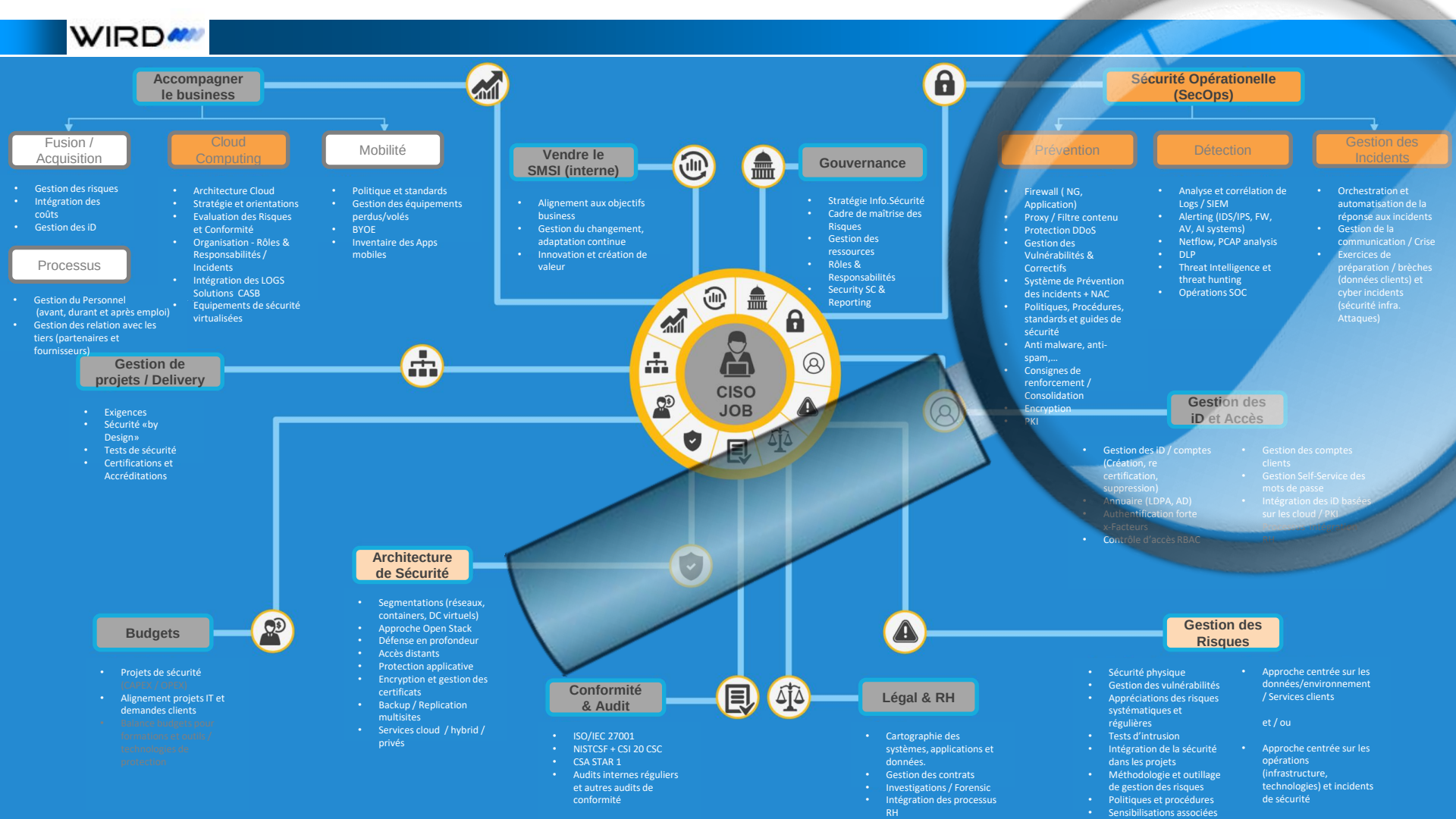
Agenda 20.20 du CISO
Quelles priorités ?

RETOUR D'EXPÉRIENCE

Olivier Luxereau

Common Romandie 2019.03.27

CORTEX
A WIRD Group Company


Accompagner le business
Fusion / Acquisition
Gestion des risques
Intégration des coûts
Gestion des iD
Cloud Computing
Architecture Cloud
Stratégie et orientations
Evaluation des Risques et Conformité
Organisation - Rôles & Responsabilités / Incidents
Intégration des LOGS Solutions CASB
Equipements de sécurité virtualisées
Mobilité
Politique et standards
Gestion des équipements perdus/volés
BYOE
Inventaire des Apps mobiles
Processus
Gestion du Personnel (avant, durant et après emploi)
Gestion des relation avec les tiers (partenaires et fournisseurs)
Vendre le SMSI (interne)
Alignement aux objectifs business
Gestion du changement, adaptation continue
Innovation et création de valeur
Gouvernance
Stratégie Info.Sécurité
Cadre de maîtrise des Risques
Gestion des ressources
Rôles & Responsabilités
Security SC & Reporting
Sécurité Opérationelle (SecOps)
Prévention
Firewall (NG, Application)
Proxy / Filtre contenu
Protection DDoS
Gestion des Vulnérabilités & Correctifs
Système de Prévention des incidents + NAC
Politiques, Procédures, standards et guides de sécurité
Anti malware, anti-spam,...
Consignes de renforcement / Consolidation
Encryption
PKI
Détection
Analyse et corrélation de Logs / SIEM
Alerting (IDS/IPS, FW, AV, AI systems)
Netflow, PCAP analysis
DLP
Threat Intelligence et threat hunting
Opérations SOC
Gestion des Incidents
Orchestration et automatisation de la réponse aux incidents
Gestion de la communication / Crise
Exercices de préparation / brèches (données clients) et cyber incidents (sécurité infra. Attaques)
CISO JOB
Gestion de projets / Delivery
Exigences
Sécurité «by Design»
Tests de sécurité
Certifications et Accréditations
Gestion des iD et Accès
Gestion des iD / comptes (Création, re certification, suppression)
Annuaire (LDPA, AD)
Authentification forte x-Facteurs
Contrôle d'accès RBAC
Gestion des comptes clients
Gestion Self-Service des mots de passe
Intégration des iD basées sur le cloud / PKI
Budgets
Projets de sécurité (CAPEX / OPEX)
Alignement projets IT et demandes clients
Balance budgets pour formations et outils / technologies de protection
Architecture de Sécurité
Segmentations (réseaux, containers, DC virtuels)
Approche Open Stack
Défense en profondeur
Accès distants
Protection applicative
Encryption et gestion des certificats
Backup / Replication multisites
Services cloud / hybrid / privés
Conformité & Audit
ISO/IEC 27001
NISTCSF + CSI 20 CSC
CSA STAR 1
Audits internes réguliers et autres audits de conformité
Légal & RH
Cartographie des systèmes, applications et données.
Gestion des contrats
Investigations / Forensic
Intégration des processus RH
Gestion des Risques
Sécurité physique
Gestion des vulnérabilités
Appréciations des risques systématiques et régulières
Tests d'intrusion
Intégration de la sécurité dans les projets
Méthodologie et outillage de gestion des risques
Politiques et procédures
Sensibilisations associées
Approche centrée sur les données/environnement / Services clients
et / ou
Approche centrée sur les opérations (infrastructure, technologies) et incidents de sécurité

WIRD CLOUD

- Datacenters en Suisse
- Protection des données
- Disponibilité et SLAs élevés
- Fonctionnalités étendues
- Prestations sur mesure
- Simple, flexible et évolutif
- Modèle de coût à l'utilisation

Storage as a service (SaaS)

- WIRDDrive Cloud Storage: Créer, sauvegarder et partager des fichiers en ligne
- WIRDS3 Object Storage: Solution de stockage objet 100% compatible S3
- WIRDBackup: Veeam Cloud Connect, NetApp, Duplicati, Synology, Rubrik, autres

Platform as a Service (PaaS)

- IaaS inclus
- Environnement de développement, d'exécution, de déploiement et de gestion d'applications
- Environnement WebApp, DB Clustering, HA applicatif
- Containers as a Service (CaaS), Docker & Kubernetes

Infrastructure as a Service (IaaS)

- Ressources informatiques virtualisées: CPU, stockage et réseau
- Services sécurité: Monitoring, firewall, load balancing, VPN
- Administration des ressources par interface web
- Managed Services: Maintenance, updates, backup and restore DataBase
- Business Continuity, Disaster Recovery Plan

Hosting

- Housing inclus
- Infrastructure dédiée
- Full Managed Services, Monitoring

Housing

- Datacentres Tier 3 / 4, certification ISO 27001
- Racks 22U & 42U, inclus alimentation 16/32A
- IP Public et Transit IP
- Cross-Connect telco, Cloud Fabrics, accès internet
- Accès sécurisé à vos infrastructures 24/7

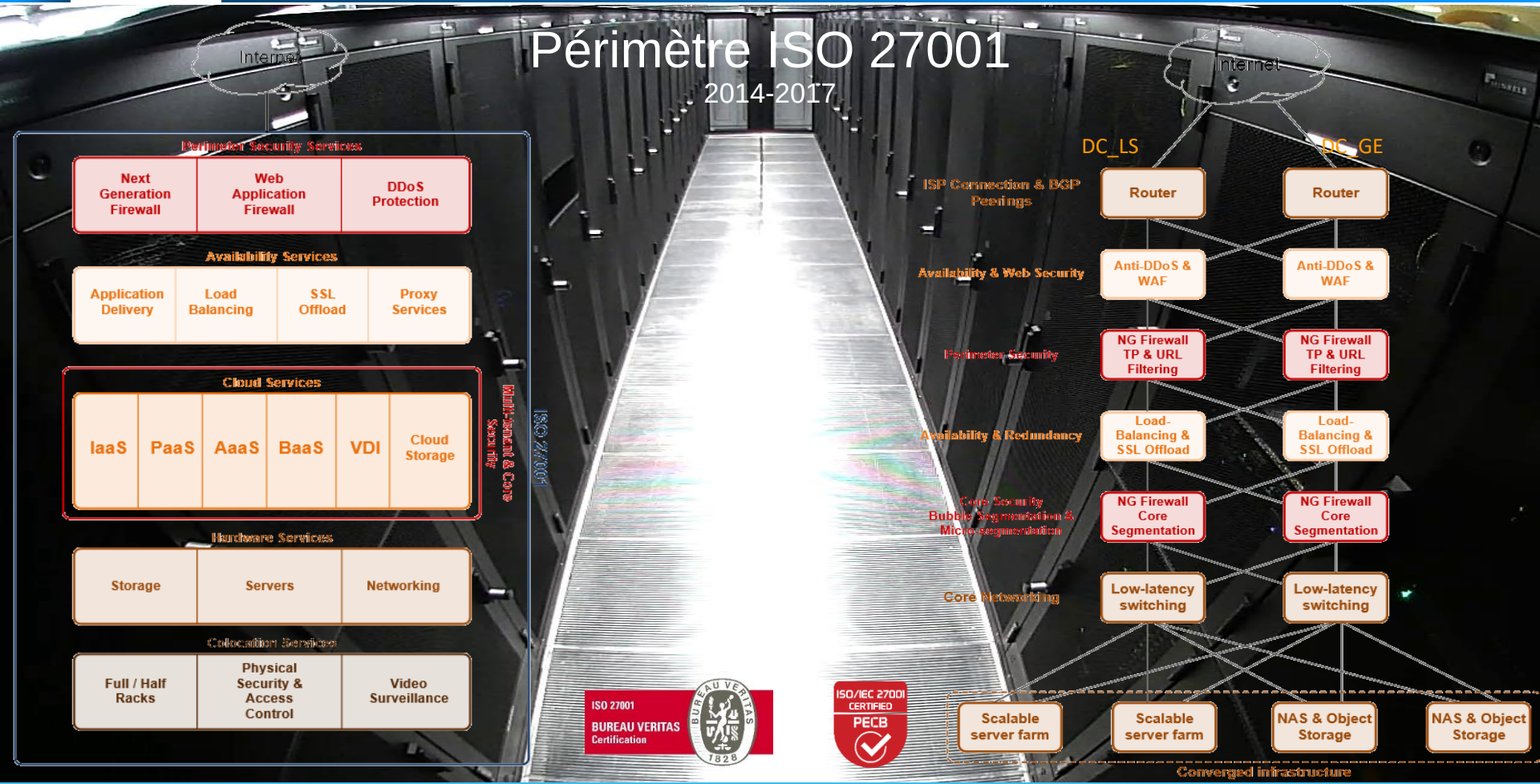
ISO 27001 CERTI TRUST

SWISSCLOUD
Powered by Cortex-IT
info@wird.cloud
www.wird.cloud

CORTEX
A WIRD Group Company

Périmètre ISO 27001

2014-2017



Modèle opérationnel de cyber sécurité depuis 2016

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

1 Planification et Organisation
Révision de la stratégie de maitrise des risques
Définition et attribution des rôles et responsabilités
Elaboration du Système de Gouvernance – Contrôle et Pilotage

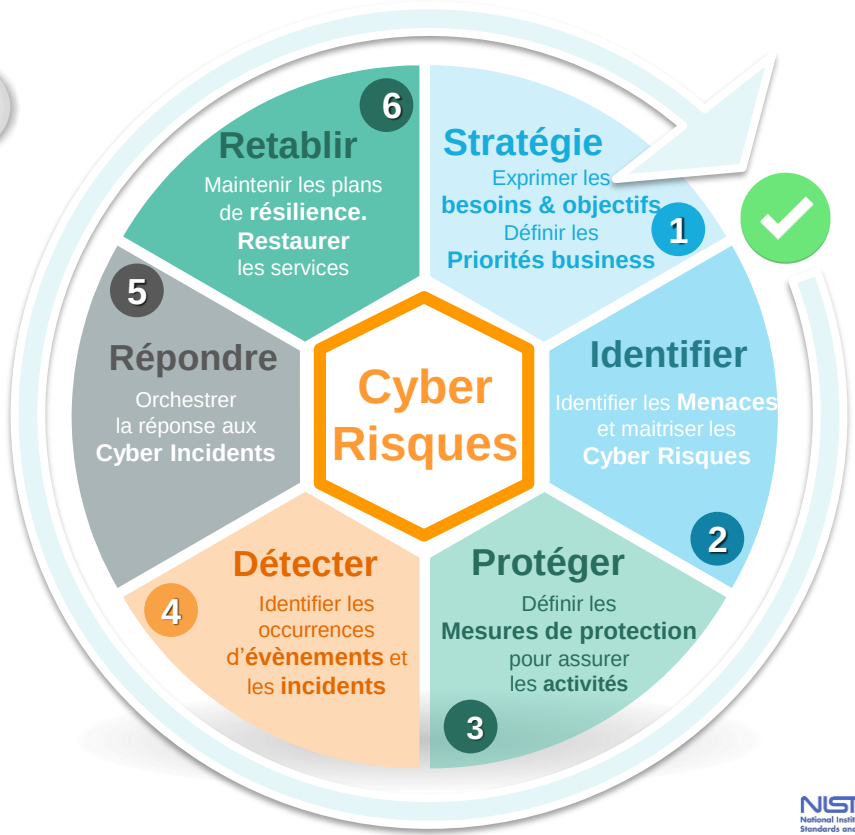
2 [ID] Gestion préventive des Risques et Tests
Identification et classification des actifs
Processus complet sur base de scénarios + Scans V et tests Intrusion
Elaboration des plans d'actions et mesures de sécurité

3 [PR] Protection technique & organisationnelle
Gestion des ID et contrôle d'accès
Evolution des systèmes de protection et Gouvernance
Politiques et standards de sécurité - Formation et Sensibilisation

4 [DE] Surveillance et Analyse
Surveillance continue de tous les systèmes et services IT / Cloud
Processus et technologies de détection des Incidents
Renforcement des procédures op. et renseignement sur les menaces

5 [RS] Réponse rapide aux cyber incidents
Solution de réponse aux incidents (cyber & clients) + Communication
Analyse des incidents et réduction des conséquences
Renforcement des mesures de protection (Techniques & Org.)

6 [RE] Rétablissement et amélioration
Application et maintient des plans de secours -restitution à l'état initial
Capitalisation des connaissances acquises
Définition des axes d'amélioration et optimisation



NIST National Institute of Standards and Technology U.S. Department of Commerce

De la gestion des Risques (opérationnels) IT

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

Méthodologie basée sur :

- EBIOS / ISO 27005 et 80 scénarios de risques (PxI)
- NIST SP 800 - Risk Assessment guide for IT systems

Ligne de base – Alignement aux standards

- Top 20 CIS Controls
  - Center for Internet Security
- CSA Cloud Control Matrix

… à [ID] : Gestion des risques basés sur les cyber incidents

2

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

Top questions pour identifier mes risques :

- Sommes-nous protégé des dernières menaces ?
- Disposons-nous de ressources et compétences suffisantes ?
- Est-ce que nous opérons avec efficacité et au même niveau de maturité que les autres fournisseurs Cloud ?
- Sommes-nous agiles et réactifs ?
- Est-ce que je communique correctement les risques aux décideurs … ?
  (et aux vendeurs → clients)

[ID] Gestion des risques Cloud

SecOps:

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

Automatisation End to End (Services de sécurité et outils)

CLIENT

Responsable de la sécurité ***dans*** le Cloud

- Données du client
- Plateformes, applications, Gestion des Identités et des accès
- Configuration de son réseau et des systèmes de protection (Firewall / WAF, proxy / LB, CASB, …)
- Données côté-client — Encryption / anonymisation Et contrôle d'intégrité
- Encryption Serveur — (Données et/ou File system)
- Protection traffic réseau — Encrypt./intégrité/Identification

WIRD.CLOUD

Responsable de la sécurité ***du*** Cloud

COMPUTE	RÉSEAUX	STOCKAGE	PLATEFORME
▪ Hosting infrastructure dédiée ▪ Services managés ▪ Monitoring	▪ IP public et Transit IP ▪ X-Connect Telco, Cloud Fabrics ▪ Accès internet	▪ WirdCloud Storage Services ▪ S3 object Storage ▪ Backup as a Service	▪ OpenStack Cloud Orchestration ▪ Environnements pour Dev., exec., et gestion d'applications Web

CYBER INCIDENT ?

Occurrence d'évènements d'origine humaine et malveillante

Principales menaces

1. Compromission machine Admin
2. Vol ID compte privilégié
3. Détournement d'outils légitimes
4. DDoS

5. Le TEMPS et les MOYENS !
   - Délai d'identification d'un incident
   - Délai de réponse
   - Durée de rétablissement
6. Vente de services et/ou solution d'infrastructure non Qualifiée

Principales cyber menaces (2018)

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

- Epidémie de campagnes de Phishing / Ransomware - cryptolocker
  - Petya
  - Wannacry
- Botnet
- Vol de données / Brèches massives
  - Facebook / cambridge analytics (87 Millions d'utilisateurs),
  - Orbitz (880 000 cartes de paiement)
  - British Airways (77 000 dossiers, 108 000 cartes de paiement, 380 000 relevés, …)
- … et leurs amendes
  - Uber : 148 Millions USD
- Vulnérabilités
  - « Hardware Intel » : Meltdown, Spectre
  - Software : OS équipements et serveurs – Commerciaux et open source

Gestion des risques basée sur la « Kill Chain»

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

Détection des comportements qui rendent les botnets rentables

- *DDoS, outbound scans, relay traffic, Spam, Click-fraud, bitcoin mining,*

Détection des attaquants qui se préparent à se déployer

- *Scans de vulnérabilités, scans réseaux bas-et-lents*

Concentration sur les données et actifs clés - Critiques

- *Transferts par étapes, exfiltration lente*

Botnet → Reconnaissance → Compromission → Exfiltration

C&C

Mouvement Latéral

Détection des canaux de communication cachés - qui contournent les pare-feu et autres systèmes basés sur les signatures

- *Outils d'accès distants personnalisés (RAT) Tunnels cachés, messages furtifs, outils d'anonymisation / encryption*

Détection des logiciels malveillants et/ou les attaquants lorsqu'ils se propagent sur le réseau

- *Spreading malware, compromised administrator credentials et portes dérobées dans l'infrastructure*

MITRE Enterprise ATT&CK™ Framework

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Image File Execution Options Injection			Forced Authentication	Network Share Discovery	AppleScript		Man in the Browser	Exfiltration Over Physical Medium	Multi-hop Proxy
Plist Modification			Hooking	System Time Discovery	Third-party Software		Browser Extensions		Domain Fronting
Valid Accounts			Password Filter DLL	Peripheral Device Discovery	Windows Remote Management		Video Capture	Exfiltration Over Command and Control Channel	Data Encoding
DLL Search Order Hijacking			LLMNR/NBT-NS Poisoning	Account Discovery	SSH Hijacking	LSASS Driver	Audio Capture		Remote File Copy
AppCert DLLs		Process Doppelgänging	Securityd Memory	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Scheduled Transfer	Multi-Stage Channels
Hooking		Mshta	Private Keys	System Information Discovery	Pass the Ticket	Mshta	Clipboard Data	Data Encrypted	Web Service
Startup Items		Hidden Files and Directories	Keychain	Security Software Discovery	Replication Through Removable Media	Local Job Scheduling	Email Collection	Automated Exfiltration	Standard Non-Application Layer Protocol
Launch Daemon		Launchctl	Input Prompt	System Network Connections Discovery	Remote Desktop Protocol	Trap	Screen Capture	Exfiltration Over Other Network Medium	Communication Through Removable Media
Dylib Hijacking		Space after Filename	Bash History	System Owner/User Discovery	Pass the Hash	Source	Data Staged	Exfiltration Over Alternative Protocol	Multilayer Encryption
Application Shimming		LC_MAIN Hijacking	Two-Factor Authentication Interception	System Network Configuration Discovery	Exploitation of Vulnerability	Launchctl	Input Capture	Data Transfer Size Limits	Standard Application Layer Protocol
AppInit DLLs		HISTCONTROL	Account Manipulation	Application Window Discovery	Shared Webroot	Space after Filename	Data from Network Shared Drive	Data Compressed	Commonly Used Port
Web Shell		Hidden Users	Replication Through Removable Media	Network Service Scanning	Logon Scripts	Execution through Module Load	Data from Local System		Standard Cryptographic Protocol
Service Registry Permissions Weakness		Clear Command History	Input Capture	Query Registry	Remote Services	Regsvcs/Regasm	Data from Removable Media		Custom Cryptographic Protocol
Scheduled Task		Gatekeeper Bypass	Network Sniffing	Remote System Discovery	Application Deployment Software	InstallUtil			Data Obfuscation
New Service		Hidden Window	Credential Dumping	Permission Groups Discovery	Remote File Copy	Regsvr32			Custom Command and Control Protocol
File System Permissions Weakness		Deobfuscate/Decode Files or Information	Brute Force	Process Discovery	Taint Shared Content	Execution through API			Connection Proxy
Path Interception		Trusted Developer Utilities	Credentials in Files	System Service Discovery		PowerShell			Uncommonly Used Port
Accessibility Features		Regsvcs/Regasm				Rundll32			Multiband Communication
Port Monitors		Exploitation of Vulnerability				Scripting			Fallback Channels
Screensaver		Extra Window Memory Injection				Graphical User Interface			
LSASS Driver		Access Token Manipulation				Command-Line Interface			
Browser Extensions		Bypass User Account Control				Scheduled Task			
Local Job Scheduling		Process Injection				Windows Management Instrumentation			
Re-opened Applications		Component Object Model Hijacking				Trusted Developer Utilities			
Rc.common	SID-History Injection	InstallUtil				Service Execution			
Login Item	Sudo	Regsvr32							
LC_LOAD_DYLIB Addition	Setuid and Setgid	Code Signing							
Launch Agent		Modify Registry							
Hidden Files and Directories		Component Firmware							
.bash_profile and .bashrc		Redundant Access							
Trap		File Deletion							
Launchctl		Timestomp							
Office Application Startup		NTFS Extended Attributes							
Create Account		Process Hollowing							
External Remote Services		Disabling Security Tools							
Authentication Package		Rundll32							
Netsh Helper DLL		DLL Side-Loading							
Component Object Model Hijacking		Indicator Removal on Host							
Redundant Access		Indicator Removal from Tools							
Security Support Provider		Indicator Blocking							
Windows Management Instrumentation Event Subscription		Software Packing							
Registry Run Keys / Start Folder		Masquerading							
Change Default File Association		Obfuscated Files or Information							
Component Firmware		Binary Padding							
Bootkit		Install Root Certificate							
Hypervisor		Network Share Connection Removal							
Logon Scripts		Rootkit							
Modify Existing Service		Scripting							

attack.mitre.org

Base de connaissances sur les tactiques et techniques d'attaques

Utilisée comme base pour le développement de modèles et de méthodologies de menace / produits et services de cybersécurité.

[PR] Système de protection contre les menaces

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

Améliorer la défense avec une plate forme coordonnée pour contrer les attaques avancées

Détection

Découvrir les menaces inconnues avec des analyses avancées

1. Détecter les attaques
2. Identifier les comportements anormaux
3. Prioriser automatiquement les menaces

Prévention

Bloquer continuellement les attaques et corriger les vulnérabilités

1. Arrêt des logiciels malveillants et exploits
2. Correction automatique des vulnérabilités
3. Découvrir et sécuriser les postes clients

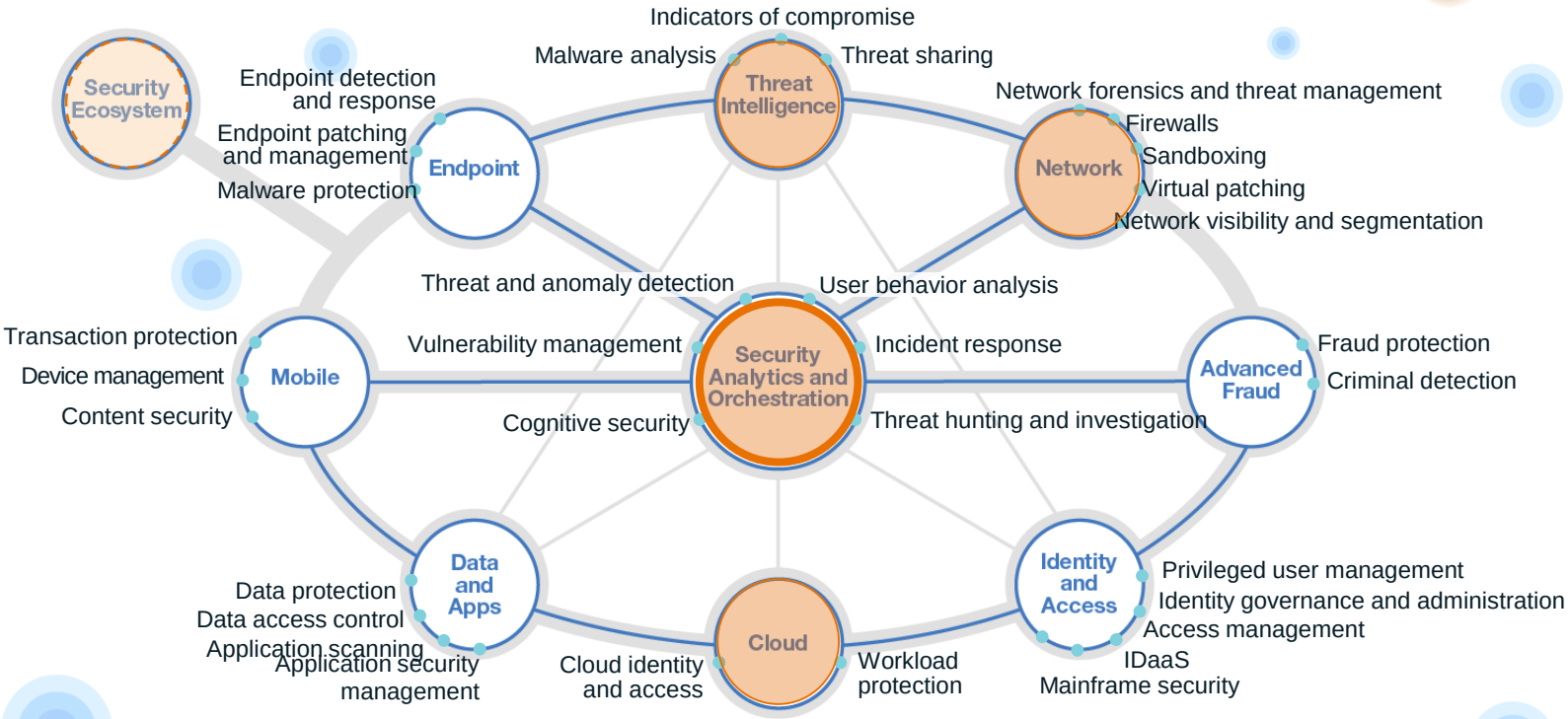
Réponse

Répondre rapidement aux incidents et avec précision

1. Orchestrer et automatiser la réponse
2. Traquer les indicateurs de menace pour analyse approfondie
3. Retenir les leçons

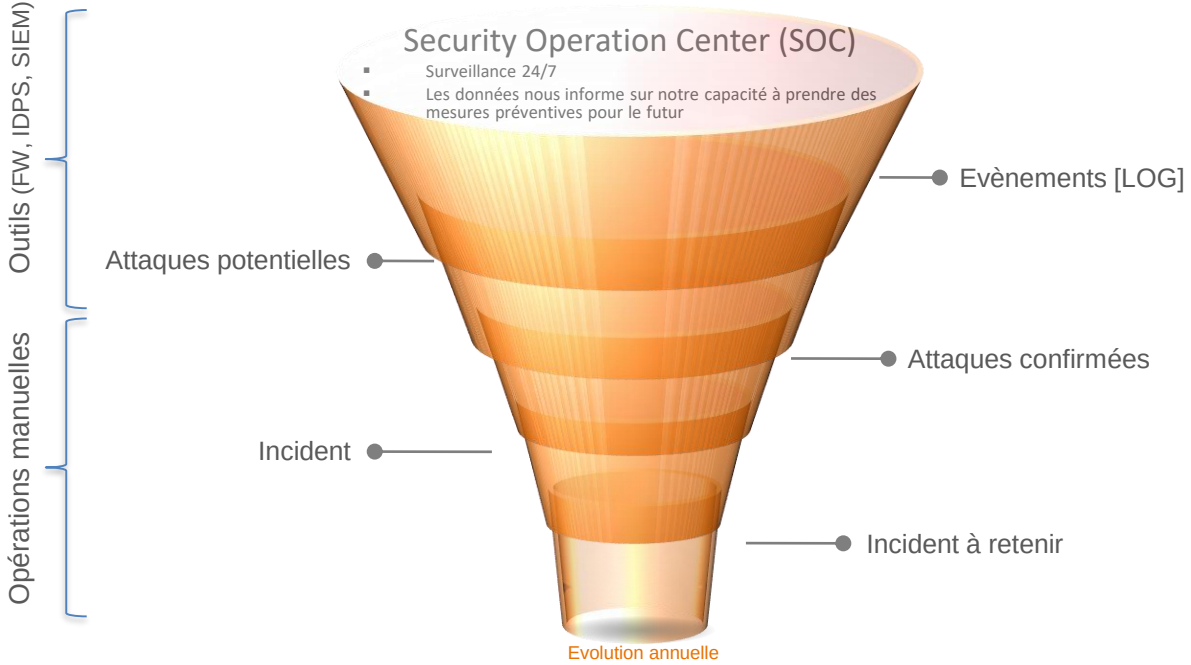
[PR] Système de protection contre les menaces

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience



Source : IBM Security Strategy Overview 2017

[DE] – DÉTECTION DES CYBER INCIDENTS



- Manque de solutions plus efficaces pour trouver et stopper plus rapidement les attaques
- Les incidents à retenir concerne essentiellement des mauvaises configurations systèmes, sans impact pour les clients

[DE] – DÉTECTION DES CYBER INCIDENTS

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

SOAR = SOA + SIR + TIP

[DE] Détecter et stopper les cyber incidents

4

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

Obj.: Disposer de moyens les plus rapides et les plus efficaces pour détecter et de stopper les attaques

- **Visibilité** d'attaque en « temps réel »
  - Déceler au plus vite les attaques (…cachées, inconnues, persistantes)
  - Détecter les vecteurs et les comportements fondamentaux d'une cyber-attaque
  - Faire la chasse, la traque non-stop aux menaces et ce de manière automatisée

- **Couverture des «angles morts»** sur
  - Tout traffic (même chiffré …) – Interne et Externe (Internet, cloud, Clients)
  - Tout type de device – Tout OS, BYOD, virtuel
  - Toute localisation – Data Center, accès distants

- **IA & ML** comme multiplicateur de force pour l'équipe sécurité / SOC
  - Faire gagner du temps au analystes et mettre un terme aux recherches sans fin
  - Disposer du contexte - au bon moment pour arrêter les attaques avant que le mal ne soit fait
  - Des nouvelles informations supplémentaires pour piloter le SIEM

[DE] Détecter et stopper les cyber incidents

4

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

Problème

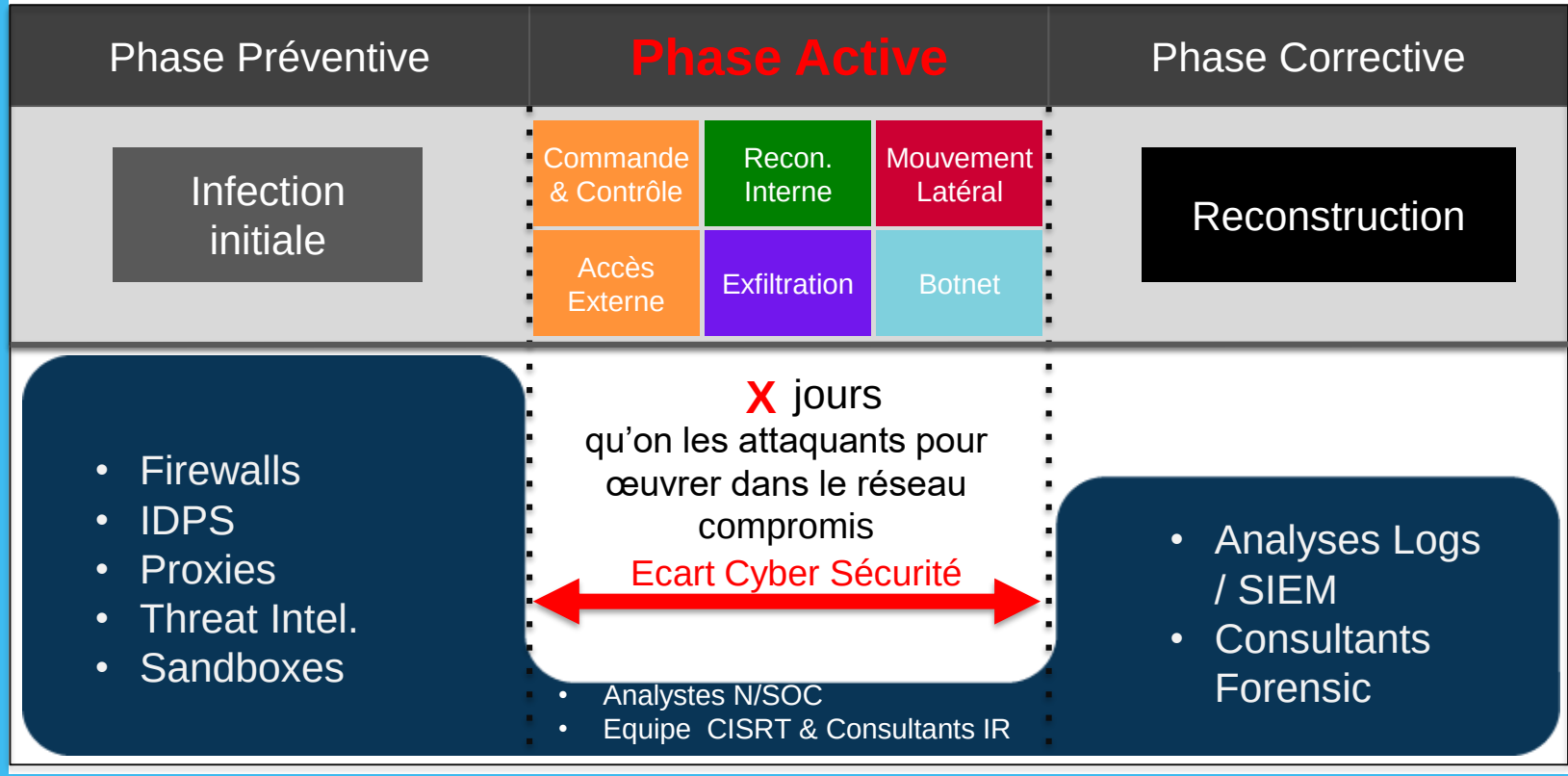
- Impossible de détecter rapidement les attaques actives (avancées)
- Manque de visibilité et d'automatisation pour identifier les attaquants déjà présents sur le réseau
- Ne peut enquêter efficacement sur les menaces
- Les analystes de la sécurité sont constamment en mode «pompier»;
  - ils n'ont pas de contexte pour confirmer les menaces et perdent du temps à traquer les informations au lieu d'arrêter les attaques
  - Les systèmes de journalisation deviennent rapidement ingérables ➔ Stress opérationnel, fatigue

Besoin

- Détection automatique des attaques et génération d'un petit nombre d'alertes précises et exploitables ➔ Fonctionnement précis et efficace
- Analyses rationnelles: Cibler les attaques qui comptent et les menaces critiques
  - Examiner les incidents avec de la TI afin de déterminer s'ils sont malveillants
- Réduire considérablement le temps d'enquête et libérer un temps précieux pour les admin./analystes
- Accélérer les enquêtes de sécurité tout en améliorant l'efficacité des activités de prévention, détection et de réaction aux menaces ➔ Analyse comportementale
- Evolutivité, agilité, facilité de déploiement et intégration dans la plateforme de sécurité existante, et …
- Réduction des coûts d'exploitation

[DE] Détecter et stopper les cyber incidents

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience



[DE] Détecter et stopper les cyber incidents

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

Phase Préventive	**Phase Active**	Phase Corrective

1. Analyse de tout le trafic (NS-EW) à la recherche de signes d'attaque cachés
2. Détection en temps réel, évitant une analyse longue et coûteuse
3. Etablir un contexte soutenant le personnel SOC et améliorer la prévention

- Firewalls
- IDPS
- Proxies
- Threat Intel.
- Sandboxes

Automatisation temps-reel de la detection dans toutes les phases actives d'une cyber attaque

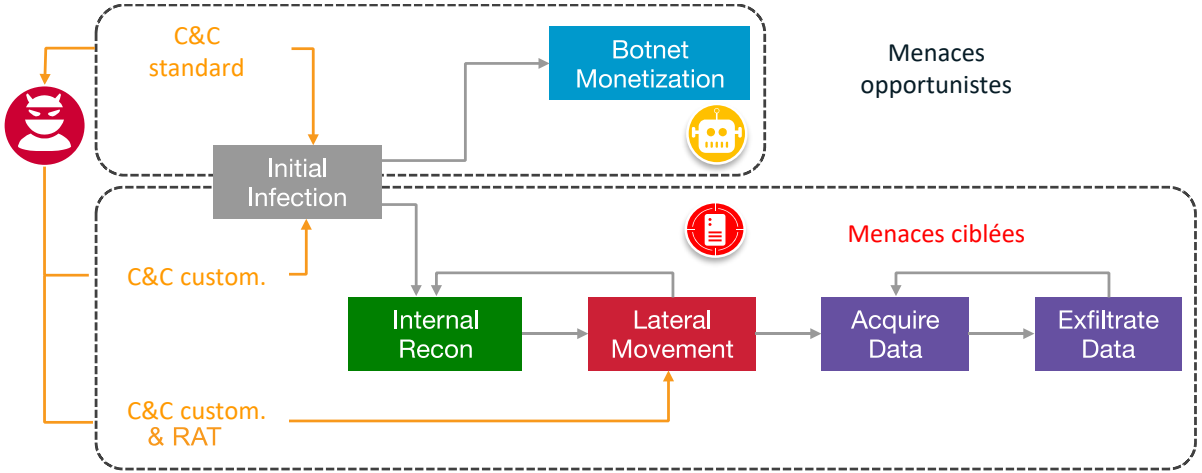
- Analystes N/SOC
- Equipe CISRT & Consultants IR

- Analyses Logs / SIEM
- Consultants Forensic

Visibilité - Détection dans toutes les phases d'une cyber attaque

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

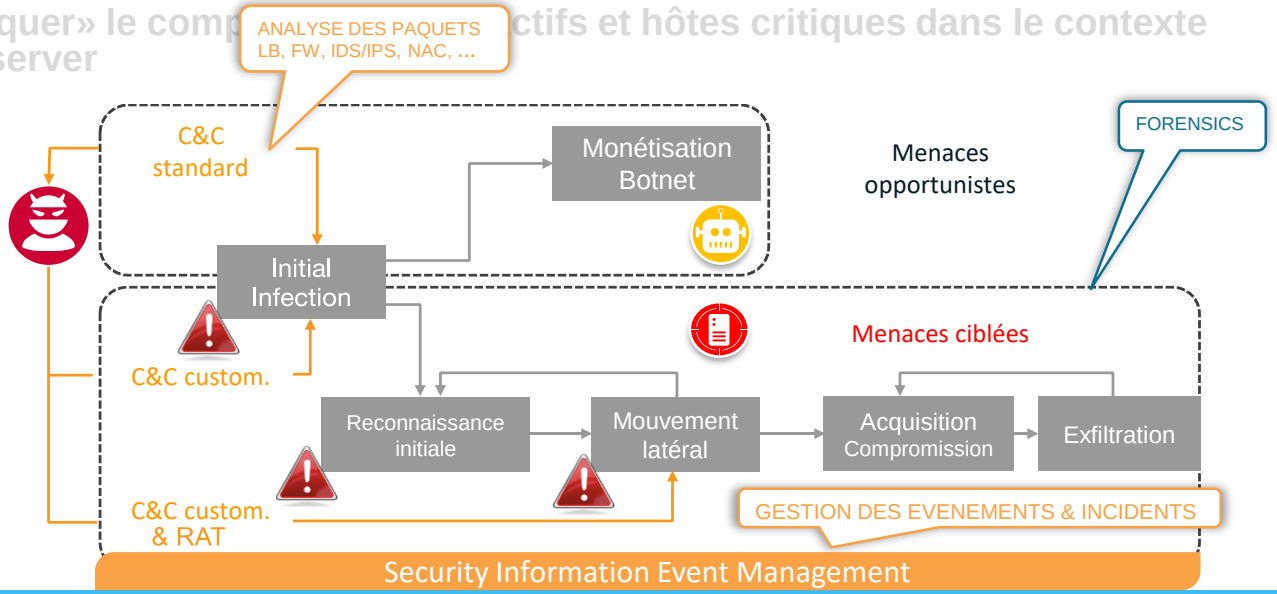
- **Les équipes ont besoin de voir les attaques, pas les évènements de sécurité**
  - « Scorer » automatiquement les événements et les hôtes en termes de risque
- **Relier les indicateurs de compromission au fil du temps**
  - Suivre facilement la menace et sa progression au fil du temps (jours, semaines voire des mois)
- **« Marquer» le comportement des actifs et hôtes critiques dans le contexte et observer**



Visibilité - Détection dans toutes les phases d'une cyber attaque

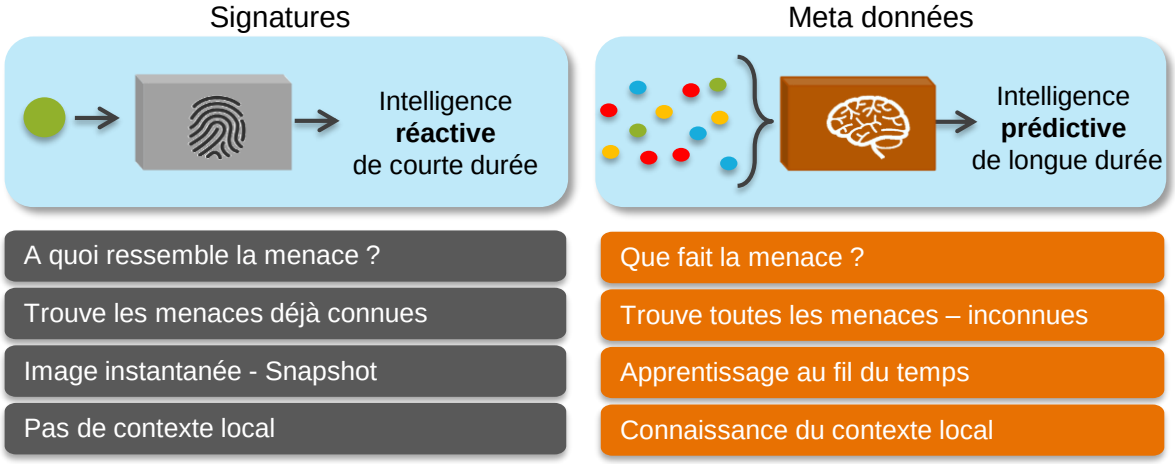
1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

- **Les équipes ont besoin de voir les attaques, pas les évènements de sécurité**
  - « Scorer » automatiquement les événements et les hôtes en termes de risque
- **Relier les indicateurs de compromission au fil du temps**
  - Suivre facilement la menace et sa progression au fil du temps (jours, semaines voire des mois)
- **« Marquer» le comp ctifs et hôtes critiques dans le contexte et observer**



Avoir une nouvelle approche pour trouver les nouvelles menaces … Compléter le SIEM

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience



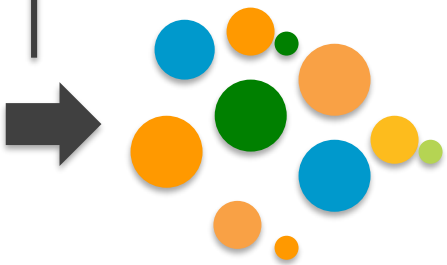
- Un SIEM ne connait que ce que les autres solutions de sécurité ont déjà détecté
  - Collecte et corrélation de logs
  - Les attaques qui ont contourné ces solutions n'auront probablement pas laisser de trace « visible » dans les logs
- Détecter les comportements d'attaques cachées qui échappent aux contrôles de signature et de réputation
  - Les SIEM dépendent d'une détection « manuelle »
  - Ils exigent beaucoup de ressources (experts) et sont chronophages
- Sont utilisés après la détection d'une attaque

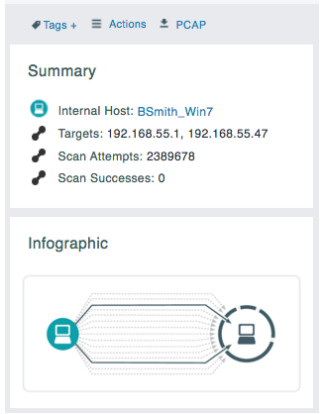
➔ Solution : Pré-corrélation avec du ML pour «scorer %» le comportement des hôtes sur le réseau
Identifier les attaques en temps réel et indiquer au SIEM où et sur quoi se concentrer

Automatisation de la détection = Réduction de la quantité de données à analyser

Rapport: les analystes ont assez de détails sur les événements pour prendre une décision et des recommandations pour les prochaines étapes

Détection : 100 à 1000 événements et segments de réseau condensés en une seule détection





Triage : Les détections sont automatiquement corrélées avec les hôtes physiques identifiés cible d'une attaque

SOC

Plateformes
- SIEM
- Incident Response

Ecosystème : Intégration aux plates-formes de protection et de réponse aux incidents

- Firewall
- Endpoint
- NAC

[DE] Détecter et stopper les cyber incidents

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

Priorités :

- **Automatisation** de la détection, l'analyse et l'exploitation des menaces
  - → Réduire les procédures et accélérer les analyses (manuelles, par exception)
- **Visibilité en temps réel** sur toutes les phases d'attaque
- **Couverture complète** de l'infrastructure
- **Renforcement de la sécurité** et rendre l'équipe SOC plus efficace
  - Supprimer le travail fastidieux exigé à des analystes de talent
  - Permettre au support (Cortex et WIRD) d'agir
- **Éviter le besoin de répondre aux incidents …**

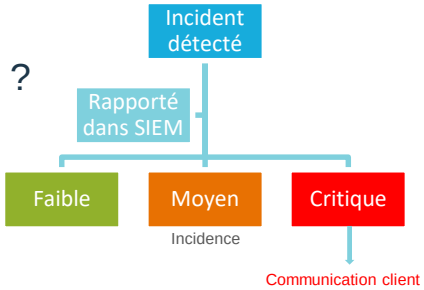
[RS] : Réponse aux incidents

5

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

Top questions pour réduire l'impact :

- Comment peut-on réduire l'impact des Cyber incident – inévitables ?
- Suis-je déjà compromis et que je ne le sais pas?
- Comment savoir que mon équipe est correctement organisée et qu'elle ne manque rien pour répondre aux incidents?



Faire face à toute cyber attaque ou situation de crise avec une plateforme intégrée de bout en bout pour les opérations de sécurité et l'orchestration de la réponse

[RS] : Réponse aux incidents

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

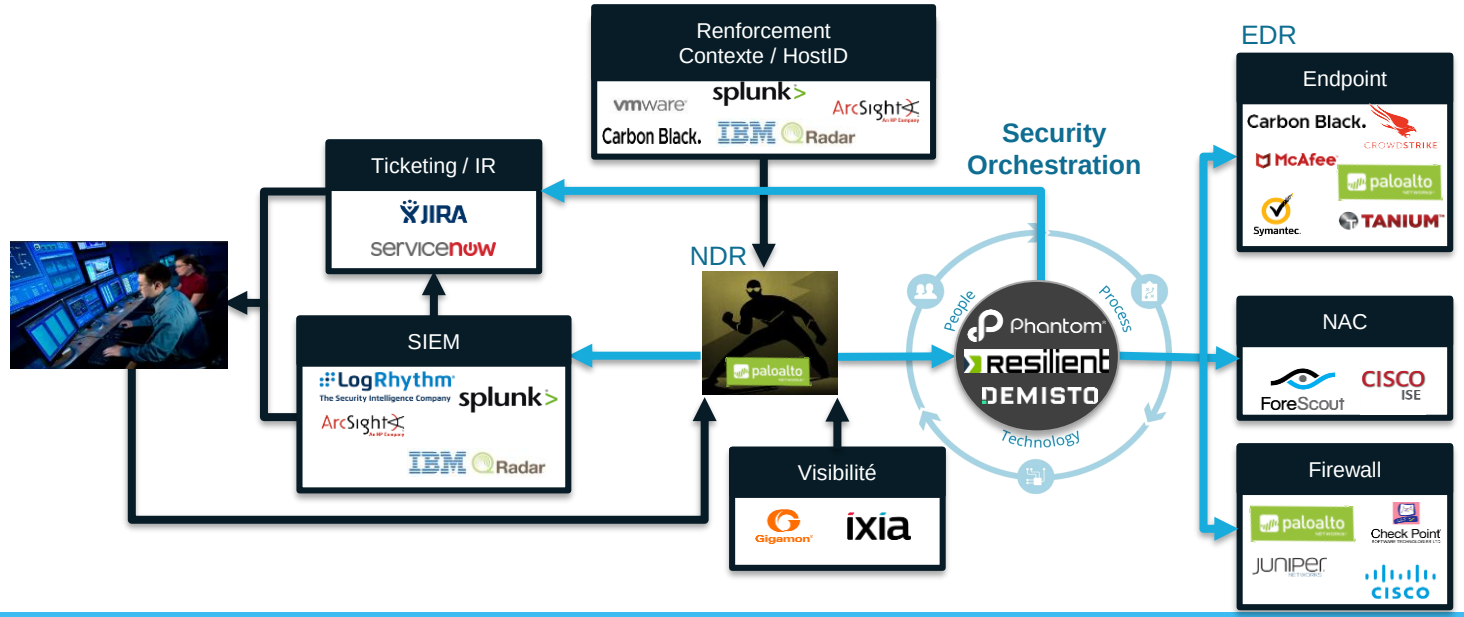
Plateforme intégrée ou écosystème de partenaires

pour améliorer la vitesse et l'efficacité de la réponse

Investigations plus rapides

Orchestration de la réponse

Intégration aux processus et solutions existantes



[RS] : Plateforme de réponse aux incidents

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

Personnes:

- Permet une collaboration entre les différents intervenants (IT, Network, SysAdmin, CSIRT et le C-Level [COO, CISO])

Processus

- Fournit des livres de lecture dynamiques (playbooks) basés sur les normes NIST / CERT / SANS, faciles à personnaliser à l'aide de procédures de sécurité opérationnelles (Techniques et organisationnelles)

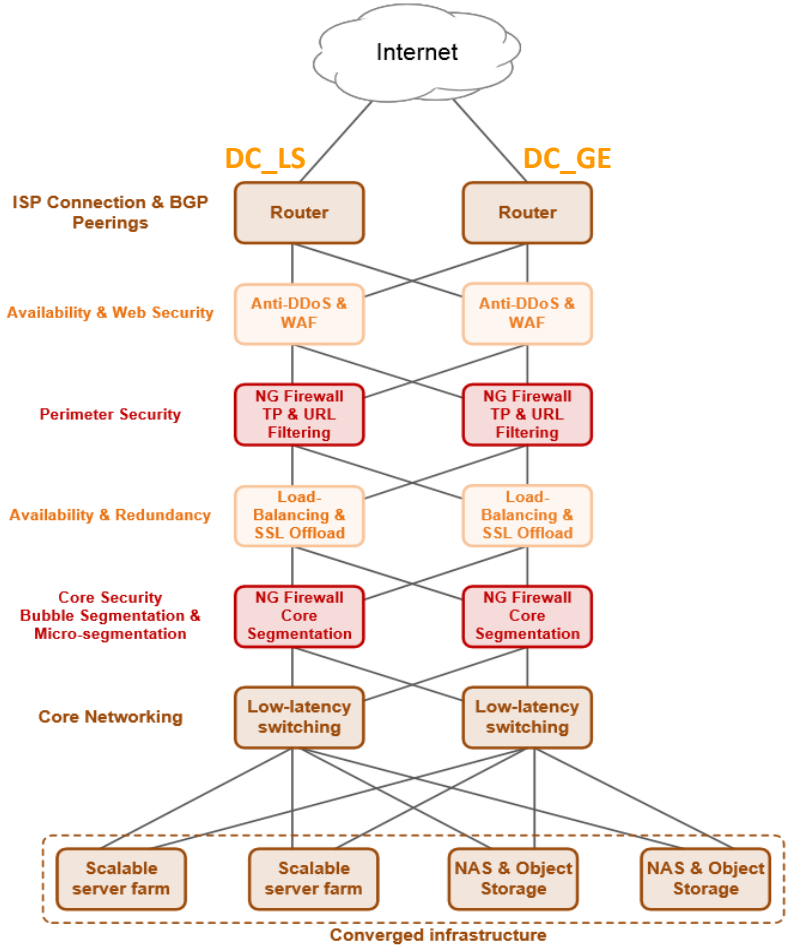
Technologies

- Ouverte et agnostique, doit s'intègrer à l'infrastructure de sécurité et constituer un concentrateur / un «Hub» pour «l'orchestration de la réponse

[RE] Rétablir

1. Stratégie
2. Risques
3. Protection
4. Détection
5. Réponse
6. Résilience

- Tous les équipements sont duplexés, en clusters dans les 2 DC en actif-passif et/ou en actif-actif pour certains
- Tests de perte de service à la demande des clients ou lors des maintenances mensuelles
- Cadre SLA / SLO



Merci pour votre attention