ⵜⴰⵖⵣⵓⵍⵜ ⵏ ⵜⵙⴰⵡⴰⵍⵜ
FACULTÉ DES SCIENCES

MARRAKECH
جامعة القاضي عياض
UNIVERSITÉ CADI AYYAD

Semlalia

كليـــــــــة العلوم
FACULTY OF SCIENCE

Investigation Numérique-Digital Forensics

Module : Pentesting et Digital Forensics
Filière : Licence en Networking, Système et Cybersécurité (S5)
Département : Informatique

Pr. Mariya Ouaissa
E-mail : m.ouaissa@uca.ac.ma

Année Universitaire 2025/2026

Plan de Cours

Partie 1 : Maîtriser la technologie SIEM

Chapitre 1 : Connaître le fonctionnement de SIEM

Chapitre 2 : Concevoir les règles de corrélation

Partie 2 : Les Méthodologies d'investigation réseaux et systèmes

Préambule

Chapitre 1 : Processus d'investigation numérique

Chapitre 2 : Répertorier les indices de compromission

Partie 3 : Maitriser les outils d'investigation

Chapitre 1 : Identifier les outils d'investigation du marché

Chapitre 2 : Appliquer les outils sur un cas pratique

Partie 4 : Rédiger des rapports d'investigation

Maîtriser la technologie SIEM (SEM / SIM)

Plan du cours

Partie 1 : Maîtriser la technologie SIEM

Chapitre 1 : Connaître le fonctionnement de SIEM

- Définition de SIEM
- Solutions du marché

Chapitre 2 : Concevoir les règles de corrélation

- Découvrir et manipuler les logs
- Utilisation de SIEM pour la détection d'intrusion (Elastic)

Plan du cours

Partie 1 : Maîtriser la technologie SIEM

Chapitre 1 : Connaître le fonctionnement de SIEM

- Définition de SIEM
- Solutions du marché

Chapitre 2 : Concevoir les règles de corrélation

- Découvrir et manipuler les logs
- Utilisation de SIEM pour la détection d'intrusion (Elastic)

Chapitre 1 : Connaître le fonctionnement de SIEM

Définition de SIEM

C’est quoi un incident de sécurité?

- Un incident de sécurité est une occurrence ou un évènement qui compromet le bon fonctionnement, la sécurité d’un système d'information ou bien la modification ou la destruction non autorisés d'informations. Autrement dit, c’est tout incident intentionnel ou non intentionnel qui constitue une menace accrue pour la sécurité informatique Il peut s'agir d'une menace suspectée, tentée, réussie ou imminente de cet accès non autorisé.

- Cela signifie que quelle que soit la réussite ou la sévérité de l'incident de sécurité, l’exécution des procédures de traçage et de suivi est primordiale pour garantir la confidentialité et la fiabilité des systèmes informatiques et empêcher qu'un événement similaire ne se reproduise à l'avenir.

- Un incident de sécurité peut être isolé ou consister en plusieurs événements qui, ensemble, indiquent que les systèmes ou les données d'une organisation peuvent avoir été compromis ou que les mesures de protection peuvent avoir échoué.

- Voici des exemples d'incidents de sécurité
  - ✓ Modifications non autorisées des systèmes, des logiciels ou des données
  - ✓ Accès non autorisé ou utilisation de systèmes, de logiciels ou de données
  - ✓ Attaque par déni de service
  - ✓ Comptes d'utilisateurs compromis

Les SOC (Security Operations Center), une solution des entreprises pour lutter contre les attaques

- Pour identifier et investiguer des incidents de sécurité, des nombreuses entreprises comptent sur un ***Security Operations Center*** **(SOC)**.
- Le SOC est une équipe dédiée à la **supervision de la sécurité du système d'information**.
- Pour ce faire, elle utilise des outils de monitoring, mais aussi des outils de collecte, d'intervention à distance et de corrélation d'événements.

•Elle recherche les signes d'un incident ou d'une compromission, par exemple des signaux faibles ou des comportements anormaux, afin de protéger le SI. Cette surveillance aide à la détection des événements de sécurité : intrusion, exécution de code non autorisé, exploits, élévation de privilèges, tentative d'accès à un compte admin, etc.

- Le SOC est donc un élément capital pour la sécurité des données de l'entreprise.

Les SOC (Security Operations Center), une solution des entreprises pour lutter contre les attaques

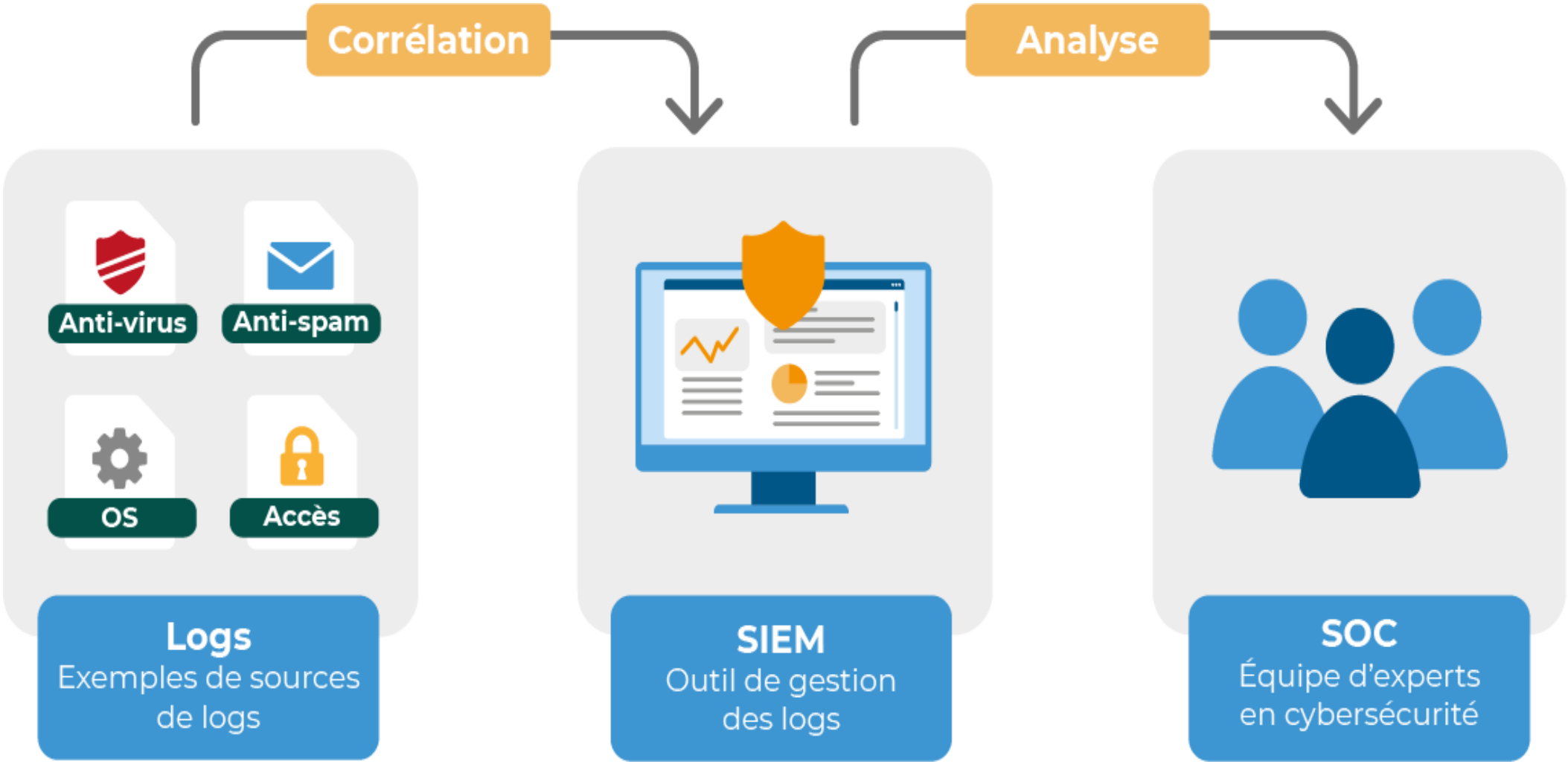
- Pour gérer les alertes et détecter des intrusions, les équipes SOC utilisent un ***Security Information Event Management* (SIEM)**. C'est un des outils centraux pour monitorer la sécurité que nous verrons plus en détail dans les prochaines parties de ce cours.

- La mission principale d'un SOC est d'**identifier, analyser et remédier aux incidents de cybersécurité**. Cela, grâce au monitoring des différents équipements, mais aussi grâce aux méthodes d'analyse et de veille.

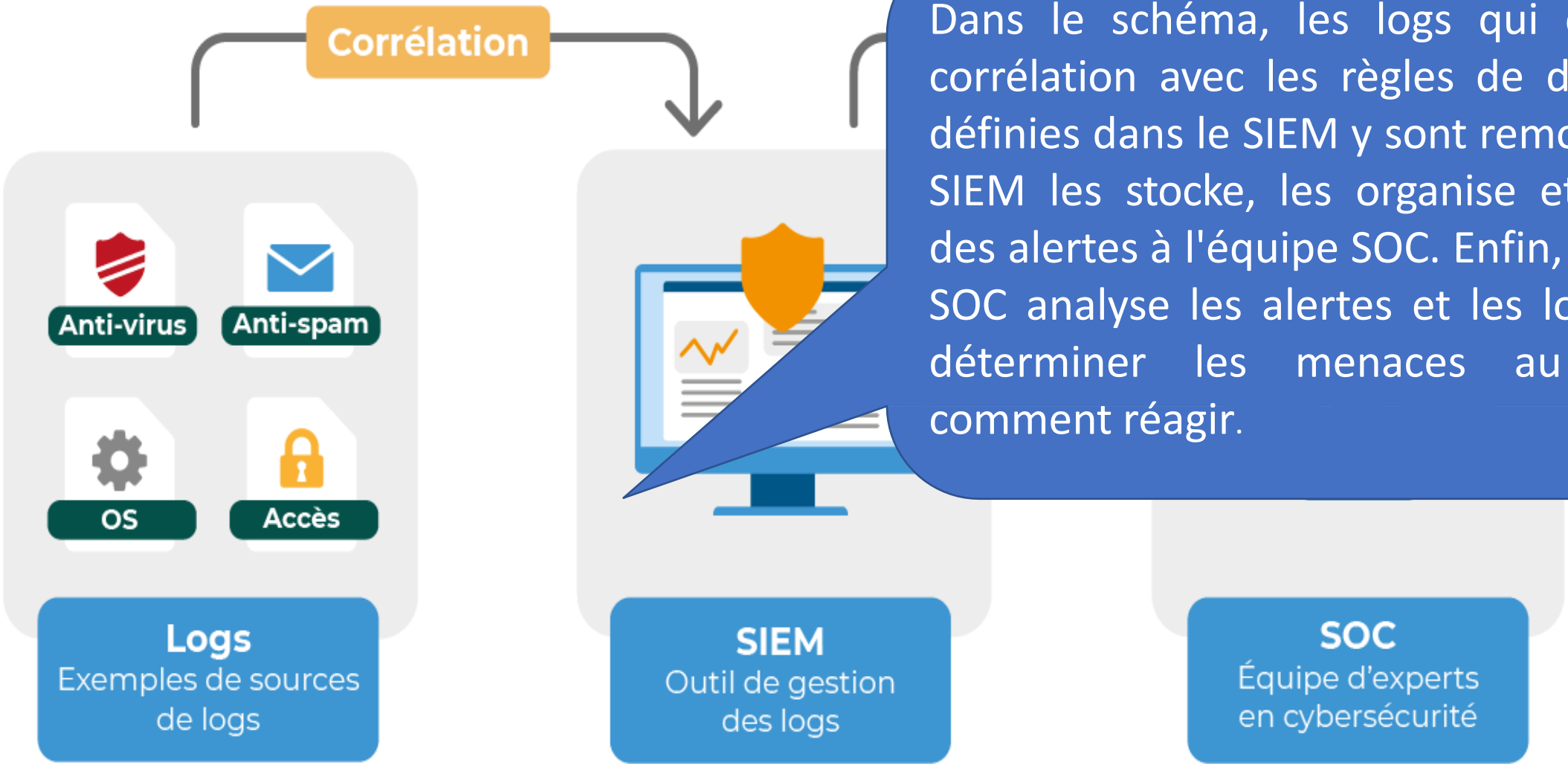
Comment installer un SOC ?

- La mise en place d'un SOC peut être compliquée et coûteuse. Toutefois, c'est un investissement à ne pas négliger pour être capable de **protéger les données** de l'entreprise, mais aussi pour **répondre rapidement** en cas de compromission. En effet, la centralisation des logs permettra des investigations plus organisées, dans le but de trouver les sources et les vecteurs de l'attaque en cas d'incident.
- La surveillance du SI en continu 24h/24 et 7j/7 permet donc de monitorer les activités réseaux, les machines, les serveurs, bref, tout élément connecté au SI.

Le schéma ci-dessous présente une architecture simplifiée avec comme point central le SIEM.



Le schéma ci-dessous présente une architecture simplifiée avec comme point central le SIEM.



Dans le schéma, les logs qui ont une corrélation avec les règles de détection définies dans le SIEM y sont remontés. Le SIEM les stocke, les organise et envoie des alertes à l'équipe SOC. Enfin, l'équipe SOC analyse les alertes et les logs pour déterminer les menaces au SI et comment réagir.

Récapitulation

- Les SOC veillent et administrent la sécurité du système d'information pour identifier, analyser les incidents de sécurité, et y remédier.
- Les bénéfices du SOC incluent la protection des données sensibles et la conformité aux règles de l'industrie.
- **Et convient aussi à déployer et mettre en place les solutions** permettant la détection et l'analyse, comme des serveurs de collecte de logs, des *Intrusion Prevention Systems* (IPS)/*Intrusion Detection Systems* (IDS), des *Endpoint Detection and Response* (EDR), un SIEM.

Maîtriser la technologie SIEM

- Le **SIEM (*Security Information and Event Management*)** est une approche du management de la sécurité. Le SIEM donne aux professionnels de la sécurité un aperçu et un historique des activités au sein de leur environnement informatique.
- Il génère des alertes basées sur l'analyse et la corrélation de plusieurs sources d'événements de sécurité.
- La technologie SIEM existe depuis plus d'une décennie. Elle a évolué initialement de la discipline de gestion des logs. Elle combine :
  - **la gestion des événements de sécurité** (SEM), qui analyse les données des journaux et des événements en temps réel pour fournir une surveillance des menaces, la corrélation des événements et la réponse aux incidents ;
  - avec **la gestion des informations de sécurité** qui collecte, analyse et établit des rapports sur les données des journaux.

Fonctionnement d’un SIEM

- Le SIEM **collecte et agrège les données de journaux** générées dans tout votre système d’information, des applications aux périphériques réseau et de sécurité, tels que les pare-feux et les détections antimalware.
- Il identifie et catégorise ensuite les incidents et événements, et les analyse. Le logiciel répond à deux objectifs principaux :
  - **Fournir des rapports** sur les incidents et événements liés à la sécurité : les connexions réussies et échouées, l'activité des logiciels malveillants et d'autres activités malveillantes possibles.
  - **Envoyer des alertes** si l'analyse montre qu'une activité s'exécute sur des ensembles de règles prédéterminées, comme par exemple l'exécution d'un logiciel malveillant, et indique ainsi un problème de sécurité potentiel.

Chapitre 1 : Connaître le fonctionnement de SIEM

Solutions SIEM du marché

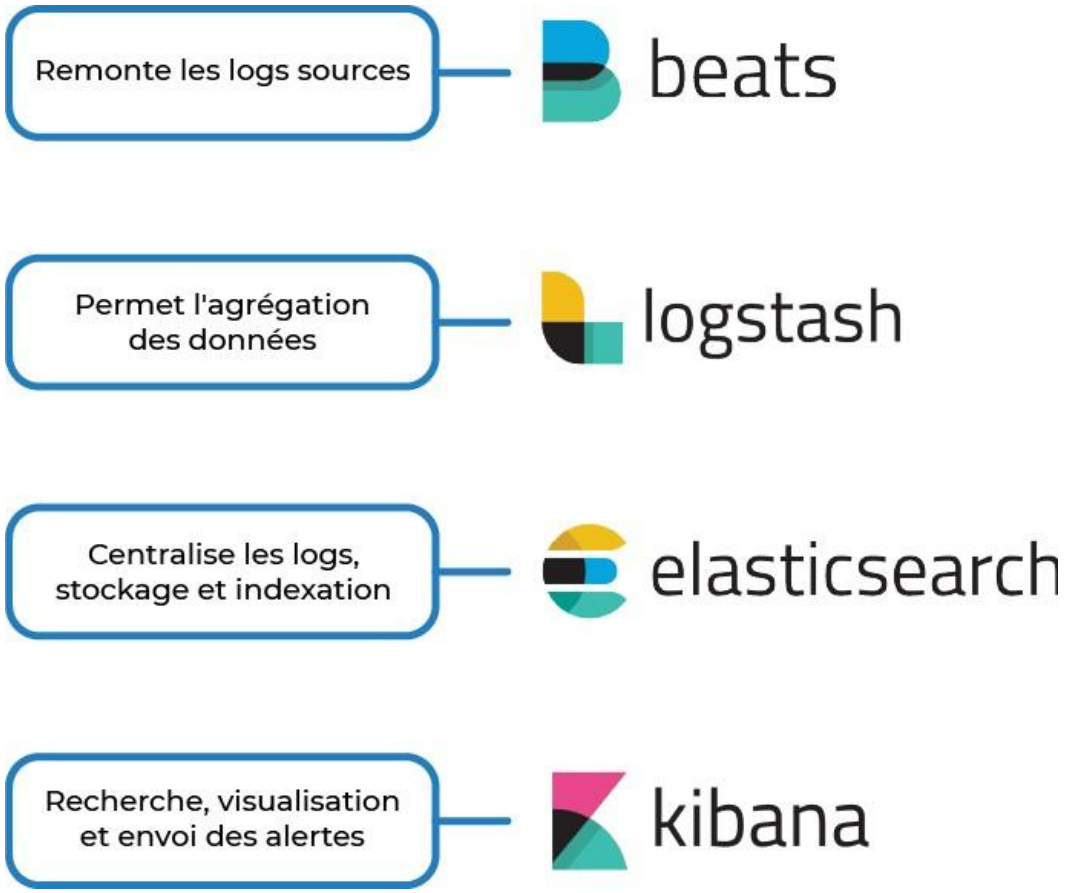
Comparaison des solutions SIEM du marché

- Vous avez le choix d'une multitude de SIEM sur le marché, des solutions libres ou open source à des solutions plus avancées (incluant des mécanismes de machine learning qui détectent les événements de sécurité, par exemple).

- Cette année, le Gartner a proposé un tableau de comparaison des meilleurs SIEM du marché (en anglais) pour l'aide à décision – je vous invite à y jeter un œil !

Le SIEM que nous allons utilisé : Elastic

- Dans ce cours, nous utiliserons **la solution open source ELK** (Elasticsearch, Logstash, Kibana) qui permet le monitoring de logs et la détection d'alerte. ELK est très intéressant, car il exploite une multitude de sources de données et les visualise de manière graphique.
- La suite ELK est composée de 4 outils, qui vous permettra de gérer vos logs dans l'ordre suivant :
  - **Beats**, pour l'envoi de logs en fonction des systèmes utilisés : Windows, Linux, logs réseau ;
  - **Logstash**, permettant de modifier les données envoyées dans ElasticSearch ;
  - **Elasticsearch,** la base de données principale pour le stockage des données ;
  - et enfin **Kibana**, l'interface graphique permettant de visualiser les données remontées au moyen de dashboards et l'envoi des alertes...



Récapitulation

- nous venons de voir le fonctionnement d'un SIEM, qui a pour objectifs :

  - de fournir des rapports sur les incidents et évènements liés à la sécurité ;
  - d'envoyer des alertes pour de probables problèmes de sécurité.

- Nous avons également vu le SIEM que nous déploierons dans la suite du cours : ELK. Il comprend ElasticSearch, Logstash, Kibana et Beats.

Plan du cours

Partie 1 : Maîtriser la technologie SIEM

Chapitre 1 : Connaître le fonctionnement de SIEM

- Définition de SIEM
- Solutions du marché

Chapitre 2 : Concevoir les règles de corrélation

- Découverte et manipulations manuelles des logs
- Utilisation de SIEM pour la détection d'intrusion (Elastic)

Chapitre 2 : Concevoir les règles de corrélation

Découvrir et manipuler les logs

Découvrir les logs

- Lorsque vous monitorez le réseau d'une entreprise, il est nécessaire d'effectuer une collecte de logs pour **comprendre et identifier des événements sur le réseau**. Cette centralisation est primordiale dans le maintien opérationnel du système d'information.

- En informatique, un **log** est un fichier qui enregistre des événements qui se produisent sur un système d'exploitation ou tout autre équipement informatique, routeur, switch, serveur. La collecte de logs vous donnera des informations sur ce qui se passe sur votre S

Comprendre les logs avant de voir Elastic

- Les logs peuvent contenir des messages entre différents utilisateurs d'un logiciel de communication, par exemple, mais également des connexions réseau, des actions de création ou de suppression de fichier, des tentatives d'accès, etc.

Types de logs

Événements (Logs)	
Événements générés par les systèmes d'exploitation, les services et les applications	Les événements (Logs) des systèmes d'exploitation, des services et des applications (en particulier les événements liées à la sécurité) sont souvent d'une grande valeur pour la détection et le traitement d'un incident, telles que l'enregistrement des événements relatifs à l'accès aux comptes et les actions qui ont été réalisées. Les entités doivent mettre en place des références exigeant l'activation des logs sur tous les systèmes et surtout sur les systèmes critiques sans oublier les postes utilisateurs. Ces logs peuvent être analysés en utilisant des règles de corrélation. Une alerte peut être générée suite à cette analyse pour indiquer un incident.

Types de logs

Événements des équipements réseaux et FW	Les événements (Logs) générés par ces équipements identifient les connexions bloquées et aussi autorisées, même s'ils fournissent peu d'informations sur la nature de l'activité. Ils peuvent être utiles pour identifier les tendances du réseau et faire des analyses comportementales comme ils peuvent être corrélés avec d'autres événements détectés par d'autres sources.
NetFlow	Les routeurs, les switchs et autres périphériques réseau peuvent fournir ces métadonnées relatives au protocole TCP/IP. Ces informations sur le flux réseau, peuvent être utilisées pour identifier des activités anormales provoquées par des logiciels malveillants, exfiltration de données, et d'autres actes de malveillance.

Emplacement	Contenu
/var/log/alternatives.log	Les logs d'update-alternatives.
/var/log/apache2/*	Les logs du serveur http apache2.
/var/log/apt/*	Les logs d'apt. Tous les paquets installés avec apt-get install, par exemple.
/var/log/aptitude	Les logs d'aptitude. Contient toutes les actions demandées, même les abandonnées.
/var/log/auth.log	Les informations d'autorisation de système. Y sont consignées toutes les connexions (réussies ou pas) et la méthode d'authentification utilisée.
/var/log/bind.log	Les logs du serveur de nom bind9, s'il sont activés.
/var/log/boot.log	Les informations enregistrées lors du démarrage du système. Ce fichier n'est pas activé par défaut.
/var/log/cron	Les informations sur les tâches cron. Enregistrement à chaque fois que le démon cron (ou anacron) commence une tâche.
/var/log/daemon.log	Les informations enregistrées par les différents daemons (processus) de fond qui fonctionnent sur le système.
/var/log/debug	Les logs de debugging.
/var/log/dmesg	Les messages du noyau Linux depuis le démarrage.
/var/log/dpkg.log	Les informations sur les paquets installés ou retirés en utilisant la commande dpkg.
/var/log/faillog	Les échecs de connexion. # faillog -u root.
/var/log/kern.log	Les informations enregistrées par le noyau. Utile pour débogguer un noyau personnalisé, par exemple.
/var/log/lastlog	Les informations de connexion récente de tous les utilisateurs. Ce n'est pas un fichier ascii. Vous devez utiliser la commande lastlog pour afficher le contenu de ce fichier.
/var/log/mail.*	Les informations du serveur de messagerie. Par exemple, sendmail enregistre des informations sur tous les éléments envoyés dans ces fichiers.
/var/log/messages	Les messages du système, y compris les messages qui sont enregistrés au démarrage. Beaucoup de choses sont enregistrées dans /var/log/ messages y compris le courrier, cron, daemon, kern, auth, etc.
/var/log/syslog	Tous les messages, hormis les connexions des utilisateurs. Plus complet que /var/log/messages.
/var/log/user.log	Les informations sur tous les journaux de niveau utilisateur

Objectifs de gestion des logs

- La gestion de votre collecte de logs consistera à mettre en place la journalisation et la centralisation. La **journalisation** est la mise en place d'un système permettant la remontée automatique de logs. L'envoi de vos logs à un point central décrit la **centralisation**, qui vous donnera une vision globale des événements du système d'information.
- Cette gestion des logs a plusieurs objectifs :
  - **Obtenir un état général du SI** et identifier des événements anormaux.
  - **Détecter les intrusions**, par exemple au moyen de solution IPS/IDS ou de règle SIEM.
  - **Retracer l'historique** et les actions d'un attaquant dans le cadre d'une investigation forensic.
  - **Visualiser les actions du SI**, définir des statistiques et identifier les signaux faibles.
- Mais avant que vous définissiez une supervision et détectiez les événements de sécurité, il est nécessaire de savoir identifier les logs d'intérêt en fonction des systèmes. Cela va optimiser votre collecte de logs, et vous évitera la remontée de logs inutiles

Identifier les logs d’intérêt

- La première étape pour monitorer la sécurité est d’**identifier les logs d’intérêt qui permettent la détection d'événements suspects**. Par exemple, si vous recevez un log d’une connexion au serveur Active Directory en dehors des heures de travail, cela peut être **un comportement anormal auquel vous devez réagir** ! Le rôle du monitoring est justement d’identifier ce type d'événement.
- Les attaquants rivalisent d’ingéniosité pour éviter les détections. Il existe plusieurs techniques permettant de **contourner le logging**. Ils peuvent, par exemple, supprimer les journaux locaux, désactiver la remontée de logs, ou encore effectuer de l’injection de processus, c'est-à-dire camoufler un code malveillant dans un programme légitime. Soyez-en conscient lors de l’analyse des logs.
- Toutefois, vous n’êtes pas obligé de monitorer tout le réseau, car cela provoquerait une surconsommation des ressources du SI, et n’apporterait pas forcément de logs pertinents.

Quels sont les logs pertinents à monitorer ?

- La liste ci-dessous propose des **logs d'intérêt à monitorer** dans le cadre de la surveillance de sécurité du SI, également recommandée par l'ANSSI.
  - Authentification.
  - Gestion des comptes et des droits.
  - Accès aux ressources.
  - Modification des stratégies de sécurité.
  - Activité des processus.
  - Activité des systèmes.

- Cette liste est un bon point de départ. Ainsi, vous éviterez un nombre ingérable de logs dans votre collecte – mais n'hésitez pas à éventuellement ajouter des logs qui sont pertinents à votre SI, même s'ils ne figurent pas dans cette liste.
- Pour aller plus loin, l'ANSSI a mis à disposition un guide de bonnes pratiques pour la mise en place de système de monitoring de logs.
- En cas d'incident de sécurité ou simplement dans le cadre de la surveillance journalière, il peut être intéressant d'explorer les logs manuellement, ce qu'on appelle également le ***parsing*** *de logs*.

Chapitre 2 : Concevoir les règles de corrélation

Utilisation de SIEM pour détection d’intrusion (Elastic)

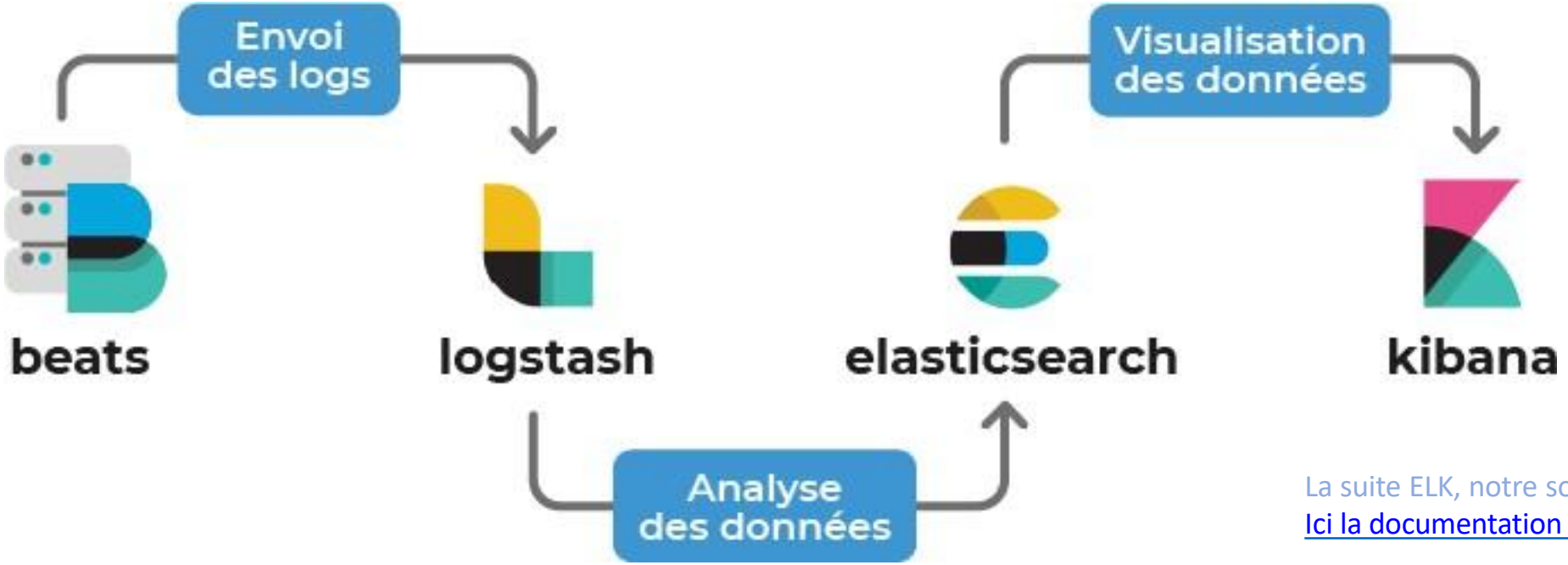
La stack ELK

ELK est une suite open source comprenant 3 composants principaux : **E**lasticsearch, **L**ogstash et **K**ibana. Beats a ensuite été ajouté pour former la stack ELK.

ELK permet l'indexation et l'analyse de données. Vous pourrez par exemple charger différents types de données, comme vos logs, et les visualiser sous forme de diagrammes personnalisés comme dans le screenshot ci-contre :

La stack ELK

- **Beats :** peut être installé sur les machines à monitorer en agent pour vous remonter les logs.
- **Logstash :** permet l'agrégation des données dans Elasticsearch.
- **Elasticsearch :** le composant principal, qui centralise les informations et y accède via une API RESTful.
- **Kibana :** permet la création de dashboards et la visualisation des données dans ElasticSearch.



La suite ELK, notre solution SIEM
Ici la documentation officielle.

Elastic Stack

User Interface

Store, Index & Analyze

Ingest

Les composants de la stack ELK

- **Remontez vos logs avec Beats**
- Beats est un ensemble d'outils permettant l'envoi de logs. Ces outils devront être installés sur les machines que vous souhaitez monitorer. Ils agiront comme des agents qui collectent les journaux d'événement et logs :
  - Filebeat : ingestion de fichiers de logs.
  - Packetbeat : ingestion de fichiers de capture réseau.
  - Auditbeat : ingestion de fichiers audit.
  - Heartbeat : vérification si un service est disponible ou non.
  - Functionbeat : monitoring des environnements cloud.
  - Journalbeat : ingestion des logs systemd.
  - Metricbeat : collection des métriques de différents systèmes.
  - Winlogbeat : collection de logs Windows.

- Pour installer les différents outils Beat, je vous invite à vous référer à la documentation.

Les composants de la stack ELK

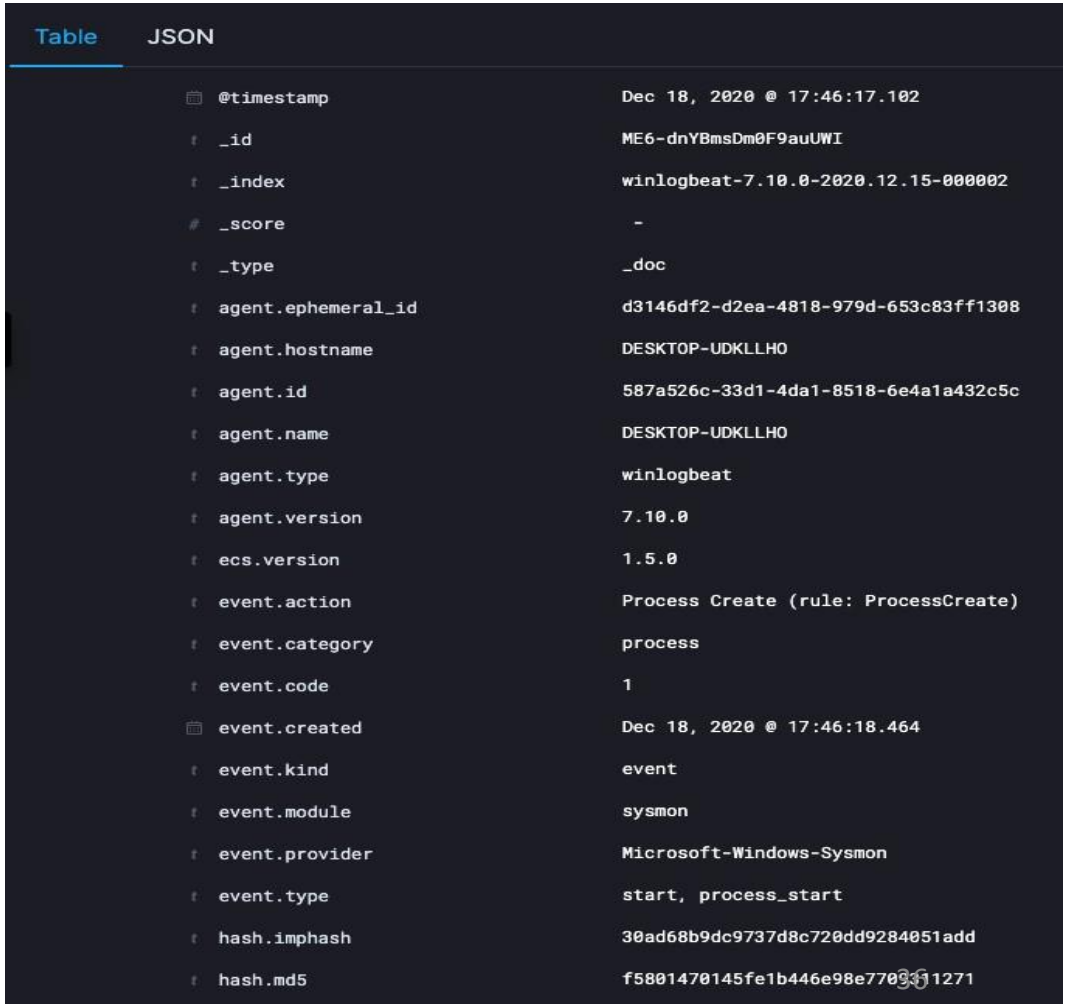
- **Agrégez les données avec Logstash**
- Logstash permet l'agrégation et le formatage de données pour l'envoi dans Elasticsearch. Logstash vous permettra donc d'envoyer différents types de données autres que des logs.
- Pour en savoir plus et installer Logstash, vous pouvez vous référer à la documentation officielle.

Les composants de la stack ELK

- **Centralisez vos données avec Elasticsearch**
  - ElasticSearch est le moteur principal de la stack ELK : c'est lui qui va stocker les données et les rendre accessibles.
  - Il peut être utilisé pour plusieurs objectifs, mais sa fonctionnalité principale est l'indexation de flux de données. Dans notre cas, cette fonctionnalité permet le stockage centralisé des logs, tels que des journaux ou des paquets réseau, par exemple. Il est donc très utile pour notre monitoring de la sécurité.
  - ***Comment Elasticsearch stocke les données remontées ?***
  - Elasticsearch stocke les données au format JSON. Ces données sont contenues dans des index qui sont des bases de données. Je vous conseille de créer un index par type de données ingérées (index1, index2...).

Les composants de la stack ELK

- **Centralisez vos données avec Elasticsearch**
  - ***Et comment sont organisés ces index ?***
  - Les index contiennent des documents dans lesquels les données sont organisées dans des “fields”, c'est-à-dire des champs. Dans le screenshot à droite, nous pouvons voir que les fields sont définis dans la colonne de gauche.
  - Pour récupérer les données, Elasticsearch fonctionne comme une API RESTful.



Les composants de la stack ELK

- **Visualisez vos données avec Kibana**
- Kibana va permettre de visualiser les données d'Elasticsearch en temps réel. Cet outil vous propose des dashboards préconfigurés pour analyser les logs qui vous sont remontés. Il est également possible de visualiser et d'explorer vos données dans la section Discover. Ceci est très utile pour visualiser vos logs et comprendre ce qu'ils contiennent. Cela vous permettra de mettre en place vos règles de SIEM plus facilement.
- Dans le screencast ci-dessous, découvrons cette fonctionnalité et la stack ELK :

En résumé : la suite ELK est composée de 4 outils :

- Beats, installé sur les machines à monitorer pour remonter les logs ;
- Logstash, qui reçoit et agrège les logs dans Elasticsearch ;
- Elasticsearch, le composant principal qui centralise les données ;
- Kibana, où l'on peut visualiser les données.