STAMUS NETWORKS

Pourquoi passer de l'IDS au NDR?

OSSIR, 11 mai 2021

Éric Leblond

Stamus Networks :

- Co-fondateur
- Directeur technique

Suricata & OISF :

- Développeur
- Membre du conseil exécutif de l'OISF

Vie précédente :

- Coreteam Netfilter
- NuFW/Edenwall

Contact :

- Twitter: @Regiteric
- Mail: el@stamus-networks.com

STAMUS NETWORKS

Founded: 2014 by Éric Leblond and Peter Manev

Headquarters: Indianapolis, USA and Paris, France

Website: www.Stamus-Networks.com

Solutions:

- *Scirius Security Platform (SSP)* – commercial network threat detection, hunting and response solution
- *Stamus Networks App for Splunk* – integration of SSP and Suricata into Splunk
- *SELKS* – open source Suricata turnkey distro
- *GopherCap* – open source PCAP playback tool

Network Traffic

Azure

aws

Cloud

On Premise

Visibility & Enrichment

Real-time event analysis

Packet flow inspection

Event enrichment

Stamus Probes
[appliance, virtual, cloud]

Correlation & Analysis

Centralized management

Hunting console

SSP

Host & asset correlation

Scirius threat detection

Event classification

Event storage

Scirius Security Platform
[appliance, virtual, cloud]

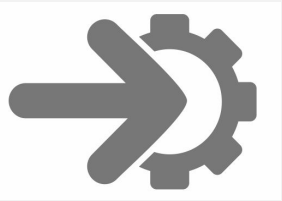
Actions & Integrations

Threat hunting

Incident investigation

Policy enforcement

Knowledge transfer



SIEM SOAR IR

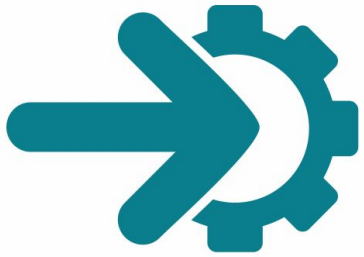
Messaging XDR

Rules, Threat Intel Feeds,
Organizational Context

Threat Radar Intel,
Custom Detection

STAMUS NETWORKS

Déploiement flexible et intégration facile



Fonctionne dans tous les environnements

- Haute performance (40 Gbps -> 100 Gbps)
- Dans le cloud ou on-premise

Intégration facile

- VPN pour les topologies complexes
- Open APIs – toutes les données sont disponibles
- Notifications et communications par Webhook

Intrusion Detection System

Wikipedia:

“An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.

Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system.

A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.”

STAMUS NETWORKS

Network Detection & Response

Gartner:

“NDR solutions use a variety of technologies, including signatures, policies, and machine learning to detect suspicious traffic on enterprise networks.

NDR tools continuously analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior.

When the NDR tools detect suspicious traffic patterns, they raise alerts.

In addition to monitoring north/south traffic that crosses the enterprise perimeter, NDR solutions can also monitor east/west communications by analyzing traffic from strategically placed network sensors. Response is also an important function of NDR solutions.

Automatic responses (for example, sending commands to a firewall so that it drops suspicious traffic) or manual responses (for example, providing threat hunting and incident response tools) are common elements of NDR tools.”

“IDS is dead” (2003, Gartner)

- Cause de la mort:
  - Va être remplacé par l’IPS
- Dans les faits:
  - Nécessaire pour la conformité
  - Au mieux pénible à utiliser
  - Inutile au pire
- Pas beaucoup mieux qu’un grep sur le réseau
- Les événements sont peu avenants :

```
01/13/2019-16:01:35.369922  [**] [1:2013504:5] ET POLICY GNU/Linux APT User-Agent Outbound likely re
lated to package management [**] [Classification: Not Suspicious Traffic] [Priority: 3] {TCP} 10.0.2
.15:33726 -> 91.189.88.149:80
```

Pourquoi l'IDS est-il toujours vivant ?

- Conformité
  - C'est une technologie de base
    - Recherche de contenu efficace
- L'IPS est limité
  - la réponse n'est pas toujours le blocage du paquet
- L'IDS a évolué
  - Reconnaissance et analyse des protocoles
  - Mots clefs dédiés aux protocoles
- IDS++ pour une meilleure visibilité
  - Combine IDS
  - et surveillance réseau orienté sécurité (NSM)

Suricata

Moteur IDS & NSM

STAMUS NETWORKS

Suricata

IDS

- Basé sur des signatures
- Support protocolaire
  - Reconnaissance indépendantes du port
  - Mots clefs
- Détection avancée
  - Script Lua
  - Dataset
- https://suricata-ids.org/

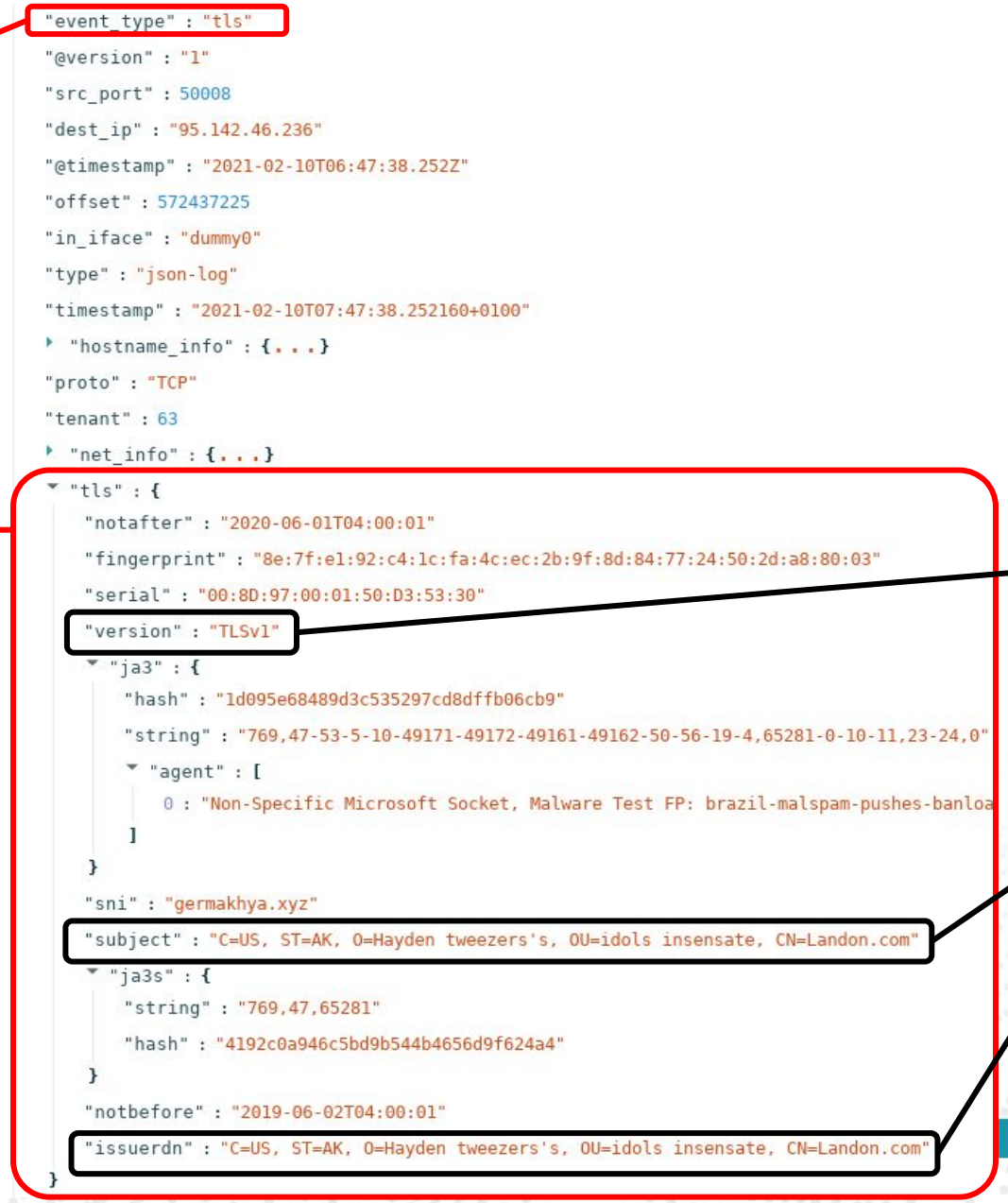
NSM

- Journalisation des transactions protocolaire
  - Internet: HTTP, TLS, DNS, ...
  - Interne: SMB, NFS, RDP, …
  - IOT: MQTT, ...
  - SCADA: ENIP, modbus
- Au format JSON
- Indépendant des alertes

Suricata: événement TLS

TLS event type

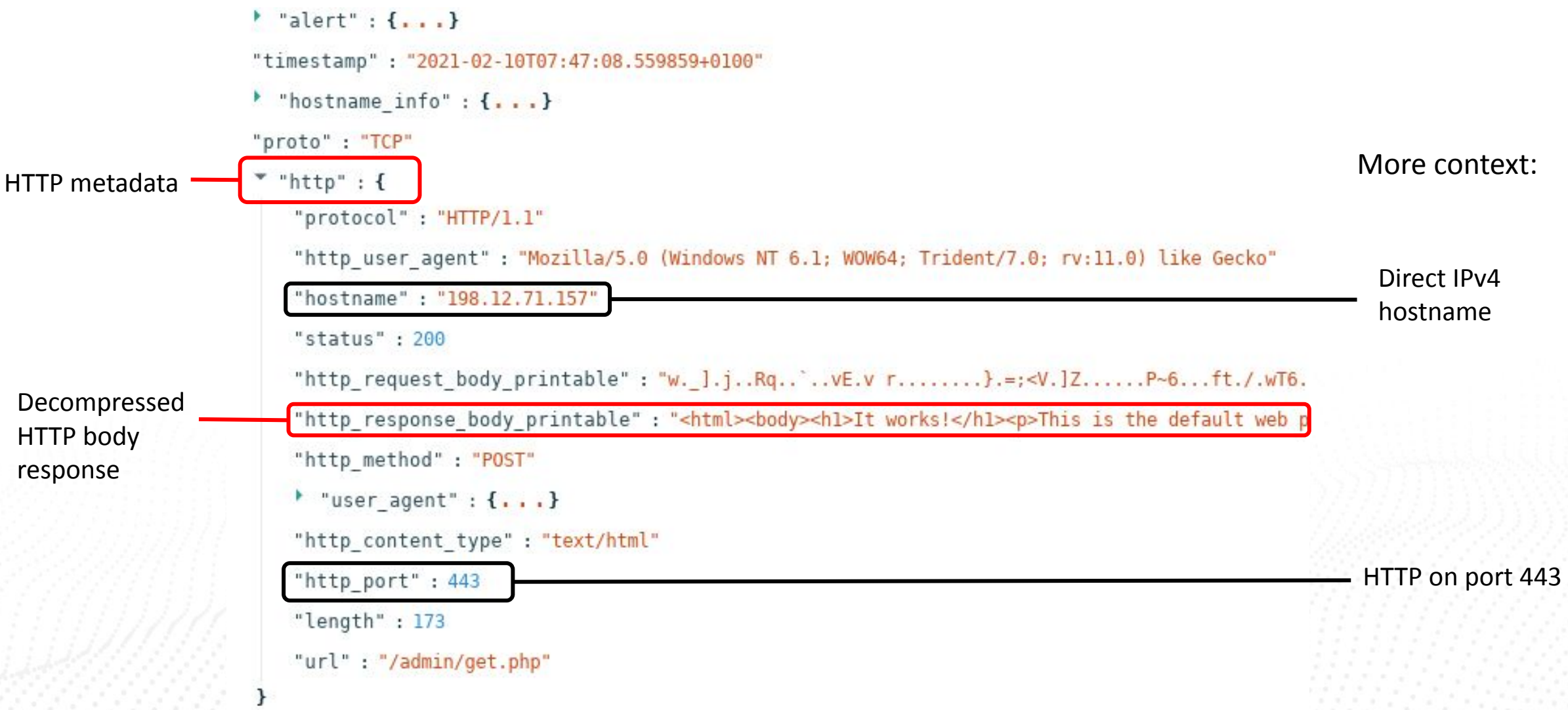
Extended TLS handshake analysis



Old fashioned TLS version

Nice self-signed certificate

Suricata: des alertes avec du contexte



L’effet arbre de Noel

- Des alertes par milliers
  - 1 millions d’alertes par jour
    - Réseau d’entreprise classique
  - Alertes contextuelles
    - Information
    - Potentiellement une indication de problème
  - 60 000 signatures dans ETPro
- Nécessité de mettre en place des process
  - Trier les alertes manuellement
  - Ou avoir une solution pour l’automatiser
  - Ou investir dans un SIEM (et son utilisation)

La mauvaise implémentation de Suricata

Quelles différences y a-t-il entre la bonne et la mauvaise implémentation de Suricata ?

La mauvaise implémentation Suricata

- N’utilise pas la sortie JSON
- Ne fournit pas de contexte pour l’analyse des alertes
  - Utilise unified 2 ou fast.log
  - Ou ne montre pas les métadonnées associées aux alertes
- Présente uniquement
  - un top 10 des alertes les plus fréquentes
  - une liste chronologique des dernières alertes
- L’analyste
  - doit faire le même travail de classification tous les jours
  - ou supprime la signature

Un exemple de classification d’alertes

- Exemple de la détection d’APT (get)
  - Mise à jour Debian
  - Preuve d’une activité
- Ne pas supprimer la signature
  - Traditionnellement fait par IP
  - Perte de contexte
- Mais prendre en compte l’environnement et la politique de sécurité
  - Sur notre ferme de serveurs
  - Seuls les dépôts officiel Debian sont autorisés
  - Et surtout pas ceux Kali Linux (et tous les outils offensifs)

Scirius Security Platform

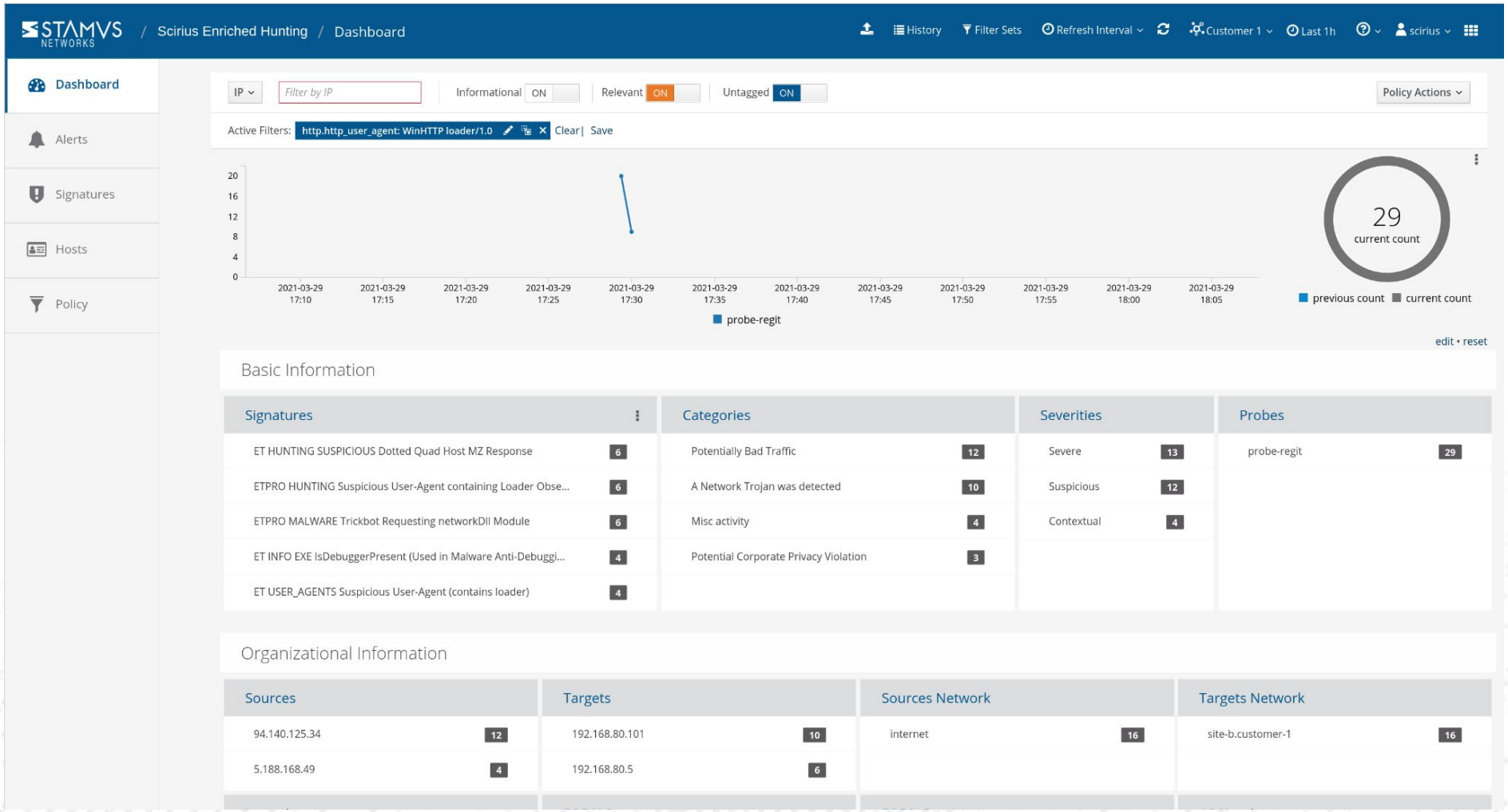
Classification et analyse

STAMUS NETWORKS

Classification dans Scirius Security Platform

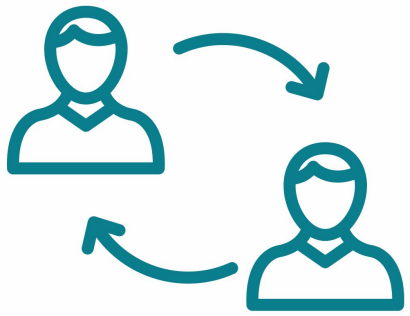
- Interface d’analyse des alertes
  - Présente les métadonnées
  - Filtre cumulatif
- Classification par métadonnées
  - Série de critères
  - Action
    - Relevant
    - Informational
  - Classification en continu

Démonstration (classification APT)



STAMUS NETWORKS

Transfert de connaissance au sein du SOC



Méthodologie d'analyse répartie

- L'analyste senior tague les événements comme "relevant" or "informational"
- Scirius NDR classifie automatiquement les événements futurs
- L'analyste junior étudie les événements marqués importants

L'analyste personnalise la solution

- Filtres sauvegardés
- Logique de détection personnalisée

Démonstration (Analyse MTA)

- Données de Malware Traffic Analysis: https://www.malware-traffic-analysis.net/
- Pcap: https://www.malware-traffic-analysis.net/2019/07/05/index.html

- Objectif:
  - Exploration dans l'interface
  - Déterminer la suite des événements

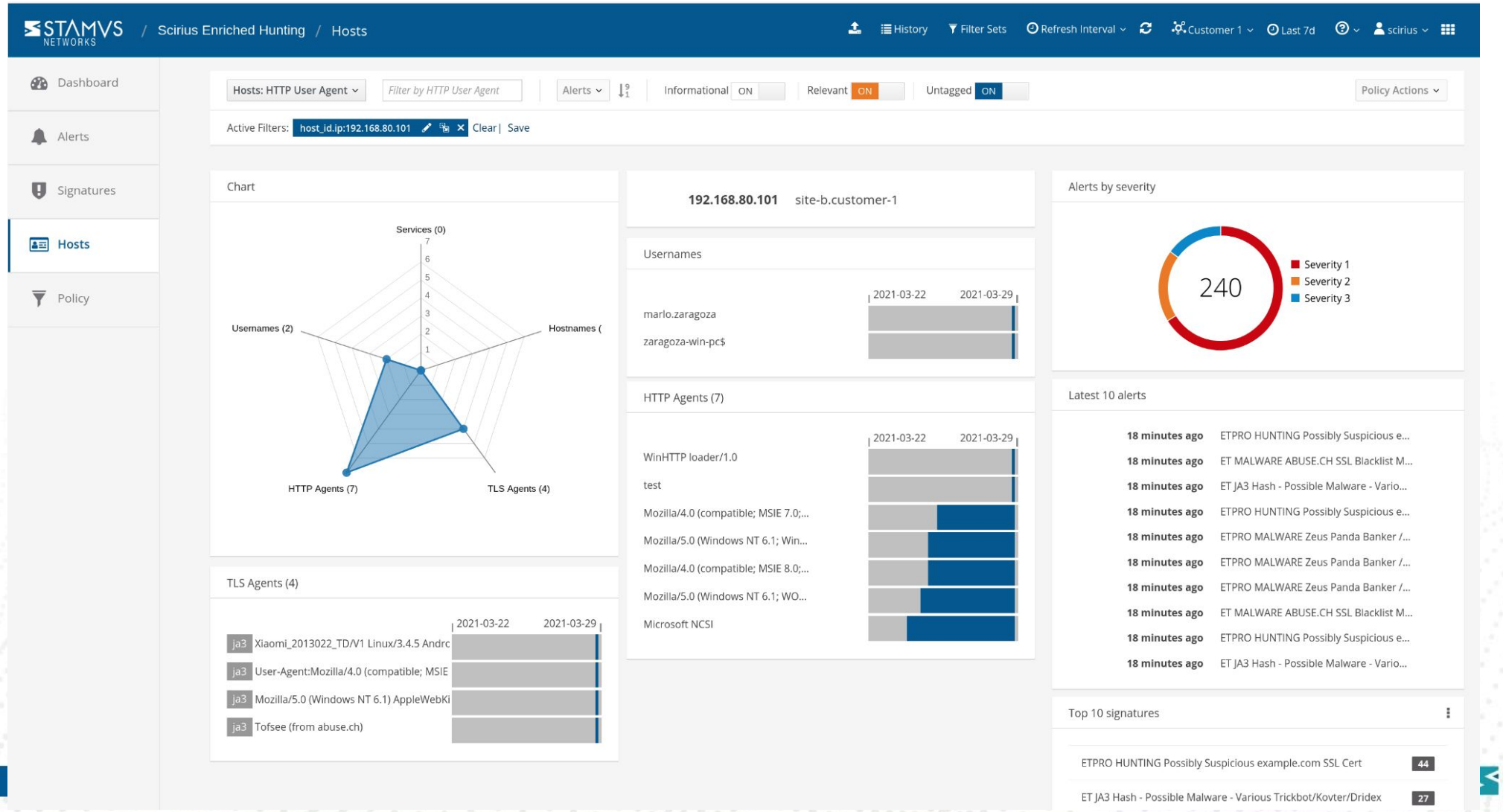
Carte d’identité des machines

- Fournit une vision d’ensemble du réseau
- Extraction des événements NSM
  - Création de caractéristiques
  - Données temporelles
- Exemple:
  - Liste des agents HTTP de l’IP
  - agent HTTP contient
    - Date de découverte
    - Date de dernière vue

Dimension extraites:

- Utilisateur
- Noms d’hôtes
- Agent HTTP
- Agent TLS
- Services

Carte d'identité des machines



Une analyse complète est une entreprise ardue

- Un nombre important d'alertes différentes
  - Travail d'analyse fastidieux
  - Potentiellement difficile de trouver les assets en danger
- Alertes multiples étalées dans le temps
  - Canal de controle
- Comprendre l'incident dans ce cas simple
  - Reste complexe
  - Nécessite expérience et méthode

Scirius Security Platform

Network Detection & Response

STAMUS NETWORKS

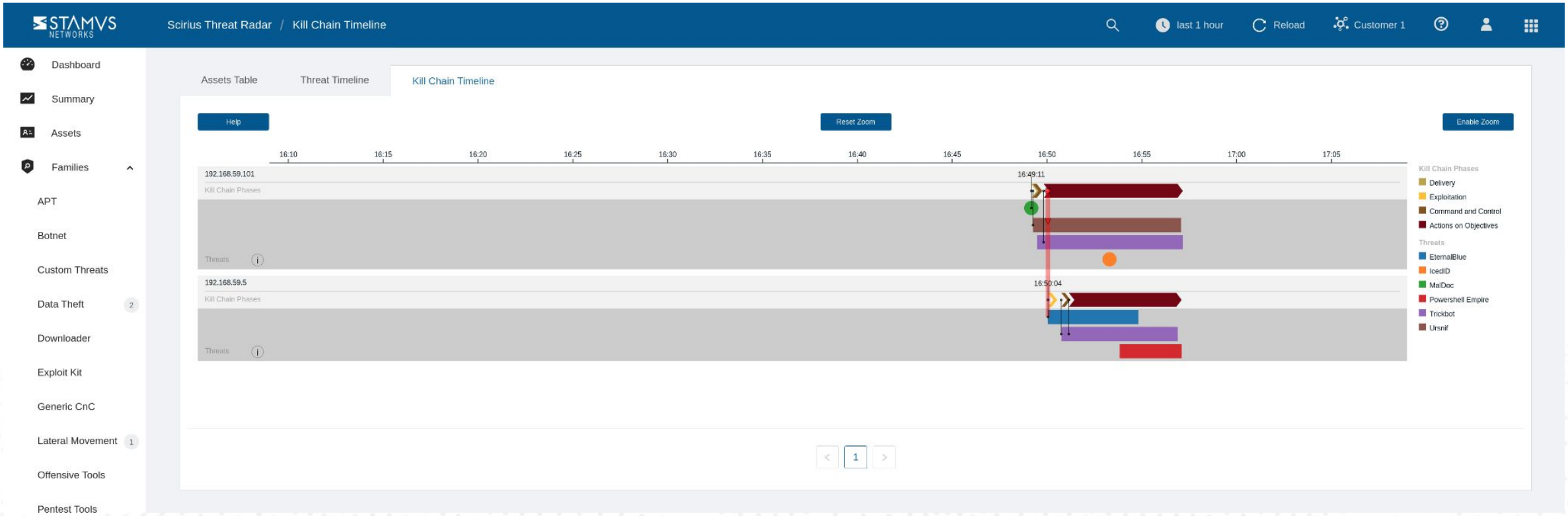
Scirius Threat Radar

- Passage à une approche par menace
  - Menace sur un asset
  - Prise en compte des étapes de la kill chain
- Détection des menaces fournie par Stamus Networks
  - Technologie de détection
    - Basé sur des signatures
    - Ou algorithmique
  - Menace avec description

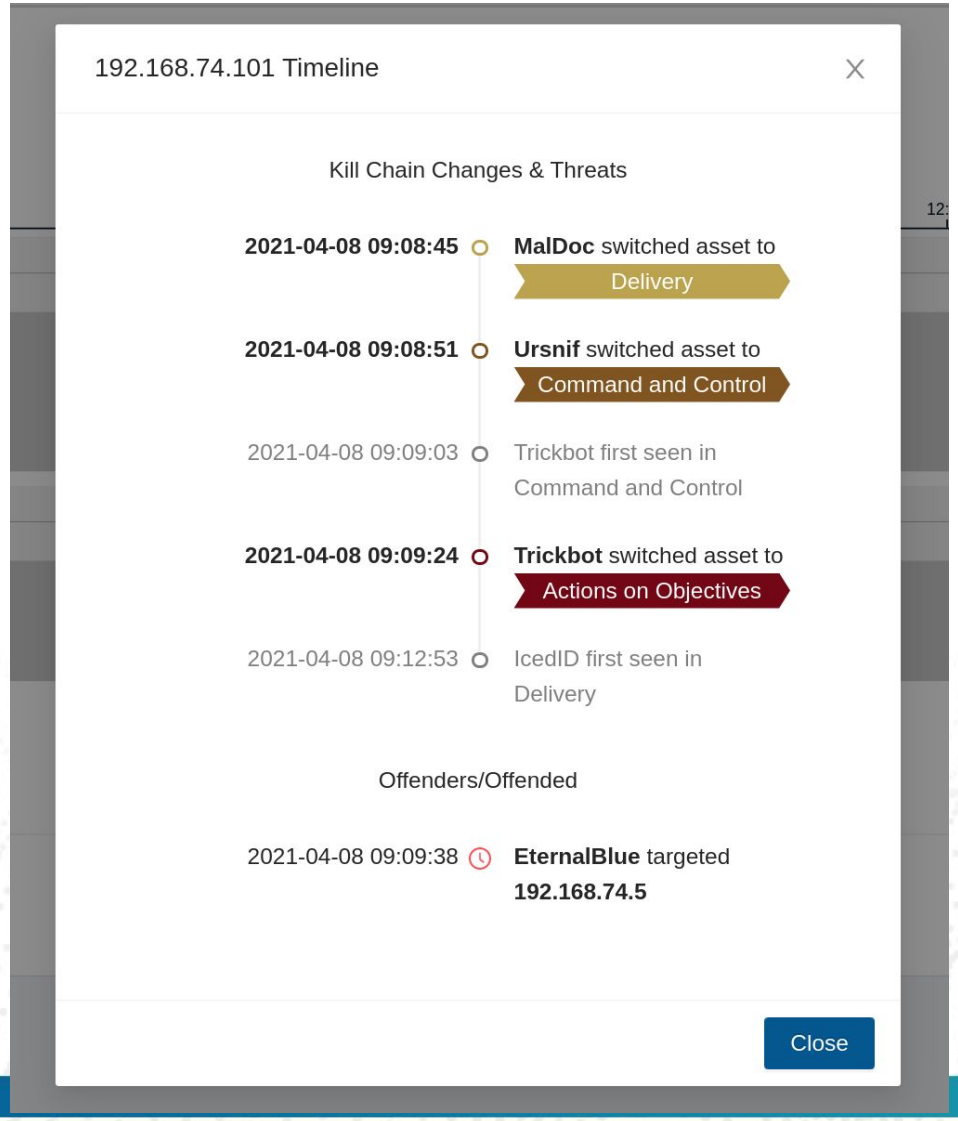
Démonstration

- Mêmes données analysées dans STR

Cinématique des attaques



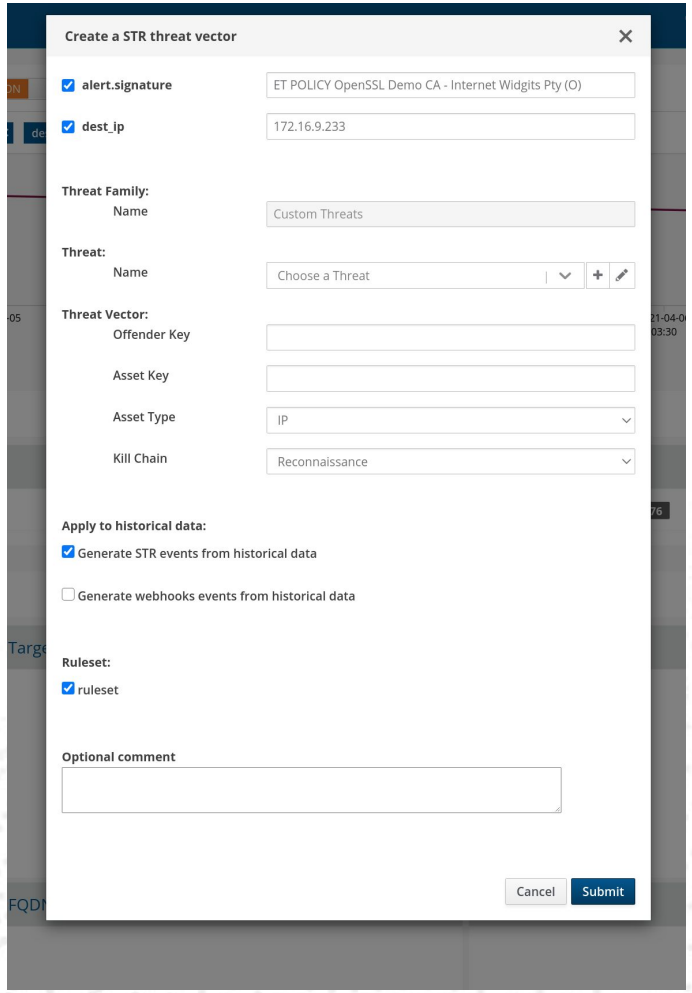
Chronologie pour un asset



STAMUS NETWORKS

Menaces définies par l'utilisateur

- Problématique
  - Une menace peut avoir une définition locale
  - Exemple de APT
- Principe
  - Création de menace locale
- Utilisation
  - Lors d'une analyse pour déterminer les assets
  - Pour escalader un événement dans un contexte donné
- Implémentation
  - Utiliser les filtres de l'interface d'analyse
  - Pour définir des événements du STR



STAMUS NETWORKS

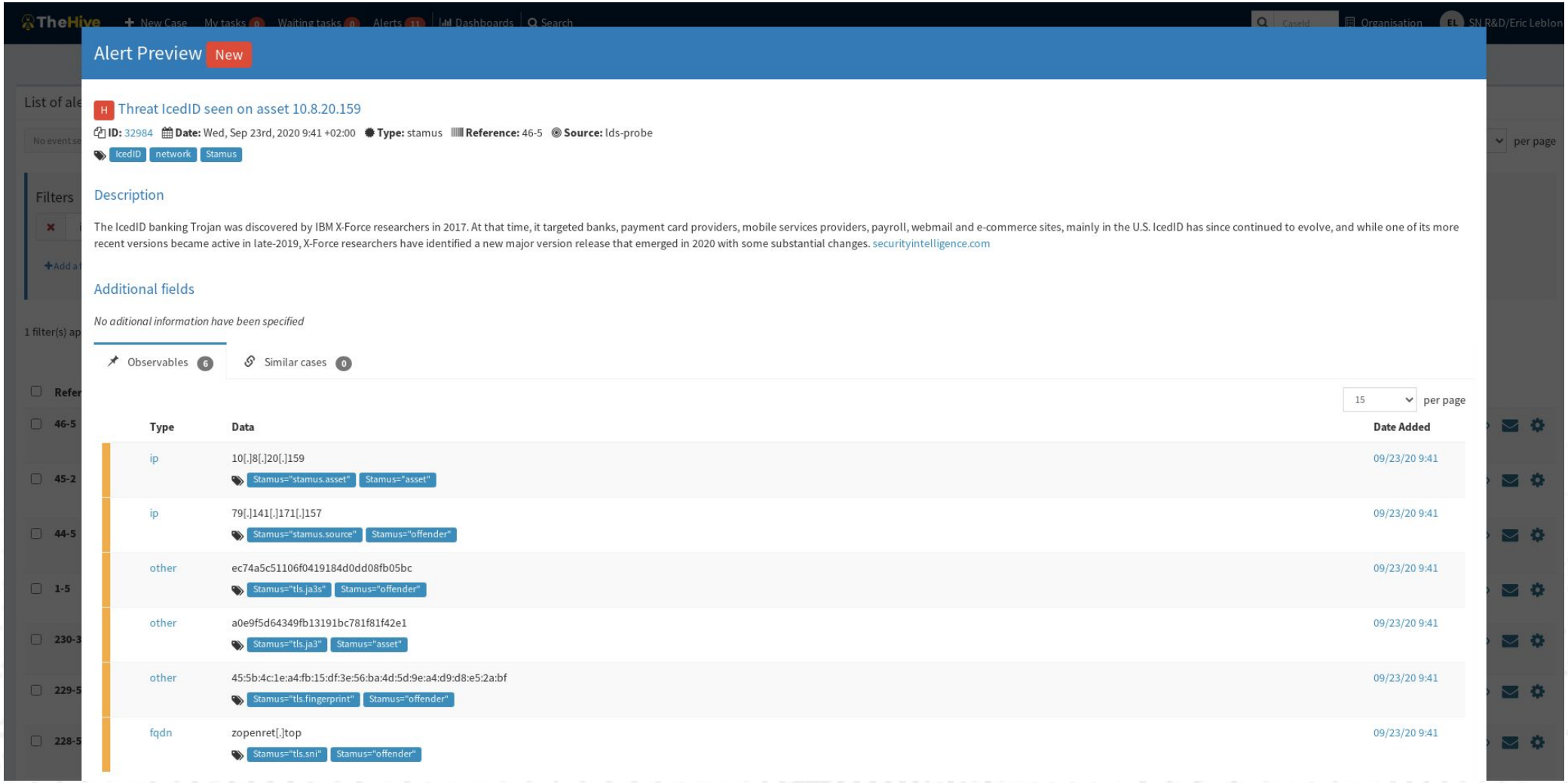
Démonstration

- Exploration dans l’interface de threat hunting
- Création d’un filtre composite
- Définition d’une menace
- Définition d’une ou plusieurs méthodes
  - Définir l’asset
  - L’étape dans la kill chain
  - Appliqué:
    - Aux événements à venir
    - Aux événements passés

Réponse par webhook

- Pour chaque webhook défini:
  - Scirius contacte un serveur externe:
    - Pour chaque nouvelle menace
    - Au changement d'étape dans la kill chain
- Avantage:
  - Un seul événement sur la découverte d'un canal de contrôle
- Implémentation:
  - Système de template
  - Accès à toutes les métadonnées
    - De l'événement sous jacent
    - De la menace
- Testé avec
  - Mattermost, Slack, TheHive, ServiceOne, Splunk

Exemple de TheHive



STAMUS NETWORKS

Exemple de TheHive

- Utilisation du langage de template jinja2
- Données disponibles :
  - Menace
  - Événement
- Code:

```
{% if event.tls %}
  {% if event.tls.sni %}
    { "dataType": "fqdn", "data": "{{ event.tls.sni | tojson }}", "tags": ["tls.sni"] },
  {% endif %}
  {% if event.tls.fingerprint %}
    { "dataType": "other", "data": "{{ event.tls.fingerprint | tojson }}", "tags": ["tls.fingerprint"] },
  {% endif %}
  {% if event.tls.ja3 %}
    { "dataType": "other", "data": "{{ event.tls.ja3.hash | tojson }}", "tags": ["tls.ja3"] },
  {% endif %}
  {% if event.tls.ja3s %}
    { "dataType": "other", "data": "{{ event.tls.ja3s.hash | tojson }}", "tags": ["tls.ja3s"] },
  {% endif %}
{% endif %}
```


STAMUS NETWORKS

Conclusion

- Scirius Network Detection & Response combine
  - un IDS basé sur Suricata
    - Avec un système de classification
  - une solution NSM
    - Données protocolaires
    - log pour chaque transaction
  - une solution de type NDR
    - Approche orientée asset et menace

- Une solution ouverte
  - API REST
  - Webhook
  - Export direct via
    - Syslog
    - Splunk forwarder
    - …
- Et performante
  - de 100Mbps à 40Gbps
  - machines virtuelles ou hardware
- Adaptée à tous les environnements
  - Sur site et/ou dans le cloud

Merci!

Stamus Networks SAS
5 Avenue Ingres
75016, Paris France

Contact@Stamus-Networks.com

Primary Point of Contact:

Eric Leblond
Directeur Technique
+33 (0) 6 49 88 06 01
el@stamus-networks.com

STAMUS NETWORKS