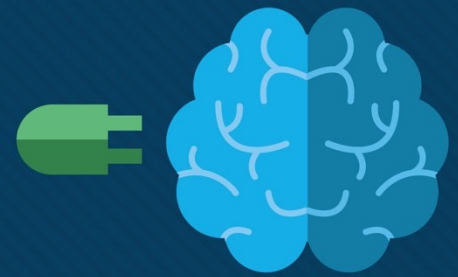


Module 27: Utilisation des données de sécurité du réseau.

CyberOps Associate v1.0

Objectifs du module

Titre du Module : Utilisation des données de sécurité du réseau.

Objectif du Module: Interpréter les données afin de déterminer la source d'une alerte.

Titre du Rubrique	Objectif du Rubrique
Une plate-forme de données commune	Expliquer comment les données sont préparées pour une utilisation dans un système de surveillance de la sécurité du réseau (NSM).
Examiner les données du réseau	Utiliser les outils Security Onion pour examiner les événements de sécurité du réseau.
Améliorer le travail des analystes en Cybersécurité.	Décrire les outils de surveillance du réseau qui améliorent la gestion du workflow.

27.1 Une plate-forme de données commune

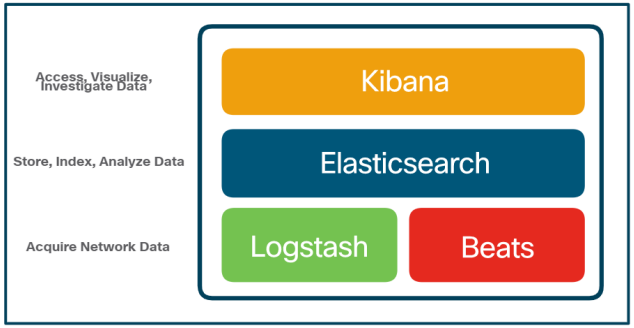
Une plate-forme de données commune

ELK

Security Onion inclut Elastic Stack qui se compose d'Elasticsearch, Logstash et Kibana (ELK).

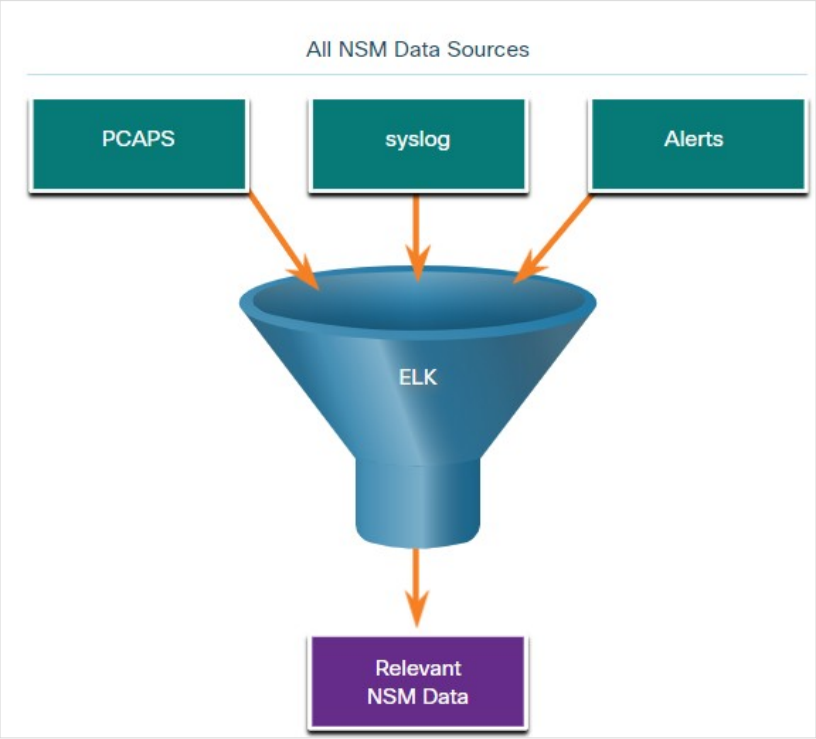
Composantes essentielles de l'ELK :

- **Elasticsearch**: Une plateforme open core permettant de rechercher et d'analyser les données d'une organisation en temps réel.
- **Logstash**: permet la collecte et la normalisation des données réseau dans des index de données qui peuvent être recherchés efficacement par Elasticsearch.
- **Kibana**: Fournit une interface graphique aux données compilées par Elasticsearch.
- **Beats**: Série de plugins logiciels qui envoient différents types de données aux magasins de données Elasticsearch.



Réduction des données

- Pour réduire les données, il est essentiel d'identifier les données de réseau qui devraient être collectées et stockées afin de réduire la charge sur les systèmes.
- En limitant le volume des données, des outils comme Elasticsearch sont beaucoup plus efficaces.



Normalisation des données

- La standardisation des données consiste à combiner des données provenant de plusieurs sources dans un format commun.
- Un schéma commun détermine les noms et les formats des champs de données requis.
- Par exemple, les adresses IPv6, les adresses MAC et les informations de date et de temps peuvent être représentées dans des formats distincts.

Formats d'adresses IPv6	Formats d'adresses MAC	Formats de date
2001:db8:acad:1111:2222::33	A7:03:DB:7C:91:AA	Monday, July 24, 2017 7:39:35pm
2001:DB8:ACAD:1111:2222::33	A7-03-DB-7C-91-AA	Mon, 24 Jul 2017 19:39:35 +0000
2001:DB8:ACAD:1111:2222:0:0:33	A70.3DB.7C9.1AA	2017-07-24T19:39:35+00:00

- La normalisation des données est nécessaire pour simplifier la recherche des événementscorrélés.

Archivage des données

- Il n'est pas possible de conserver indéfiniment les données de surveillance de la sécurité des réseaux (NSM) en raison de problèmes de stockage et d'accès.
- La période de rétention de certains types de données de sécurité du réseau est parfois régie par des règles de conformité.
- Par défaut, les données des alertes Sguil sont conservées pendant 30 jours. Cette valeur est définie dans le fichier **securityonion.conf**.
- Les données Security Onion peuvent toujours être archivées sur un périphérique de stockage externe, en fonction des besoins et l'infrastructure de l'entreprise.

***Remarque**: Les emplacements de stockage des différents types de données Security Onion peuvent varier en fonction de l'implémentation utilisée.*

Travaux pratiques - Convertir les données dans un format universel

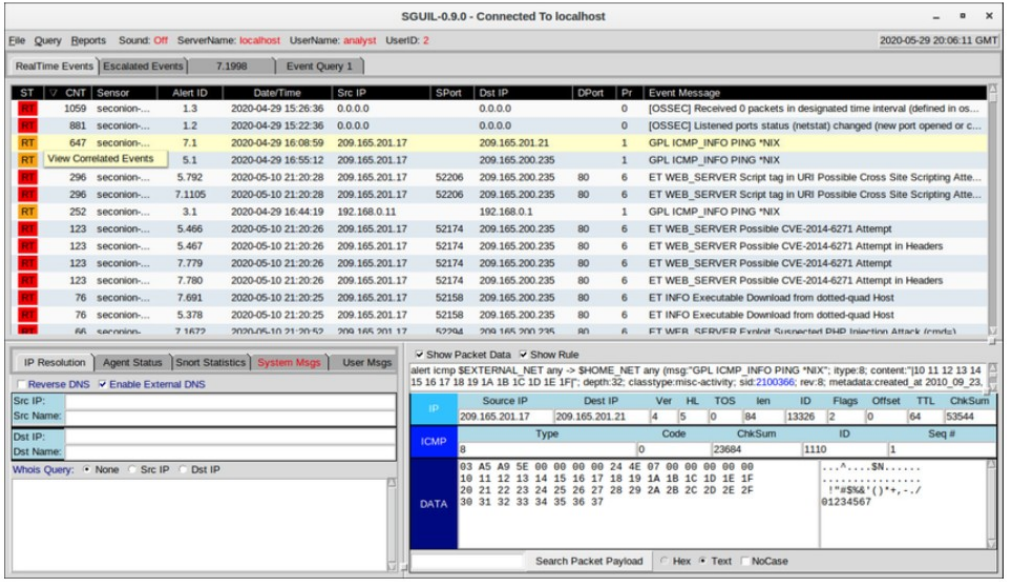
Au cours de ces travaux pratiques, vous aborderez les points suivants:

- **Partie 1**: Utiliserez les outils de ligne de commande pour normaliser manuellement les entrées de journal.
- **Partie 2**: Le champ timestamp doit être normalisé.
- **Partie 3**: Le champ IPv6 exige une normalisation.

27.2 Examiner les données du réseau

Utilisation de Sguil

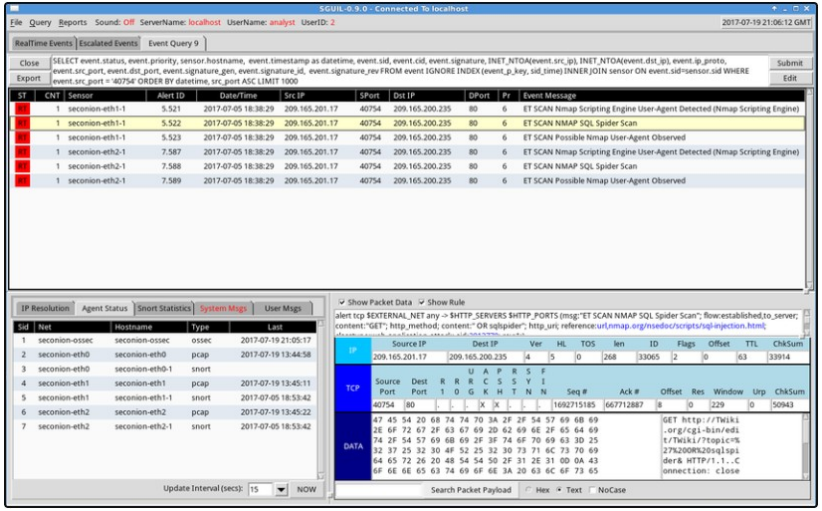
- L'analyste en cybersécurité consulte Sguil en priorité dans Security Onion pour vérifier la présence d'alertes.
- Sguil met automatiquement en corrélation les alertes similaires sur une même ligne et vous permet d'afficher les événements mis en corrélation sur cette ligne.
- Pour mieux comprendre ce qui s'est passé sur le réseau, il peut être utile de trier la colonne **CNT** pour afficher les alertes avec la fréquence la plus élevée.



Alertes Sguil triées sur CNT

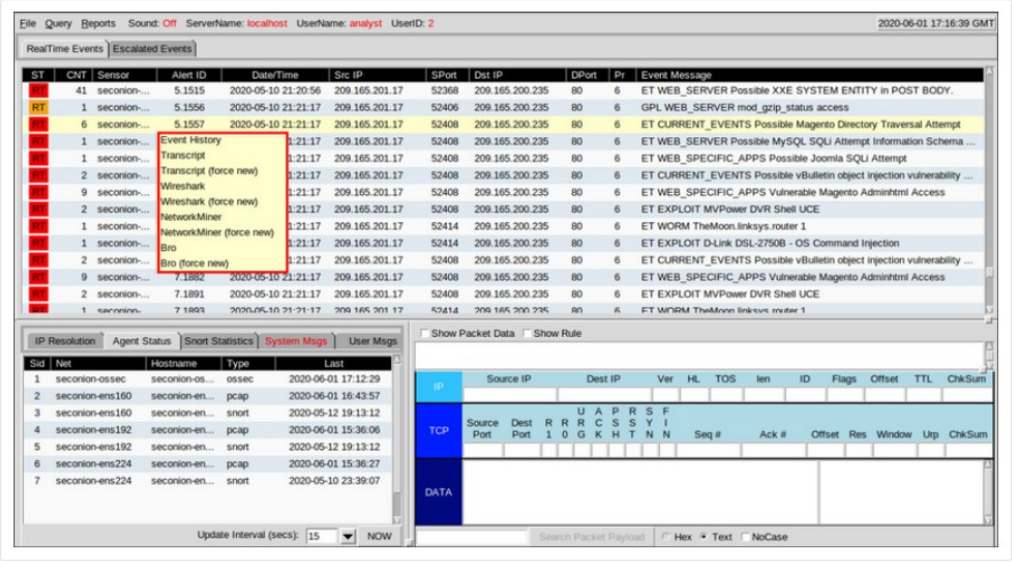
Requêtes Sguil

- Les requêtes peuvent être créées dans Sguil à l'aide du générateur de requêtes. Il simplifie la construction de requêtes dans une certaine mesure.
- Un analyste en cybersécurité doit connaître les noms de champ et certains problèmes liés aux valeurs de ces champs pour construire efficacement des requêtes en Sguil.
- Par exemple, Sguil stocke les adresses IP dans une représentation sous forme d'entier.



Basculement depuis Sguil

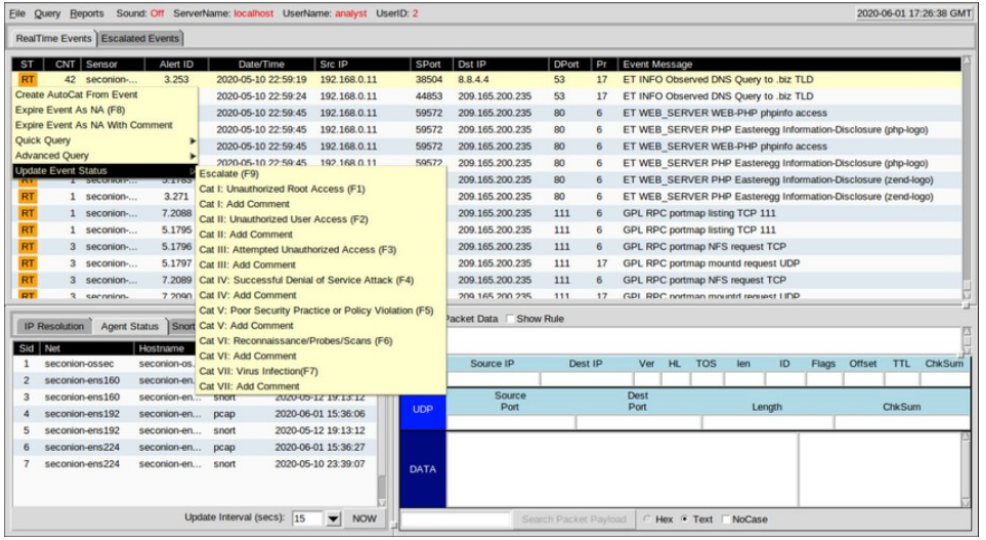
- Sguil permet à l'analyste en cybersécurité de basculer vers d'autres outils et sources d'information.
- Les fichiers journaux sont disponibles dans Elasticsearch.
- Les captures de paquets pertinentes peuvent être affichées dans Wireshark.
- Sguil permet d'accéder aux informations PRADS (Passive Real-time Asset Detection System) et SANCP (Security Analyst Network Connection Profiler).



***Remarque**: l'interface Sguil fait référence à PADS au lieu de PRADS.*

Gestion des événements dans Sguil

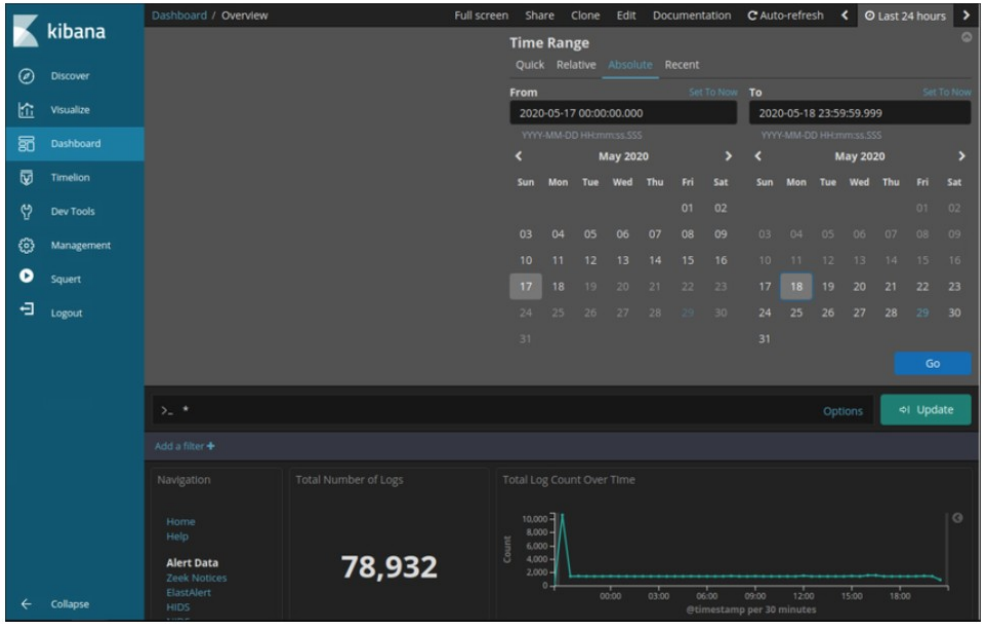
- Sguil est une console qui permet à un analyste de la cybersécurité d'enquêter, de vérifier et de classer les alertes de sécurité.
- Trois tâches peuvent être accomplies dans Sguil pour gérer les alertes:
  - Les alertes qui se sont avérées être des faux positifs peuvent être obsolètes.
  - Un événement peut être escaladé en appuyant sur la touche F9.
  - Il est possible de catégoriser un événement.



- Sguil comprend sept catégories prédéfinies qui peuvent être attribuées via un menu illustré dans la figure ou en appuyant sur la touche de fonction correspondante.

Utilisation d'ELK

- Logstash et Beats sont utilisés pour l'ingestion de données dans Elastic Stack.
- Kibana, qui est l'interface visuelle dans les journaux, est configuré pour afficher les dernières 24 heures par défaut.
- Les journaux sont ingérés dans Elasticsearch dans des index ou bases de données distincts en fonction d'une plage de temps configurée.
- La meilleure façon de surveiller les données dans Elasticsearch est de créer des tableaux de bord visuels personnalisés.



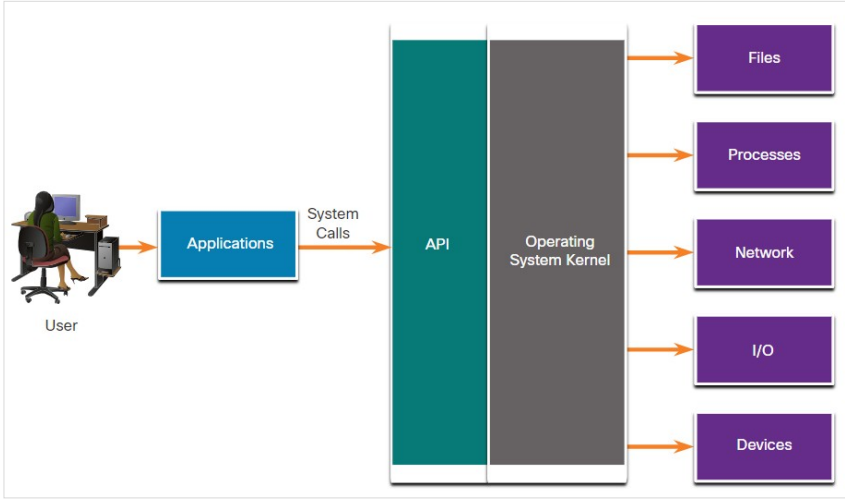
Requêtes dans ELK

- Elasticsearch est basé sur Apache Lucene, une bibliothèque logicielle de moteurs de recherche open source qui offre des fonctions d'indexation et de recherche en texte intégral.
- En utilisant les bibliothèques logicielles Lucene, Elasticsearch a son propre langage de requête basé sur JSON appelé Query Domain Specific Language (DSL).
- Avec JSON, les requêtes Elasticsearch utilisent des éléments tels que Opérateurs Booléens, Champs, Plages, Caractères Génériques, Regex, Recherche Floue, Recherche Textuelle.
- Elasticsearch a été conçu pour interagir avec les utilisateurs utilisant des clients basés sur le Web qui suivent le cadre HTTP REST.
- Les méthodes utilisées pour exécuter les requêtes sont URI, cURL, JSON et Dev Tools.

***Remarque**: Les requêtes de recherche d'Elasticsearch avancée dépassent le cadre de ce cours. Au cours des travaux pratiques, les instructions de requête complexes vous seront fournies, le cas échéant.*

Examiner les appels d'API et les processus

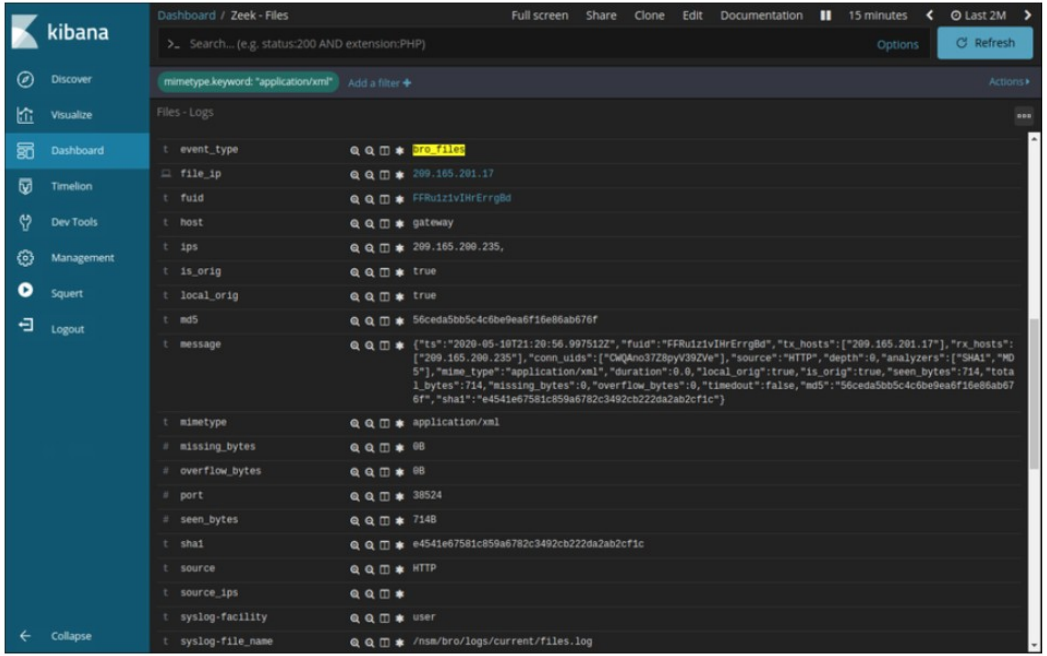
- Les applications interagissent avec le système d'exploitation par le biais d'appels système vers l'interface de programmation (API) de ce dernier.
- Si un malware peut berner le noyau d'un système d'exploitation pour le pousser à effectuer des appels système, de nombreux exploits sont possibles.
- Les règles OSSEC détectent les changements dans les paramètres basés sur l'hôte.
- Ces règles OSSEC déclenchent une alerte dans Sguil.
- Basculer sur Kibana à l'adresse IP hôte permet de choisir le type d'alerte en fonction du programme qui l'a créée.



- Le filtrage des indices OSSEC donne une vue des événements OSSEC qui se sont produits sur l'hôte, y compris les indicateurs que le logiciel malveillant peut avoir interagi avec le noyau du système d'exploitation.

Examiner les détails des fichiers

- Dans Sguil, si un analyste en cybersécurité trouve le fichier suspect, la valeur de hash peut être transmise à un site, afin de déterminer s'il s'agit d'un programme malveillant connu.
- Dans Kibana, Zeek Hunting peut être utilisé pour afficher des informations concernant les fichiers entrés dans le réseau.
- Notez que dans Kibana, le type d'événement est affiché sous la forme**bro_files**, même si le nouveau nom pour Bro est Zeek.



Travaux pratiques - Tutoriel sur les expressions régulières

Au cours de ces travaux pratiques, vous aborderez les points suivants:

- Utiliserez un tutoriel en ligne pour découvrir les expressions régulières.
- Décrirez les informations correspondant à des expressions régulières particulières.

Travaux pratiques - Extraire un fichier exécutable d'une capture PCAP

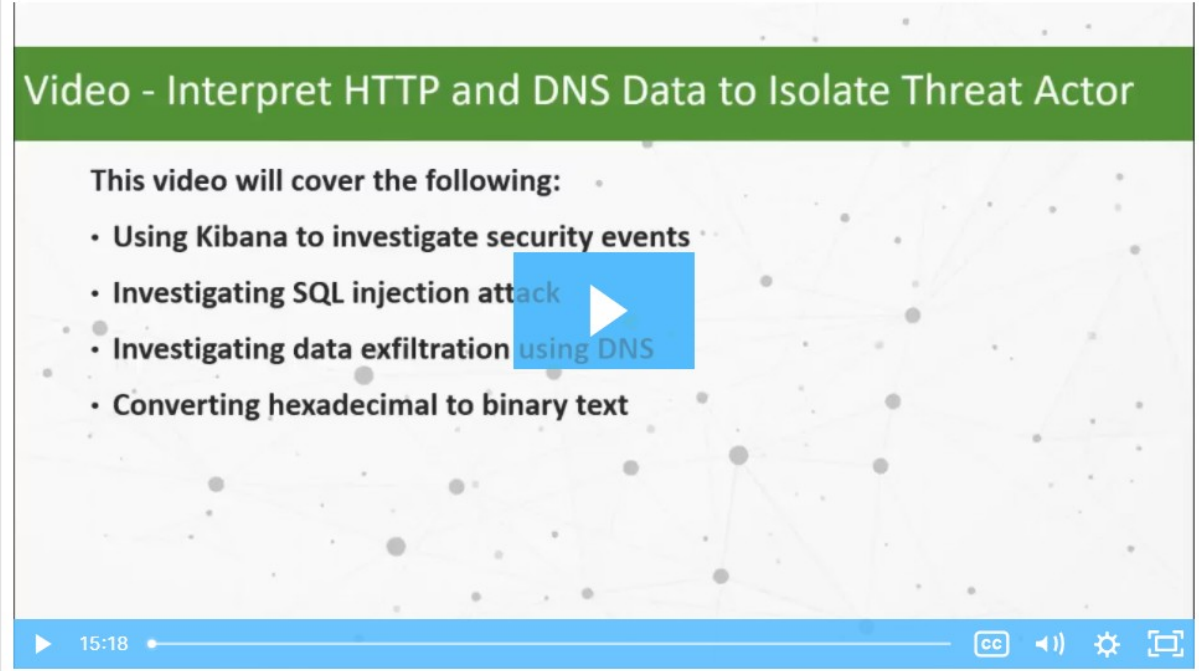
S'il est essentiel de consulter les fichiers journaux, il l'est également de comprendre comment sont effectuées les transactions réseau au niveau des paquets.

Ces travaux pratiques ont l'objectif suivant:

- Analyser le trafic dans un fichier pcap précédemment capturé et extraire un fichier exécutable à partir de ce fichier.

Vidéo - Interpréter les données HTTP et DNS pour isoler l'acteur de la menace

Regardez la vidéo pour visionner une présentation pas à pas du travaux pratiques Security Onion interpret les données HTTP et DNS pour isoler un acteur de menace



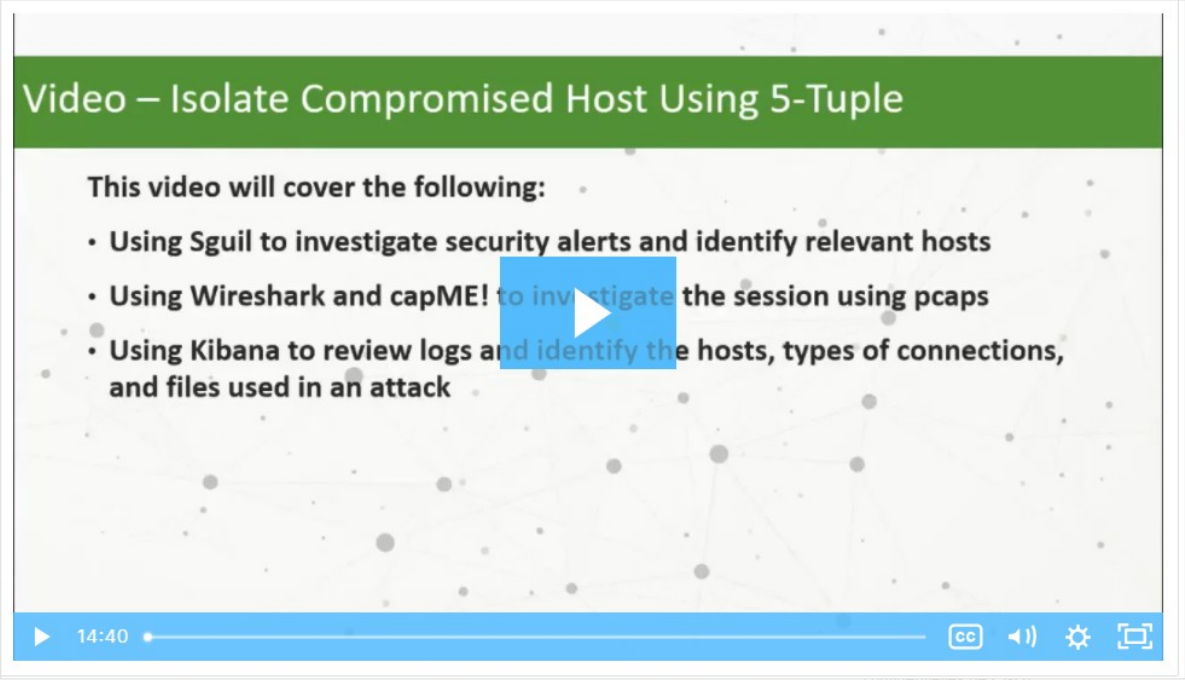
Travaux pratiques - Interpréter les données HTTP et DNS pour isoler un acteur de menace

Ces travaux pratiques ont l'objectif suivant:

- Étudiez les exploits d'injection SQL et d'exfiltration DNS à l'aide des outils Security Onion.

Vidéo - Isoler l'hôte compromis à l'aide de 5-tuple

Regardez la vidéo pour visionner une présentation pas à pas de l'hôte compromis Security Onion Isolate à l'aide du laboratoire 5-Tuple.



Travaux pratiques - Isoler un hôte compromis en utilisant un 5-tuple

Ces travaux pratiques ont l'objectif suivant:

- Utilisez les outils Security Onion pour enquêter sur un exploit.

Travaux pratiques - Enquêter sur l'exploitation des logiciels malveillants

Ces travaux pratiques ont l'objectif suivant:

- Utiliser Security Onion pour enquêter sur un logiciel malveillant plus complexe et utilise un kit d'exploitation pour infecter les hôtes.

Travaux pratiques - Examiner une attaque sur un hôte Windows

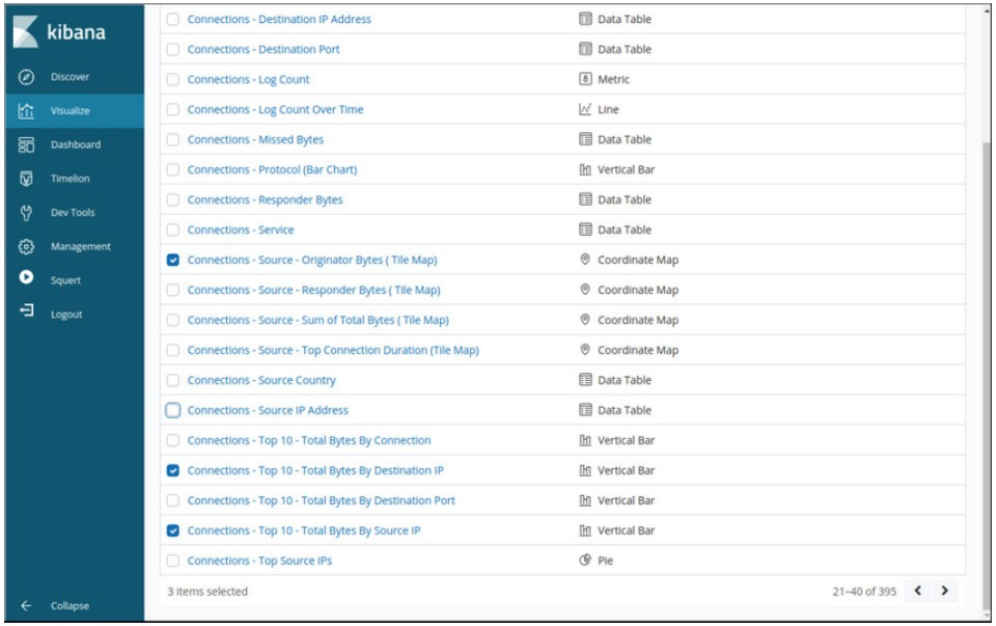
Au cours de ces travaux pratiques, vous aborderez les points suivants:

- Examiner une attaque sur un hôte Windows
- Utilisez Sguil, Kibana et Wireshark dans Security Onion pour enquêter sur l'attaque.
- Examinez les artifacts d'exploitation.

27.3 Améliorer le travail des analystes en cybersécurité

Tableaux de bord et visualisations

- Les tableaux de bord offrent une combinaison de données et de visualisations qui permettent aux analystes de la cybersécurité de se concentrer sur des détails et des informations spécifiques.
- Généralement, les tableaux de bord sont interactifs.
- Kibana permet de concevoir des tableaux de bord personnalisés.
- En outre, d'autres outils inclus dans Security Onion, fournissent une interface visuelle aux données NSM.



Gestion des workflows

- Les workflows sont la séquence de processus et de procédures par laquelle les tâches de travail sont exécutées.
- Gérer les workflows de SOC:
  - Améliore l'efficacité de l'équipe cyberopérations
  - Renforce la responsabilisation du personnel
  - Permet de s'assurer que toutes les alertes potentielles sont traitées correctement
- Sguil fournit des fonctionnalités élémentaires de gestion des workflows, mais ne convient pas aux grands déploiements. Il existe des systèmes tiers disponibles qui peuvent être personnalisés.
- Les requêtes automatiques améliorent l'efficacité des workflows de cyberopérations Ces requêtes recherchent automatiquement les incidents complexes qui peuvent contourner d'autres outils.

27.4 Récapitulation de l'utilisation des données de sécurité du réseau

Qu'est-ce que j'ai appris dans ce module?

- Une plate-forme de surveillance de la sécurité réseau telle que ELK ou Elastic Stack doit unir les données à des fins d'analyse.
- ELK se compose d'Elasticsearch, Logstash et Kibana avec des composants, Beats, ElastaLert et Curator.
- Les données réseau doivent être réduites de manière à ce que seules les données pertinentes soient traitées par le système NSM.
- Les données réseau doivent également être normalisées pour convertir les mêmes types de données en formats cohérents.
- Sguil fournit une console qui permet à un analyste de la cybersécurité d'enquêter, de vérifier et de classer les alertes de sécurité.
- Les visualisations Kibana fournissent des informations sur les données NSM en représentant de grandes quantités de formats de données plus faciles à interpréter.
- La gestion du flux de travail ajoute de l'efficacité au travail de l'équipe SOC.


CISCO