Retour d'expérience et perspectives pour la simulation de SI et le test de produits de LID

Journée « Défis technologiques de la cybersécurité : Evaluation des solutions du supervision de la sécurité »

Frédéric Guihéry – Responsable des activités R&D

31 janvier 2017

AMOSSYS en bref

Audit

- Audits de conformité
- Audits techniques
- Tests d'intrusion
- PASSI – LPM qualifié par l'ANSSI

Recherche & Développement

- Etudes en Cybersécurité
- Preuves de concepts
- Thèses, Conférences

Conseil

- Gestion des risques SSI
- Confiance numérique
- Sécurité des SI industriels

Logiciels Innovants sur-mesure

- Logiciels ad-hoc de sécurité défensive et offensive
- Outillage des laboratoires d'AMOSSYS

CERT

- Investigation numérique
- Analyse de malwares
- Remédiation de systèmes

Evaluation

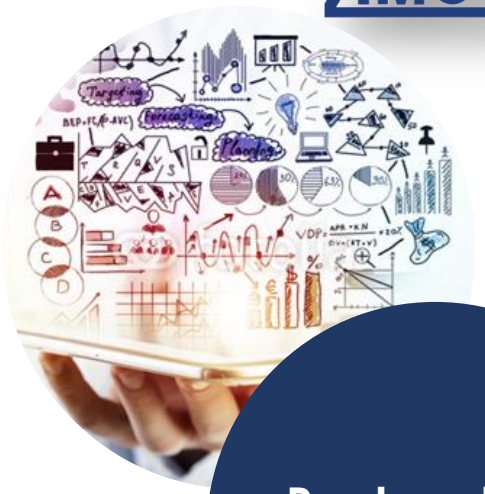
- CESTI agréé ANSSI et accrédité COFRAC
- CSPN et Critères Communs
- Agrément cryptographie
- Agrément évaluation logicielle d'API (systèmes industriels)
- Agrément dans le domaine équipements matériels avec boîtiers sécurisés

www.amossys.fr

Laboratoire d'études et de R&D

Domaines d'expertise

- LID (prévention, détection, réaction à incidents, supervision, …)
- Informatique de confiance et durcissement système
- Sécurité des systèmes industriels (ICS/Scada, Smart Grids, …)
- Sécurité mobile/embarqué (Android, IoT, compteurs, etc.)
- Rétro-ingénierie de protocoles, logiciels et systèmes
- Analyse de vulnérabilités



Recherche & Développement

www.amossys.fr

Laboratoire d'évaluation

Le CESTI Amossys

Evaluation

✓ **Evaluation par la méthodologie CSPN**

Permet d'obtenir un certain niveau de confiance d'un produit de sécurité.

✓ **Evaluation par la méthodologie Critères Communs**

Certification qui permet de s'assurer de la conformité et de la robustesse d'un produit au regard d'un cahier des charges ou de spécifications techniques. Cette méthodologie bénéficie d'une reconnaissance internationale.

Le + Amossys

- ✓ Agrément Cryptographie.
- ✓ Agrément évaluation logicielle d'API (systèmes Industriels).
- ✓ Agrément dans le domaine des équipements matériels avec boîtiers sécurisés.

Nos travaux dans le domaine de la LID

Nos travaux en Lutte Informatique Défensive

Plusieurs axes de R&D et de prestations

- AMOSSYS **évalue les PDIS** (Prestataires de Détection des Incidents de Sécurité), en partenariat avec le LNE, pour l'ANSSI
- Études, conception et développement relatif aux **sondes réseau et hôtes**
- **Méthodologies d'évaluation** de produits de LID
- **Retour d'expérience** d'évaluation de sécurité d'un ensemble important de produits de LID
- **Formations** dispensées dans le domaine de la LID (détection d'intrusion, réaction à intrusion, analyses post-mortem)
- Réalisation d'une **plateforme** pour l'évaluation de produits de LID
- Études sur l'élaboration de **stratégies de détection**

Nos travaux en Lutte Informatique Défensive

Partenaires et clients

- **DGA MI**
  - R&D en LID et analyse de produits de LID
- **ANSSI**
  - Evaluation de produits de LID selon les schémas CSPN et CC
  - Evaluation de conformité des prestataires PDIS
- **Thales**
  - Travaux de R&D relatifs aux sondes
- **LNE**
  - Evaluation de conformité des prestataires PDIS
- **Supélec**
  - Co-encadrement d'une thèse CIFRE relative aux méthodologies d'évaluation de NIDS
  - Travaux de R&D en LID
- **INRIA / IRISA**
  - Co-encadrement d'une thèse CIFRE relative à la détection des cyberattaques par l'utilisation des méthodes d'apprentissage automatique

Nos travaux en Lutte Informatique Défensive

Catégories d'équipements évalués

- **Sondes**
  - Sondes / Capteurs spécifiques **système**
  - Sondes / Capteurs spécifiques **réseau**
  - Sondes / Capteurs **intégrés à des composants fonctionnels**
  - Sondes / Capteurs **intégrés à des composants de sécurité**
- **SIEM** (collecte, agrégation, corrélation, vérification, etc.)
- **Console** de visualisation
- **Scanners** de vulnérabilités
- **Outils d'administration de la sécurité réseau**

Nos travaux en Lutte Informatique Défensive

Thèse en cours

- Thèse sur la **détection d'attaques par l'utilisation des méthodes d'apprentissage automatique**
  - Réalisée par Alban Siffer
  - Encadrement Amossys / IRISA (équipes EMSEC / DREAM)

Retour d’expérience et perspectives en évaluation de produits de LID

Evaluation en LID : Retour d'expérience et perspectives

CSPN : un socle pour l'évaluation des produits de LID

- **Le schéma CSPN**
  - Analyse de conformité
  - Analyse de robustesse
  - Analyse de vulnérabilité
  - (Analyse d'impact)

  - Evaluation en temps contraint

Evaluation en LID : Retour d'expérience et perspectives

CSPN : un socle pour l'évaluation des produits de LID

- D'une part : **analyse des fonctions de sécurité**

Evaluation en LID : Retour d'expérience et perspectives

CSPN : un socle pour l'évaluation des produits de LID

- D'une part : **analyse des fonctions de sécurité**
  - Authentification et gestion des privilèges
  - Protection des communications
  - Protection du mécanisme de mise à jour
  - Journalisation des événements
  - Intégrité du logiciel et de sa configuration
  - Protection des signatures
  - …

Evaluation en LID : Retour d'expérience et perspectives

CSPN : un socle pour l'évaluation des produits de LID

- Et d'autre part : **analyse des fonctions métier**

Evaluation en LID : Retour d'expérience et perspectives

CSPN : un socle pour l'évaluation des produits de LID

- Et d'autre part : **analyse des fonctions métier**
  - **NIDS**
    - Décodage protocolaire
    - Détection d'anomalies
    - Analyse des flux
    - Gestion de la base des signatures
    - Détection d'intrusions
    - …

Evaluation en LID : Retour d'expérience et perspectives

CSPN : un socle pour l'évaluation des produits de LID

- Et d'autre part : **analyse des fonctions métier**
  - **SIEM**
    - **Collecte** des événements
    - **Normalisation** des événements et incidents
    - **Filtrage** des événements et incidents
    - **Enrichissement** des événements et incidents
    - **Agrégation** des événements et incidents
    - **Gestion de la base des signatures**
    - **Corrélation** d'événements
    - **Vérification** des incidents potentiels
    - **Visualisation** et Dashboard
    - **Ticketing** et **Reporting**
    - …

Evaluation en LID : Retour d'expérience et perspectives

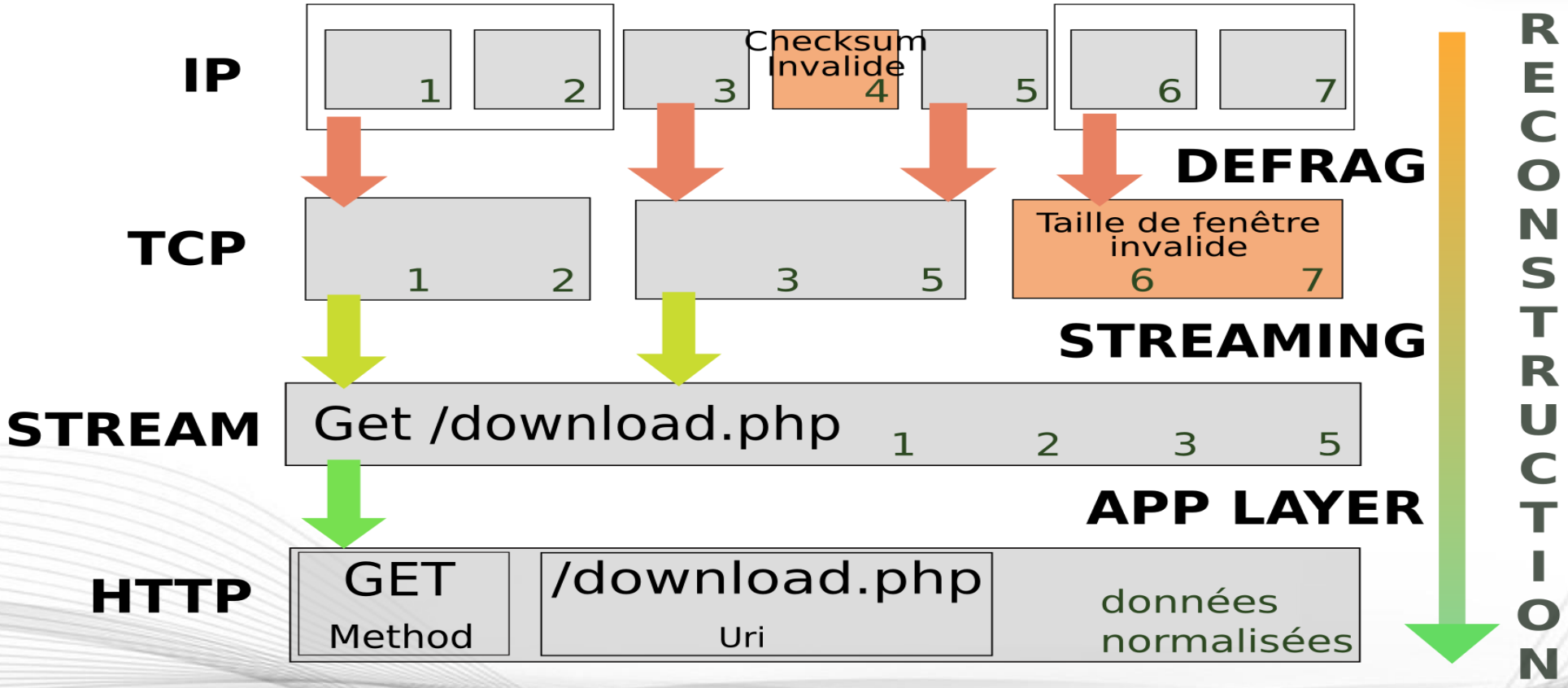
CSPN : un socle pour l'évaluation des produits de LID

- Actuellement, l'évaluation d'un produit de LID selon le schéma CSPN consiste principalement à
  - Etudier la conformité des fonctions métier et des fonctions de sécurité
  - Analyser la robustesse des fonctions métier

  - **L'efficacité des fonctions métier reste assez peu explorée**
    - Seule exception : analyse de la résistance à l'évasion protocolaire

Evaluation en LID : Retour d'expérience et perspectives

La normalisation de trafic et les évasions protocolaires



Evaluation en LID : Retour d'expérience et perspectives

La normalisation de trafic et les évasions protocolaires

Chaque pile IP interprète différemment les ambigüités des paquets IP et TCP réseau

- Exemple : deux segments TCP dont les numéros de séquence se chevauchent

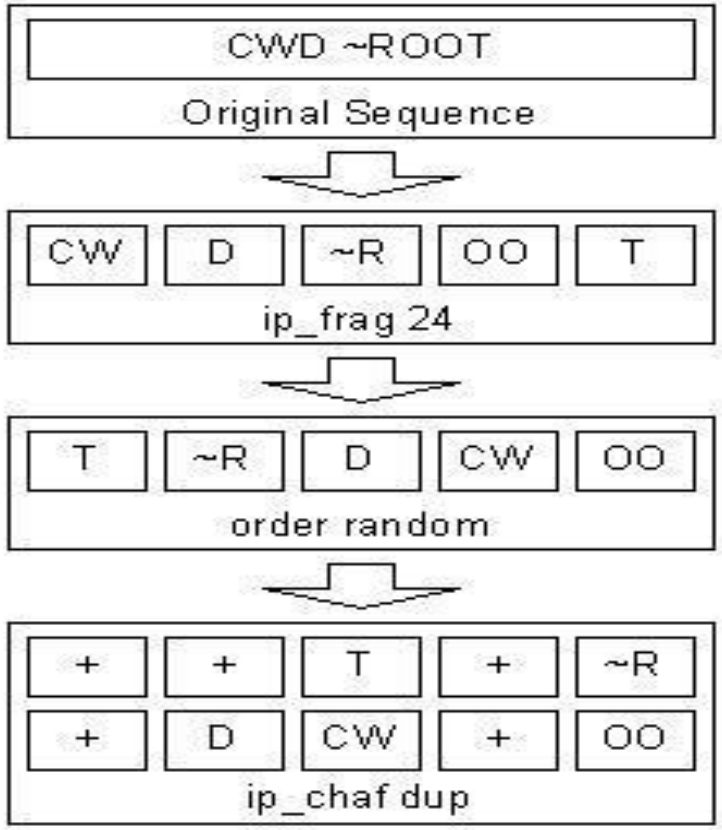
Complexité de la normalisation HTTP

- Plusieurs formats d'encodage (ASCII, UTF-8, base64, etc.)
- Parsing fiable pour l'extraction des champs

Ces constats sont à la base des attaques par « évasion protocolaire »

Evaluation en LID : Retour d'expérience et perspectives

La normalisation de trafic et les évasions protocolaires



Our original attack sequence fits within one packet.

Using the "ip_frag 24" option splits the sequence into packets with payloads of 24 bytes or less

Using the "order random" option puts the fragments in random order.

Using the "ip chaf dup" option inserts duplicate packets copying the header from a valid portion of the stream, but with invalid TCP options, garbage payloads, or invalid checksums.

Exemples d'évasions avec Fragroute

Evaluation en LID : Retour d'expérience et perspectives

La normalisation de trafic et les évasions protocolaires

- **Tous les NIDS/NIPS que l'on a évalués sont exposés à ce type d'attaque**
  - A une échelle plus ou moins importante

Evaluation en LID : Retour d'expérience et perspectives

L'analyse de la base des signatures

- Analyse de la pertinence des signatures
  - Problématique du taux de faux positif
- Analyse de la complétude
  - Problématique du taux de faux négatif

- **=> Travaux historiquement très académiques**

Evaluation en LID : Retour d'expérience et perspectives

L'analyse de la base des signatures

- Analyse de la vitesse/fréquence de mise à jour de la base
- Evaluation de l'expressivité des langages de définition des règles de détection/corrélation
  - Capacité d'analyse syntaxique
    - Analyse de la richesse du langage (motifs / expressions rationnelles / hash / etc.)
      - **Aujourd'hui bien géré par les NIDS et les méthodes d'évaluation**
  - Capacité d'analyse événementielle / comportementale
    - **Aujourd'hui plutôt bien géré par certains NIDS et SIEM, mais peu d'outils et de méthodes d'évaluation disponibles** (cf. Travaux sur la génération de trafic)

Evaluation en LID : Retour d'expérience et perspectives

L'évaluation des capacités de Threat Intelligence

- **Constat** : beaucoup de solutions NIDS / SIEM intègrent désormais des mécanismes de Cyber Threat Intelligence (CTI)
  - Infrastructure de gestion des IOC déployable en interne
    - CIF – Collective Intelligence Framework
    - MISP platform
    - …
  - Alimentation automatisée en IOC depuis feeds publics / payants

Evaluation en LID : Retour d'expérience et perspectives

L'évaluation des capacités de Threat Intelligence

Exemple du moteur de « Threat intelligence » de Bro

- Comparaison d'objets observés (URL, hash de fichiers, etc.) par rapport à des listes d'indicateurs de compromission
- Indicateurs supportés
  - Intel::ADDR
  - Intel::URL
  - Intel::SOFTWARE
  - Intel::EMAIL
  - Intel::DOMAIN
  - Intel::USER_NAME
  - Intel::FILE_HASH
  - Intel::FILE_NAME
  - Intel::CERT_HASH

Evaluation en LID : Retour d'expérience et perspectives

L'évaluation des capacités de Threat Intelligence

- Exemple d'une liste d'URLs suspectes

```
#fields indicator indicator_type meta.source meta.url meta.do_notice meta.if_in
badChinese.biz Intel::DOMAIN mandiant - T DNS::IN_REQUEST
badRussian.org Intel::DOMAIN mandiant - T HTTP::IN_HOST_HEADER
badCorse.net   Intel::DOMAIN mandiant - T SMTP::IN_FROM
...
```

- Exploitation dans un scrip Bro

```
@load base/frameworks/files
@load base/frameworks/notice
@load frameworks/files/hash-all-files
@load frameworks/intel/seen
@load frameworks/intel/do_notice

redef Intel::read_files = {
    "/path/datasets_bad_domains.txt"

    # See results int intel.log
};
```

Evaluation en LID : Retour d'expérience et perspectives

L'évaluation des capacités de Threat Intelligence

- Questions ouvertes
  - Comment évaluer l'apport des mécanismes de Threat Intelligence ?
  - Comment estimer la fiabilité des sources de renseignement ?
    - Fiabilité de l'information
    - Fiabilité de l'infrastructure source
    - Fraicheur des IOC

Evaluation en LID : Retour d'expérience et perspectives

L'évaluation d'une stratégie de détection

- **Objectifs** :
  - Evaluer la capacité des produits de LID à implémenter des stratégies de détection et de collecte
  - Evaluer le couplage avec les process et l'équipe du SOC

Evaluation en LID : Retour d'expérience et perspectives

L'évaluation du couplage avec les process et l'équipe SOC

- La vision métier est-elle prise en charge dans les produits de LID
  - Le SIEM intègre-t-il les processus et le workflow de l'équipe SOC ?
  - Le lien entre l'équipe SOC/CSIRT est-il entièrement géré et de manière efficace ?
    - Risque de duplication d'information (voire perte d'information) entre les outils SOC et CSIRT
  - Le SIEM est-il adapté pour chaque profil métier ?

Evaluation en LID : Retour d'expérience et perspectives

L'évaluation du couplage avec les process et l'équipe SOC

Les profils d'une équipe SOC

- **Level 1 analyst, first responder, real-time analyst**
  - *Inspect alerts and the associated traffic to eliminate false positives (triage analysis)*
- **Level 2 analyst**
  - *Escalation analysis, investigate suspicious activity received from triage analysis*
- **Correlation analyst**
  - *Search for patterns and trends in current and historical data*
- **Threat analyst**
  - *Gain insight into the identity, motives and sponsorship of attackers and forecast upcoming attack*
- **Incident handler, incident responder**
  - *Implement a course of action in reaction to a confirmed incident*
- **Forensic analysts**
  - *Work in support of a law enforcement investigation*

Source : The real work of computer network defense Analysts

Evaluation en LID : Retour d'expérience et perspectives

L'évaluation d'une stratégie de détection

- **Besoin d'une plateforme** permettant de
  - Mettre en place un environnement maitrisé (inventaire connu)
  - Générer du trafic maitrisé (de vie et d'attaque)
    - Le **réalisme** assure l'exactitude de l'évaluation
    - La **contrôlabilité** assure la reproductibilité de l'évaluation

Evaluation en LID : Retour d'expérience et perspectives

Les fonctionnalités attendues d'une plateforme de simulation

- Simulation de réseaux hétérogènes
- Simulation d'utilisateurs
- Simulation de données de vie statiques
- Simulation d'actions système et applicatives
- Simulation de trafic réaliste (légitime et d'attaque)

Evaluation en LID : Retour d'expérience et perspectives

La simulation de trafic réaliste

- **Besoin en simulation de trafic réaliste (légitime et d'attaque)**

- **Approches**
  - Rejeu de pcaps : réaliste mais incontrôlable
  - Trafic synthétique : irréaliste mais contrôlable
  - Méthode hybride : réaliste et contrôlable
    - Principe :
      - Modélisation du trafic au travers de captures réseaux
      - Paramétrage des couches réseaux avec le modèle pour générer un trafic
  - Instrumentation d'applications (clients web, mail, etc.) : réaliste et contrôlable

Evaluation en LID : Retour d'expérience et perspectives

La simulation de trafic réaliste

- **L'approche par instrumentation d'applications** (clients web, mail, lecteurs PDF, doc, etc.)
  - Objectifs
    - Manipuler les données de vie statique
    - Simuler implicitement des actions système / applicatives
    - Simuler implicitement du trafic réseau réaliste
  - Exemple : simuler des mouvements de souris et un vrai clic dans un navigateur
  - Approches
    - Agent déployé dans l'OS et contrôlant le serveur X
    - API de débogage et d'accessibilité des clients
    - Sans agent (depuis l'hyperviseur)

Evaluation en LID : Retour d'expérience et perspectives

La simulation de trafic réaliste

- **L'approche hybride**
  - **Contribution thèse (G. Bossert)**
    - Machine de Mealy Stochastique à Transitions Déterministes
      - Des transitions déterministes mais messages de sorties Indéterministes
      - La prise en compte du temps de réaction
  - **Équivalences assurées**
    - Syntaxique (vocabulaire du protocole)
    - Sémantique (grammaire du protocole)
    - Temporelle (temps de réaction)
  - Intéressant pour **évaluer les moteurs d'analyse événementielle / comportementale** des NIDS / SIEM

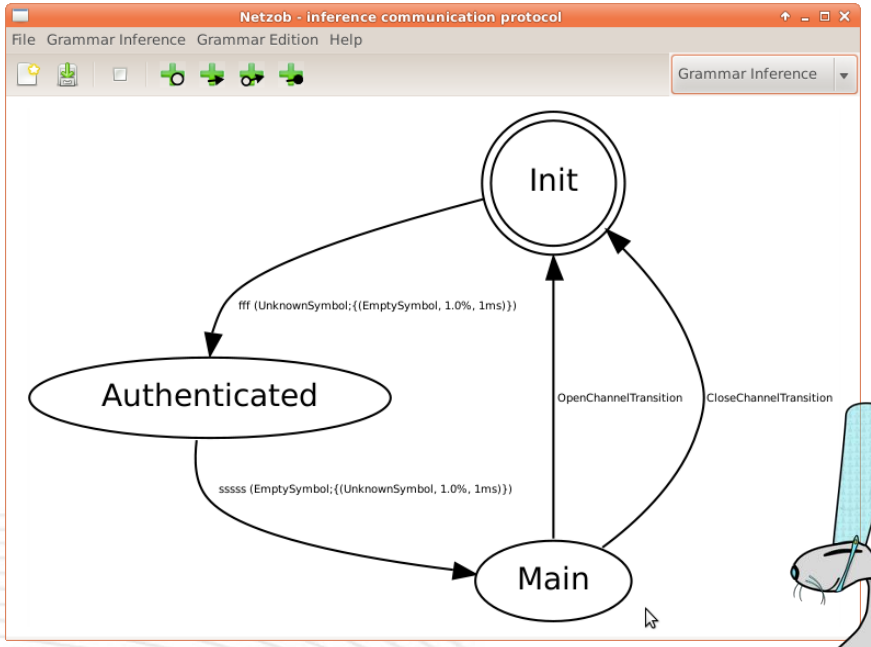
Evaluation en LID : Retour d'expérience et perspectives

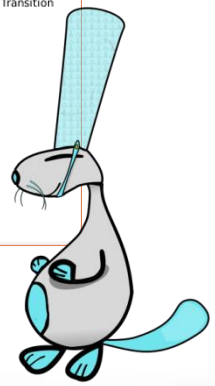
La simulation de trafic réaliste

- **Travaux de thèse sur l'approche hybride de génération de trafic**
  - Rétro-ingénierie de protocoles propriétaires ou de malwares
  - Apprentissage du canal de communication d'un botnet
  - Génération de trafic suivant un modèle appris
- **Publications**
  - Modélisation et simulation du canal de communication d'un botnet pour l'évaluation des NIDS,
    - **SAR-SSI 2011**, G. Bossert, G. Hiet, T. Hénin
  - The future of protocol reversing and simulation applied on ZeroAccess botnet
    - **29C3**, F. Guihéry, G. Bossert
  - Reverse and Simulate your Enemy Botnet C&C
    - **BlackHat Abu Dhabi'12**, G. Bossert, F. Guihéry

Evaluation en LID : Retour d'expérience et perspectives

La simulation de trafic réaliste





L'outil Netzob

- Semi-automated reverse specification of proprietary protocols.
- Identification of Message Format.
- Discovery of the state machine.
- Generation of realistic traffic to test security products.
- Simulation of client / server.
- "Smart-fuzzing" for implementations robustness analysis.
- Academic (PHD) and operationnal work.

GitHub https://github.com/AMOSSYS/Netzob

www.amossys.fr

Evaluation en LID : Retour d'expérience et perspectives

L'évaluation d'une stratégie de détection

- **Objectif** : évaluer la capacité à détecter des menaces
  - Exemple de liste des incidents redoutés (ETSI_ISG_ISI , Annexe B de l'ISO27035) :
    - Exploitation d'une vulnérabilité
    - Elévation de privilèges
    - Exfiltration de données
    - Propagation virale
    - Utilisation d'un mécanisme de persistance
    - Déni de service
    - Accès non autorisé à une ressource
    - Usurpation d'identité
    - Actions non conformes à la politique de sécurité

Evaluation en LID : Retour d'expérience et perspectives

L'évaluation d'une stratégie de détection

- **Constat** : écart sémantique entre **menaces / incidents redoutés** présents dans une stratégie de détection et les **signatures / IOC** implémentés dans les outils

Evaluation en LID : Retour d'expérience et perspectives

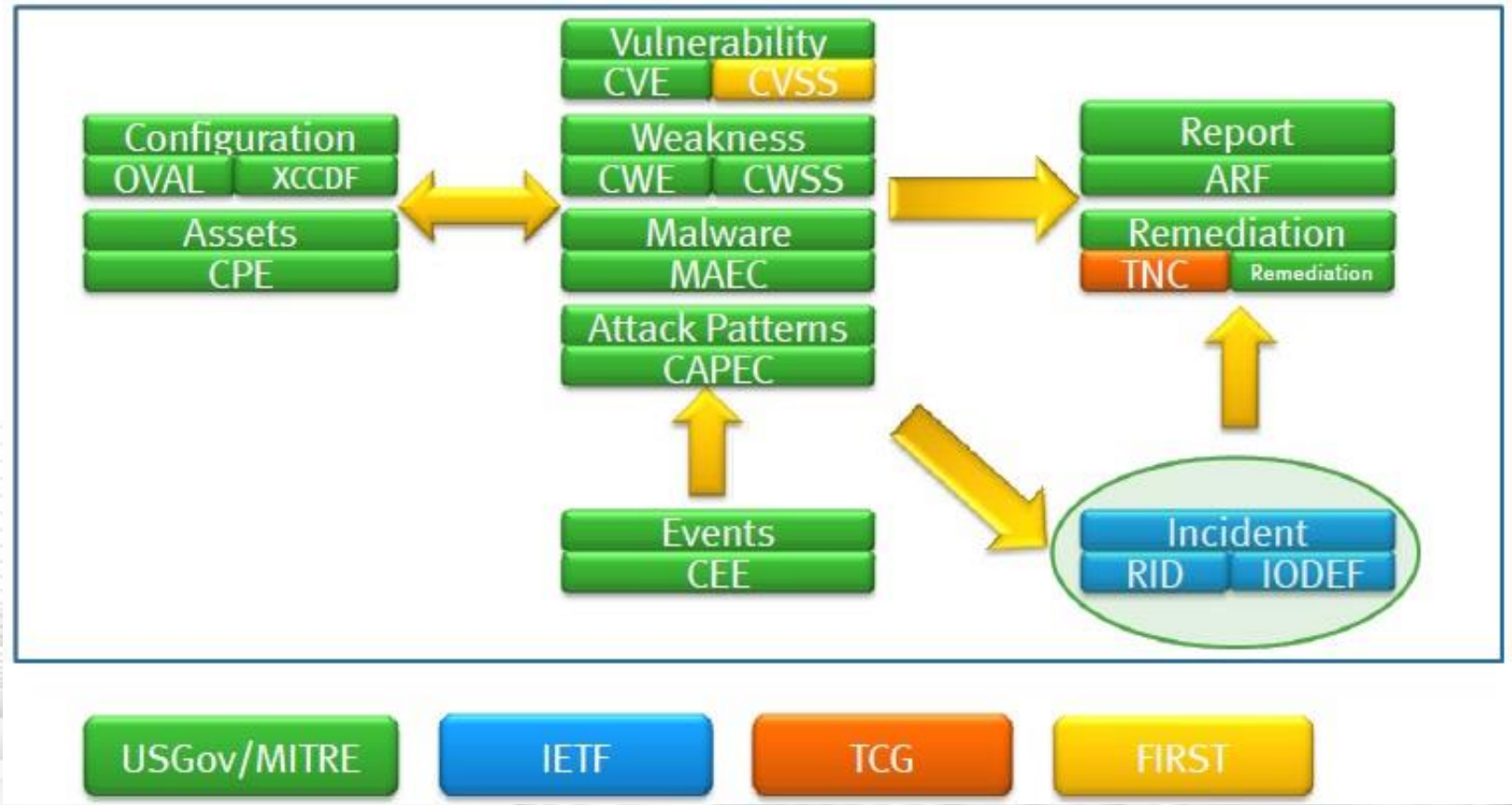
Utilisation du modèle Cyber Kill Chain

Objectif : pouvoir évaluer l'efficacité du produit de LID à détecter chaque étape de la kill chain

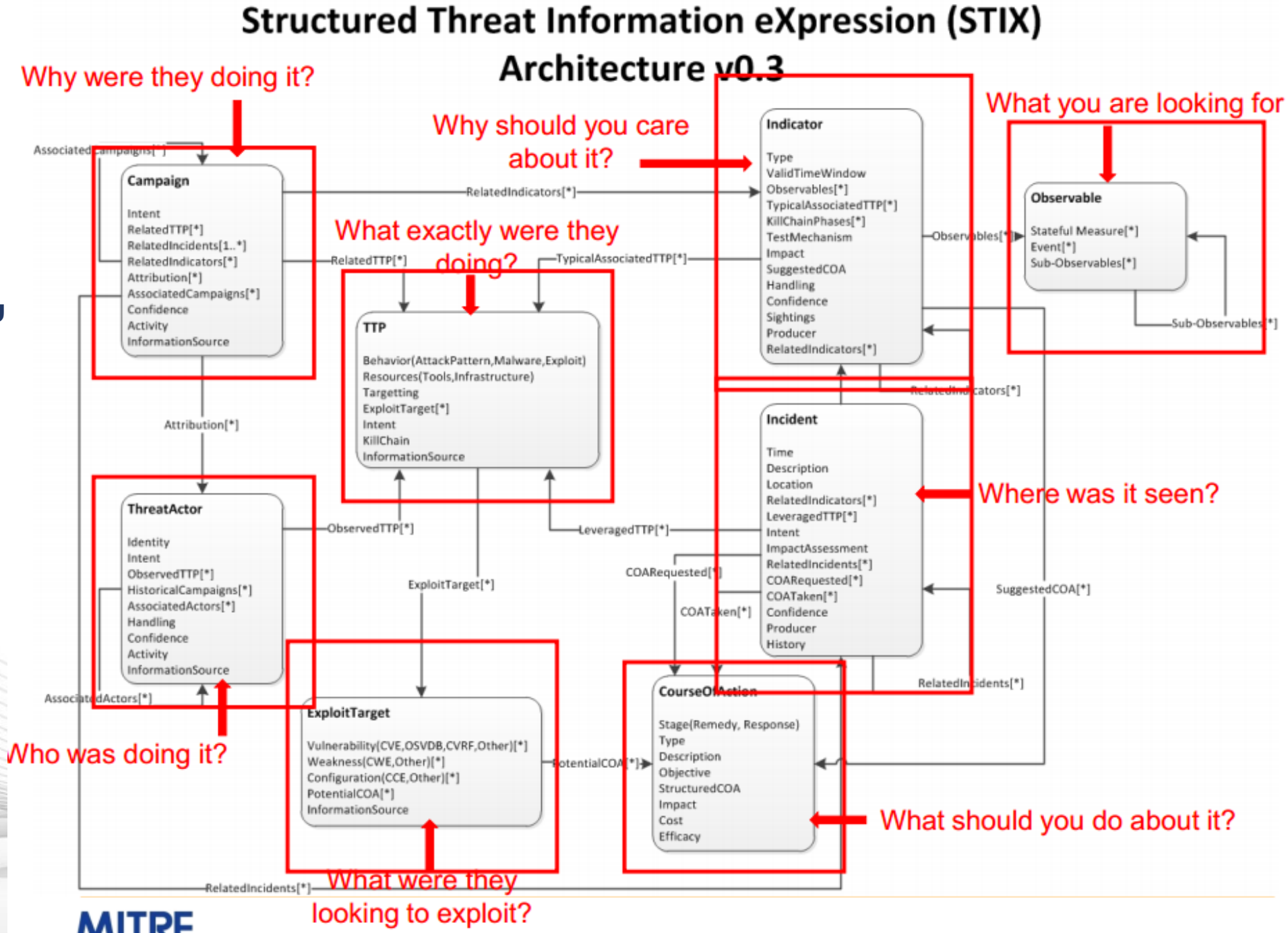
Evaluation en LID : Retour d'expérience et perspectives

Simulation de SI et d'activités

- Approche intéressante : **utiliser les standards pour la modélisation** des SI simulés et des actions / événements insérés



Structuration du standard STIX



MITRE

Evaluation en LID : Retour d'expérience et perspectives

Conclusion / axes de R&D

- Quelques axes de R&D
  - Renforcer l'évaluation de l'efficacité / robustesse des fonctions métier des produits LID
  - Pouvoir évaluer l'implémentation d'une stratégie de détection et de collecte
    - « Fermer » l'écart sémantique entre menaces/incidents redoutés et signatures de détection
  - Pouvoir évaluer l'adéquation des outils de LID aux processus et aux équipes SOC/CSIRT

Merci pour votre attention !

Nous contacter :

4 bis Allée du Bâtiment
35000 RENNES

02 99 23 15 79

https://www.amossys.fr

contact@amossys.fr

Retrouvez-nous également sur les réseaux sociaux :

www.amossys.fr