Chapitre 4 : Protection de l’entreprise

Ce chapitre aborde une partie des technologies et processus utilisés par les professionnels de la cybersécurité lorsqu’ils protègent le réseau, les équipements et les données d’une entreprise. Ce chapitre traite brièvement en premier lieu des nombreux types de pare-feu, d'appliances de sécurité et de logiciels habituellement utilisés, notamment les bonnes pratiques.

Puis, s’ensuit l’explication des réseaux de zombies, de la chaîne de frappe, de la sécurité basée sur le comportement, ainsi que de l’utilisation de NetFlow pour surveiller le réseau.

La troisième section parle de l’approche de Cisco en matière de cybersécurité, dont l’équipe CSIRT et le guide sur la sécurité. Elle traite brièvement des outils que les professionnels de la cybersécurité utilisent pour détecter et prévenir les attaques réseau.

Types de pare-feu

Un pare-feu est un mur ou une partition conçu pour prévenir la propagation du feu d’une partie du bâtiment vers une autre. En informatique, un pare-feu est conçu pour contrôler, ou filtrer, les communications autorisées à entrer dans un dispositif ou dans un réseau, ainsi que celles autorisées à en sortir. La figure illustre cette propriété. Un pare-feu peut être installé sur un seul ordinateur afin de protéger cet ordinateur (pare-feu propre à un hôte unique). Il peut également être un périphérique réseau autonome qui protège tout un réseau d’ordinateurs et tous les appareils hôtes sur ce réseau (pare-feu basé sur le réseau).

Au fil des années, comme les attaques informatiques et les attaques du réseau sont devenues plus sophistiquées, de nouveaux types de pare-feu ont été élaborés pour répondre à différents objectifs dans la protection d'un réseau. Voici une liste des types de pare-feu courants :

* **Pare-feu de la couche réseau** : filtrage basé sur les adresses IP sources et de destination
* **Pare-feu de la couche transport** : filtrage basé sur les ports de données sources et de destination et filtrage basé sur les états de connexion
* **Pare-feu de la couche application** : filtrage basé sur les applications, les programmes ou les services
* **Pare-feu pour applications sensibles au contexte** : filtrage basé sur l'utilisateur, l'appareil, le rôle, le type d'application et le profil de la menace
* **Serveur proxy** : filtrage des demandes de contenu Web comme les URL, les domaines, les médias, etc.
* **Serveur proxy inverse** : placé à l'avant des serveurs Web, les serveurs proxy inverses protègent, masquent, déchargent et distribuent l'accès aux serveurs Web
* **Pare-feu NAT (traduction d'adresses de réseau)** : cache ou masque les adresses privées des hôtes du réseau
* **Pare-feu propre à un hôte unique** : filtrage des ports et des appels de service du système sur le système d'exploitation d'un seul ordinateur

Balayage des ports

Le balayage des ports est un processus de sondage d’un ordinateur, d’un serveur ou d’un autre hôte de réseau pour détecter les ports ouverts. Dans le domaine des réseaux, un identifiant appelé numéro de port est attribué à chaque application exécutée sur un périphérique. Ce numéro de port est utilisé sur les deux extrémités de la transmission pour que les bonnes données soient transmises vers l’application adéquate. Il est possible d’utiliser le balayage des ports de manière malveillante en tant qu’outil de reconnaissance pour identifier le système d’exploitation et les services exécutés sur un ordinateur ou sur un hôte. Un administrateur réseau peut également l’utiliser de façon inoffensive pour vérifier les politiques de sécurité du réseau.

Afin d’évaluer le pare-feu de votre propre réseau d’ordinateurs, ainsi que la sécurité de vos ports, vous pouvez utiliser un outil de balayage des ports comme Nmap pour détecter tous les ports ouverts sur votre réseau. Le balayage des ports peut être considéré comme un précurseur d’une attaque réseau et ne doit pas, par conséquent, être effectué sur des serveurs publics sur Internet ou sans permission sur un réseau d’entreprise.

Pour effectuer le balayage des ports d'un ordinateur sur votre réseau domestique local avec Nmap, téléchargez et lancez un programme tel que Zenmap, fournissez l'adresse IP cible de l'ordinateur que vous souhaitez analyser et choisissez un profil de balayage par défaut, puis appuyez sur Scan (Balayer). Le balayage Nmap présentera un rapport de tous les services en cours d’exécution (p. ex., services Web, services de messagerie, etc.) et les numéros des ports. Le balayage d’un port entraîne habituellement l’une des trois réponses suivantes :

* **Ouvert ou Accepté** : l'hôte répond en indiquant qu'un service est en attente de requête sur le port.
* **Fermé, Refusé ou Pas en attente de requête** : l'hôte répond en indiquant que les connexions au port seront refusées.
* **Filtré, Ignoré ou Bloqué** : il n'y avait aucune réponse de la part de l'hôte.

Pour exécuter le balayage des ports de votre réseau à partir de l’extérieur du réseau, vous devrez lancer le balayage à partir de l’extérieur de ce réseau. Cela impliquera l’exécution d’un balayage de ports Nmap contre votre pare-feu ou contre l’adresse IP publique de votre routeur. Pour connaître votre adresse IP publique, utilisez un moteur de recherche comme Google avec la demande « quelle est mon adresse IP ». Le moteur de recherche vous renverra votre adresse IP publique.

Pour exécuter un balayage de ports pour six ports communs par rapport à un routeur ou par rapport à un pare-feu, rendez-vous sur le Scanner de ports en ligne Nmap à l’adresse <https://hackertarget.com/nmap-online-port-scanner/> et entrez votre adresse IP publique dans la barre de saisie : adresse IP à analyser... puis appuyez sur Quick Nmap Scan. Si la réponse est ouverte pour l’un des ports : 21, 22, 25, 80, 443 ou 3389, alors un transfert de port a probablement été activé sur votre routeur ou sur votre pare-feu, et vous utilisez des serveurs sur votre réseau privé, tel qu’illustré dans la figure.

# Appliance de sécurité

Il n'existe actuellement aucun appareil de sécurité ni élément technologique qui puisse résoudre tous les besoins en matière de sécurité du réseau. Puisqu’il faut implémenter plusieurs outils et appliances de sécurité, il est important que ces outils et appliances fonctionnent en harmonie. Les appliances de sécurité sont plus efficaces lorsqu’ils composent un système.

Les appliances de sécurité peuvent être des périphériques autonomes, par exemple un routeur ou un pare-feu, une carte qui peut être installée dans un périphérique réseau, ou un module avec son propre processeur et sa propre mémoire cache. Elles peuvent également être des outils logiciels fonctionnant sur un périphérique réseau. Voici quelques exemples d’appliances de sécurité appartenant à ces catégories générales :

**Routeurs**: les routeurs de services intégrés Cisco (ISR), exposés dans la Figure 1, ont plusieurs fonctionnalités de pare-feu en plus de leurs fonctions de routage, notamment le filtrage du trafic, la capacité d'exécuter un système de prévention des intrusions (IPS), le chiffrement, ainsi que les fonctionnalités VPN pour la mise en tunnel chiffrée et sécurisée.

**Pare-feux**: les pare-feu de nouvelle génération de Cisco disposent de toutes les fonctionnalités d'un routeur ISR, ainsi que de l'analyse et de la gestion de réseau avancées. Cisco Adaptive Security Appliance (ASA) avec fonctionnalités de pare-feu est illustré dans la Figure 2. L’appliance de sécurité adaptatif Cisco (ASA) avec des fonctionnalités de pare-feux est illustré dans la Figure 2.

**IPS**: les périphériques IPS de nouvelle génération de Cisco, illustrés dans la Figure 3, sont dédiés à la prévention des intrusions.

**VPN**: les appliances de sécurité de Cisco disposent d'un serveur et de technologies client pour réseau privé virtuel (VPN). Le VPN est conçu pour la mise en tunnel chiffrée et sécurisée.

**Malware/Antivirus**: Cisco Advanced Malware Protection (AMP) accompagne les routeurs, les pare-feu, les périphériques IPS, ainsi que les appliances de sécurité de la messagerie et du Web de nouvelle génération. Cisco AMP peut également être installé en tant que logiciel sur des ordinateurs hôtes.

**Autres périphériques de sécurité**: cette catégorie comprend les appliances de sécurité de la messagerie et du Web, les périphériques de déchiffrement, les serveurs de contrôle d'accès client et les systèmes de gestion de la sécurité.

Détecter les attaques en temps réel

Le logiciel n’est pas parfait. Lorsqu’un pirate informatique exploite une faille dans une partie d’un logiciel avant que le créateur n’y remédie, on appelle cela une attaque 0-day. À cause de la complexité et du nombre d’attaques 0-day découvertes aujourd’hui, les attaques de réseau sont de plus en plus souvent réussies et la performance d’une défense est maintenant mesurée selon la promptitude de la réponse du réseau contre une attaque. La capacité de détecter en temps réel les attaques dès qu’elles ont lieu, ainsi que la capacité de les arrêter immédiatement ou quelques minutes après l’événement constituent l’objectif idéal. Malheureusement, de nombreuses entreprises et organisations actuelles ne peuvent détecter les attaques qu’après plusieurs jours, voire même quelques mois, après l’attaque.

* **Analyse en temps réel d'un périphérique à un terminal**: la détection des attaques en temps réel nécessite une analyse active pour identifier les attaques en utilisant le pare-feu et les périphériques réseau IDS/IPS. Il convient d’avoir également recours à la détection de malware client/serveur de nouvelle génération en relation avec des centres internationaux de menaces en ligne. Aujourd’hui, les périphériques et les logiciels d’analyse active doivent détecter les anomalies du réseau en utilisant une analyse contextuelle et une détection de comportement.
* **Attaques DDoS et réponse en temps réel**: l'attaque par déni de service (DDoS) est l'une des menaces d'attaque les plus importantes nécessitant une réponse et une détection en temps réel. Il est extrêmement difficile d’empêcher les attaques DDoS, car elles proviennent de centaines, voire de milliers d’hôtes zombies et elles apparaissent comme du trafic légitime, tel qu’illustré par la figure. Pour de nombreuses entreprises et organisations, les attaques DDoS survenant régulièrement paralysent les serveurs Internet et la disponibilité du réseau. La capacité à détecter et à répondre aux attaques DDoS en temps réel est capitale.

# Se protéger des malwares

Comment luttez-vous contre la présence permanente d’attaques 0-day, ainsi que contre les menaces persistantes avancées (APT) qui volent les données sur de longues périodes ? Utilisez une solution de détection avancée de malware au niveau de l'entreprise qui offre une détection de malware en temps réel est une option.

Les administrateurs réseau doivent constamment surveiller le réseau pour trouver des signes de malware ou de comportements qui révèlent la présence d’une APT. Cisco dispose de la solution Advanced Malware Protection (AMP) Threat Grid qui analyse des millions de fichiers et les fait correspondre par rapport à des centaines de millions d'autres artefacts de malware analysés. Cela offre une vue globale des attaques et campagnes de malware et de leur distribution. AMP est un logiciel client/serveur déployé sur des terminaux d’hôtes, comme un serveur autonome ou sur d’autres périphériques de sécurité du réseau. La figure montre les avantages d'AMP Threat Grid.

Meilleures pratiques de sécurité

De nombreuses organisations nationales et professionnelles ont publié des listes des bonnes pratiques de sécurité. Ci-après une liste de quelques bonnes pratiques de sécurité :

* **Effectuer une évaluation des risques**: connaître la valeur de ce que vous protégez vous aidera à justifier les dépenses liées à la sécurité.
* **Créer une politique de sécurité**: créez une politique qui présente clairement les règles, les postes, les charges et les attentes de l'entreprise.
* **Mesures de sécurité physique**: limitez l'accès aux salles de mise en réseau et aux emplacements des serveurs, et à ce qui implique des mesures d'extinction des incendies.
* **Mesures de sécurité des ressources humaines**: une enquête approfondie doit être faite sur les employés en vérifiant leurs antécédents.
* **Effectuer et tester les sauvegardes**: effectuez régulièrement des sauvegardes et testez la récupération des données à partir des sauvegardes.
* **Maintenir les correctifs de sécurité et les mises à jour**: mettez régulièrement à jour le serveur, le client, ainsi que les systèmes d'exploitation et les programmes des périphériques réseau.
* **Utiliser des contrôles d'accès**: configurez les rôles des utilisateurs et les niveaux de privilège, ainsi qu'une authentification rigoureuse des utilisateurs.
* **Tester régulièrement la réponse en cas d'incident**: employez une équipe responsable de la gestion des incidents et testez les scénarios de réponses urgentes.
* **Implémenter un outil de surveillance, d'analyse et de gestion du réseau**: choisissez une solution de sécurité qui s'intègre avec d'autres technologies.
* **Implémenter des appliances de sécurité du réseau**: utilisez des routeurs, des pare-feu et d'autres appliances de sécurité de nouvelle génération.
* **Implémenter une solution de sécurité complète pour les terminaux**: utilisez des logiciels antimalware et antivirus professionnels.
* **Former les utilisateurs**: formez les utilisateurs et les employés aux procédures sécurisées.
* **Crypter les données**: cryptez toutes les données sensibles de l'entreprise, notamment les e-mails.

Certaines des directives les plus utiles se trouvent dans les archives organisationnelles telles que le centre de ressources de sécurité de l’Institut national des normes et de la technologie (NIST), comme illustré dans la figure.

Le SANS Institute est l’une des organisations pour la formation en cybersécurité les plus connues. Allez [ici](https://www.sans.org/about/) pour en savoir plus sur le SANS Institute et les types de formations et de certifications offerts.

# Botnet

Un botnet est un réseau de zombies connecté à Internet. Un individu ou un groupe malveillant est capable de le contrôler. Un ordinateur robot est généralement infecté en visitant un site Web, en ouvrant une pièce jointe d’un e-mail ou en ouvrant un fichier média infecté.

Un réseau de zombies peut avoir des dizaines de milliers, voire même des centaines de milliers de robots. Ces robots peuvent être activés pour distribuer un malware, pour lancer des attaques DDoS, pour distribuer un pourriel ou pour exécuter une attaque de mot de passe brutale. Les réseaux de zombies sont généralement contrôlés à partir d’un serveur de commande et de contrôle.

Les cybercriminels loueront souvent à des tiers des réseaux de zombies, moyennant des frais, à des fins néfastes.

La figure montre comment un filtre du trafic de botnets est utilisé pour informer la communauté mondiale de sécurité sur les emplacements des réseaux de zombies.

# La chaîne de frappe dans la cyberdéfense

Dans la cybersécurité, la chaîne de frappe est constituée des étapes d’une attaque des systèmes d’information. Développée par Lockheed Martin en tant que cadre de sécurité pour une détection des incidents et une réponse dans ce cas, la chaîne de frappe est composée des étapes suivantes :

**Étape 1. Reconnaissance**: l'agresseur rassemble des informations concernant la cible.

**Étape 2. Préparation**: l'agresseur crée un exploit et une charge utile malveillante à envoyer à la cible.

**Étape 3. Livraison** : l'agresseur envoie l'exploit et la charge utile malveillante à la cible par e-mail ou par une autre méthode.

**Étape 4. Exploitation** : l'exploit est exécuté.

**Étape 5. Installation** : le malware et les portes dérobées sont installés sur la cible.

**Étape 6. Commande et contrôle** : le contrôle à distance de la cible est obtenu via un canal ou par un serveur de commande et de contrôle.

**Étape 7. Action** : l'agresseur effectue des actions malveillantes comme le vol d'information, ou exécute des attaques supplémentaires sur d'autres périphériques depuis l'intérieur du réseau en suivant de nouveau les étapes de la chaîne de frappe.

Pour lutter contre la chaîne de frappe, les défenses de la sécurité du réseau sont conçues sur la base de ses étapes. Voici quelques questions sur les défenses de sécurité d'une entreprise, basées sur la chaîne de frappe :

• Quels sont les indicateurs d’attaque à chaque étape de la chaîne de frappe ?

• Quels outils de sécurité sont nécessaires pour détecter les indicateurs d’attaque à chacune de ces étapes ?

• Y a-t-il des lacunes dans la capacité de l'entreprise à détecter une attaque ?

D'après Lockheed Martin, comprendre les étapes de la chaîne de frappe a permis de mettre en place des obstacles défensifs, de ralentir l'attaque et de finalement prévenir la perte de données La figure montre comment chaque étape de la chaîne de frappe correspond à une augmentation dans le niveau d’effort et le coût pour bloquer les attaques et y remédier.

Sécurité comportementale

La sécurité basée sur le comportement est une forme de détection des menaces qui ne dépend pas de signatures malveillantes connues, mais utilise plutôt un contexte informationnel pour détecter les anomalies dans le réseau. La détection basée sur le comportement implique la capture et l’analyse du flux de communication entre un utilisateur sur le réseau local et une destination locale ou distante. Lorsqu'elles sont capturées et analysées, ces communications révèlent le contexte et les modèles de comportement qui peuvent être utilisés pour détecter les anomalies. La détection basée sur le comportement peut découvrir la présence d’une attaque par une modification du comportement normal.

* **Honeypots** : un honeypot est un outil de détection basée sur le comportement qui appâte d'abord l'agresseur en attirant son modèle prévu de comportement malveillant, puis, lorsque le pirate se trouve dans le honeypot, l'administrateur réseau peut capturer, enregistrer et analyser son comportement. Ce honeypot permet à un administrateur d’obtenir plus de connaissances et d’élaborer une meilleure défense.
* **Architecture de solutions de protection contre les cyberattaques de Cisco** : il s'agit d'une architecture de sécurité qui utilise la détection basée sur le comportement et les indicateurs pour offrir une meilleure visibilité, un meilleur contexte et un meilleur contrôle. L’objectif consiste à découvrir qui lance l’attaque, de quoi il s’agit, à quel moment elle survient et de quelle manière. Cette architecture de sécurité utilise de nombreuses technologies de sécurité pour atteindre cet objectif.

# NetFlow

La technologie NetFlow est utilisée pour rassembler des informations relatives au flux de données à travers un réseau. Les informations NetFlow peuvent être assimilées à une facture de téléphone pour votre trafic réseau. Elles vous montrent qui et quels périphériques sont dans votre réseau, et quand et comment les utilisateurs et les périphériques y ont accédé. NetFlow est un composant important dans la détection et l’analyse basées sur le comportement. Les commutateurs, les routeurs et les pare-feu équipés de NetFlow rapportent des informations sur les données qui entrent sur le réseau, qui en sortent et qui le traversent. Les informations sont envoyées à NetFlow Collectors qui collecte, stocke et analyse les enregistrements NetFlow.

NetFlow est capable de collecter des informations sur l’utilisation via différentes caractéristiques sur la manière dont les données sont déplacées dans le réseau, tel qu’illustré par la figure. En recueillant des informations sur les flux de données du réseau, NetFlow est capable d’établir une référence sur les comportements sur plus de 90 attributs différents.

# CSIRT

De nombreuses grandes organisations ont une équipe responsable de la gestion des incidents en matière de sécurité informatique (CSIRT) pour recevoir, examiner et répondre aux rapports d’incidents de sécurité informatique, tel qu’illustré dans la Figure 1. La mission principale d’une CSIRT est d’aider à garantir la protection de l’entreprise, de son système et de ses données en effectuant des enquêtes approfondies sur les incidents de sécurité informatique. Pour empêcher les incidents de sécurité, Cisco CSIRT offre une évaluation proactive des menaces, une planification de mesures d’atténuation, une analyse des tendances d’incidents, ainsi qu’un examen de l’architecture de sécurité, tel qu’illustré dans la Figure 2.

La CSIRT de Cisco collabore avec le Forum pour les équipes de sécurité et de gestion des incidents (FIRST), le NSIE (National Safety Information Exchange), le DSIE (Defense Security Information Exchange) et le Centre d’analyse et de recherche pour les opérations DNS (DNS-OARC, DNS Operations Analysis and Research Center).

Il existe des organisations CSIRT nationales et publiques comme la Division CERT de l’Institut de génie logiciel de l’Université Carnegie Mellon, qui sont là pour aider les organisations et les CSIRT nationales à élaborer, à exploiter et à améliorer leurs capacités de gestion des incidents.

Guide sur la sécurité

La technologie est en évolution permanente. Cela implique que les cyberattaques évoluent également. De nouvelles vulnérabilités et méthodes d’attaque sont découvertes continuellement. La sécurité devient une préoccupation importante des entreprises à cause de la réputation qui en résulte et de l’impact financier provenant des brèches dans la sécurité. Les attaques ciblent des réseaux critiques et des données sensibles. Les entreprises devront avoir des plans pour anticiper les failles, les gérer et reprendre leurs activités.

L’une des meilleures méthodes pour se préparer contre une brèche dans la sécurité est de l’empêcher. Il doit y avoir des conseils sur l’identification du risque de cybersécurité pour les systèmes, les ressources, les données et les capacités, mais également sur la protection du système par la mise en œuvre de protection et de formation du personnel et sur la détection d’événements de cybersécurité dès que possible. Lorsqu'une brèche dans la sécurité est détectée, des mesures appropriées doivent être prises pour minimiser son impact et ses dégâts. Le plan de réponse doit être flexible, avec plusieurs options d'action pendant la brèche. Après que la brèche est maîtrisée et que les systèmes et services compromis sont restaurés, les mesures et processus de sécurité devront être mis à jour pour inclure les leçons apprises durant la brèche.

Toutes ces informations doivent être compilées dans un guide sur la sécurité, soit un ensemble de demandes reproductibles (rapports) comparées à des sources de données d'événements de sécurité qui conduisent à la détection d'un incident et à la réponse appropriée. Le guide sur la sécurité doit, de préférence, réaliser les actions suivantes :

* Détecter les machines infectées par les malwares
* Détecter les activités suspectes dans le réseau
* Détecter les tentatives irrégulières d'authentification
* Décrire et comprendre le trafic entrant et sortant
* Fournir des informations récapitulatives, dont les tendances, les statistiques et les décomptes
* Offrir des statistiques et des mesures utilisables et faciles d'accès
* Faire correspondre les événements avec toutes les sources de données pertinentes

Outils pour la prévention et la détection des incidents

Voici quelques-uns des outils utilisés pour détecter et empêcher les incidents de sécurité :

* **SIEM**: un système de gestion des événements et des informations de sécurité (SIEM) est un logiciel qui collecte et analyse les alertes et les registres de sécurité, ainsi que d'autres données historiques et en temps réel provenant des périphériques sur le réseau.
* **DLP**: un logiciel de prévention des pertes de données (DLP) est un logiciel ou un système matériel conçu pour éviter le vol de données sensibles ou la fuite de ces données d'un réseau. Un système DLP peut se concentrer sur l’autorisation d’accès aux fichiers, l’échange de données, la copie des données, la surveillance des activités de l’utilisateur, et bien plus encore. Les systèmes DLP sont conçus pour surveiller et protéger les données en trois états différents : les données en cours d’utilisation, les données en cours de transfert et les données au repos. Les données en cours d’utilisation sont axées sur le client, celles en cours de transfert se réfèrent aux données transitant à travers le réseau, tandis que les données au repos désignent le stockage des données.
* **Cisco ISE et TrustSec** : Cisco ISE (Identity Services Engine) et Cisco TrustSec renforcent l'accès aux ressources réseau en créant des politiques de contrôle d'accès basé sur le rôle qui segmentent l'accès au réseau (invités, utilisateurs mobiles, employés) sans complexité supplémentaire. La classification du trafic est basée sur l’identité de l’utilisateur ou du périphérique. Cliquez sur Lire dans la figure pour en savoir plus sur ISE.
* Cliquez [ici](https://contenthub.netacad.com/legacy/I2CS/2.1/fr/course/files/4.3.3.1%20Video%20-%20Fundamentals%20of%20ISE.pdf) pour lire la transcription de cette vidéo.

# DS et IPS

Un système de détection d’intrusion (IDS), illustré dans la figure, est un périphérique réseau dédié ou l’un des nombreux outils dans le serveur ou dans le pare-feu qui analyse les données par rapport à une base de données de règles ou de signatures d’attaque pour détecter un trafic malveillant. Si une correspondance est détectée, l’IDS enregistrera la détection et enverra une alerte à un administrateur réseau. Le système de détection d’intrusion n’intervient pas lorsqu’une correspondance est détectée, c’est-à-dire qu’il n’empêche pas la survenue d’une attaque. La fonction de l’IDS est simplement de détecter, d’enregistrer et de rapporter.

L’analyse effectuée par l’IDS ralentit le réseau (ralentissement appelé latence). Pour éviter le retard du réseau, un IDS est habituellement mis offline, séparé du trafic réseau normal. Les données sont copiées ou mises en miroir par un commutateur, puis envoyées à l’IDS pour une détection offline. Il y a également les outils IDS qui peuvent être installés en avant d’un système d’exploitation d’un ordinateur hôte, comme Linux ou Windows.

Un système de prévention des intrusions (IPS) dispose de la capacité de bloquer ou de refuser un trafic selon une règle positive et une correspondance de signature. Snort est l’un des systèmes IPS/IDS les plus connus. La version commerciale de Snort appartient à la filiale Sourcefire de Cisco. Sourcefire est capable d’effectuer une analyse en temps réel du trafic et des ports, une ouverture de session, une recherche et une mise en correspondance de contenus. Cet outil peut également détecter les sondes, les attaques et les balayages de ports. Sourcefire s’intègre également à d’autres outils tiers pour la création de rapport et pour l’analyse des performances et des enregistrements.

# Conclusion

Le début de ce chapitre a commencé par présenter certaines technologies et certains processus utilisés par les professionnels de la cybersécurité pour protéger le réseau, l'équipement et les données d'une entreprise. Ceux-ci comprennent les types de pare-feu, d'appliances de sécurité et de logiciel.

Il a également traité les réseaux de zombies, la chaîne de frappe, la sécurité basée sur le comportement et l’utilisation de NetFlow pour surveiller un réseau.

Enfin, l’approche de Cisco en matière de cybersécurité, notamment l’équipe CSIRT et le guide sur la sécurité y ont été expliqués. Ce chapitre traite aussi, brièvement, des outils que les professionnels de la cybersécurité utilisent pour détecter et empêcher les attaques réseau, notamment SIEM, DLP, Cisco ISE et TrustSec, ainsi que des systèmes IDS et IPS.

Si vous souhaitez découvrir plus en détail les concepts de ce chapitre, référez-vous à la page des [ressources et activités supplémentaires](https://contenthub.netacad.com/legacy/I2CS/2.1/fr/course/files/IntroCybersecurity%20-%20Additional%20Resources%20and%20Activities.pdf) dans les Ressources des étudiants.