CEI : Analyse des protocoles standards d'échange pour la détection d'intrusion

ISSANCHOU DAMIEN – RICTER DIANE

PRÉSENTATION DU 21-12-2018

CentraleSupélec

La force de l'innovation

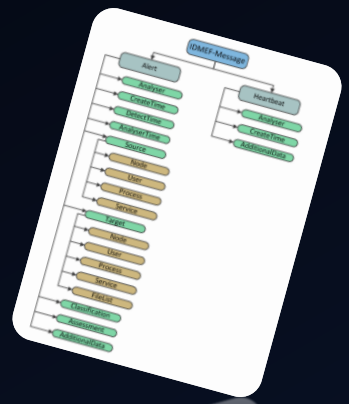
Plan

1. Sujet du CEI
   1. Contexte : Prelude et IDMEF
   2. But du CEI
   3. Référence: IDXP
2. Définition du besoin
3. Choix du protocole
   1. Liste des protocoles
   2. Comparaison de protocoles
   3. Critères de sélection
4. La suite du CEI
   1. Nos 1ères impressions
   2. Décision et Implémentations

1. Sujet du CEI

1. Contexte : Prelude et IDMEF
2. But du CEI
3. Référence: IDXP

1. Contexte : Prelude et IDMEF



- Prelude est un SIEM français développé par CS.
  - Solution de supervision de sécurité
  - Alerte en temps réel des tentatives d'intrusion et des menaces
  - Plusieurs fonctions d'investigation et de *reporting*
  - « Prelude SIEM fournit donc une vision globale du niveau de sécurité des systèmes afin de prévenir les attaques, les intrusions et autres infections virales. »

- IDMEF est un modèle de données pour représenter les alertes de sécurité
  - Implémenté dans Prelude
  - Décrit par la RFC 4765
  - Utilisé en BE

1. Contexte : Prelude et IDMEF

- ✓ IDMEF est repris par le projet SECEF pour:
  - Créer une version 2
  - Normaliser cette version
  - L'implémenter

- ✓ A ce stade nous avons donc un format d'alerte !

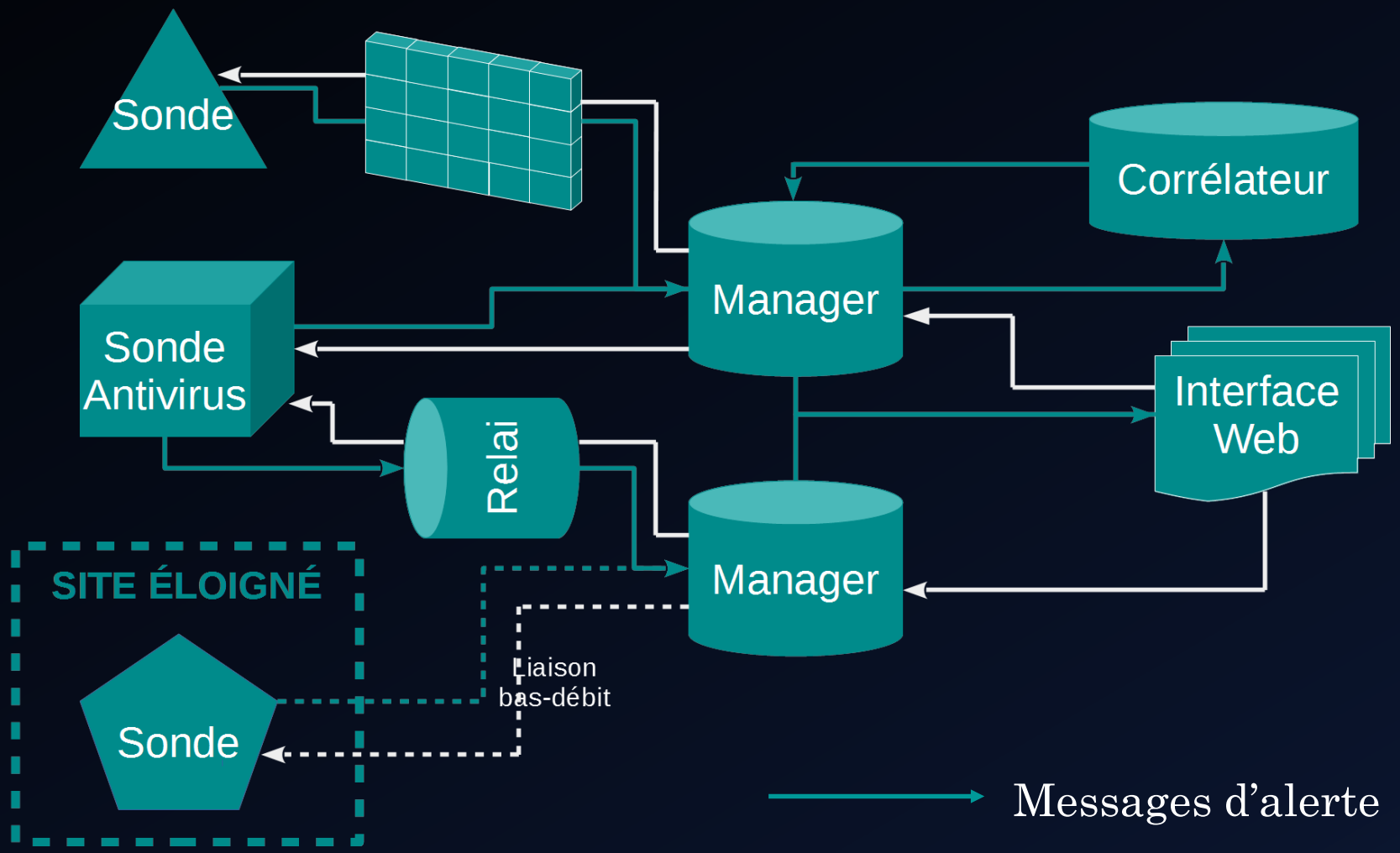
- Mais **comment effectuer le transport** de ce format d'alerte entre les différents modules d'une architecture de détection d'intrusion ?

2. But du CEI

- Trouver parmi les **protocoles de transport existants**, un moyen pour effectuer **les échanges de messages IDMEF** en premier lieu et des **messages d'administration** des sondes dans un second temps.

  - ✓ Spécification du besoin
  - Etude des alternatives possibles
  - Prototypage d'une ou deux solutions

2. But du CEI


Sonde
Corrélateur
Manager
Sonde
Antivirus
Interface
Web
Relai
Manager
SITE ÉLOIGNÉ
Liaison
bas-débit
Sonde
Messages d'alerte
Message d'administration

3. Référence: IDXP

- IDXP est un **protocole de transport** pour l'échange des messages **IDMEF.**
  - Décrit par la RFC 4767

- Problèmes :
  - Basé sur un framework nommé BEEP décrit par la RFC 3080
  - BEEP n'a été que peu utilisé en pratique
  - **IDXP n'a jamais été implémenté**

- L'étude de ce protocole nous permet cependant de **définir les prérequis** recherchés

2. Définition du besoin

2. Définition du besoin

- Obligatoirement :
  - Protocole existant et public
  - Communication non limitée à sonde -> SIEM
  - Indépendant du format de données transportées (non spécifique à IDMEF)
  - Implémentation(s) portable(s)
  - Performance : plusieurs milliers d'objets par seconde

- Recommandé :
  - Implémentation(s) libre(s)
  - Utilisation comme un bus applicatif (abonnement, lecture, écriture,..)
  - Ouverture possible vers les IOTs/les mobiles

3. Choix du Protocole

1. Liste des protocoles
2. Comparaison de protocoles
3. Critères de sélection

1. Liste des Protocoles

- BEEP/IDXP
  - Référence
  - Transport des messages IDMEF
- AMQP (*Advanced Message Queuing Protocol*)
  - Protocole d'échange entre systèmes de messagerie en point par point et en diffusion/abonnement
  - Transport de messages binaires et textuels
  - Exemple d'utilisation : ApacheQPid, Rocksteady par Google
- Apache Kafka (Protocole + Implémentation)
  - OVNI : pour des systèmes de messagerie, de stockage redondant et de transport de flux
  - Transport de messages textuels et binaires
- Syslog
  - Pour les systèmes Unix
  - Transport de messages de journalisation
  - Exemple d'utilisation : syslog sous Linux

1. Liste des Protocoles

- MQTT (*Message Queuing Telemetry Transport*)
  - Pour les systèmes de messageries par diffusion/abonnement orienté IOTs
  - Transport de messages textuels ou binaires
  - Exemple d'utilisation : Facebook Messenger

- WBEM *(Web-Based Enterprise Management*) / WMI (*Windows Management Instrumentation*)
  - Pour les système de gestion interne Windows
  - Transport de messages de gestion (paramétrage et log)
  - Exemple d'utilisation : outils de diagnostic de Windows

- TAXII (*Trusted Automated eXchange of Indicator Information*)
  - Pour les systèmes de veille en temps réel
  - Transport de CTI (cyber threat intelligence) au format textuel
  - Exemple d'utilisation : Eset fournit de la threat intel via TAXII

2. Comparaison de Protocoles

- Tableau de comparaison des protocoles : ici

3. Critères de sélection

- Licence / portabilité
- Activité du projet / renommée du standard
- Disponibilité et Tolérance
- Intégrité
- Authentification
- Performance

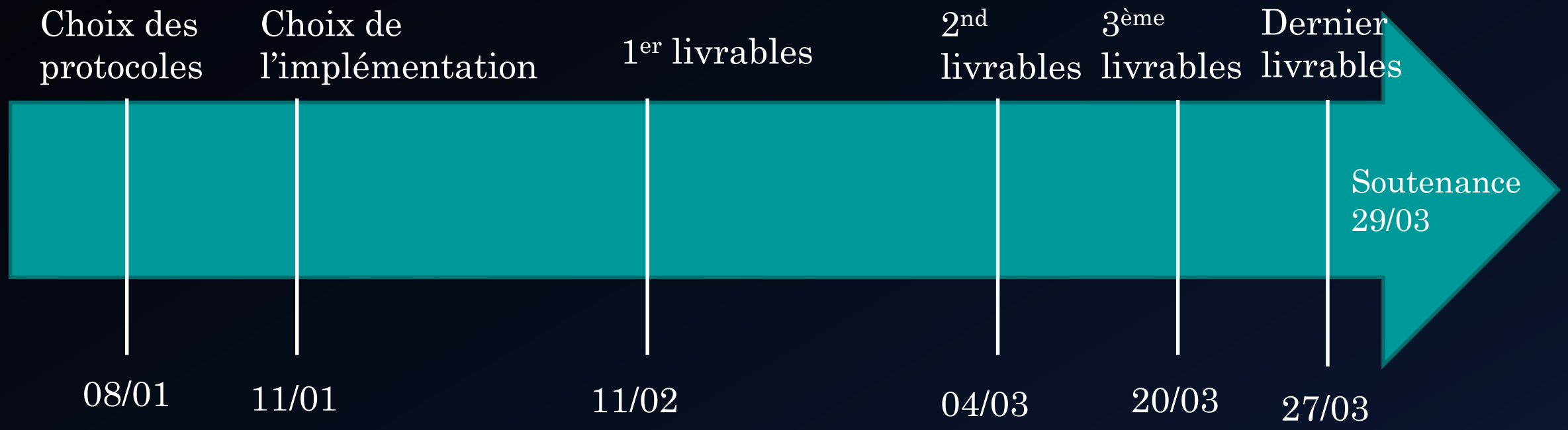
4. La suite du CEI

1. Nos 1ères impressions
2. Décision et Implémentations

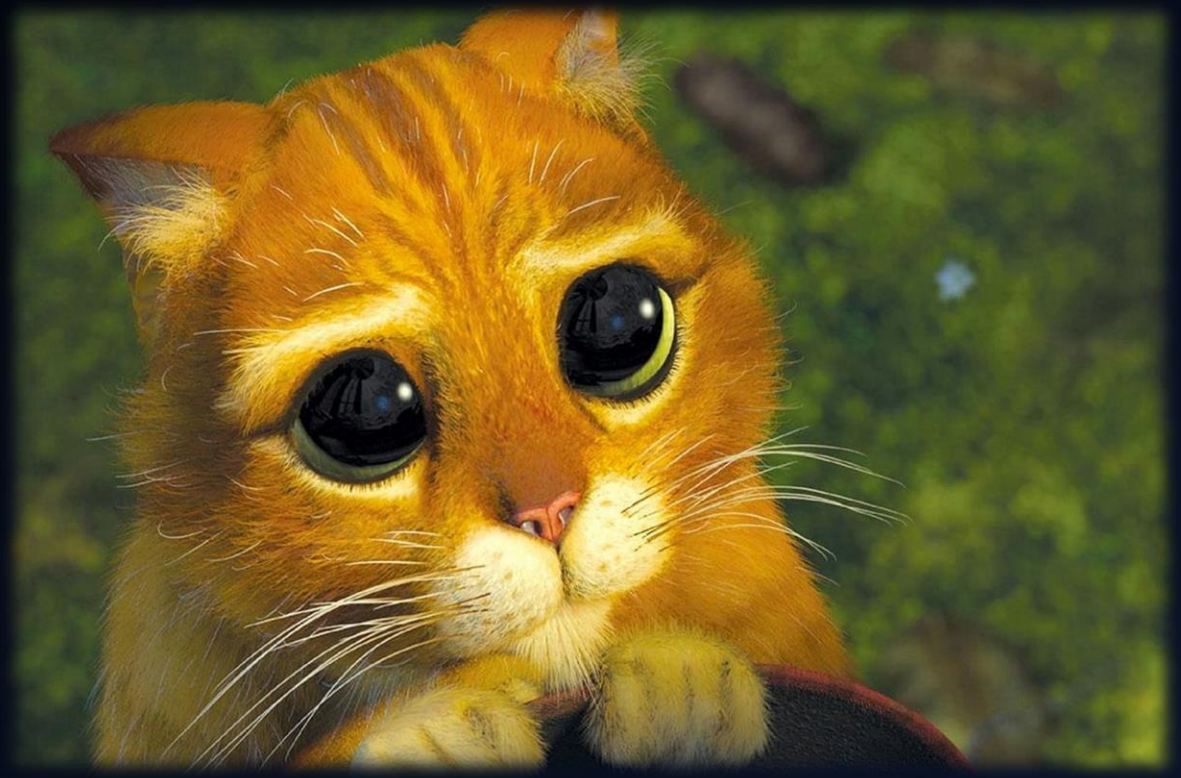
1. Nos premières impressions

- Protocoles éliminés :
  - × IDXP : inactif
  - × WMI : données = ressources Windows, trop spécifique
- Protocoles possibles :
  - ✓ MQTT
  - ✓ Apache Kafka
- Protocole à creuser :
  - AMQP
  - TAXII : pas assez d'information dans la doc
  - Syslog

2. Reste à faire



Avez-vous des questions ?



Merci de votre attention