https://latribunelibre.com/emploi/ingenieur-securite-siem-elk-f-h

INGÉNIEUR SÉCURITÉ SIEM ELK F/H

Organisme employeur
Hardis

Type de poste
Temps plein

Secteur
PROGRAMMATION INFORMATIQUE

Lieu du poste
69387, LYON 07, LYON, France

Date de publication
29 août 2024 à 13:02

Valide jusqu'au
28.09.2024

Description

Hardis Group poursuit sa croissance sur son activité SOC et recrute un Ingénieur Sécurité SIEM ELK F/H pour intervenir dans un contexte de gestion de solution SIEM.

Sous la responsabilité du Team Leader de l'équipe SOC, dans une équipe de 10 personnes dédiées à la sécurité, vous interviendrez principalement sur le développement du SIEM et la construction des règles de détection.

Vos missions principales seront :
- Analyse des sources de données à intégrer dans le SIEM et identification des données pertinentes,
- Réalisation de préconisations auprès des équipes techniques pour réaliser les exports de logs
- Configuration des briques d'ingestion coté Elastic (Logstash, filebeat, fleet agent) pour ingérer les données et organiser les index de manière optimale
- Analyse des volumes ingérés pour définir le capacity planning des besoins en stockage de la solution

Sur la base du MITRE Att&ck, configurer des règles d'analyse permettant de lever des alertes de sécurité :

- Identification des besoins
- Rédaction des spécifications des règles à implémenter
- Implémentation des règles
- Tests pour validation de la qualité des règles en vue de limiter au maximum les faux positifs

- Réalisation de la documentation et de l'amélioration des procédures
- Rédaction des documentations associés aux configurations mises en place
- Définition des fiches réaction à suivre sur les alertes générées

Qualifications

Hardis Group poursuit sa croissance sur son activité SOC et recrute un Ingénieur Sécurité SIEM ELK F/H pour intervenir dans un contexte de gestion de solution SIEM.

Sous la responsabilité du Team Leader de l'équipe SOC, dans une équipe de 10 personnes dédiées à la sécurité, vous interviendrez principalement sur le développement du SIEM et la construction des règles de détection.

Vos missions principales seront :
- Analyse des sources de données à intégrer dans le SIEM et identification des données pertinentes,
- Réalisation de préconisations auprès des équipes techniques pour réaliser les exports de logs

- Configuration des briques d'ingestion coté Elastic (Logstash, filebeat, fleet agent) pour ingérer les données et organiser les index de manière optimale
- Analyse des volumes ingérés pour définir le capacity planning des besoins en stockage de la solution

Sur la base du MITRE Att&ck, configurer des règles d'analyse permettant de lever des alertes de sécurité :

- Identification des besoins
- Rédaction des spécifications des règles à implémenter
- Implémentation des règles
- Tests pour validation de la qualité des règles en vue de limiter au maximum les faux positifs

- Réalisation de la documentation et de l'amélioration des procédures
- Rédaction des documentations associés aux configurations mises en place
- Définition des fiches réaction à suivre sur les alertes générées