LOGO ORGANISME ACADEMIQUE

ADISCA N°	
Date du rapport de stage :	**19/03/2025**

MEMOIRE TECHNIQUE ARIANEGROUP

TITRE DU RAPPORT :	**Comparatif des outils de surveillance réseau**
APPPRENTI :	Maxime Laville
Date de l'alternance :	Du 04/12/2023 au 31/07/2025
TUTEUR D'ENTREPRISE :	**R.L**
Service :	Systems & Products CyberSecurity Engineer
ORGANISME D'ACCUEIL :	**ARIANEGROUP**
Adresse :	51/61 route de Verneuil BP71040 78131 LES MUREAUX CEDEX
ORGANISME ACADEMIQUE :	**Aurlom BTS+**
Adresse :	118 Avenue Jean Jaurès 75019, PARIS
TUTEUR PEDAGOGIQUE :	Corentin, DAGUET

Exemplaire Papier n° 1/ Y : Prénom, Nom
Exemplaire Papier n° 2/ Y : Prénom, Nom
Exemplaire Papier n° 3/ Y : Prénom, Nom
Exemplaire Papier n° 4/ Y : Prénom, Nom
Exemplaire Papier n° 5/ Y : Prénom, Nom
Exemplaire Papier n° 6/ Y : Prénom, Nom

MENTION DE PROPRIETE

Ce document et les informations qu'il contient sont propriété d'ArianeGroup. Il ne doit pas être utilisé à d'autres fins que celles pour lesquelles il a été remis. Il ne peut être ni reproduit, ni divulgué à des tiers (en tout ou partie) sans l'accord préalable et écrit d'ArianeGroup. ArianeGroup SAS –Tous droits réservés. // This document and the information it contains are property of ArianeGroup. It shall not be used for any purpose other than those for which it was supplied. It shall not be repro-duced or disclosed (in whole or in part) to any third party without ArianeGroup prior written consent. ArianeGroup SAS – All rights reserved.

CLAUSE DE DEONTOLOGIE

Les activités d'ArianeGroup intéressent la défense et la sécurité nationale et les intérêts fondamentaux de la nation. Ses salariés et sous-traitants sont soumis à un devoir de discrétion professionnelle et ne sont pas autorisés à diffuser ou rendre accessible ces informations à des personnes ou organismes non-autorisés. Les informations auxquelles j'ai eu l'accès pendant mon apprentissage en entreprise sont non-publiques, voire confidentielles.

De fait, ce document à vocation académique ne comporte aucun nom et chiffres réels. Les informations qu'il contient sont propriété d'ArianeGroup. Il ne doit pas être utilisé à d'autres fins que celles pour lesquelles il a été remis. Il ne peut être ni reproduit, ni divulgué à des tiers (en tout ou partie) sans l'accord préalable et écrit d'ArianeGroup SAS.

2024/2025

Mission professionnelle N°2

LAVILLE, Maxime

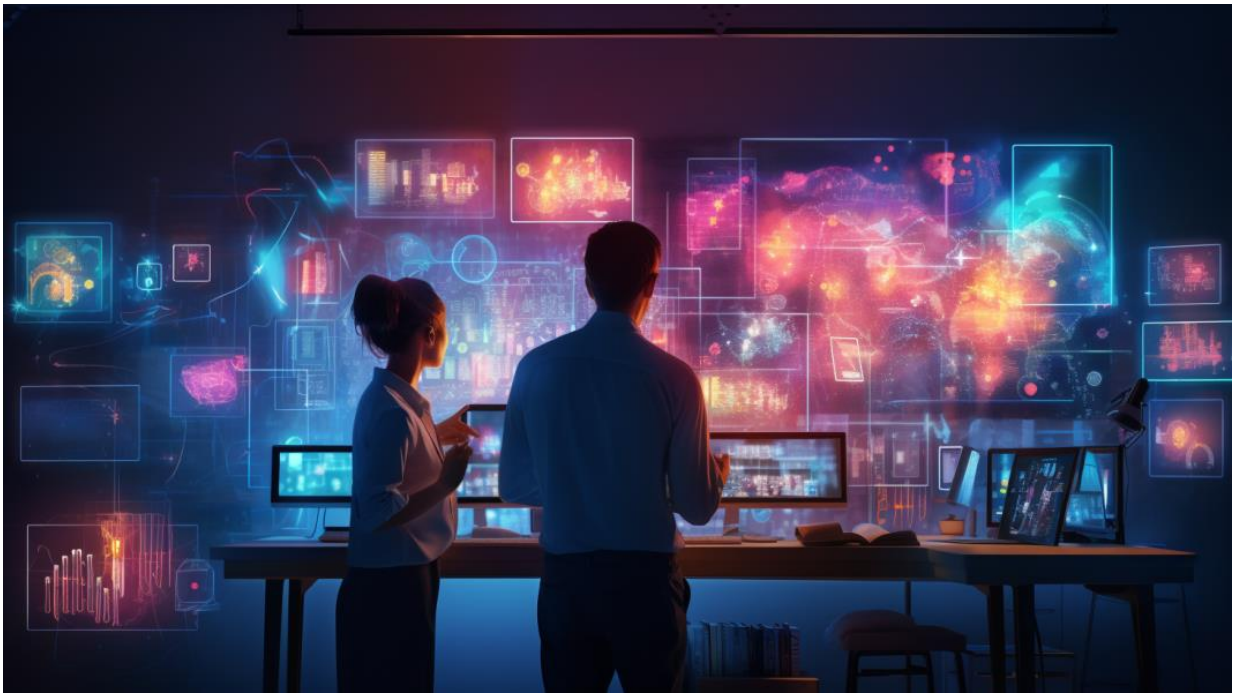
ArianeGroup

19/03/2025

Comparatif des outils de surveillance réseau.

Description :

Cette mission consiste à réaliser une étude comparative entre différents types d'outils de surveillance réseau comme Arkime ou Zeek. L'objectif étant de déterminer lequel de ces outils correspond le plus à nos besoins en les testant et en s'appuyant sur différents critères prédéfinis.



Validation de la mission professionnelle :

Nom	Date	Tampon
Maxime Laville	19/03/2025	

S o m m a i r e

Table des illustrations

1 FORMALISATION DU BESOIN

L'objectif est de pouvoir espionner un réseau, ayant une topologie de type anneau, afin de détecter toute activité frauduleuse. Pour cela, une solution COTS doit être envisagée et elle devra permettre de :

- Collecter et archiver un grand volume de trafic réseau en provenance de plusieurs ports miroirs. Certains de ces ports miroirs sont placés sur une même infrastructure avec une topologie en anneau, il faut donc pouvoir éliminer les duplicatas sans jamais perdre de paquets uniques.
- Permettre de visualiser et surveiller en temps réel la constitution du réseau.
- Connaitre les équipements connectés réseau.
- Quels sont les informations connues pour chacun de ces équipements.
- Connaitre les flux et les protocoles de communication entre les différents équipements
- Avoir la possibilité d'ajouter manuellement nos connaissances des équipements (rôle, nom, etc.).

1.1 ANALYSE DES CHOIX

Les différentes solutions logicielles se sont avant tout portés sur des outils de surveillance réseau étant open-source et compatibles Linux. Une liste restreinte a été proposée par une personne de notre équipe ayant déjà abordé ce sujet.
Evidemment, trouver un outil permettant de rassembler tous nos besoins n'était clairement pas facile voir même peu probable. Le but était surtout de trouver l'outil qui répondait au mieux à nos besoins.
Les outils sélectionnés sont les suivants :

- CheckMK RAW
- OpenNMS Horizon
- Nagios Core
- Zeek
- Arkime

2 DESCRIPTIF DES OUTILS

2.1 CHECKMK RAW

Figure 1 – Présentation de CheckMK RAW

CheckMK est un outil de surveillance réseau léger, idéal pour les infrastructures simples. Avec une interface intuitive, il permet la surveillance en temps réel et une détection d'intrusion de base. Ses besoins en ressources sont faibles, et il offre des alertes par e-mail et SMS.
Cependant, ses capacités d'analyse du trafic sont limitées et il ne supporte pas la capture de paquets.

2.1.1 **Fonctionnalités de CheckMK RAW**

Besoins	**Fonctionnalités de CheckMK RAW**
Collecte et archivage de trafic réseau en grand volume	Peut collecter des données réseau via des agents et des plugins. L'architecture Nagios sous-jacente permet d'utiliser des plugins réseau pour surveiller le trafic en provenance ports miroirs.
Elimination des duplicatas sans perte de paquets	Fonctionnalités basiques d'analyse réseau, mais CheckMK RAW n'inclut pas directement de déduplication avancée. Des plugins ou outils externes peuvent être intégrés pour des besoins spécifiques.
Surveillance en temps réel de la constitution du réseau	Surveillance en quasi-temps réel via l'interface Web. Permet de voir les événements et alertes instantanément, bien que moins optimisé que la version Enterprise.
Identification des équipements présents sur le réseau	Détection automatique des équipements réseau via des agents et découverte SNMP. Peut identifier les équipements et les services disponibles.
Informations connues pour chaque équipement	Affiche les informations de base des équipements (adresse IP, statut, etc.) et fournit des détails limités sans plugins ou outils supplémentaires.
Suivi de communications entre équipements et des protocoles utilisés	Surveillance réseau basique possible avec SNMP et agents, mais pas de capture directe de protocoles spécifiques dans CheckMK RAW, plugins tiers nécessaires pour cette fonctionnalité.
Ajout manuel d'informations sur les équipements (nom, rôle, etc.)	Supporte l'ajout manuel de notes et d'informations complémentaires pour chaque équipement, permettant une personnalisation limitée.

Complémentarité : CheckMK RAW peut être complété avec des plugins ou des outils externes pour répondre pleinement aux besoins avancés de surveillance réseau et de déduplication.
Visualisation réseau : Il permet une visualisation basique en temps réel, mais les fonctionnalités de suivi détaillé des protocoles réseau peuvent nécessiter une intégration externe.

2.2 OPENNMS HORIZON

Figure 2 – Présentation d'OpenNMS Horizon

OpenNMS est une solution puissante et évolutive, adaptée aux grandes infrastructures. Elle nécessite Java et fonctionne principalement sur des systèmes Linux.
Cet outil offre une surveillance en temps réel avancée et une bonne intégration avec d'autres systèmes grâce à ses API, en plus de fournir des alertes par e-mail et SMS. Il est particulièrement robuste pour des réseaux de grande envergure, bien qu'il ne prenne pas en charge la capture de paquets.

2.2.1 **Fonctionnalités d'OpenNMS Horizon**

Besoins	**Fonctionnalités de OpenNMS Horizon**
Collecte et archivage de trafic réseau en grand volume	Supporte la collecte à grande échelle via SNMP, NetFlow, sFlow, et IPFIX. OpenNMS Horizon peut archiver des métriques de trafic et des journaux en utilisant des bases de données extensibles, comme Cassandra.
Elimination des duplicatas sans perte de paquets	Horizon inclut des mécanismes de corrélation d'événements et de suppression de duplicatas. L'architecture peut être configurée pour filtrer les données en double sans perte d'intégrité dans la collecte.
Surveillance en temps réel de la constitution du réseau	Interface Web en temps réel avec tableaux de bord personnalisables, cartes de réseau dynamiques, et affichage instantané des alertes et de la disponibilité des services.
Identification des équipements présents sur le réseau	Détection automatique avancée des équipements via SNMP, ICMP, et autres protocoles. OpenNMS Horizon crée une base d'actifs avec un inventaire détaillé des équipements présents sur le réseau.
Informations connues pour chaque équipement	Horizon collecte et affiche des informations détaillées pour chaque équipement (adresse IP, nom d'hôte, système d'exploitation, utilisation des ressources, etc.). Données enrichies via plugins pour une visibilité accrue.
Suivi de communications entre équipements et des protocoles utilisés	Horizon supporte NetFlow, sFlow, et IPFIX, ce qui permet de surveiller les communications entre équipements et d'identifier les protocoles utilisés entre eux, avec affichage graphique et analyse de flux.
Ajout manuel d'informations sur les équipements (nom, rôle, etc.)	Permet l'ajout manuel de métadonnées sur chaque équipement, facilitant l'attribution de rôles, de noms spécifiques, et de notes, directement dans l'interface d'OpenNMS Horizon.

2.3 NAGIOS CORE

Figure 3 – Présentation de Nagios Core

Nagios Core est bien adapté aux PME recherchant des fonctionnalités de base de surveillance réseau.
Avec une interface graphique simple, il offre une surveillance en temps réel et des alertes par e-mail et SMS.
Il est facile à installer sur des systèmes Linux et est souvent utilisé pour la surveillance réseau de base sans analyse avancée du trafic ou capture de paquets.

2.3.1 **Fonctionnalités de Nagios Core**

Besoins	Fonctionnalités de Nagios Core
Collecte et archivage de trafic réseau en grand volume	Nagios Core est principalement axé sur la surveillance de l'état des services et des hôtes. Il n'a pas de fonctionnalités natives pour la collecte et l'archivage de trafic réseau. Peut nécessiter des plugins tiers.
Elimination des duplicatas sans perte de paquets	Pas de gestion directe des duplicatas dans les données de trafic réseau. Nagios Core manque de déduplication intégrée et pourrait nécessiter une configuration de plugins tiers pour cette fonctionnalité.
Surveillance en temps réel de la constitution du réseau	Interface Web basique permettant de visualiser les états des hôtes et services en quasi-temps réel, mais avec des options de visualisation limitées pour les flux de trafic et la topologie réseau.
Identification des équipements présents sur le réseau	Identification des équipements possible via SNMP et autres plugins de découverte réseau. Les équipements et leurs statuts peuvent être surveillés si configurés manuellement ou avec des scripts personnalisés.
Informations connues pour chaque équipement	Capable de collecter des informations basiques telles que l'état, l'adresse IP, et la disponibilité des équipements, mais nécessite des plugins SNMP ou personnalisés pour des détails supplémentaires.
Suivi de communications entre équipements et des protocoles utilisés	Nagios Core n'a pas de support natif pour la surveillance des communications réseau par protocole. L'intégration de plugins NetFlow, sFlow ou autres sont nécessaires pour une analyse de flux de communication.
Ajout manuel d'informations sur les équipements (nom, rôle, etc.)	Offre la possibilité d'ajouter des notes et informations personnalisées pour chaque équipement dans les configurations manuelles, permettant une documentation de base dans les fichiers de configuration.

2.3 ZEEK

Figure 4 – Présentation de Zeek

Zeek est conçu pour les environnements nécessitant une analyse avancée du trafic réseau et des fonctionnalités de sécurité en temps réel.
Fonctionnant sur Linux, il capture et analyse les paquets, et se concentre sur la détection d'intrusions.
Bien qu'il puisse manquer de fonctionnalités de surveillance traditionnelles, c'est un excellent choix pour les analyses détaillées et le logging du trafic.

2.3.2 Fonctionnalités de Zeek

Besoins	Fonctionnalités de Zeek
Collecte et archivage de trafic réseau en grand volume	Zeek est spécifiquement conçu pour capturer et analyser des gros volumes de trafic réseau en temps réel. Il peut être configuré pour collecter des données provenant de plusieurs ports miroirs sans difficulté.
Elimination des duplicatas sans perte de paquets	Zeek possède des capacités avancées de déduplication et de filtrage de paquets, adaptées aux topologies complexes, comme les réseaux en anneau, garantissant la précision des données collectées.
Surveillance en temps réel de la constitution du réseau	Zeek collecte et analyse en temps réel, mais n'a pas d'interface native de visualisation. Il est souvent intégré avec d'autres outils (comme Kibana ou Grafana) pour des tableaux de bord en temps réel.
Identification des équipements présents sur le réseau	Zeek peut détecter les équipements et leurs activités sur le réseau en analysant les paquets réseau, créant un inventaire des équipements visibles selon leur comportement et leur trafic réseau.
Informations connues pour chaque équipement	Zeek capture des informations détaillées (adresses IP, ports, services utilisés) pour chaque équipement identifié, avec des données enrichies pour chaque connexion observée.
Suivi de communications entre équipements et des protocoles utilisés	Zeek analyse en profondeur les flux de données et enregistre les protocoles utilisés (HTTP, DNS, FTP, etc.) ainsi que les communications entre équipements, permettant une cartographie détaillée des interactions.
Ajout manuel d'informations sur les équipements (nom, rôle, etc.)	Zeek peut être configuré avec des scripts pour enrichir les données des équipements avec des informations supplémentaires, bien qu'il ne fournisse pas d'option d'ajout manuel directement dans son interface.

Spécialisation dans l'analyse réseau : Zeek est hautement optimisé pour l'analyse détaillée du trafic réseau et la collecte de métadonnées, mais il nécessite des outils supplémentaires pour l'archivage et la visualisation.
Déduplication et gestion des flux : Grâce à ses capacités de traitement des paquets et d'analyse avancée, Zeek est idéal pour les topologies complexes sans nécessiter de configuration supplémentaire pour éliminer les duplicatas.
Scalabilité pour grandes infrastructures : Zeek est très efficace pour gérer et surveiller des infrastructures de grande envergure, mais pour une visualisation complète, des intégrations tierces sont recommandées.

2.4 ARKIME

Figure 5 – Présentation d'Arkime

Arkime est conçu pour capturer les paquets réseau, avec des capacités de recherche avancées via Elasticsearch.
Il convient aux infrastructures nécessitant une analyse approfondie du trafic réseau.
En plus de sa scalabilité élevée, Arkime offre une interface graphique et une interface de commande pour une gestion flexible, bien qu'il n'inclue pas de détection d'intrusions intégrée.

2.4.1 **Fonctionnalités d'Arkime**

Besoins	**Fonctionnalités d'Arkime**
Collecte et archivage de trafic réseau en grand volume	Arkime est conçu pour capturer et stocker un gros volume de trafic réseau en temps réel, avec une architecture évolutive pour gérer plusieurs ports miroirs et de grands volumes de données.
Elimination des duplicatas sans perte de paquets	Arkime ne possède pas de déduplication native des paquets. Cependant, il peut être couplé à des outils de traitement pour filtrer les doublons si nécessaire.
Surveillance en temps réel de la constitution du réseau	Fournit une interface Web pour visualiser les sessions réseau capturées en temps réel, avec des tableaux de bord permettant une navigation rapide dans les données et une recherche par filtres.
Identification des équipements présents sur le réseau	Arkime enregistre les adresses IP et autres métadonnées des sessions, ce qui permet d'identifier les équipements et de suivre leurs connexions sur le réseau en fonction de l'activité et sur la base du trafic capturé.
Informations connues pour chaque équipement	Les sessions capturées par Arkime contiennent des informations détaillées telles que les adresses IP, les ports, les protocoles et les métadonnées associées, offrant un aperçu complet des activités de chaque équipement.
Suivi de communications entre équipements et des protocoles utilisés	Arkime enregistre les communications de session et les protocoles (HTTP, DNS, etc.) utilisés, permettant une analyse détaillée des interactions entre équipements et des protocoles réseau en cours.
Ajout manuel d'informations sur les équipements (nom, rôle, etc.)	Arkime permet l'ajout de tags personnalisés et de notes sur les sessions capturées, offrant une capacité d'annotation pour documenter les rôles, noms, et autres détails sur les équipements réseau.

Conçu pour l'archivage réseau à grande échelle : Arkime excelle dans la capture et le stockage massif de données réseau, idéal pour les environnements nécessitant une conservation à long terme de données de sessions.
Visualisation et navigation efficace : Avec son interface Web intuitive, Arkime facilite la visualisation en temps réel et la recherche des données réseau, mais n'est pas spécifiquement conçu pour la gestion d'inventaire d'équipements.

3 CONCLUSION

Suite à l'étude des outils de surveillance réseau, Zeek et Arkime sont pour le moment les outils répondants le plus à nos besoins.

La capture et l'analyse des paquets à une importance cruciale ainsi que de pouvoir l'archiver, cela nous permet par la suite d'avoir une surveillance constante sur le trafic réseau.