

Livre blanc

# Cinq fonctionnalités proposées par Corelight pour aider les analystes Sécurité à préserver la sécurité de leur réseau

## Les données collectées et traitées par les capteurs Corelight sont de solides atouts pour les centres d'opérations de sécurité (SOC)

S'appuyant sur le framework Zeek, la solution de détection et réponse aux cybermenaces NDR (*Network Detection and Response*) de Corelight aide les analystes Sécurité à être plus performants en transformant le trafic réseau en données plus rapides, plus utiles et plus puissantes. Voici pourquoi :

- 1. Les données collectées par Corelight apportent aux analystes Sécurité tout ce dont ils ont besoin** — Elles couvrent sous une forme détaillée, granulaire et exploitable les multiples protocoles réseau qu'ils utilisent.
- 2. Avec les données Corelight, les recherches deviennent simples et rapides** — Parce qu'elles sont formatées, organisées et interconnectées, les analystes trouvent rapidement les informations dont ils ont besoin.
- 3. Corelight permet à votre équipe d'accéder aux fichiers extraits** — Notre solution est capable d'extraire de manière évolutive tout fichier transmis sur le réseau.
- 4. Corelight détecte les tentatives « frauduleuses » au niveau des protocoles** — Notre technique de détection dynamique des protocoles (*Dynamic Protocol Detection*) traque les leurreurs et les erreurs.
- 5. Corelight apporte aux analystes une exceptionnelle flexibilité** — Le langage de script intégré autorise un haut niveau de personnalisation, d'automatisation et d'analyse.

Contrairement aux approches produisant trop (PCAP) ou trop peu de données (NetFlow), Zeek offre le juste équilibre, sans sacrifier le contexte ou la facilité d'utilisation.

Chris Sanders, chercheur en sécurité, formateur SOC et auteur du best-seller *Practical Packet Analysis a dit* :

L'acquisition est le seul domaine où les données collectées par Zeek n'obtiennent pas un score parfait. Chris Sanders note en effet qu'elles sont « difficilement personnalisables », et que leur collecte et leur traitement exigent une très grande puissance. Mais cette remarque concerne le logiciel libre Zeek, alors que Corelight propose un framework Zeek de qualité entreprise associé à des capteurs prêts à l'emploi.

### Avec les données Corelight, les analystes disposent de toutes les informations dont ils ont besoin

Au lieu de mixer des appliances et des outils de sécurité tels que les journaux DNS et de pare-feu, dont la portée est limitée et l'analyse croisée difficile, Corelight propose une vision complète dédiée à la sécurité des différents événements qui se déroulent dans le réseau. Nos journaux Zeek couvrent plus de 35 protocoles de réseau, l'analyse de nouveaux protocoles étant prise en charge sur demande.

#### Extrait d'un log Zeek pour une requête DNS

**1. Horodatage** (308930716.700706) — Cet horodatage de l'ordre de la microseconde provient du réseau lui-même *via* le matériel NIC (*Network Interface Card*). La réponse à un incident ayant pour objectif de reconstituer un « récit », il est essentiel que l'horodatage soit d'une précision sans faille.

#### **2. Identifiant unique de connexion (CUID)**

(CNFhPo1bq5dJD3wzJ6) — Cet identifiant UID est spécifique à la connexion et permet à un analyste de « pivoter » facilement en exposant les différents journaux associés et en comprenant ce qui s'est passé avant et après. Cette approche est nettement plus efficace que la mise en correspondance manuelle d'horodatage (*matching timestamps*).

**3. Un enregistrement détaillé plus complet des appels** (172.16.238.131 54304 172.16.238.2 53 udp) — Les cinq valeurs numériques (« 5-tuple ») — port et IP source (172.16.238.131 54304), port et IP de destination (172.16.238.2 53), et protocole utilisé (udp) — indiquent les détails omis par les journaux des serveurs DNS.

**4. Délai aller-retour** (0,004850) — Mesurée en secondes, cette valeur peut révéler une attaque de l'homme du milieu (« *man-in-middle* »), des erreurs de configuration réseau, et/ou d'importants problèmes de performance réseau.

**5. Contenu de la réponse** (74.125.225.81, 74.125.225.82, etc.) — La victime reçoit une adresse IP malveillante qui disparaît du cache après seulement quelques secondes. Or, ces données révèlent précisément ce que le client a vu.

## Avec les données Corelight, les recherches deviennent simples et rapides

En ayant la possibilité d'accéder à des données hautement interconnectées, structurées et facilement consultables, les équipes de sécurité deviennent plus productives, limitant ainsi les risques métier en identifiant et en remédiant aux dangers avant qu'ils ne se propagent. Mais en quoi les journaux Zeek de Corelight sont-ils davantage performants pour les recherches ? Tout d'abord, ils se présentent dans un format de journal unique et accessible, qui peut être exporté vers n'importe quel système de gestion des incidents et événements de sécurité (SIEM) ou pipeline de données ; ensuite, ils sont spécifiquement formatés et reliés. Il est inutile d'ingérer et de procéder à l'analyse croisée des données réseau provenant de différentes sources.

## Les journaux de Corelight contiennent les données correspondant aux couches connexion et application, c'est-à-dire aux contenus les plus importants

Des centaines, voire des milliers de paquets peuvent être transmis lors du téléchargement d'un unique document PDF potentiellement malveillant. Zeek assimile et analyse ces paquets, enregistrant de manière compacte les éléments clés du fichier transféré. Ces données peuvent être difficilement extraites de l'interface PCAP, et en aucun cas des flux NetFlow.

### Avantages des données Corelight

**1. 100 % signal, 0 % bruit** : pertinentes et lisibles par des opérateurs humains, les données résumant la connexion, les événements de fichier et le flux HTTP sont enregistrées, contrairement aux paquets capturés (PCAP) bruts.

**2. Identifiants uniques (UID) de connexion et de fichier** : seul Zeek fournit ces identifiants uniques en étiquetant le fichier pour permettre de « pivoter » rapidement sur d'autres connexions. Cette approche facilite les recherches dans tous les logs associés à ladite connexion (DNS, HTTP, fichier, etc.).

**3. Hachages de fichiers** : Zeek génère les hachages MD5, SHA-1 et SHA-256 pour tous les fichiers, de sorte que les intervenants ont la possibilité de les comparer aux référentiels de logiciels malveillants, aux listes noires et aux autres journaux Zeek.

## Corelight permet aux équipes Sécurité d'accéder aux fichiers extraits

Extraire et réassembler des fichiers sont deux tâches complexes à de nombreux égards, qu'il s'agisse de l'identification du protocole, de l'identification et du réassemblage des flux de paquets, de l'extraction des fichiers intégrés au dialogue avec l'application ou de la modulation de l'extraction lorsque la charge est importante. L'activation de l'extraction de fichiers dans les produits d'autres fournisseurs exerce souvent un impact négatif sur les performances.

Pour sa part, Corelight excelle dans l'extraction de fichiers à grande échelle en permettant d'analyser intégralement la syntaxe du protocole et de l'identifier de manière efficace. Le pipeline d'exportation optimisé par Corelight ne procédant pas à la réextraction des fichiers dupliqués qui traversent un réseau, le capteur peut s'adapter aux environnements à haut débit sans perte importante et sans impact négatif sur la capacité d'analyse des autres capteurs.

## Corelight sait contourner l'utilisation de leurres au niveau des protocoles

La plupart des protocoles réseau utilisent des ports connus. Toutefois, les attaquants peuvent envoyer des données sur n'importe quel port, ce qu'ils font fréquemment en se connectant de façon masquée à des ports non standard (par exemple, en envoyant du trafic HTTP sur le port SSH). Au lieu de se fier aux ports ou à de simples signatures pour identifier les protocoles, Zeek utilise la validation de l'analyse syntaxique (*parsing*) pour analyser le contenu de la connexion et vérifier quel protocole est utilisé. Cette approche permet d'identifier des situations similaires à l'exemple indiqué ci-après, où un attaquant cache ses communications C&C (commande et contrôle) à l'intérieur de ce qui se présente comme une connexion SSL.

```
{ "_path": "dpd", "_write_ts": "2018-01-15T17:11:57.552839Z", "ts": "2018-01-15T17:11:57.552839Z", "uid": "CpPNAD4SAqvPZf0h5b", "id.orig_h": "1.2.3.4", "id.orig_p": 3908, "id.resp_h": "5.6.7.8", "id.resp_p": 443, "proto": "tcp", "analyzer": "SSL", "failure_reason": "Invalid version late in TLS connection. Packet reported version: 4753" }
```

### Journal Zeek DPD d'une soi-disant connexion SSL

Le log Zeek présenté ci-dessus montre l'établissement de la connexion (*handshake*) SSL entre l'hôte (1.2.3.4) et le serveur (5.6.7.8), chaque premier message (« hello ») étant correctement analysé comme de type SSL. La syntaxe du paquet suivant devrait également être analysée comme étant un paquet de données SSL, mais le processus échoue, ce qui montre qu'en fait, cette connexion n'est pas de type SSL. Il s'agit d'un attaquant qui tente de dissimuler une porte dérobée (« *backdoor* ») en déguisant ses communications. Corelight détecte automatiquement ce type d'évasion de protocole à grande échelle.

### Avec Corelight, les analystes de sécurité disposent d'une exceptionnelle flexibilité

La plateforme de surveillance Zeek met à la disposition des analystes de sécurité un large éventail de possibilités. En effet, outre un langage de script intégré, elle permet de rédiger des scripts pouvant être utilisés avec les journaux après avoir été écrits ou avant la génération des données. Tous les journaux Zeek peuvent être personnalisés pour inclure de nouveaux détails ; il est également possible de générer des logs Zeek entièrement nouveaux. Grâce à cette fonctionnalité, les équipes Sécurité peuvent automatiser des analyses telles que la détection de menaces ou la surveillance des performances réseau.

L'environnement Intelligence Framework est l'un des frameworks de script les plus couramment utilisés au sein de la communauté Zeek. Par exemple, lorsqu'un nom DNS à surveiller est spécifié, le script examiner tous les protocoles et génère une alerte chaque fois que ce nom apparaît.

Le framework Zeek constitue une option plus flexible et plus extensible, qui permet de décider exactement à quelles données vous souhaitez accéder et comment les analyser. Cette démarche diffère la plupart des produits actuels, où la logique d'analyse demeure opaque et où les clients

doivent s'appuyer sur l'éditeur pour actualiser la couverture et intégrer les menaces récemment détectées. Enfin, l'expérience acquise depuis par la communauté open source Zeek plus de 20 ans permet aux clients de Corelight de bénéficier des scripts réalisés par ses membres.

<sup>1</sup> Saldich, Alan. Corelight, Inc. *Bro is an IDS. Not, It's Not*. 2018. <http://www3.corelight.com/bro-is-an-ids-no-its-not>

<sup>2</sup> Critères mis au point par Chris Sanders, fondateur d'Applied Network Defense. [www.investigationtheory.com](http://www.investigationtheory.com)

<sup>3</sup> Kreibich, Christian. Corelight, Inc. *Extensibility as a Guiding Principle*. 2017. <https://corelight.blog/2017/12/06/extensibility-as-a-guiding-principle/>

<sup>4</sup> Mens, Jan-Piet. *BIND querylog: know your flags*. 2011. <https://jpmens.net/2011/02/22/bind-querylog-know-your-flags/>

<sup>5</sup> Image utilisée sous licence pour un usage commercial par Corelight et disponible sur le site [www.istockphoto.com](http://www.istockphoto.com). L'image téléchargée vient du site: <http://blogs.teradata.com/data-points/wp-content/uploads/2014/02/Open-Your-Mind-to-All-The-Data3-983x1024.jpg>

<sup>6</sup> Source du script: <https://github.com/salesforce/ja3>



Les défenseurs ont toujours cherché à prendre de la hauteur pour voir plus loin et mieux repousser d'éventuelles attaques. En leur offrant une vue imprenable sur votre réseau, Corelight aide les entreprises à déjouer les tentatives d'agression et à repousser leurs adversaires. Nous recueillons, interprétons et connectons les données qui comptent pour les défenseurs.

**info@corelight.com | +1 510 281 0760**