Lutte Informatique Défensive

SOC, HIDS et SIEM

Georges Bossert - SEKOIA
Frédéric Guihéry - AMOSSYS

23 novembre 2018 - Université Rennes 1

SEKOIA

AMOSSYS
EXPERT IN CYBERSECURITY

Surveillance des événements système

Importance des logs

Pourquoi les logs sont importants ?

Importance des logs

Très utiles dans plusieurs situations

- Détection d'intrusion (recherche de signature)
  - En temps réel
  - Application de nouvelles signatures sur des anciens logs
- Investigation en phase de réponse à incidents
  - Compréhension d'une attaque
  - Qualification de l'impact et de l'étendue
  - Peut servir de preuve
- Analyse de patterns sur le long terme
- Recherche de signaux faibles
- ...

Mécanismes de journalisation intégrés aux OS

Permet de surveiller

- l'activité système/utilisateur
- les tentatives d'authentification
- les ressources accédées par les utilisateurs/processus
- les actions privilégiées réalisées
- …

Mécanismes de journalisation intégrés aux OS

Production de journaux

- Dans des formats hétérogènes
  - Event Logs sous Windows
    - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor
  - ETW (Event Tracing for Windows) sous Windows
  - syslog, sous Unix et de nombreuses applications
  - W3C Extended Log File Format, pour les serveurs web
  - …
- Stockés localement ou centralisés

Sondes hôte

Composant déployé sur

- Postes de travail
- Serveurs
- Certain équipements réseau
- …

Sondes hôte

Capture l'activité système

- Mesure d'intégrité de fichiers/de processus
- Contrôle d'intégrité par rapport à une liste blanche
- Contrôle d'accès à des ressources
- Réalise des actions spécifique (cas des HIDS/HIPS)
- …

Sondes hôte

Fonctionnalités attendues d'un HIDS/HIPS

- Analyse du changement d'état de ressources
- Surveillance des actions sensibles
- Identification de fichiers malveillants par recherche de signatures
- Recherche de fichiers malveillants
- Inspection de journaux
- Remontée de logs à la demande

Sondes hôte

Fonctionnalités liées aux solutions « Endpoint protection »

- Liste blanche d'applications autorisées
- Contrôle d'accès aux ressources
- Durcissement contre l'exploitation de vulnérabilités
- Exécution de binaires « inconnus » dans des sandbox

Sondes hôte

Fonctionnalités liées aux antivirus

- Identification de malwares par signature
- Identification de comportements malveillants
    - Exemple : injection dans un processus, puis ouverture d'une socket en écoute

Sondes hôte

Fonctionnalités liées aux solutions « Endpoint Detection and Response » (EDR)

- Détection des incidents de sécurité.
- Contenir l'incident au niveau du Endpoint (blocage de processus ou de trafic réseau)
- Aide à l'investigation sur les incidents de sécurité (récupération d'artefacts complets…)
- Réponse à incident et capacité à lancer des actions de remédiation

Focus sur quelques fonctionnalités d'une sonde hôte

Analyse des changements d'état

Objectif : identifier les ressources sensibles altérées

- Exemples de ressources à monitorer
  - Contrôle d'intégrité d'un système de fichiers

    /etc/shadow

    /etc/sudoers
  - Surveillance des processus en cours d'exécution

    S'assurer que le processus ntp est toujours actif

Surveillance des actions sensibles

Objectif : identifier les actions ou enchaînements d'actions sensibles

- Exemples d'actions sensibles à surveiller
  - Tentatives d'authentification multiples
  - Ouverture de socket en écoute
  - Opérations en "sudo"
  - Requêtes DNS contenant de grandes quantités de données (risque de canal caché avec exfiltration d'informations sensibles)

Recherche de fichiers malveillants

Objectif : identifier simplement les fichiers potentiellement malveillants

- Sert essentiellement en analyse post-mortem « permanente » (*hunting*)
- Idée : scanner régulièrement le parc du SI à la recherche de traces de compromissions
- En complément d'un antivirus qui, lui, « protégera » le système en temps réel

Exemples d’outils de type sondes hôte

Auditd

Outil d'audit très complet sous Linux

```
$ sudo apt-get install auditd

Modifier fichier de configuration /etc/audit/rules.d/audit.rules

  -w /etc/passwd -p wra -k login_file_access
  -a exit,always  -F arch=b64 -S execve -k audit_execve

$ service auditd restart
$ service auditd status

# Vérifier résultat dans /var/log/audit/audit.log
```

Samhain

- Outil développé par Samhain Labs (allemand)
- Fonctionnalités
  - Contrôle d'intégrité d'un système de fichiers
  - Contrôle sur base d'un politique
    Journalisation/alertes en cas de déviation
- Quelques avantages
  - Protection locale de la base de référence (empreinte du système) et de la politique au travers d'une signature GPG
  - Sécurité du protocole de communication avec le serveur

Nom de la section	Description
[ReadOnly]	Surveille toutes les modifications sur les fichiers • propriétaire • groupe • permissions • type de fichier • numéro de périphérique • liens matériels • liens symboliques • numéro d'inode • somme de contrôle • taille • date de dernière modification (mtime) • date de dernier changement de statut (ctime)
[LogFiles]	Tout est surveillé sauf les dates (atime, ctime et mtime), la taille du fichier et la signature
[GrowingLogFiles]	Équivalent à [LogFiles] excepté que la modification de la taille du fichier est ignorée seulement si la taille a augmenté
[Attributes]	Surveille les changements sur les droits (propriétaire, groupe, permissions), le type de fichier et le numéro de périphérique
[IgnoreAll]	Permet de s'assurer de l'existence d'un fichier mais ignore les modifications sur les métadonnées

Possibilités de configuration

```
[ReadOnly]
dir = 0/

[Attributes]
file = /tmp
file = /dev
file = /media
file = /proc
file = /sys

[ReadOnly]
dir = 99/boot
dir = 99/bin
dir = 99/sbin

[GrowingLogFiles]
dir = 99/var/log

(…)
```

Exemple d’une politique

```
<trail>
[…]
<log sev="RCVT" tstamp="2013-12-12 17:35:25+0100" remote_host="wheezy" >
<log sev="CRIT" tstamp="2013-12-12 17:35:24+0100"  msg="POLICY [ReadOnly] --------T-"
path="/bin/malware.bin" ctime_old="2013-12-12T15:56:25" ctime_new="2013-12-12T16:35:20"
mtime_old="2013-12-12T15:56:25" mtime_new="2013-12-12T16:35:20"  />
<sig>608CB6500D9071907FE2C3212A6CB7520D0AC55C91DC6A7E</sig></log>
[…]
</trail>
```

Exemple de résultat d'un contrôle

OSSEC

- Outil développé par Trend Micro (Japon)
- Fonctionnalités
  - Analyse des journaux de nombreux produits
  - Contrôle d'intégrité de fichiers
  - Contrôle d'intégrité de la base de registres
  - Contrôle distant (de routeurs, pare-feu, switchs, etc.) au travers de connexions SSH
  - Réactions possibles (exécution de commandes)

```
<localfile>
<log_format>apache</log_format>
<location>/var/log/apache/*_error.log</location>
</localfile>
```

```
<rule id="5555" level="3">
<match>: password changed for</match>
<description>User changed password.</description>
</rule>
```

Exemples de configuration

Yara

- Outil développé par Victor Manuel Alvarez (Virus Total)
- Fonctionnalités
  - Recherche de patterns dans des fichiers
  - Richesse en termes d'expressivité des règles
  - Supporte les expressions conditionnelles
  - Compréhension des formats exécutables
  - …
- Récent, mais très utilisé dans le domaine d'analyse de compromission « à froid »
- Intéressant lorsqu'il est intégré aux agents hôte afin de recherche rapidement une signature sur les systèmes de fichiers d'un SI

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

Exemple de règle de détection

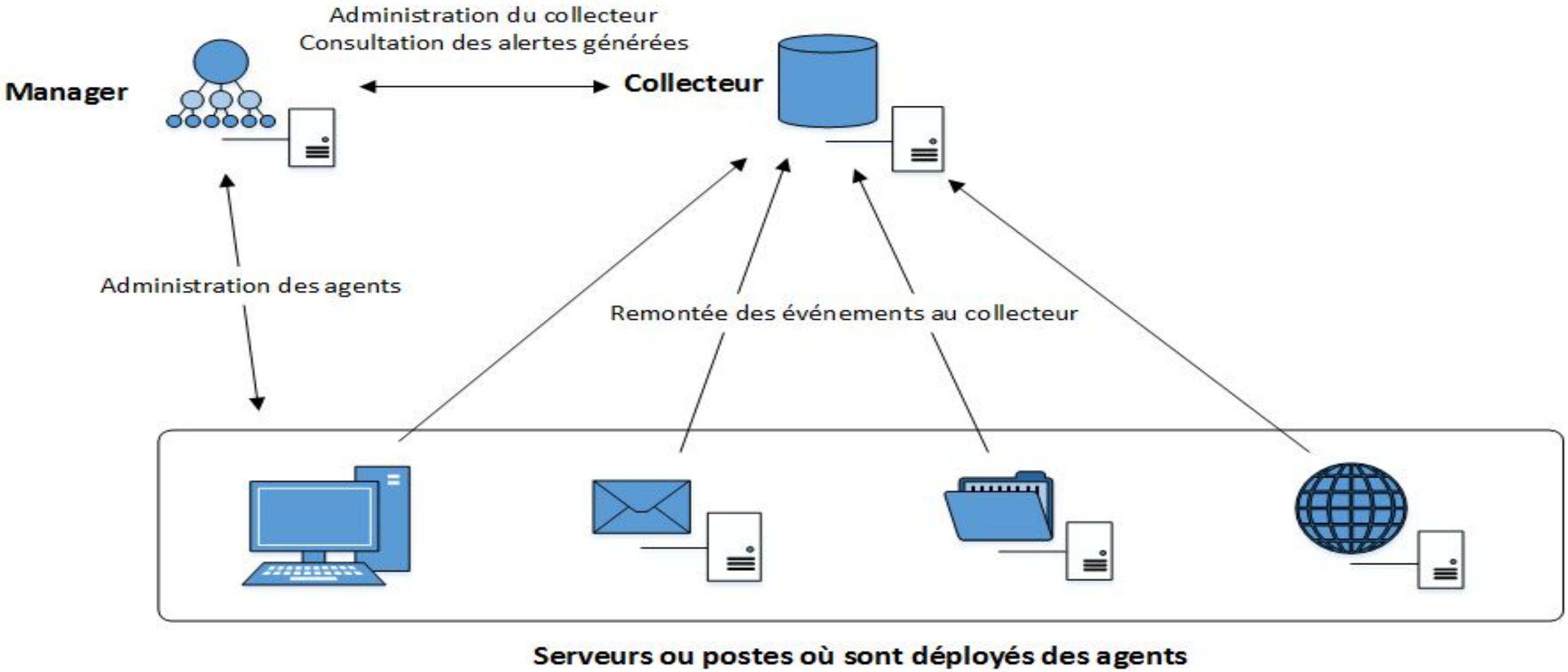
Phase de collecte et d'analyse des événements

Collecte et analyse

Objectif principal : identifier les incidents de sécurité et produire des notifications

- Rôle joué par un SIEM (Security Information Management System)
- Composant central en charge de la capture des logs et de leur analyse

2nd objectif d'un SIEM : assister l'équipe pour la mise en œuvre de contre-mesures automatique, manuelle et organisationnelles



Architecture Manager-Collecteurs

Le SIEM

Quelles fonctionnalités sont attendues dans un SIEM ?

Fonctionnalités attendues

Gestion des agents

- Déploiement des agents sur les systèmes cibles
- Canal de contrôle des agents
- Mise à jour des agents
- Déploiement de configuration/modules

Fonctionnalités attendues

Gestion des événements

- Collecte des événements
- Normalisation des événements
- Filtrage des événements
- Agrégation des événements
- Enrichissement des événements

Fonctionnalités attendues

Gestion des incidents

- Corrélation des événements en incidents
- Enrichissement des incidents
- Vérification des incidents
- Analyse des incidents

Fonctionnalités attendues

Réactions aux incidents

- Reporting et visualisation des incidents
- Notification
- Réalisation d'actions suite à un incident
- Archivage et journalisation

Les points importants de chaque étape

Collecte des événements

- Plusieurs modes
  - Remontée passive (mode push) : communication initiée par les agents
  - Remontée active (mode pull) : communication à l'initiative du collecteur
- Plusieurs formats à prendre à en charge en entrée (syslog, snmp, NetFlow, CEE, IDMEF, etc.)
- Attention à la sécurisation du canal de communication de collecte
  - Authentification par certificat
  - Politique de déploiement/gestion des certificats

Types d'événements collectés

- Evénements de sécurité
  - Alerte d'un NIDS/NIPS
  - Alerte d'un HIDS/HIPS
  - Comportement suspect au niveau du pare-feu
  - Comportement suspect au niveau d'un antivirus réseau/hôte
  - Comportement suspect au niveau d'un reverse proxy intégrant un WAF (Web Application Firewall)
  - …

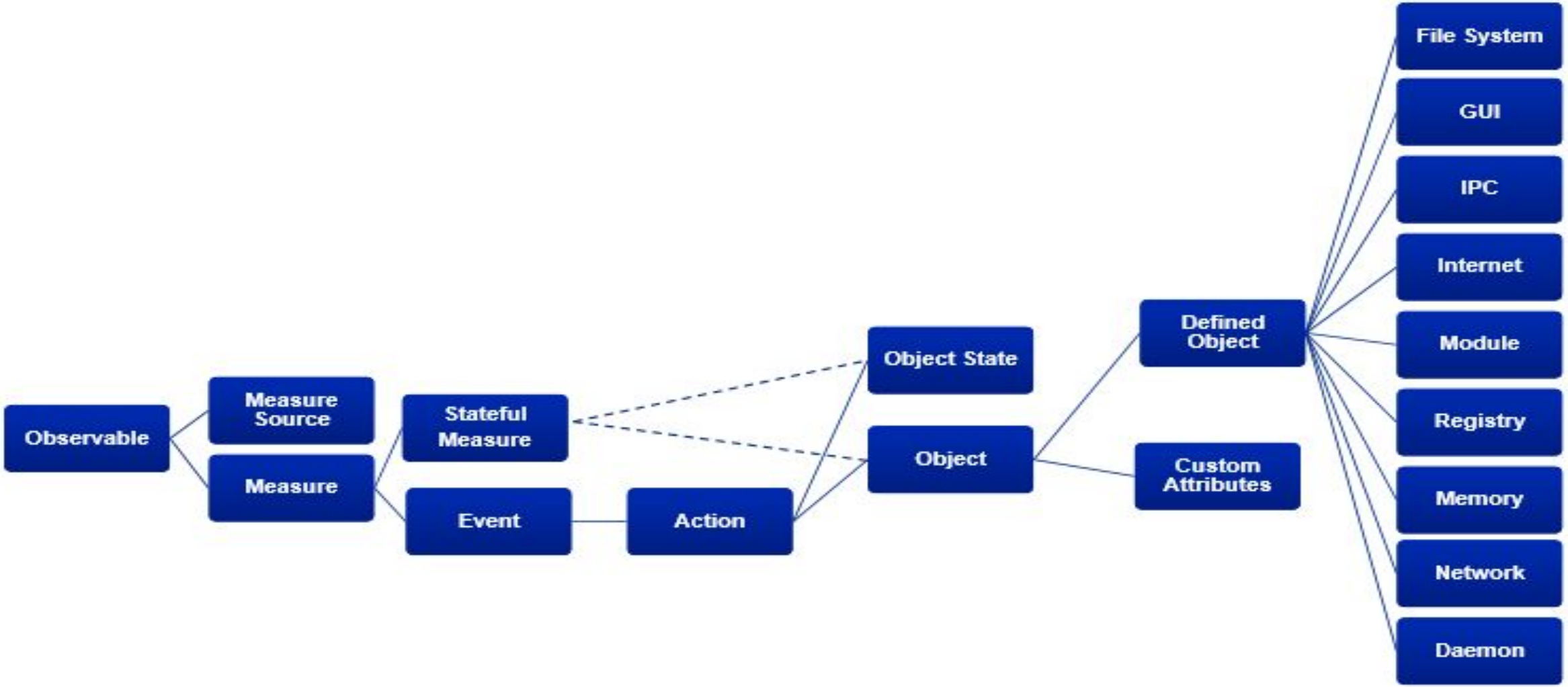
Types d'événements collectés

- Evénements « système » remontés par les sondes hôte
  - Entrées sur le système de fichiers
  - Clés/valeurs d'une base de registre
  - Empreinte mémoire d'un processus
  - En cas de suspicion de compromission sur certains postes
  - Liste des ports ouverts
  - Liste des connexions réseau ouvertes
  - Liste des processus en cours d'exécution
  - Liste des utilisateurs déclarés/connectés
  - IPC ouvertes entre les processus
  - Privilèges/tokens associés aux processus…

Collecte des événements

Standard CybOX

- Cyber Observable eXpression (CybOX)
- Langage permettant d'exprimer des événements ou états sur des objets/ressources



Standard CybOX

- Account
- Disk
- Disk Partition
- DNS Cache
- Email Message
- File
- GUI
- Library
- Package
- Memory
- Network Connection
- Network Route
- Linux Package
- Product
- Service
- Socket
- System
- User Session
- Volume
- Win Critical Section
- Win Driver
- Win Event
- Win Event Log
- Win Kernel
- Win Kernel Hook
- Win Handle
- Win Mailslot
- Win Mutex
- Win Named Pipe
- Win Network Route
- Win Prefetch
- Win Registry
- Win Semaphore
- Win System Restore
- Win Task
- Win Thread
- Win Waitable Timer
- X509 Certificate

...

(more on the way)

Standard CybOX

Normalisation des événements

Objectif : transformer les différents événements remontés par les sondes dans un format pivot

- Principe
  - Compréhension de plusieurs formats en entrée (syslog, Windows Event Log, etc.)
  - Production des événements dans un format pivot
    - Souvent propriétaire au produit

Normalisation des événements

Processus de standardisation des journaux

- syslog : standard de fait
  - Entête formalisé avec options
  - Code de catégorie/origine (kernel, user, etc.)
  - Code de gravité (error, warning, debug, etc.)
  - Puis message non structuré (!)

```
Sep 14 14:09:09 stationXYZ dhcp service[warning] 110 content of message
```

Normalisation des événements

Processus de standardisation des journaux

- Volonté d'harmoniser les mécanismes de journalisation tout en structurant les données
- Résultat : CEE – Common Event Expression

Normalisation des événements

Common Event Expression (CEE)

- Open Event Expression Language (OEEL)
  - Parsing et normalisation des données
- Common Event Rule Expression (CERE)
  - Règles pour la recherche de patterns, le filtrage et la corrélation des données
- Common Event Scoring System (CESS)
  - Système de scoring des événements suivant différents facteurs
- ...

Normalisation des événements

- Exemple d'implémentation de CEE : **lumberjack**
  - Projet soutenu par les auteurs de systemd/journald, rsyslog et Syslog-ng
  - Exemple d'événement structuré (en JSON)

```
"p:Event": [
  {
    "p:time": "2001-12-31T12:00:00",
    "p:op": "login",
    "p:uid": "500",
    "p:proc": "/sbin/unix_chkpwd",
    "p:tty": "pts/0",
    "p:srchost": "example.com",
    "p:username": "keith",
    "p:results": "success"
  }
]
```

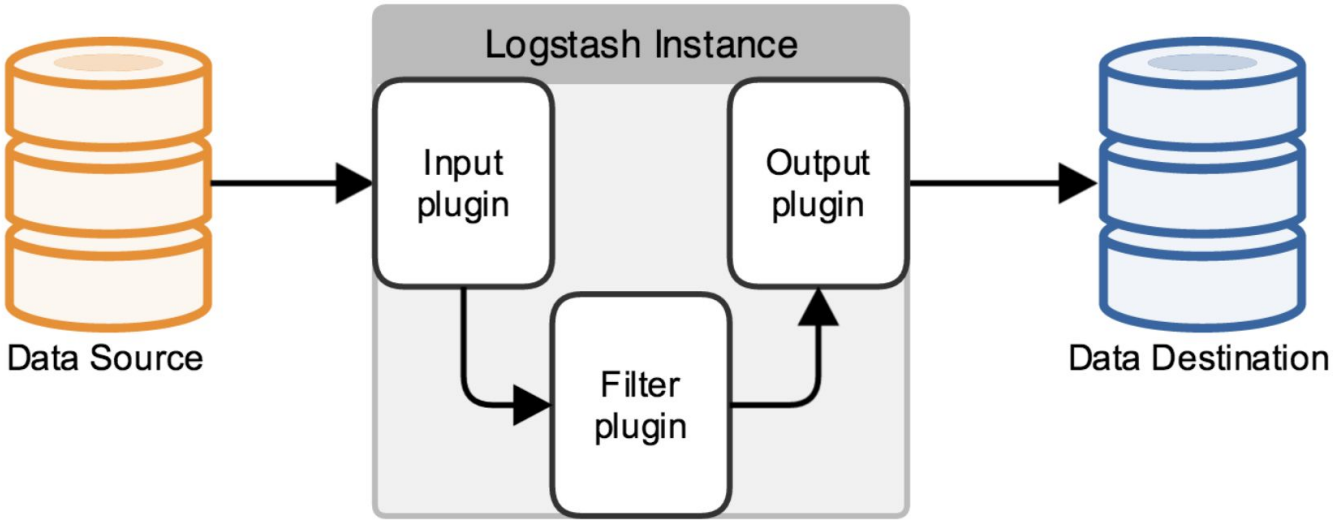
Filtrage des événements

Objectif : limiter la quantité de données à traiter

- Deux mode
  - Filtrage sur l'agent
  - Filtrage sur le collecteur
- Principes
  - Filtrage sur les types d'événement
  - Filtrage par pattern
  - Filtrage par cible attaquée (réseau hors périmètre)
  - Filtrage par impact / priorité

Exemple de collecte/normalisation/filtrage

- Combinaison d'outils
  - auditd pour la production des logs
  - logstash pour la récupération, la normalisation (moteur *grok*) et le filtrage
  - elasticsearch pour l'indexation des logs et la recherche
  - kibana pour le rendu visuel, l'analyse



Agrégation des événements

Objectif : associer des événements initialement distincts dans un méta-événement

- Eviter la redondance d'information
- Supprimer les événements dupliqués
- Agréger des événements unitaires proches
  - Scan de port 1..1024 puis 1025…2048 depuis la même source

Enrichissement des événements

Objectif : réduire les faux positifs et assister l'analyse/l'expert pour la corrélation

- Principe : ajouter de la sémantique et du contexte aux données initiales des événements et incidents
- Utilisation de plusieurs bases
  - Base des biens / inventaire du SI
  - Base des vulnérabilités

Enrichissement des événements

Base des biens / inventaire du SI

- Contenu
  - Topologie réseau
  - Machines en place
  - Logiciels installés et versions
  - Configurations
- Plusieurs approches de construction
  - Inventaire manuel du SI
  - Inventaire automatique avec agent
  - Inventaire automatique sans agent, par des moyens de fingerprinting actif/passif

Enrichissement des événements

Base des biens / inventaire du SI

- Importance de l'utilisation de standards pour l'interopérabilité entre solutions d'éditeurs
- CPE : Common Platform Enumeration
  - Standard formalisant les désignations de machine et services et de leurs versions
- CCE : Common Configuration Enumeration
  - Standard formalisant la gestion de configuration d'un SI

Enrichissement des événements

Base des biens / inventaire du SI

- Exemples de désignations CPE

```
cpe:/a:zonelabs:zonealarm_internet_security_suite:7.0
cpe:/o:redhat:enterprise_linux:4:update5:ws
cpe:/h:intel
cpe:/a:jon_smith:tool_name:1.2.3
cpe:/a:adobe:reader
```

Enrichissement des événements

Base des biens / inventaire du SI

- Exemple de désignation CCE

D:CCE-3121-1

Description: The "restrict guest access to application log" policy should be set correctly.

Technical: (1)HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Application\RestrictGuestAccess

Mechanisms: (2) defined by Group Policy

Parameter: enabled/disabled

Enrichissement des événements

Base des vulnérabilités

- Recensement
  - Vulnérabilités déjà identifiées (avec un scanner par exemple)
  - Vulnérabilités théoriquement présentes sur les systèmes en place du fait de leur configuration

Enrichissement des événements

Base des vulnérabilités

- Standard
  - CVE : Common Vulnerabilities and Exposures
  - Couplé avec CPE, permet de lister les vulnérabilités présentes sur des plateformes

Corrélation des événements

Objectif : analyser les événements et méta-événements pour identifier des incidents de sécurité

- Principes
  - Utilisation d'une base de comportements malveillants
  - Création et utilisation de scripts de vérification et d'analyse

```
<IDMEF-Message version="1.0">
  <Alert ident="abc123456789">
    <Analyzer analyzerid="hq-dmz-analyzer62">
      <Node category="dns">
        <location>Headquarters Web Server</location>
        <name>analyzer62.bigcompany.com</name>
      </Node>
    </Analyzer>
    <CreateTime ...</CreateTime>
    <Source ident="abc01">
      <Node ident="abc01-01">
        <Address ident="abc01-02" category="ipv4-addr">
          <address>222.121.111.112</address>
        </Address>
      </Node>
    </Source>
    <Target ident="def01">
      <Node ident="def01-01" category="dns">
        <name>www.bigcompany.com</name>
        <Address ident="def01-02" category="ipv4-addr">
          <address>123.234.231.121</address>
        </Address>
      </Node>
      <Service ident="def01-03">
        <portlist>5-25,37,42,43,53,69-119,123-514</portlist>
      </Service>
    </Target>
    <Classification origin="vendor-specific">
      <name>portscan</name>
      <url>http://www.vendor.com/portscan</url>
    </Classification>
  </Alert>
</IDMEF-Message>
```

Standard : IDMEF (RFC 4765) – Intrusion Detection Message Exchange Format

Corrélation des événements

Standards IDMEF/IODED

- **IDMEF** : utilisé juste après la collecte, il permet aux informations normalisées en événements de sécurité d'être agrégées, corrélées, stockées en base de données et affichées

- **IODEF** : plus complet que le format IDMEF, il est utilisé après l'étape de corrélation pour structurer les données en vue d'un reporting et d'un traitement par un système de réponse

Vérification des incidents

Objectif : s'assurer que le système attaqué est véritablement vulnérable

- Deux grands approches
  - Comparer une tentative d'intrusion (alerte de l'IDS) par rapport à la configuration CPE de la cible
  - Vérifier si les conséquences de l'attaque sont observables sur le système

Vérification des incidents

Vérification des conséquences de l'attaque

- Exemples
  - Changement de privilège d'un processus
  - Fichiers suspects sur la cible
  - Nouveau port en écoute
  - Présence d'une ligne particulière dans un fichier de log
  - …

Vérification des incidents

Vérification des conséquences de l'attaque

- Approche possible :
  - Recherche d'indicateurs de compromission (IOC) ciblés par rapport à l'incident (cible visée et surface attaquée)

Vérification des incidents

Vérification des conséquences de l'attaque

- Standards
  - OpenIOC (Mandiant)
  - CybOX (MITRE) : Cyber Observable eXpression
  - MAEC (MITRE) : Malware Attribute Enumeration and Characterization

Vérification des incidents

Exemple de définition OpenIOC pour l'identification du malware Zeus sur un système

```
<ioc id="…" last-modified="2011-10-28T19:28:20">
  <short_description>Zeus</short_description>
  <description>Finds Zeus variants, twexts, sdra64, ntos</description>
  <keywords/>
  <authored_by>Mandiant</authored_by>
  <definition>
    <Indicator operator="OR" id="…">
      <Indicator operator="AND" id="…">
        <IndicatorItem id="…" condition="contains">
          <Context document="ProcessItem" search="ProcessItem/name" type="mir"/>
          <Content type="string">winlogon.exe</Content>
        </IndicatorItem>
        <IndicatorItem id="…" condition="contains">
          <Context document="ProcessItem" search="ProcessItem/HandleList/Handle/Type" type="mir"/>
          <Content type="string">File</Content>
        </IndicatorItem><Indicator operator="OR" id="…">
        <IndicatorItem id="…" condition="contains">
          <Context document="ProcessItem" search="ProcessItem/HandleList/Handle/Name" type="mir"/>
          <Content type="string">system32\sdra64.exe</Content>
```

Vérification des incidents

Vérification des conséquences de l'attaque

- Difficultés
  - Les conséquences d'une attaque sont souvent liées au mécanisme d'exploitation de la vulnérabilité, plutôt qu'à la vulnérabilité en elle-même
  - Ce qui étend l'espace de recherche

Analyse des incidents

Objectif : évaluer l'impact des intrusions détectées sur le système et sur les biens

- Fonctionnalités
  - Identification des services métier impactés par une attaque
  - Priorisation des incidents en fonction de leur impact
  - Vérification de l'intégrité du composant ciblé

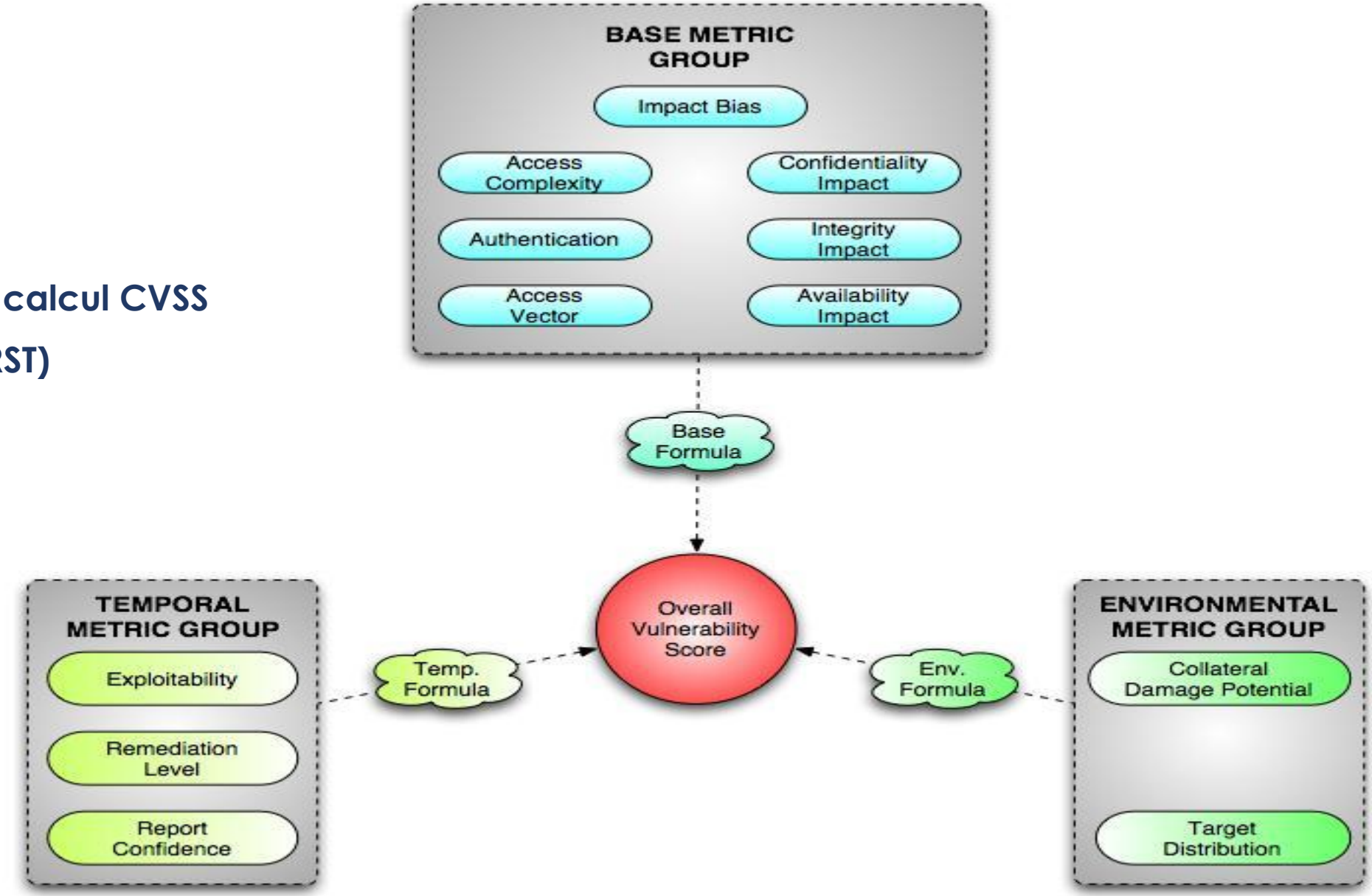
Analyse des incidents

Standard CVSS

- Common Vulnerability Scoring System
  - Permet de qualifier / pondérer l'impact d'une vulnérabilité
    - Type d'impact : DoS, RCE, élévation de privilèges, etc.
    - Vecteur : Distant sans authentification, local, accès physique, etc.
    - ...

Critères de calcul CVSS

(source: FIRST)



Reporting et visualisation des incidents

Principes

- Assister l'équipe opérationnelle du SoC
- Utilisation de tableaux de bord paramétrés
- Suivi des incidents
  - Suivi quantitatif et géographique
  - Priorisation
  - Analyse d'impact
  - Traitements/remédiation

Exemples de SIEM

LogRythm

- Outil développé par LogRythm Inc. (USA)
- Fonctionnalités
  - Moteur de corrélation capable de détecter une attaque réussie d'un échec
  - Capacités de remédiation suite à une alerte
  - Capacités d'enrichissement passif des événements

AlienVault USM

- Outil développé par AlienVault (USA)
- Fonctionnalités
  - Mode passif de collecte
  - Événements collectés normalisés dans un format unique et placés dans la base de données selon une taxonomie propriétaire
  - Filtrage réalisé à la source par les agents ou sur le manager

AlienVault USM

- Autres fonctionnalités
  - Plugins permettent d'enrichir les alertes avec des informations telles que
    - les ports ouverts
    - les vulnérabilités éventuelles
    - les modifications du système
    - les intrusions
  - Livré avec plus de 2.500 règles permettant la détection d'attaques élémentaires
  - Catégorise les tentatives d'intrusion selon le risque encouru
  - Capacité de déterminer quel en a été l'impact (déni de service, modification non-autorisée, etc.)

Splunk

- Outil développé par Splunk (USA)
- Fonctionnalités
  - Mode passif de collecte
  - Événements collectés normalisés dans un format unique et placés dans la base de données selon une taxonomie propriétaire
  - Filtrage réalisé à la source par les agents ou sur le manager
  - Capacités d'enrichissement par rapport à une base de biens
  - Capacités de réaction (scripts bash/Python)

SELKS

- Plateforme développée par Stamus Network
- Combinaison de
  - Suricata : sonde NIDS/NIPS
  - Elasticsearch : moteur d'indexation de données
  - Logstash : outil de parsing et transformation de logs
  - Kibana : interface web pour la visualisation de tableaux de bord
  - Scirius : interface web de gestion des signatures Suricata
  - EVE : gestion des alertes