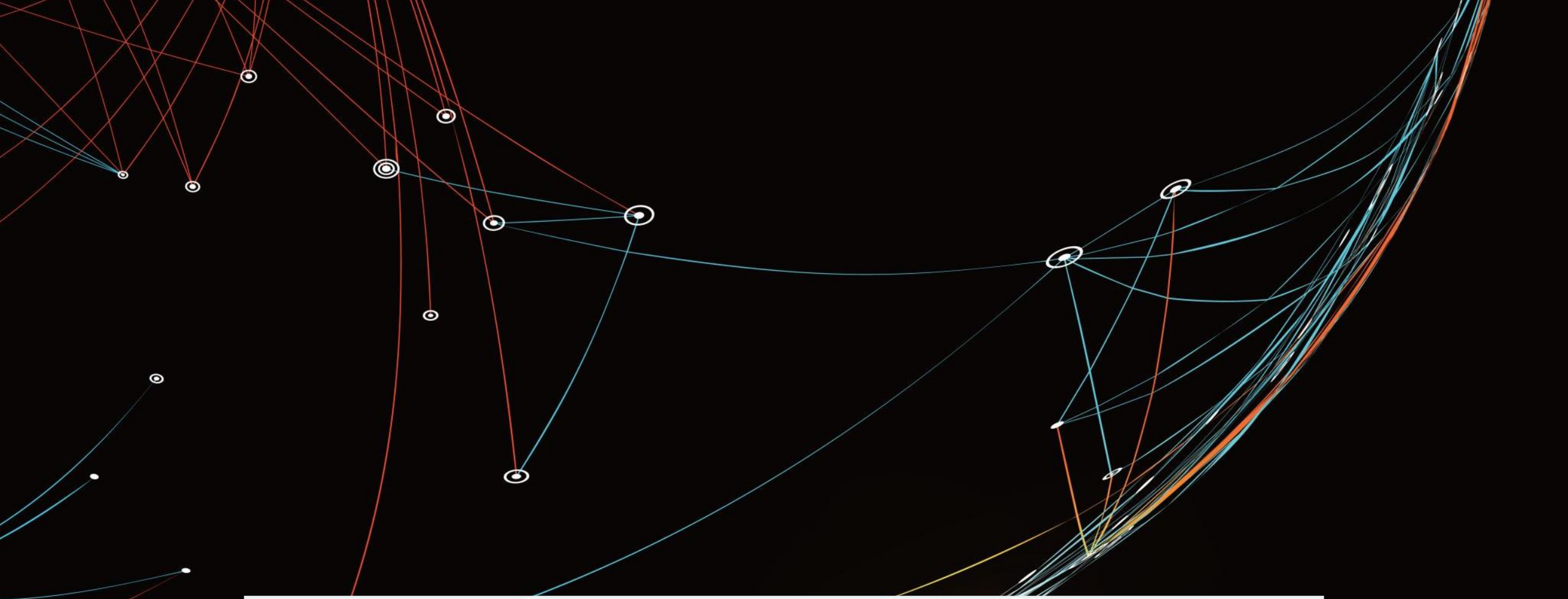


Sécurité Réseau

Louis ANEST GRIT 2019 24/01/2022

Programme

- Qu'est-ce que la sécurité ?
- Un peu d'histoire et quelques chiffres
- Panorama de la sécurité
- Solutions uniformisées ou granulaires ?
- L'avènement des instances virtualisées
- Périmètres abordés
- Choisir et dimensionner une solution
- Mise en place
- Croissance d'une infrastructure
- Fortinet & FortiGate
- Cybersécurité

Qu’est-ce que la sécurité informatique ?

- La sécurité informatique consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes.
- Ne prends pas en compte que le hardware et le Software
- La donnée au centre de la sécurité

traceability

La donnée au centre de la sécurité

- Availability :
  - La donnée est accessible le plus de temps possible
- Integrity :
  - Pas de modifications non autorisée ou non détectée
- Confidentiality :
  - L'accès à la donnée est restreint aux utilisateurs habilités

Avec les Nouvelles problématiques se rajoutent :

- Reliability :
  - L'infrastructure est sécurisée et tolérante aux pannes et sécurisée
- Traceability:
  - Les accès a la donnée sont tracés
- Non Repudiation :
  - Chaque interaction est enregistrée de manière claire et irréfutable

Quelques Dates…

- 1982 : Introduction par les services secrets américains d'un bug dans le logiciel Canadien de gestion du gazoduc transsibérien,
- 1986 : The Brain, premier Virus Informatique,
- 1988 : Internet Worm : premier ver informatique qui se propagea aux Etats-Unis. Apparition des CERT en Réaction,
- 1990s Emergence de la culture cybersécurité, du Hacking,
  - 1990 : Premier Virus Polymoprhe,
  - 1995 : Premier Macro-Virus.

Quelques Dates…

- 2000s : Démocratisation du hacking.
  - 2000 : premier Ddos Médiatisé
  - 2001 : code red cause 2 Milliard de dollars dommages avec 350 000 serveurs infectés
  - 2005 : Apparition de PoisonIvy, un RAT encore utilisé aujourd'hui ciblant les industries chimiques et de la défense.
- 2010s Avènement des Ransomwares
  - 2010 Stuxnet
  - 2016 TeslaCrypt & CryptXXX
  - 2017 Wannacry

Quelques Faits…

- Objets connectés : intelligents et donc vulnérables on estime qu'il y aura 75B objets connectés en 2025 (x3 par rapport a 2019)
- Les fournisseurs d'accès à Internet (FAI) aux Etats-Unis peuvent maintenant vendre l'historique de navigation des internautes sans leur consentement
- WannaCry & Petya ont fait des ravages, apparition de Ransomware As A Service
- Recrudescences de violations de données de grande ampleur
- Densification des attaques qui se font de plus en plus entreprenantes et complexes

Quelques Chiffres…

- 22% nombre d'entreprises estimant leurs données protégées
- Plus de 90% des centres médicaux ont subis au moins une brèche de données ces dernières années
- Augmentation du nombre d’attaque de 400% dues a la crise sanitaire
- + 50% de perte financière des entreprises françaises due aux cyberattaques
- + 10 % de budget investit dans la cybersécurité
- + 9 % de cyberattaques
- coût des cyberattaques par an, à presque doublé en 4 ans pour les entreprises françaises (3,7M € actuellement)
- 6 milliards c'est le nombre d'individus attaqués d'ici 2022

Quelques Chiffres…

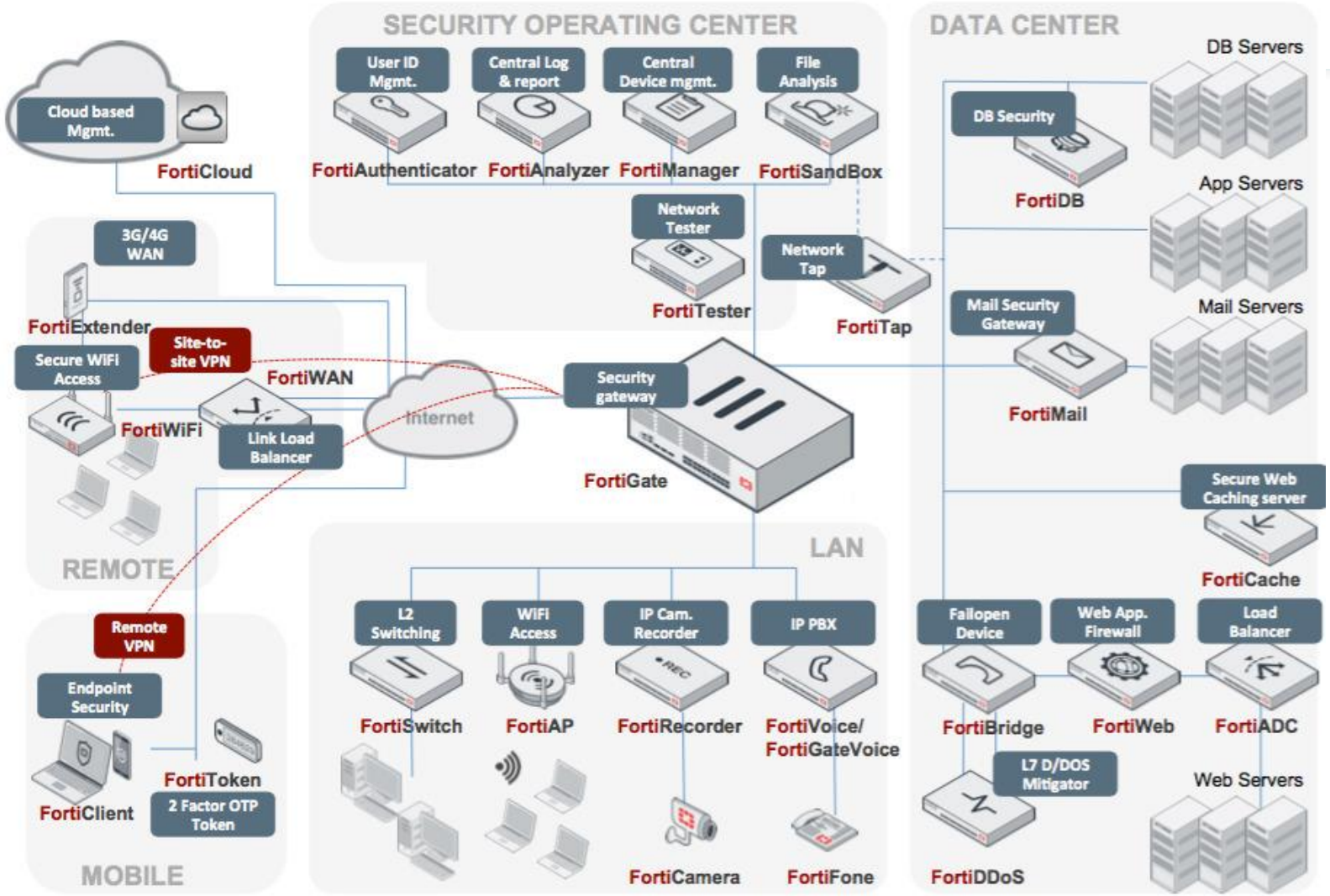
- Les acteurs de la menace :
  - 92% Externe à l'entreprise
  - 6% Interne à l'entreprise
  - < 1 % Partenaires

- Les motivations des attaques :
  - 59% Financière
  - 38 % Espionnage

- Les données compromises :
  - 47% des données personnelles
  - 26% des données confidentielles
  - 22 % des données internes
  - 17 % des références, diplômes, certificats, brevets …

Panorama de la sécurité

Panorama de la sécurité



Solutions uniformisées ou granulaires ?

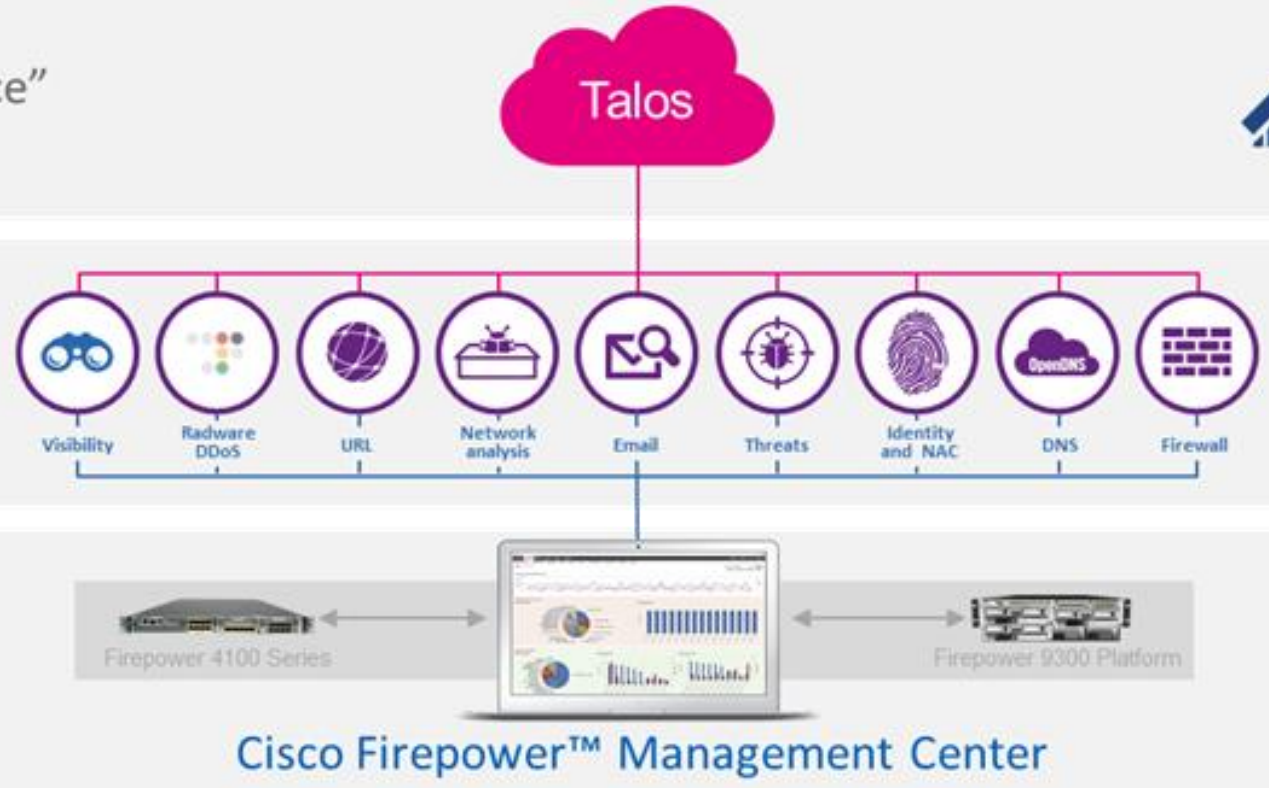
- Idée d'infrastructure granulaire plus ancienne, relative aux constructeurs étant pure player de leurs domaines.
- Solutions uniformisées apparaissent avec les gros constructeurs tels que Cisco ou Fortinet.
- Solutions uniformisées plus efficaces et facile a maintenir.
- Solutions granulaires plus sécurisées et tolérantes aux failles.

Cisco et Talos

"Shared Security intelligence"

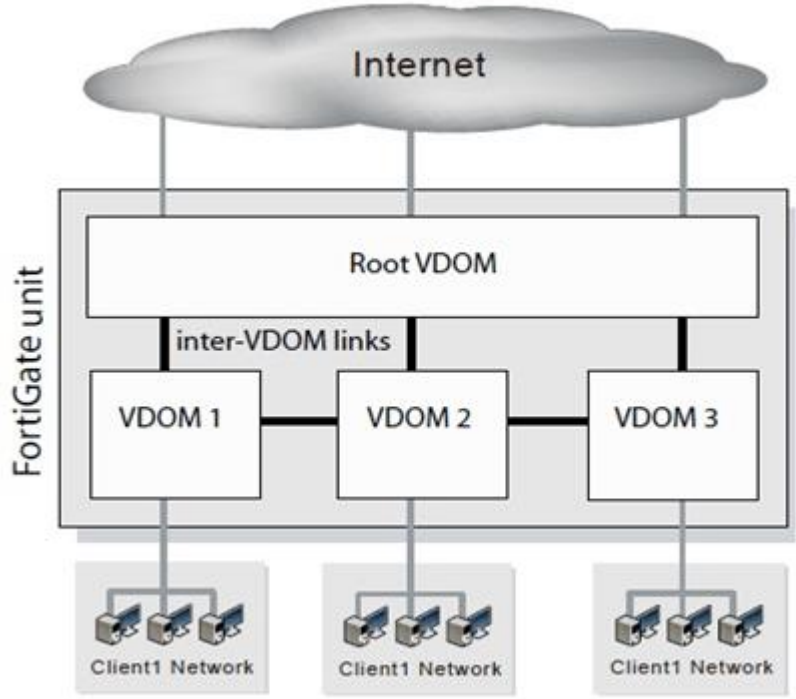
Globalisation
Contextualisation

Pilotage Centralisé
Confinement automatisé

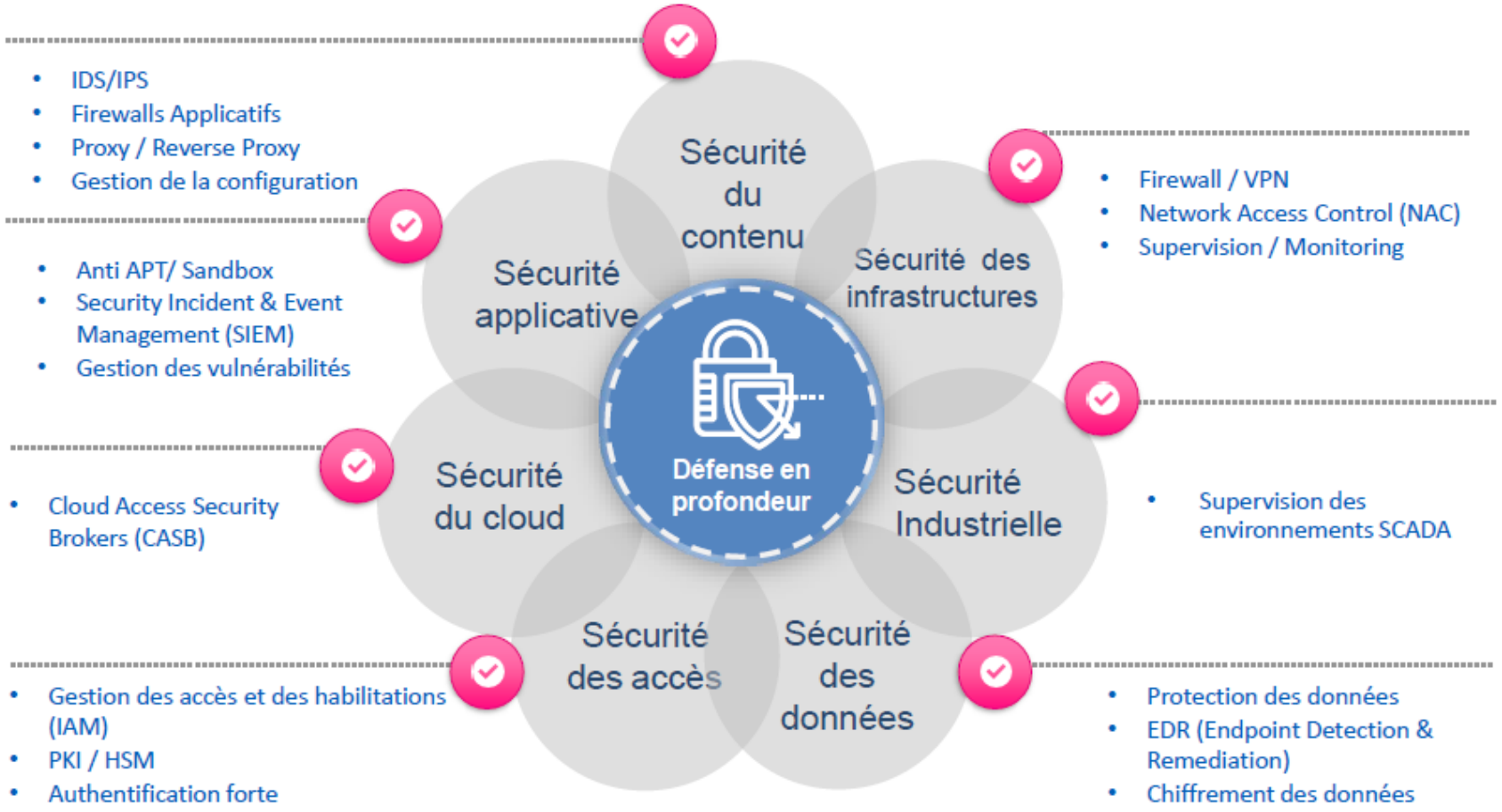


Les instances Virtualisées

- Minimisation des coûts
- Evolution de la VRF
- Scalable dans les limites du Hardware
- Deviens rapidement la norme
- Change des architectures classiques
- Surdimensionnement du Hardware nécessaire



Solutions


Sécurité du contenu
Sécurité applicative
Sécurité des infrastructures
Sécurité du cloud
Défense en profondeur
Sécurité Industrielle
Sécurité des accès
Sécurité des données
IDS/IPS
Firewalls Applicatifs
Proxy / Reverse Proxy
Gestion de la configuration
Anti APT/ Sandbox
Security Incident & Event Management (SIEM)
Gestion des vulnérabilités
Firewall / VPN
Network Access Control (NAC)
Supervision / Monitoring
Cloud Access Security Brokers (CASB)
Supervision des environnements SCADA
Gestion des accès et des habilitations (IAM)
PKI / HSM
Authentification forte
Protection des données
EDR (Endpoint Detection & Remediation)
Chiffrement des données

Sécurité du Contenu

- **Intrusion Detection System/Intrusion Prevention System**
  - Analyse et compare le trafic a une base de donnée connue
- **Firewall Applicatif (WAF)**
  - Firewall mis en avant d'une application pour contrôler les données des paquets reçus et la protéger des attaques
- **Proxy/Reverse Proxy**
  - Mécanisme d'intermédiaire captant tout le trafic entrant (Proxy Inverse) ou sortant (Proxy)
- **Gestion de Configuration**
  - Gestionnaire de version de configuration, sauvegardes et déploiement automatisé

Sécurité des Infrastructures

Identity Services Engine

- **Firewall et VPN**
  - Organe de sécurité central du réseau permettant une segmentation du réseau et du trafic sécurisé. Gestion des accès nomade
  - Différence entre Firewall et NGFW (Next-Gen Firewall)
- **Network Access Control**
  - Système de contrôle d'accès au réseau permettant d'attribuer des permissions dynamiques en fonction des attributs réseau
- **Supervision et Monitoring**
  - Solutions de supervision temps réel de l'infrastructure

Sécurité Industrielle

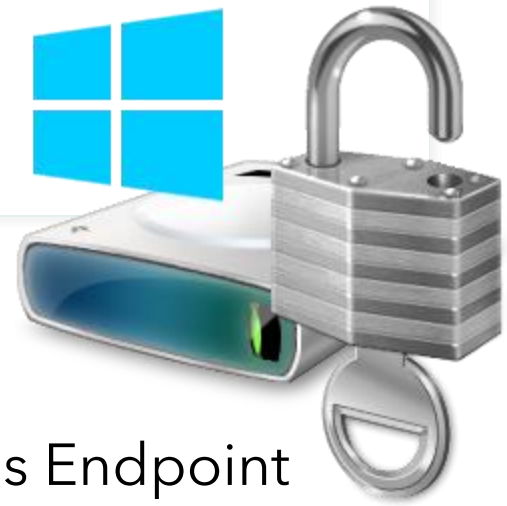
sentryo
CYBERSECURITY FOR THE INDUSTRIAL INTERNET

- La sécurité industrielle a des contraintes très différentes des environnements bureautique
- On ne peux pas bloquer de trafic en industriel et un reboot ou arrêt des systèmes est inenvisageable hors des périodes de maintenance
- Certains constructeurs proposent des Appliance durcies et conçues pour des environnement industriels

SIEMENS

Schneider Electric

Sécurité des Données



- **EPP / EDR**
  - EPP : Endpoint Protection Platform, Système de protection des Endpoint « classique » avec Antivirus, Protection Web etc…
  - EDR : Endpoint Detection & Remediation, nouveaux systèmes permettant de détecter les comportements suspects avant une attaque.
- **Chiffrement & Protection des données**
  - Chiffrement du disque, protection des données via segmentation des droits et GPO. Validités de celles-ci Via certificats

kaspersky

Sécurité des Accès

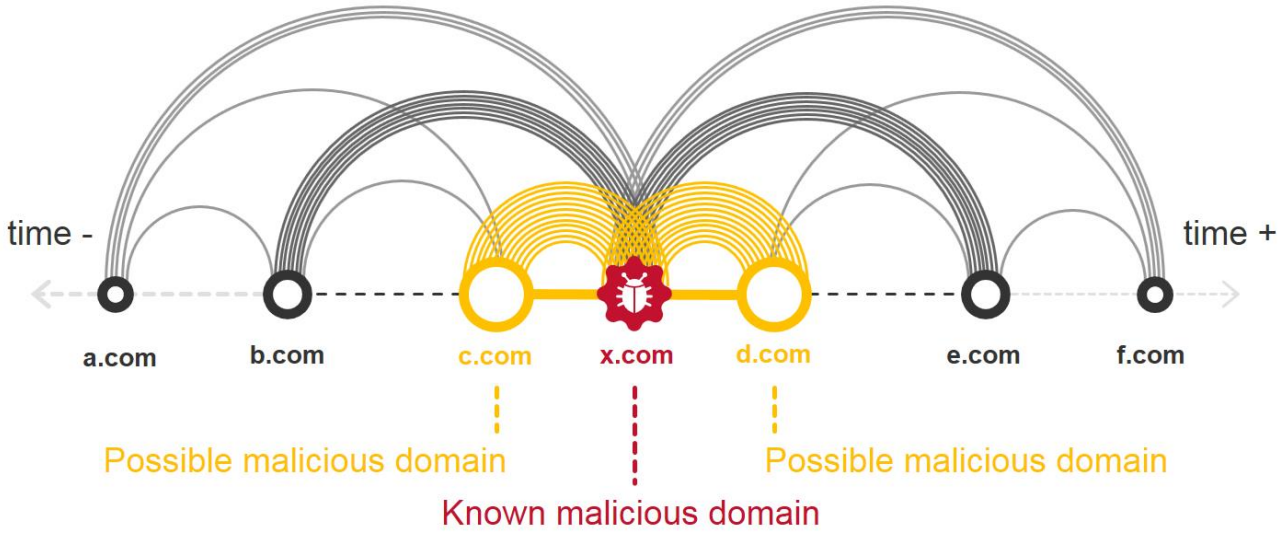
- **IAM : Identity and Access Management**
  - Gestion des habilitations des utilisateurs, que ce soit mot de passe, accès logiciels, annuaires…
- **HSM : Hardware Security Module**
  - « boite noire » du réseau gérant les clés cryptographiques
- **Authentification Forte**
  - Multiplication des moyens d'authentification pour renforcer la sécurité des connexion utilisateurs

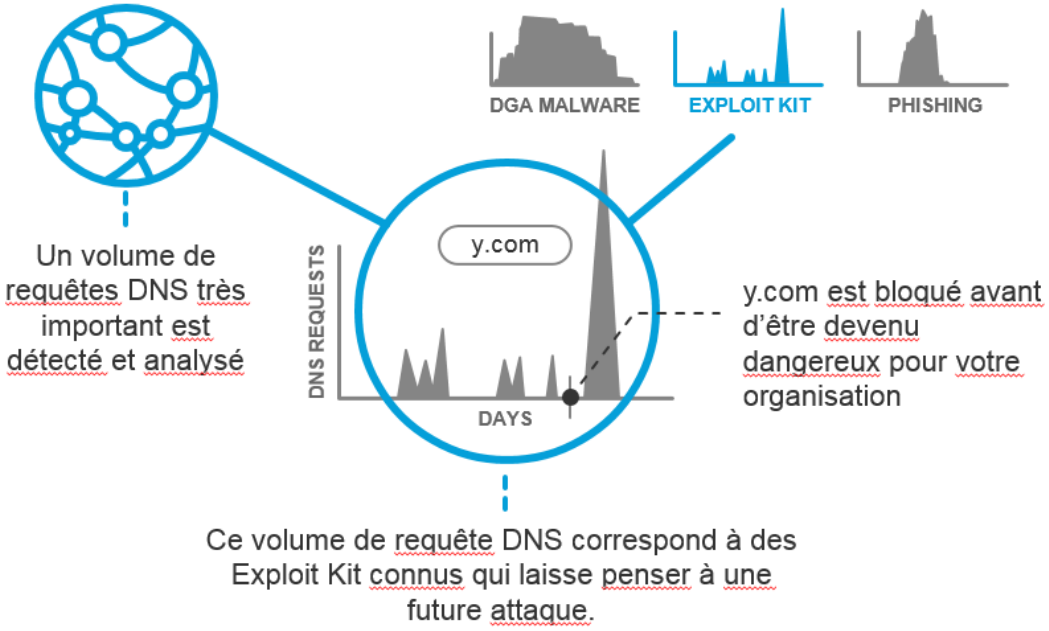
Sécurité du Cloud

- **Cloud Access Security Broker**
  - Solution de Broker se plaçant entre les utilisateur et les services cloud. Applique des politiques de sécurité et monitore l'activité utilisateur.
  - Avertis les administrateurs en cas d'activité suspectes

Sécurité Applicative

- Anti APT
  - Enregistrement des Attaques APT mondiales et analyse prédictives des variations de celles-ci

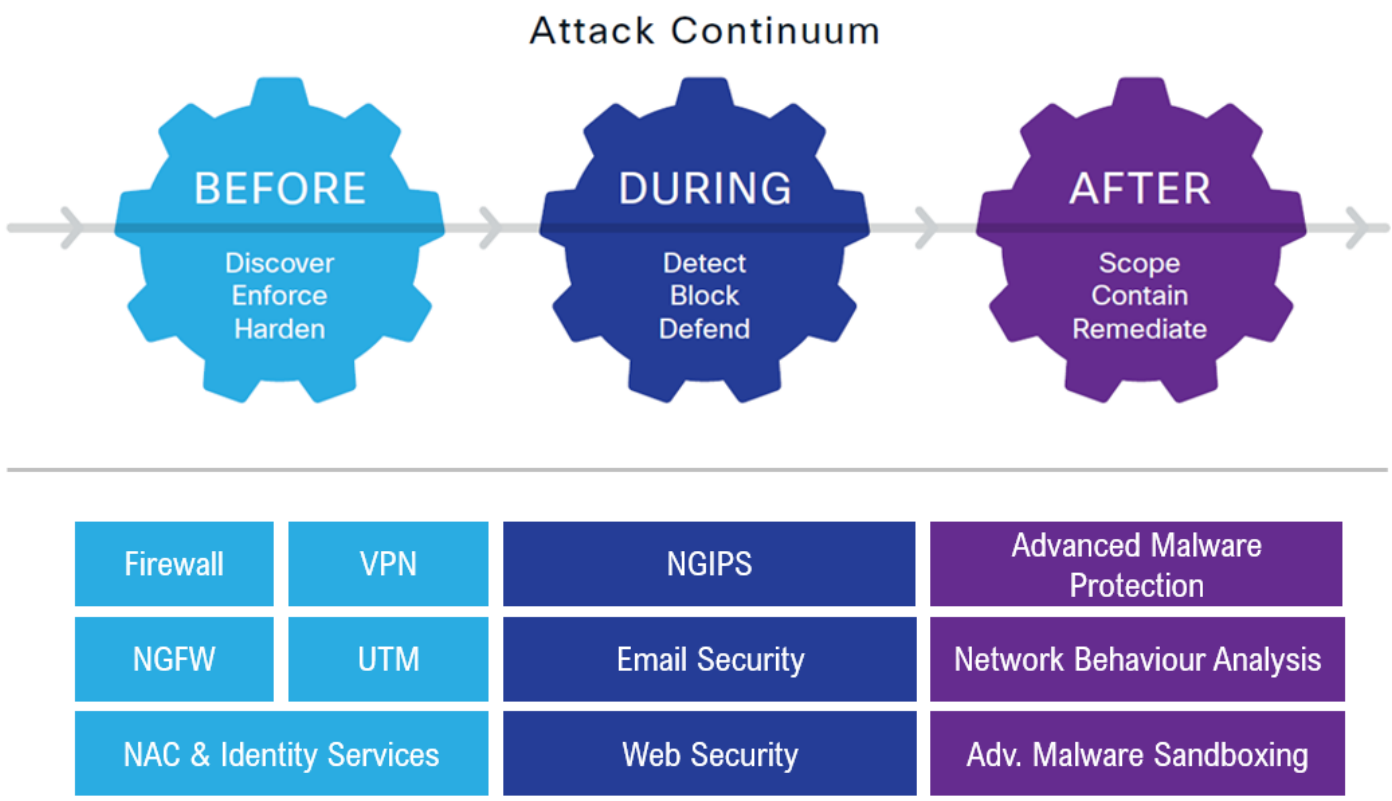


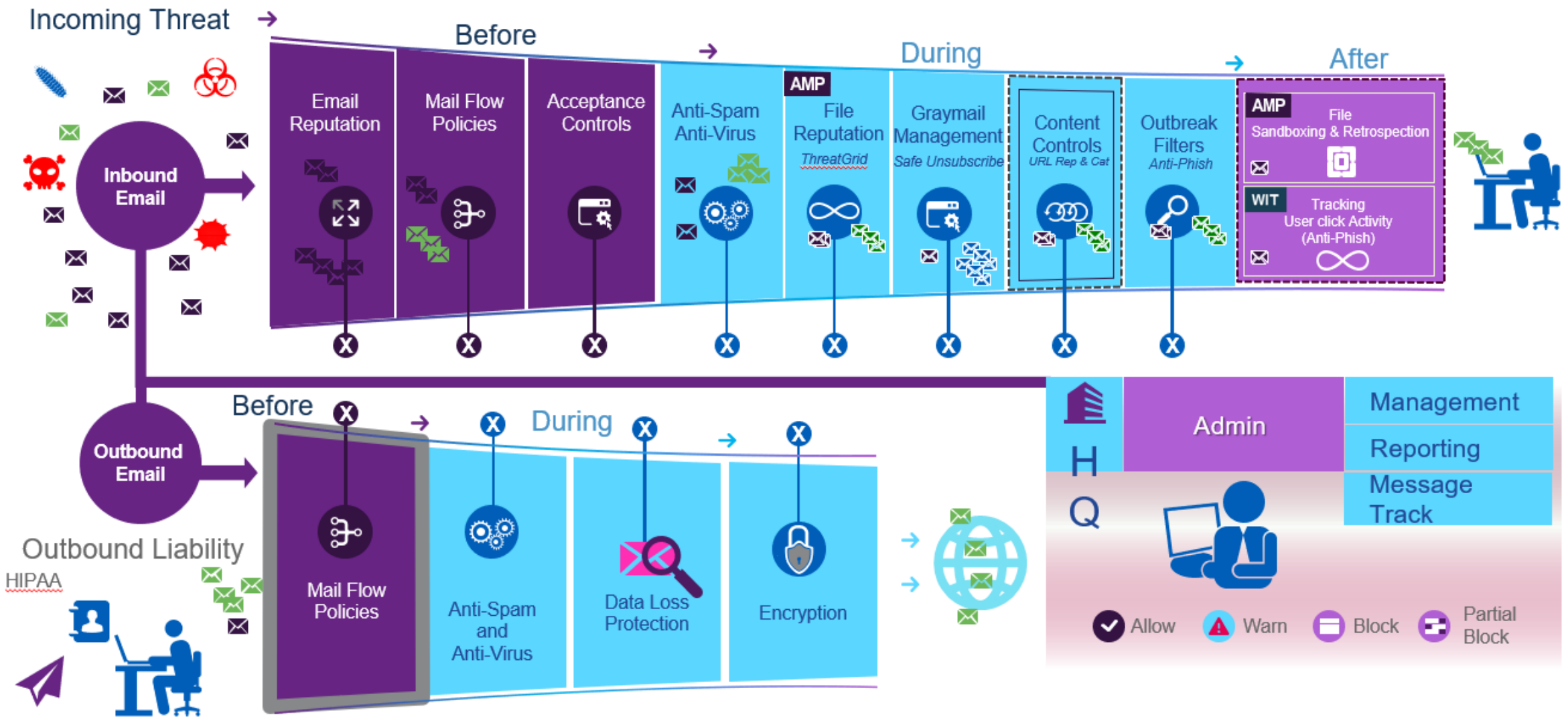


Siem & Vulnerability Management

- Security Incident & Event Manager
  - Enregistrement des évènements et synthèse des différentes menaces de l'infrastructure gérée.
- Vulnerability management
  - Scans de vulnérabilité et aide a la priorisation des menaces

Le continuum d'une attaque




Incoming Threat
Before
During
After
Inbound Email
Email Reputation
Mail Flow Policies
Acceptance Controls
Anti-Spam Anti-Virus
AMP
File Reputation
ThreatGrid
Graymail Management
Safe Unsubscribe
Content Controls
URL Rep & Cat
Outbreak Filters
Anti-Phish
AMP
File Sandboxing & Retrospection
WIT
Tracking User click Activity (Anti-Phish)
Outbound Email
Before
During
Outbound Liability
HIPAA
Mail Flow Policies
Anti-Spam and Anti-Virus
Data Loss Protection
Encryption
HQ
Admin
Management
Reporting
Message Track
Allow
Warn
Block
Partial Block

Choisir et dimensionner ses solutions

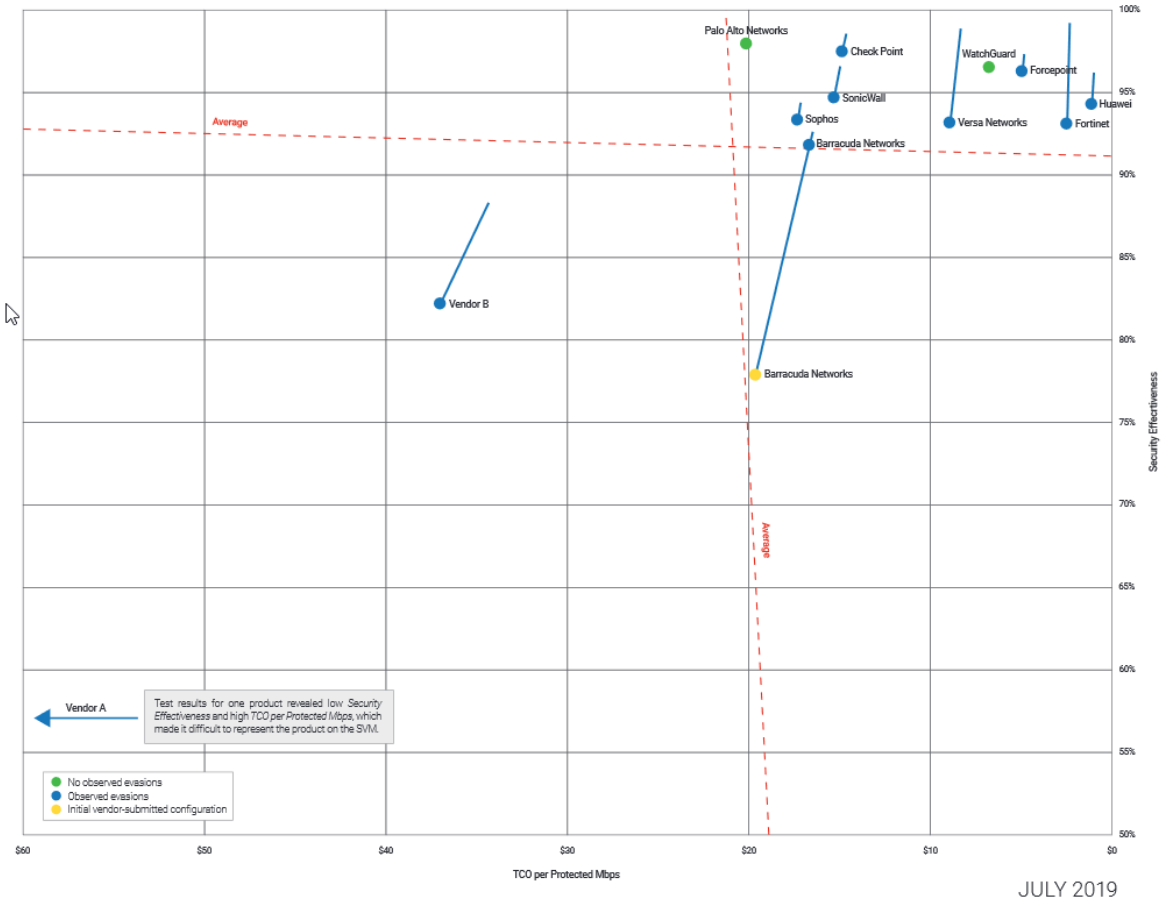
- Besoins spécifiques
- Usages
- Evolutivité
- Gartner magic Quadrant
- NSS Labs
- Support Associé
- Sizing Guides
- Prix

Gartner®

NSS LABS

Gartner Magic Quadrant

NSS Labs



Vendor	Block Rate	Evasions	Stability and Reliability	Security Effectiveness
Barracuda Networks	92.7%	99%	100%	91.7%
Check Point Software Technologies	98.4%	99%	100%	97.4%
Forcepoint	97.2%	99%	100%	96.2%
Fortinet	99.0%	94%	100%	93.0%
Huawei	96.2%	98%	100%	94.2%
Palo Alto Networks	97.9%	100%	100%	97.9%
SonicWall	97.6%	97%	100%	94.7%
Sophos	94.2%	99%	100%	93.3%
Versa Networks	99.0%	94%	100%	93.1%
WatchGuard	96.5%	100%	100%	96.5%
Vendor A	98.3%	79%	100%	77.7%
Vendor B	88.4%	93%	100%	82.2%

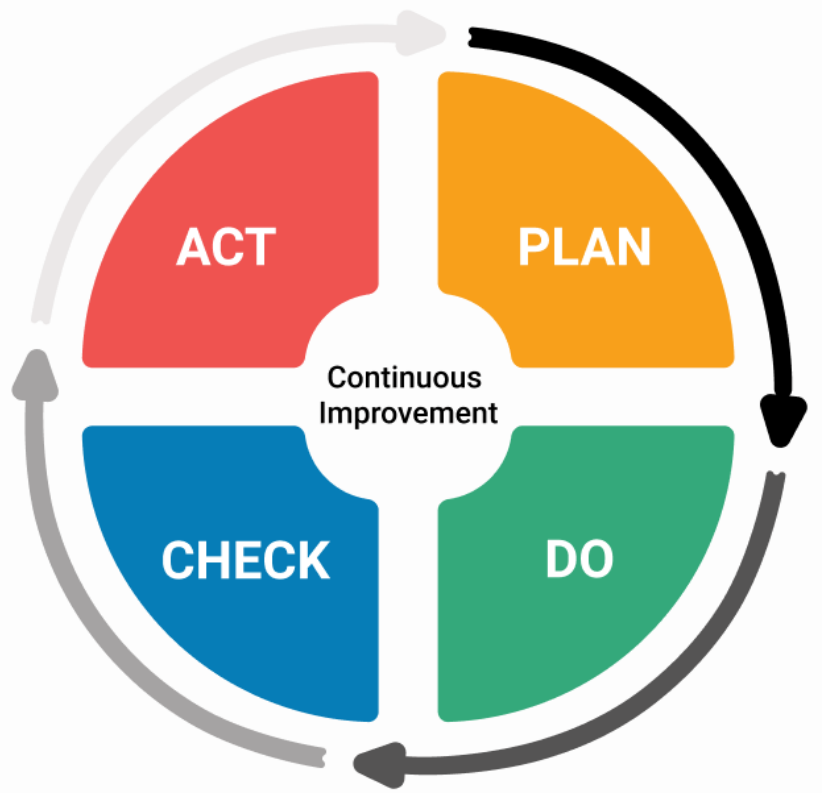
JULY 2019

Sizing Guides

Users	FortiGate Unit	Models	Interface	Threat Protection Throughput	Other Comments
1-10	Fortigate 30E	FG-30E	5xGE	Max 40-50Mbps	
		FWF-30	5XGE		
5-30	FortiGate 50E	FG-50E	7xGE	Max 100Mbps	This unit has higher latency than 60E, Less packets per second
		FWF-50E	7xGE		
		FWF-50E-2R	7xGE		
		FG-51E	7xGE		Includes 32Gb Storage
10-40	Fortigate 60E	FG-60E	10xGE	150-180Mbps	
		FG-61E	10xGE		Includes 128Gb SSD
		FWF-60E	10xGE		
		FWF-61E	10xGE		Includes 128Gb SSD
		FG-60E-DSL	9GE + 1 inbuild xDSL modem		Inbuilt DSL Modem
		FWF-60E-DSL	9GE + 1 inbuild xDSL modem		Inbuilt DSL Modem
40-80	Fortigate 80E	FG-80E	14GE - 2x shared copper/fiber	150-200Mbps	
		FG-81E	14GE - 2x shared copper/fiber		Includes 128Gb SSD
80-180	Fortigate 100E	FG-100E	18GE - 2x shared Copper/fiber	200-250Mbps	
		FG-101E	18GE - 2x shared Copper/fiber		Includes 480Gb SSD

Mise en place d'un projet de sécurité

- Modèle PDCA
  - Plan : Etude
  - Do : Réalisation
  - Check : Recette, Contrôle
  - Act : SAV, maintenance

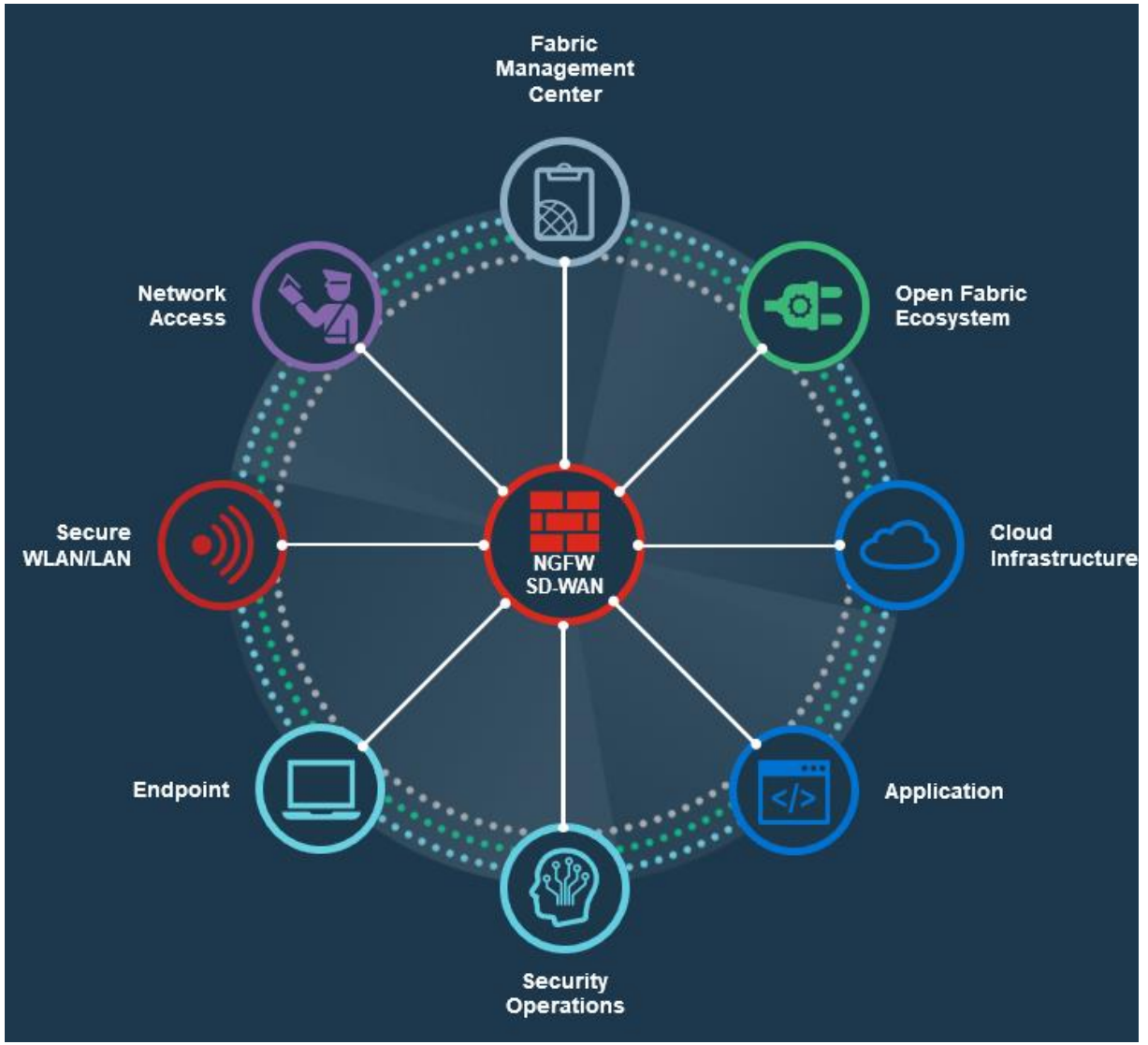


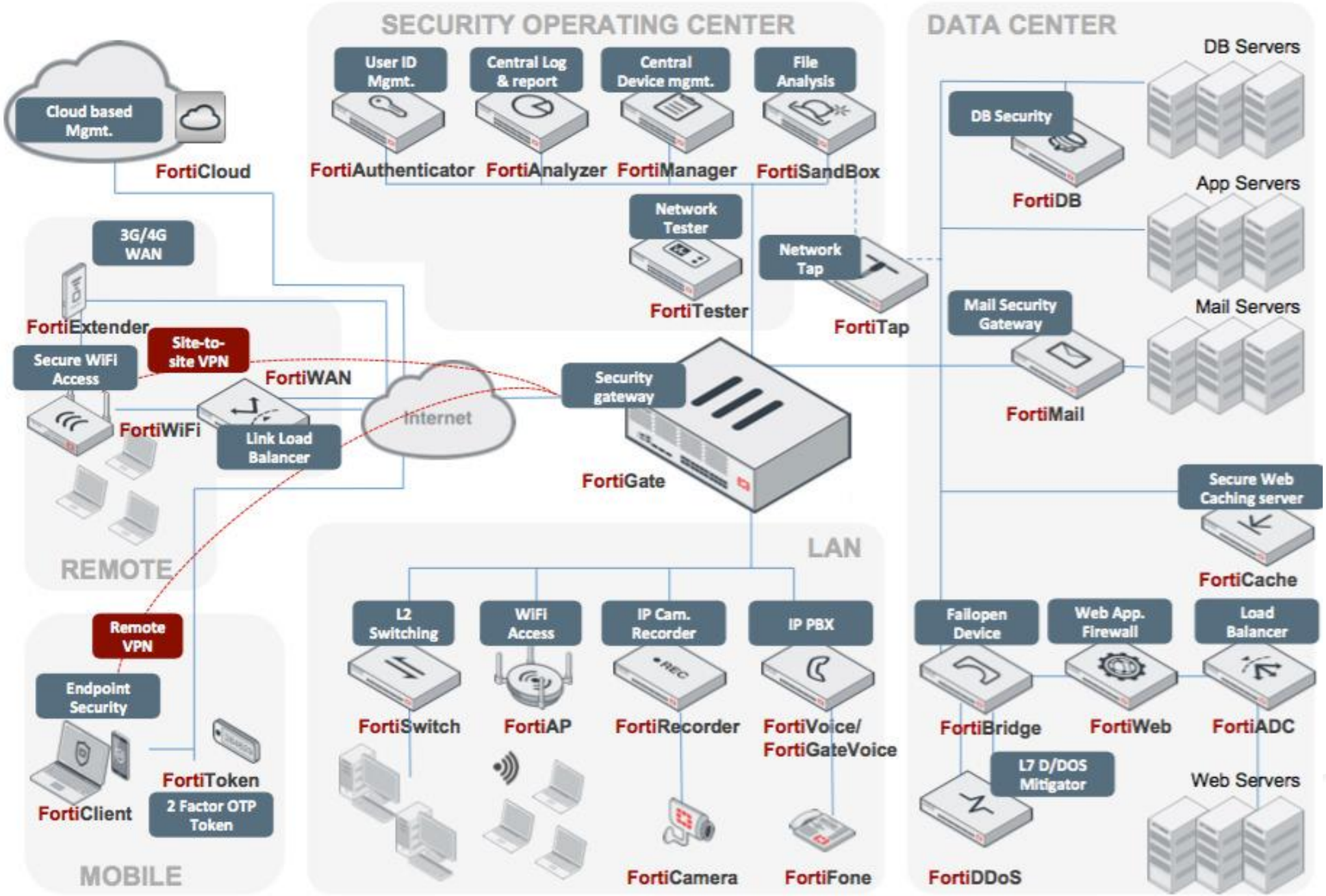
Projet type

- Etude
  - Planification matérielle, des ressources
  - Evaluation des risques
- Réunion de lancement
  - Validation de l'étude avec le Client
- Réalisation
  - Réunions Jalons le cas échéant
- Réunion de clôture.

Fortinet & Fortigate

- Entreprise crée en 2000
- PDG : Ken Xie
- CA : 1,8 Milliard de Dollars (2018)
- Historiquement constructeur de Firewall : Fortigate
- Solutions de sécurité et d'exploitation réseau complète




SECURITY OPERATING CENTER
DATA CENTER
LAN
REMOTE
MOBILE
Cloud based Mgmt.
FortiCloud
User ID Mgmt.
Central Log & report
Central Device mgmt.
File Analysis
FortiAuthenticator
FortiAnalyzer
FortiManager
FortiSandBox
Network Tester
FortiTester
Network Tap
FortiTap
DB Servers
DB Security
FortiDB
App Servers
Mail Security Gateway
FortiMail
Mail Servers
3G/4G WAN
FortiExtender
Secure WiFi Access
Site-to-site VPN
FortiWAN
FortiWiFi
Link Load Balancer
Internet
Security gateway
FortiGate
Secure Web Caching server
FortiCache
L2 Switching
WiFi Access
IP Cam. Recorder
IP PBX
FortiSwitch
FortiAP
FortiRecorder
FortiVoice/ FortiGateVoice
FortiCamera
FortiFone
Failopen Device
Web App. Firewall
Load Balancer
FortiBridge
FortiWeb
FortiADC
L7 D/DOS Mitigator
FortiDDoS
Web Servers
Remote VPN
Endpoint Security
FortiClient
FortiToken
2 Factor OTP Token

Fortigate

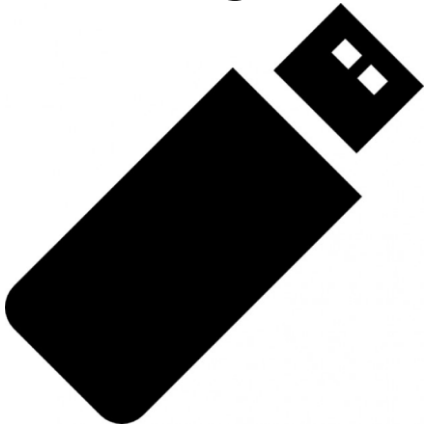
- NGFW et produit phare de la marque Fortinet
- Capacités de Firewall de Base
- Fonctionnement « flow-based » et « proxy-based »
- UTM
- Intégration Frabric
- SD-WAN

Cybersécurité

Spyware
Botnet
Spyware
ChevalDeTroie
Baiting
Blastware
Ransomware
Malware
Zombie
Worm
Botnet
Hoax
DDOS
Phreaking
APT
XSS
Whaling
Adware
Ransomware
Spyware
ZeroDay
Virus
Phreaking
SpearFishing
Phishing
Worm
Virus
Blastware
Vers
ZeroDay
Phishing
ChevalDeTroie
SQLInjection
Spearfishing
Ghostware
Swatting
Trojan
Keylogger
Vers
ZeroDay
Zombie
Ransomware
Blastware
Keylogger
Trojan
Hoax
Spam
DDOS
Zombie
BufferOverflow
Blastware
SpearFishing
Malware
Ghostware

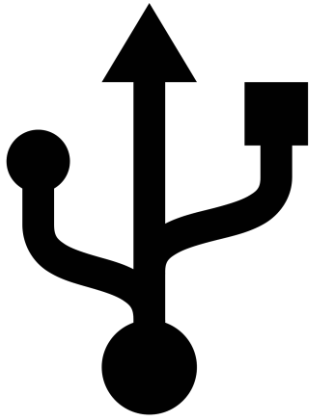
Principaux vecteurs d'attaques

Stockage USB

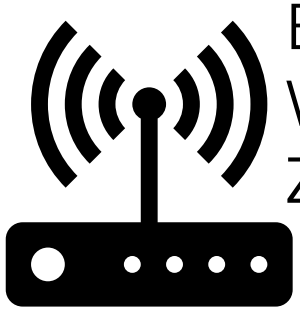


Ondes RF

HID

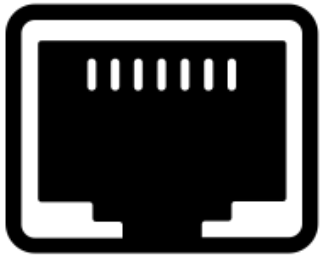


Sans-fil

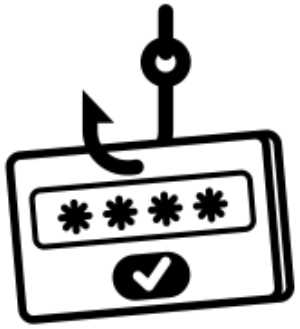


Bluetooth
Wi-Fi
Zigbee

Ethernet

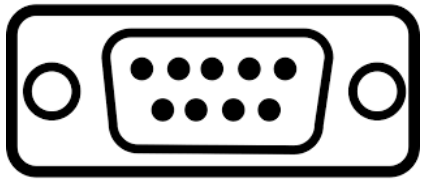


Phishing



Social Engineering

Liaison Série



Qu’est-ce qu’un Exploit ?

- Un exploit est un élément permettant d’exploiter une faille de sécurité.

- L’objectif est de récupérer un accès, d’augmenter ses droits d’accès ,d’extraire des données ou d’interrompre l’accès à une machine ou à un service.

- Formes multiples d’infections et d’exploits :

Fichier

Infecté

Infrastructure

Obsolète

Erreur humaine

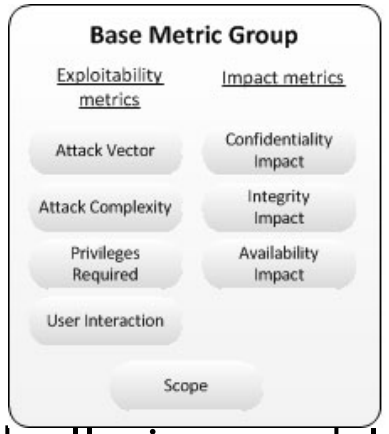
Phishing

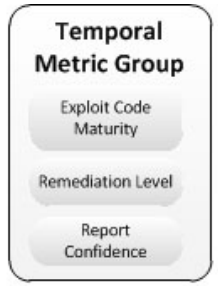
Mauvaise

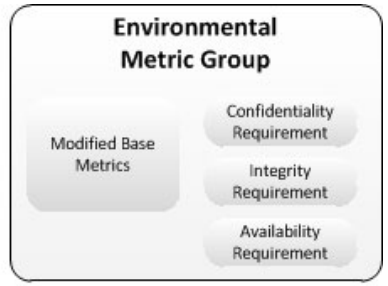
Configuration

Le Common Vulnerability Scoring System

- Moyen d'uniformiser les études de vulnérabilités
- Reconnu comme fiable
- Trois métriques :
  - Base : Impact maximal de la vulnérabilité, échelle immuable et unique
  - Temporel : Evaluation dans le temps
  - Environnemental : conséquences de la vulnérabilité sur le système
- Attribution d'un score servant a évaluer le niveau de risque de la vulnérabilité







Conséquences d'une attaque

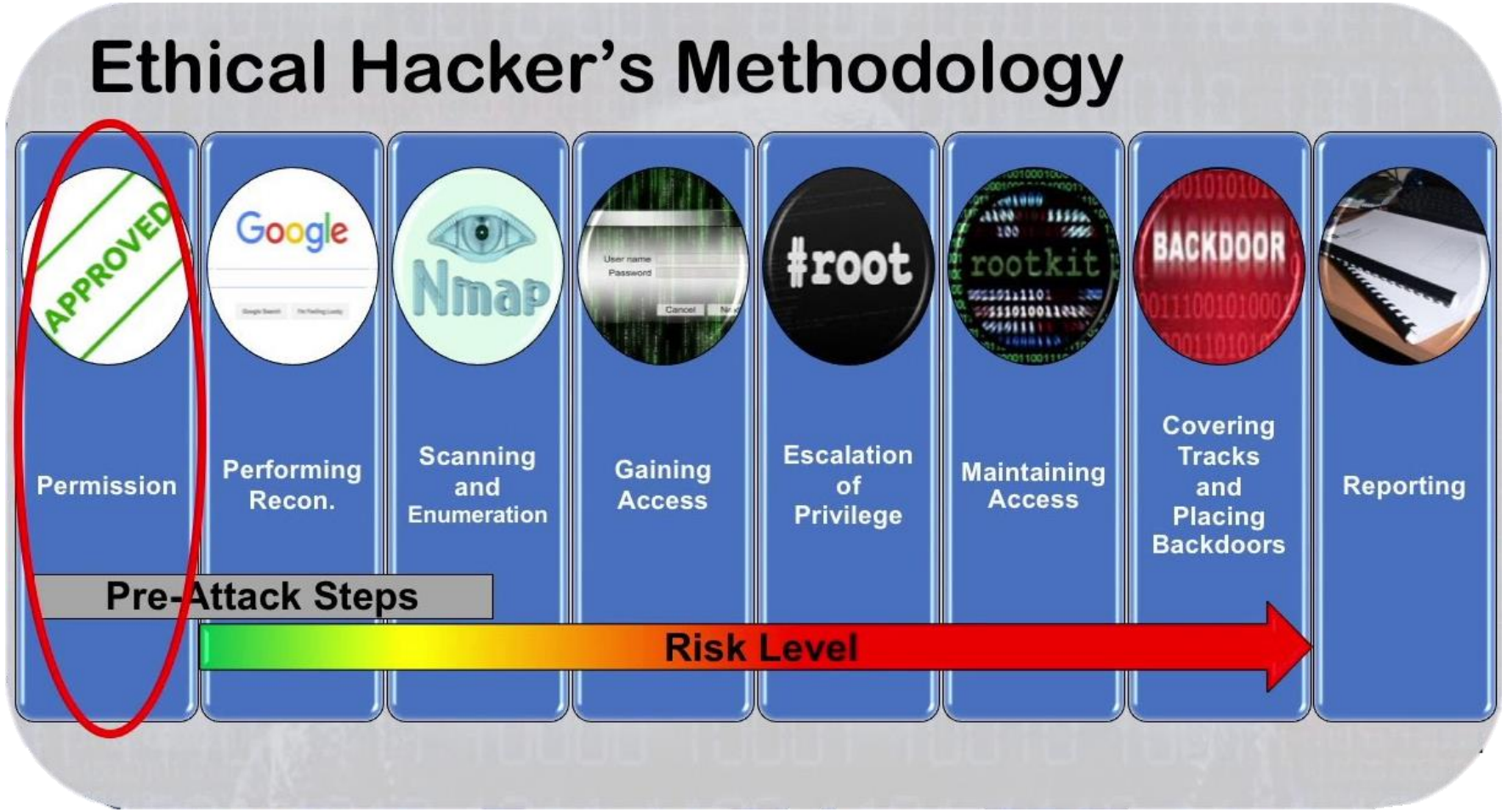
Des conséquences locales…

- Exfiltration de fichiers,
- Récupération de mots de passe,
- Déni de service,
- Usurpation d'identité,
- Compromission de la machine,
- Cryptage des données,
- Machines Zombie.

portant atteinte à toute l'entreprise…

- Paralysie du système d'information
- Demande de Rançon
- Atteinte à la vie privée
- Atteinte à l'E-crédibilité
- Fuite de données sensibles (brevets, rapport d'analyses, infos personnelles)
- Forte réduction des capacités du réseau

Cheminement d'une attaque informatique

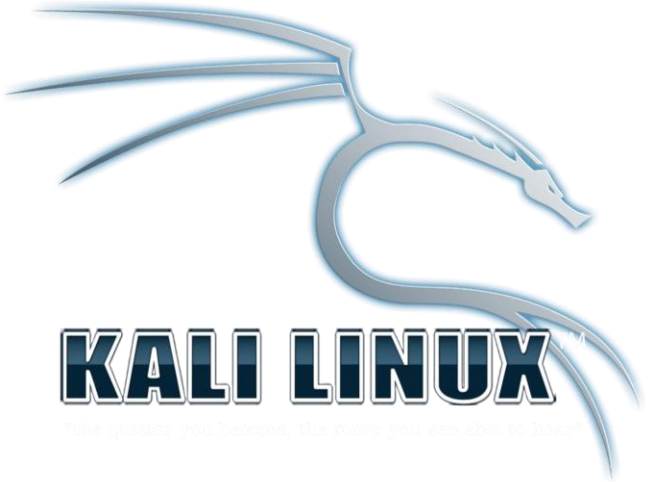


Le Hacking se démocratise

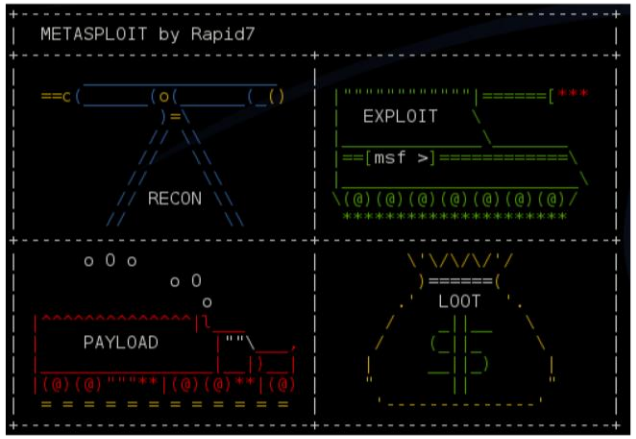
SHODAN

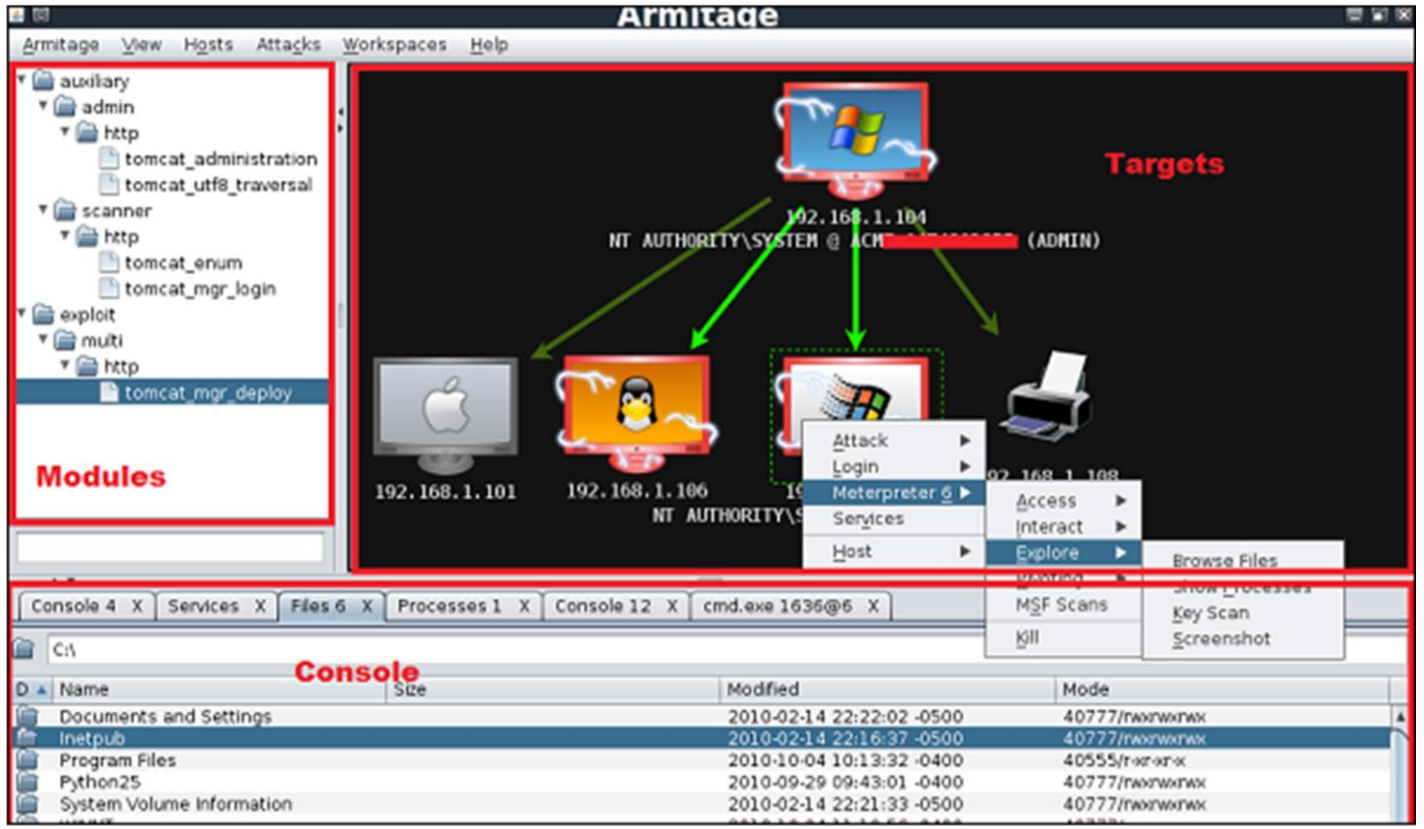
Du hardware spécialisé à portée de main

Les Logiciels se multiplient



Plus besoin de ligne de Commande…





LE TP