réseau et du système.....	24
1.5 Types de SIEM.....	24
1.6 Conclusion.....	25
2. Chapitre 02 : Sélection des outils SIEM.....	27
2.1 Introduction.....	28
2.2 Le Magic Quadrant de Gartner pour les fournisseurs d'outils de SIEM.....	28
2.3 Outils SIEM (Juin 2021).....	29
2.3.1 Splunk Enterprise Security.....	30
2.3.2 Plateforme LogRhythmSIEM.....	30
2.3.3 IBM QRadar SIEM.....	31
2.3.4 McAfee Enterprise Security Manager.....	32
2.3.5 SIEM RSA NetWitness Platform.....	32
2.4 SIEM Open Source.....	33
2.5 Critères à vérifier lors du choix d'un SIEM.....	34
2.6 Les solutions SIEM Open Source populaires.....	36
2.6.1 Elastic Security (SIEM de la suite ELK) :.....	36
2.6.2 AlienVault OSSIM.....	37
2.6.3 OSSEC.....	38
2.6.4 Wazuh.....	39
2.6.5 Splunk free.....	40
2.6.6 SIEMonster.....	41

2.7 Comparaison entre les Outils SIEM Open Source et notre choix :	42
2.8 Solution choisie :	44
2.9 Conclusion	44
3. Chapitre 03 : Le SIEM Elastic Stack (ELK) et les scénarios proposés.	46
3.1 Introduction	47
3.2 Scénarios d'expérimentation	47
3.2.1 La surveillance du réseau de capteurs	47
3.2.2 La surveillance des évènements du système Windows	49
3.3 Présentation d'Elastic Stack	50
3.3.1 Beats.....	50
3.3.2 Logstash	51
3.3.3 Elasticsearch.....	52
3.3.4 Kibana	53
3.3.5 Elastic SIEM.....	54
3.4 Conclusion	55
4. Chapitre 04 : Déploiement d'Elastic Stack comme solution SIEM.	56
4.1 Introduction	57
4.2 Composants de l'environnement du projet	57
4.3 Architecture de l'environnement du projet	58
4.4 Installation et configuration des composants de l'environnement	59
4.4.1 Mosquitto.....	59
4.4.2 Node-Red	61
4.4.3 Elasticsearch.....	62
4.4.4 Logstash	63
4.4.5 Kibana	64
4.4.6 Filebeat.....	64
4.4.7 Auditbeat, Packetbeat et Winlogbeat	66
4.5 Résultats : Suivi et visualisation de la surveillance avec ELK Suite	66
4.5.1 Scénario réseaux de capteurs	66
4.5.2 Scénario Windows.....	69
4.6 Conclusion	72
Conclusion Générale	73
Bibliographie et Webographie :	74

Liste des figures :

Figure 1. Architecture de base d'un SIEM.....	09.
Figure 2. Schéma Format IDMEF.....	11.
Figure 3. Schéma Format IODEF.....	12.
Figure 4. Exemple d'une règle de corrélation.....	13.
Figure 5. Tableaux de bord SIEM (SolarWinds dashboard).....	14.
Figure 6. SIEM Magic Quadrant By Gartner Juin 2021.....	23.
Figure 7. Capture d'écran montrant le tableau de bord Splunk.....	23.
Figure 8. Capture d'écran montrant le tableau de bord LogRhythm.....	24.
Figure 9. Capture d'écran montrant le tableau de bord QRadar SIEM.....	24.
Figure 10. Capture d'écran montrant le tableau de bord McAfee SIEM.....	25.
Figure 11. Capture d'écran montrant le tableau de bord RSA NetWitness SIEM.....	26.
Figure 12. Tableau résumant les critères exigés lors du choix d'un SIEM.....	28.
Figure 13. Capture d'écran montrant le tableau de bord ELK.....	28.
Figure 14. Capture d'écran montrant le tableau de bord OSSIM.	29.
Figure 15. Capture d'écran montrant le tableau de bord OSSEC.....	30.
Figure 16. Capture d'écran montrant le tableau de bord Wazuh.....	31.
Figure 17. Capture d'écran montrant le tableau de bord Splunk free.....	32.
Figure 18. Capture d'écran montrant le tableau de bord SIEMonsterSiem.....	33.
Figure 19. Tableau comparatif des outils SIEM Open Source.....	34.
Figure 20. La Suite Elastic.....	38.
Figure 21. La plateforme Beats.....	39.
Figure 22. Logstash.....	40.
Figure 23. Kibana.....	42.
Figure 24. Elastic SIEM.....	43.
Figure 25. Hosts.....	43.

Figure 26. Network.....	43.
Figure 27. Timeline.....	43.
Figure 28. Topologie MQTT.....	44.
Figure 29. L'Interface de Node-RED.....	46.
Figure 30. Architecture du projet.....	48.
Figure 31. Architecture modifiée du projet.....	49.
Figure 32. Service mosquitto créé.....	50.
Figure 33. Le réseau de capteurs.....	55.
Figure 34. Les messages de journalisation mosquitto.....	56.
Figure 35. Les mesures capturées par sujet.....	57.
Figure 36. Tableau de bord des mesures capturées.....	58.
Figure 37. Tableau de bord d'Auditbeat (processus).....	62.
Figure 39. Tableau de bord de Packetbeat.....	63.
Figure 40. Les messages de journalisation expédiés par Winlogbeat.....	64.
Figure 41. Tableau de bord de Winlogbeat.....	64.