Module 1 – Fondamentaux techniques et règlementaires

Fondamentaux de la sécurité des SI et réseaux

Séquence 3 : Architecture et équipements de sécurité

OIDANEOS

Présentation de la séquence
Objectifs et notions abordées

Découvrir le rôle et les interactions des firewalls, antivirus, IDS/IPS, VPN

- Les principes d'architecture de sécurité
- Les équipements pour la protection des réseaux
- La protection des terminaux
- L'analyse, la gestion et l'orchestration
- Les composants cloud et les accès distants

Les principes d’architecture de sécurité

Les principes d'architecture de sécurité

Les niveaux d'abstraction de l'architecture

Architecture conceptuelle	Offre une vue d'ensemble et se concentre sur la structure globale et les principes clés sans entrer dans les détails techniques
Architecture logique	Décompose les composants conceptuels en services spécifiques comme l'authentification, le chiffrement et l'autorisation
Architecture physique	Décrit la mise en œuvre réelle avec du matériel, des logiciels et des configurations

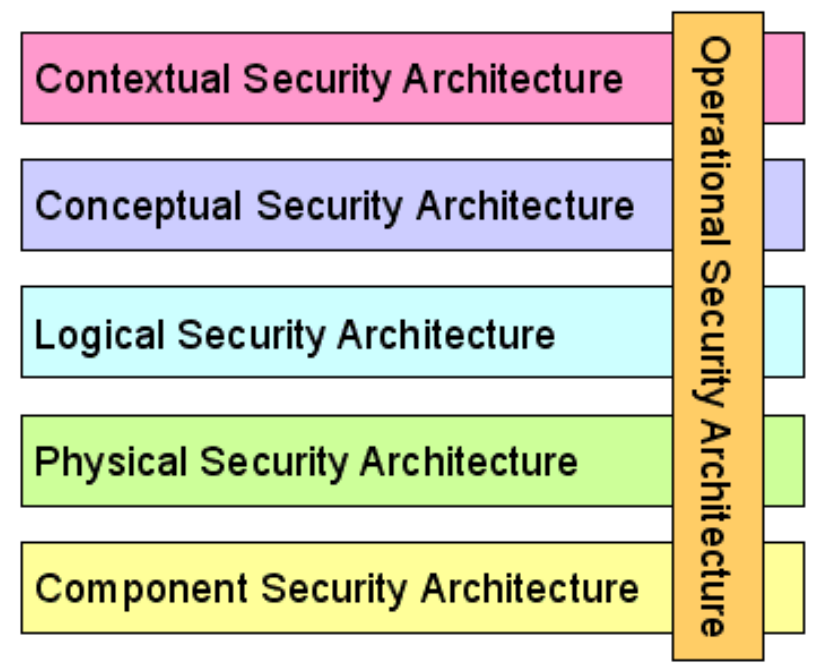
Les principes d'architecture de sécurité

Les principes fondamentaux de conception

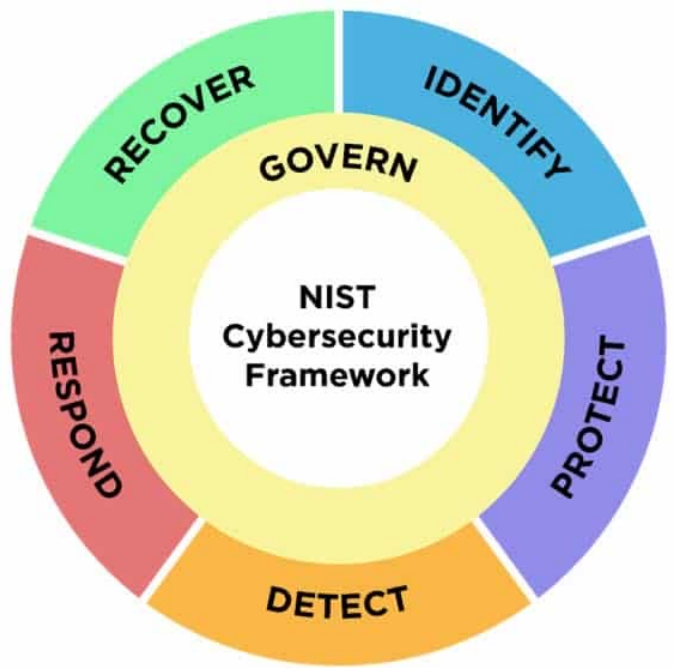
- Principe du moindre privilège
- La défense en profondeur
- Le « Secure By Default »
- Le Zero Trust
- La séparation des tâches
- L'échec sécurisé

Les principes d'architecture de sécurité

Les modèles et cadres de référence



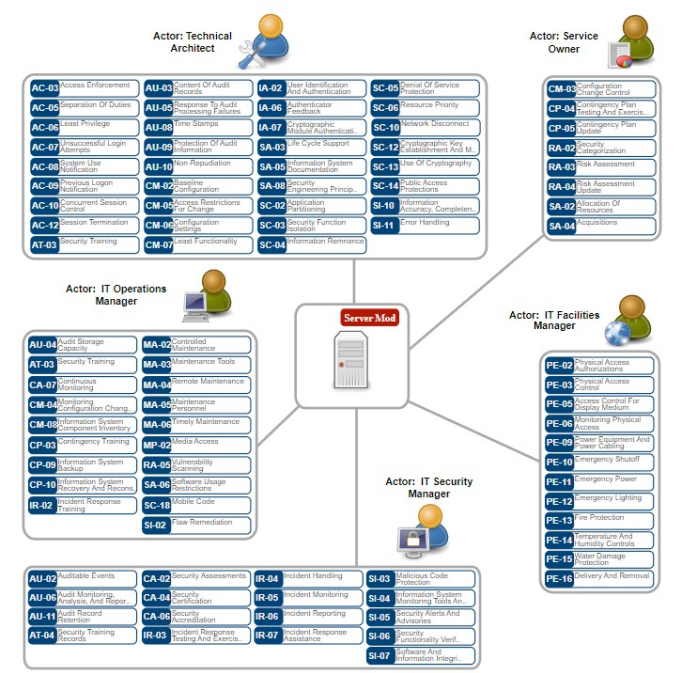
SABSA



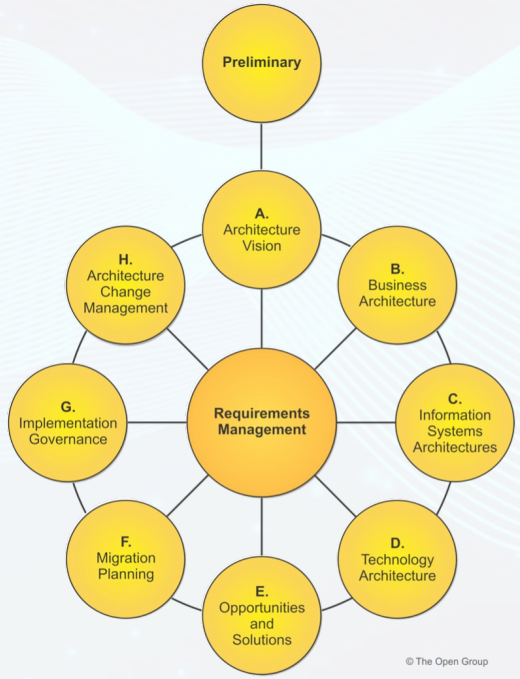
NIST CSF

Les principes d'architecture de sécurité

Les modèles et cadres de référence



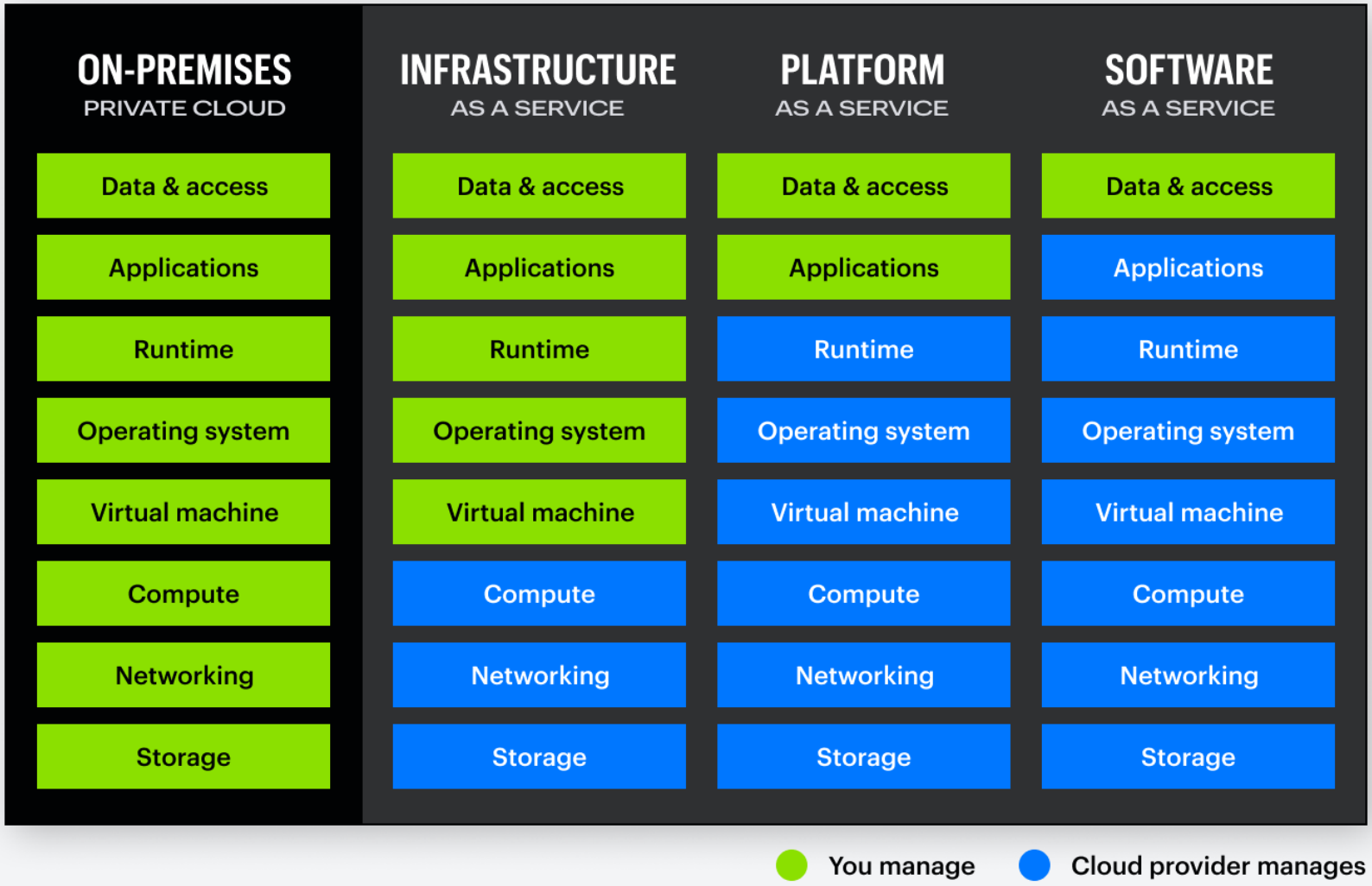
OSA



TOGAF

Les principes d'architecture de sécurité

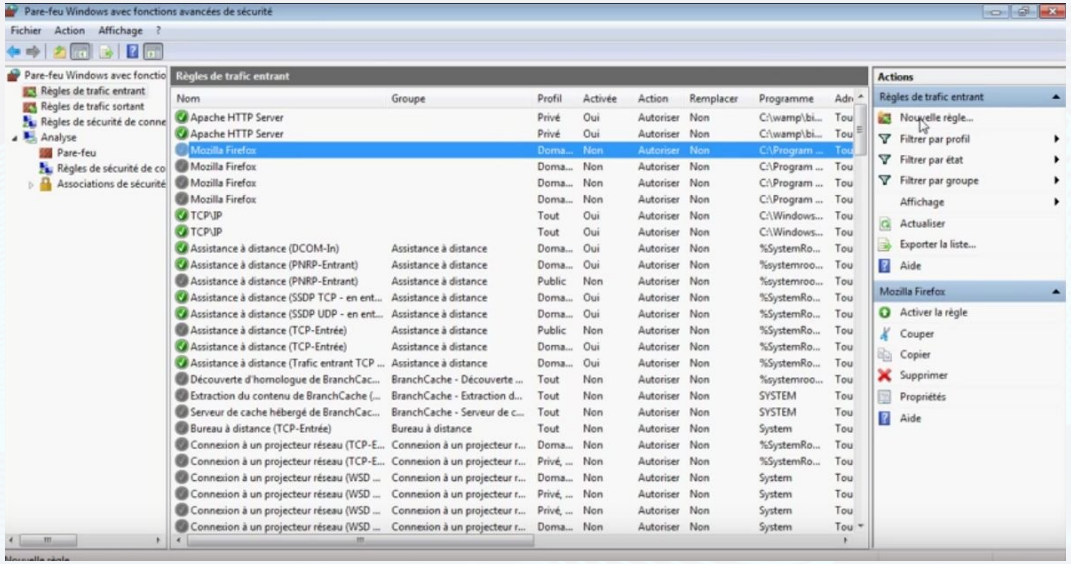
La responsabilité partagée



Les équipements pour la protection des réseaux

Les équipements pour la protection réseau

Le pare-feu : types et format



Pare-feu matériel

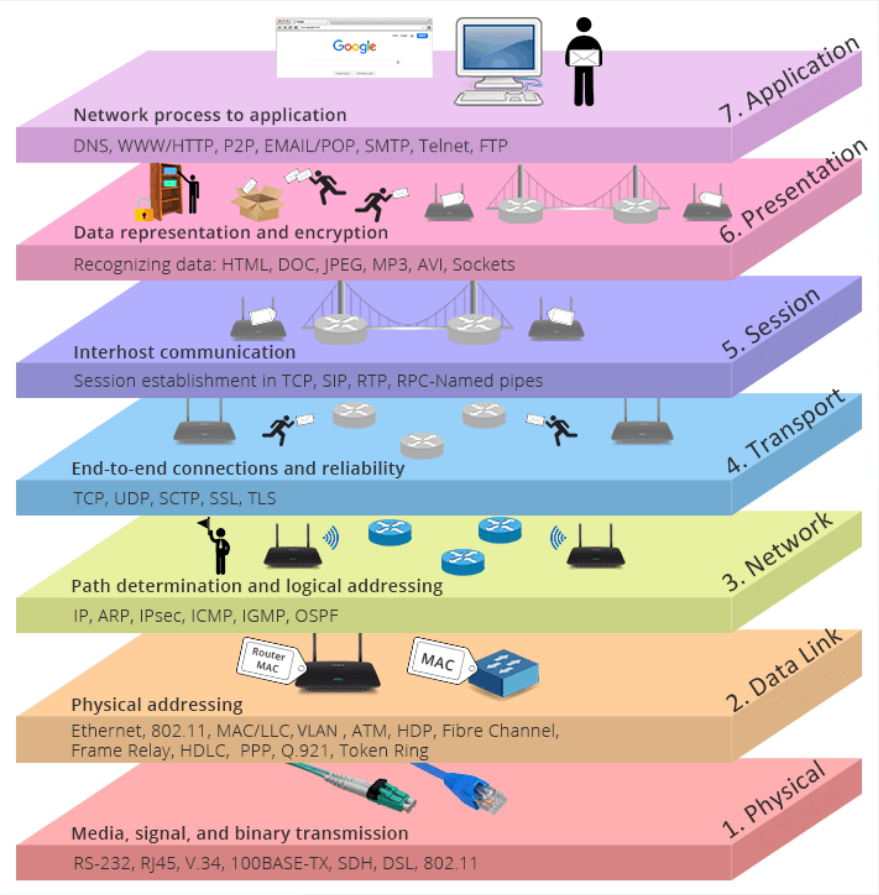
- Équipement autonome ou intégré à un routeur
- Privilégié pour les grandes entreprises

Pare-feu logiciel

- Installé sur un ordinateur ou un serveur.
- Filtre le trafic spécifiquement pour la machine sur laquelle il réside.
- Plus facile à configurer et idéal pour un usage personnel

Les équipements pour la protection réseau

Le pare-feu : technologies et niveau d'inspection



Pare-feu applicatif (couche 7)

Passerelles de niveau circuit (couche 5)

Filtrage de paquets (couche 3 et 4)

Inspection multicouche avec état (Stateful Inspection)

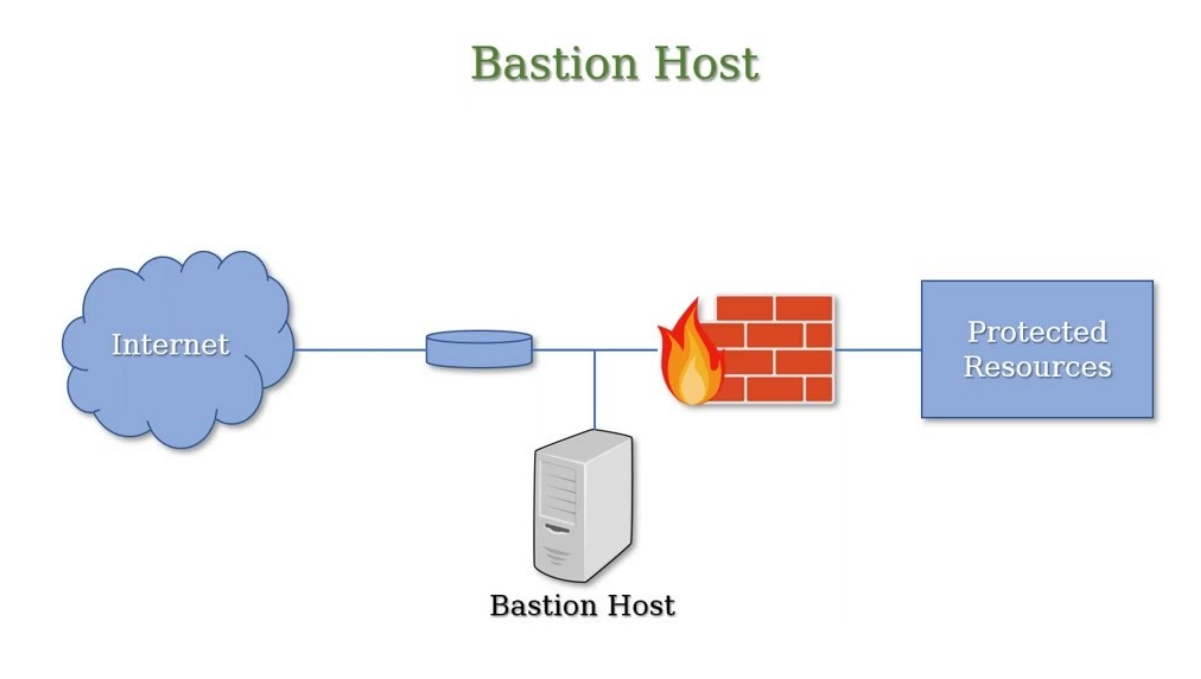
Les équipements pour la protection réseau

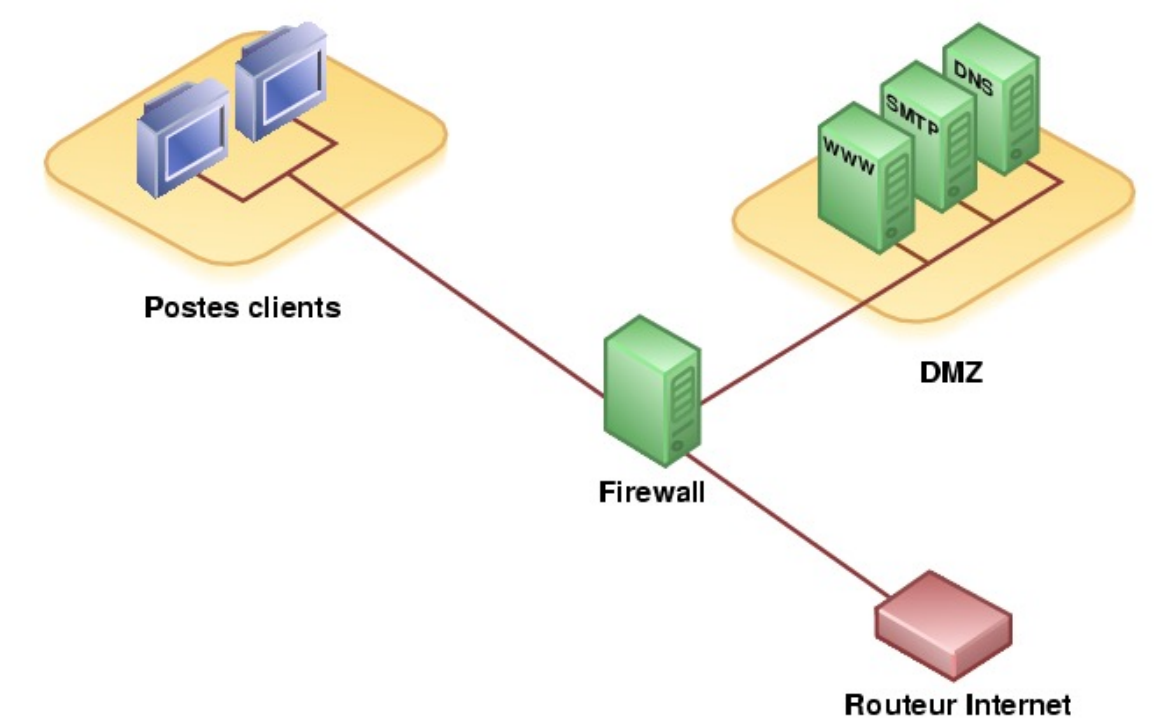
Le pare-feu : fonctions et services principaux

- Contrôle d’accès
- Routage et NAT
- Journalisation et alertes
- Services additionnels

Les équipements pour la protection réseau

Le pare-feu : architectures de déploiement





Les équipements pour la protection réseau
IDS : principes et types

Système de gestion de la sécurité qui rassemble et analyse les informations d'un ordinateur ou d'un réseau pour identifier des violations de politiques de sécurité.

Network IDS (NIDS)	Host IDS (HIDS)
• Surveille tout le trafic réseau en analysant chaque paquet (en-têtes IP/TCP et données applicatives) à la recherche d'anomalies. • Il est généralement installé **en parallèle** du flux (via une duplication des paquets), ce qui signifie qu'il n'interrompt pas directement le trafic.	• Installé directement sur un hôte (serveur ou poste de travail), il analyse les logs d'audit, les applications et les modifications de fichiers. • Il est particulièrement efficace pour détecter les menaces internes et les changements non autorisés sur le système.

Les équipements pour la protection réseau

IDS : méthodes de détection

- Reconnaissance de signature
- Détection d'anomalies
- Anomalie de protocole

Les équipements pour la protection réseau
IPS : principes et types

L'IPS est une évolution de l'IDS, développée pour pallier l'insuffisance d'une simple alerte. Sa caractéristique majeure est qu'il est installé en ligne (in-line) par rapport au flux de trafic, lui permettant de bloquer ou d'arrêter le trafic malveillant en temps réel.

Content-based IPS	Rate-based IPS
• Inspecte le contenu des paquets à la recherche de signatures spécifiques pour rejeter les entrées malveillantes connues.	• Surveille les taux de trafic pour prévenir les attaques DoS et DDoS en comparant les statistiques en temps réel avec des seuils prédéfinis.

Les équipements pour la protection réseau

IDS/IPS : fonctionnement interne et flux d'information

Les équipements pour la protection réseau
Comparatif IDS/IPS

Caractéristique	IDS	IPS
Positionnement	Passif (en parallèle)	Actif (en ligne / in-line)
Action	Réactif (alerte)	Proactif (bloque le trafic)
Faux Positifs	Tolérables (génèrent de la fatigue d'alerte)	Critiques (peuvent bloquer du trafic légitime, créant un DoS)

Les équipements pour la protection réseau
Les passerelles Web sécurisées

Solution de sécurité critique conçue pour protéger les sessions web des utilisateurs contre les cybermenaces.

- Filtrage d'URL
- Décryptage SSL
- Contrôle des applications
- Détection et prévention des menaces

- Sécurité du périmètre dans l'architecture réseau
- Intégration dans le modèle SASE

La protection des terminaux (endpoints)

La protection des terminaux
Les antivirus

Programme installé sur des ordinateurs ou des appareils mobiles pour empêcher leur infection par des logiciels malveillants. Initialement créés pour détecter et supprimer les virus informatiques, ils luttent désormais contre tous les types de malwares.

Détection basée sur la signature

Analyse heuristique

La protection des terminaux
Les antivirus nouvelle génération (NGAV)

Analyse comportementale

Établissement d'une base de référence

Protection contre les attaques sophistiquées

Technologies spécifiques :

- Prévention par injection de mémoire
- Blocage des LOLBins
- Technologie de déception

La protection des terminaux
Les EDR (Endpoint Detection and Response)

Introduite en 2013, cette technologie est conçue pour surveiller en permanence les terminaux (ordinateurs, serveurs, etc.) afin de détecter et de répondre aux cybermenaces telles que les ransomwares et les malwares

La protection des terminaux
Les EDR (Endpoint Detection and Response)

- Analyse comportementale
- Visibilité en temps réel
- Gestion des alertes
- Remédiation rapide
- Threat hunting

La protection des terminaux
Le MDM (Mobile Device Management)

Solution logicielle permettant l'administration et la sécurisation des appareils mobiles tels que les smartphones, les tablettes et les ordinateurs portables au sein d'une organisation

- Gestion de la sécurité
- Contrôle à distance
- Gestion des applications
- Contrôle matériel
- Inventaire

La protection des terminaux
Le MDM (Mobile Device Management)

Modèle	Description	Avantages	Inconvénients
BYOD (Bring Your Own Device)	L'employé utilise son appareil personnel pour le travail	Réduction des coûts, satisfaction de l'employé	Risques de sécurité accrus, problèmes de confidentialité
CYOD (Choose Your Own Device)	L'entreprise propose une liste d'appareils approuvés au choix de l'employé	Meilleur contrôle, standardisation du matériel	Coût initial plus élevé, choix limité pour l'employé
COPE (Corporate Owned Personally Enabled)	L'entreprise fournit l'appareil mais autorise l'usage personnel	Équilibre entre contrôle et flexibilité	Problèmes potentiels de vie privée (surveillance de l'usage perso)
COBO (Corporate Owned Business Only)	L'appareil appartient à l'entreprise et est réservé strictement au travail	Modèle le plus sûr, séparation totale des données	Satisfaction limitée des employés, faible flexibilité

L’analyse, la gestion et l’orchestration

L’analyse, la gestion et l’orchestration
Le SIEM (Security Information and Event Management)

Le SIEM (Security Information and Event Management) est une solution de gestion de la sécurité qui combine deux fonctions essentielles : le SEM (Security Event Management), qui gère les événements en temps réel, et le SIM (Security Information Management), qui s'occupe de la collecte, de l'analyse et du rapport de données historiques

- Agrégation et consolidation de données
- Détection des menaces
- Corrélation des événements
- Investigation informatique

L’analyse, la gestion et l’orchestration

Le SIEM (Security Information and Event Management)

Avantages	Limites
• Efficacité opérationnelle	• Fatigue d’alerte
• Prévention et hiérarchisation	• Temps de latence
• Réduction des coûts	• Complexité des données

L’analyse, la gestion et l’orchestration

Le SOAR (Security Orchestration, Automation and Response)

Le SOAR (Security Orchestration, Automation and Response) est une plateforme ou un ensemble de logiciels conçus pour renforcer le niveau de cybersécurité d'une entreprise en automatisant et en orchestrant les réponses aux incidents.

- Orchestration
- Automatisation
- Intervention
- Intégration

L'analyse, la gestion et l'orchestration

Le SOAR (Security Orchestration, Automation and Response)

Playbook

Hiérarchiser et normaliser

Réduire l'écart de connaissances

L'analyse, la gestion et l'orchestration

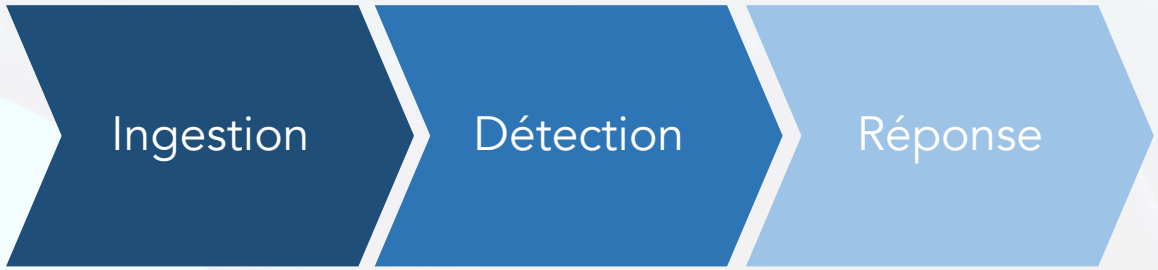
Le SOAR (Security Orchestration, Automation and Response)

Nécessite d'avoir un niveau de maturité élevé en matière de sécurité

- Gestion du volume
- Machine Learning
- Efficacité

L'analyse, la gestion et l'orchestration
Le XDR (Extended Detection and Response)

Plateforme unifiée de détection d'incidents de sécurité et de réponse.
Il collecte et corrèle automatiquement les données provenant de plusieurs composants de sécurité propriétaires pour offrir une vision globale



- Visibilité unifiée
- Productivité accrue
- Analyse avancée

Les composants cloud et les accès distants

Les composants cloud et les accès distants

Le CASB (Cloud Access Security Broker)

Solution logicielle stratégique conçue pour sécuriser l'utilisation des services cloud au sein d'une organisation. Selon les sources, il agit comme un point de contrôle intermédiaire entre les utilisateurs et les applications cloud

Visibilité et contrôle du SaaS

Protection contre la perte de données (DLP)

Application des politiques d'accès

Les composants cloud et les accès distants

Le ZTNA (Zero Trust Network Access)

Solution de sécurité moderne qui régit l'accès aux applications d'une organisation en appliquant les principes du modèle "Zero Trust" (confiance zéro).

Absence de confiance implicite	Applications cachées	Vérification continue	Accès granulaire

Les composants cloud et les accès distants
Le SASE (Secure Access Service Edge)

Architecture de sécurité conçue par Gartner qui combine plusieurs composants de sécurité et de réseau distincts en une solution unique, intégrée et basée sur le Cloud

Architecture « Cloud native »

Réseau

Sécurité

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Firewall as a Service (FWaaS)
- Zero Trust Network Access (ZTNA)
- Data Loss Prevention (DLP)

Les composants cloud et les accès distants

Le SASE (Secure Access Service Edge)

Avantages	Inconvénients
• Réduction de la complexité et des coûts	• Points de défaillance unique
• Amélioration des performances	• Dépendance vis-à-vis du fournisseur
• Évolutivité et agilité	• Investissement initial
• Visibilité accrue	