Sensibilisation Cybersécurité / Hacking

Module 01

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES
07 63 53 46 81
CONSEILS@BCOPIN.COM

Emergence des cyberattaques

Bilan des Cyberattaques

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Les enjeux

Les enjeux économiques

- Les cybercriminels sont passés d'attaque d'individu à attaque d'entreprise.
- Aucun secteur économique n'est à l'abri (surtout le secteur bancaire et financier).

Les enjeux sociétaux

- Forte évolution du trafic illicite.
- Atteinte aux mineurs / Propagande / Terrorisme.

Les enjeux juridiques et normatifs

- Difficultés de collaboration avec les autres pays.
- Mise en place de la RGPD

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Les 3 grands principes de la sécurité d'informatique

La confidentialité

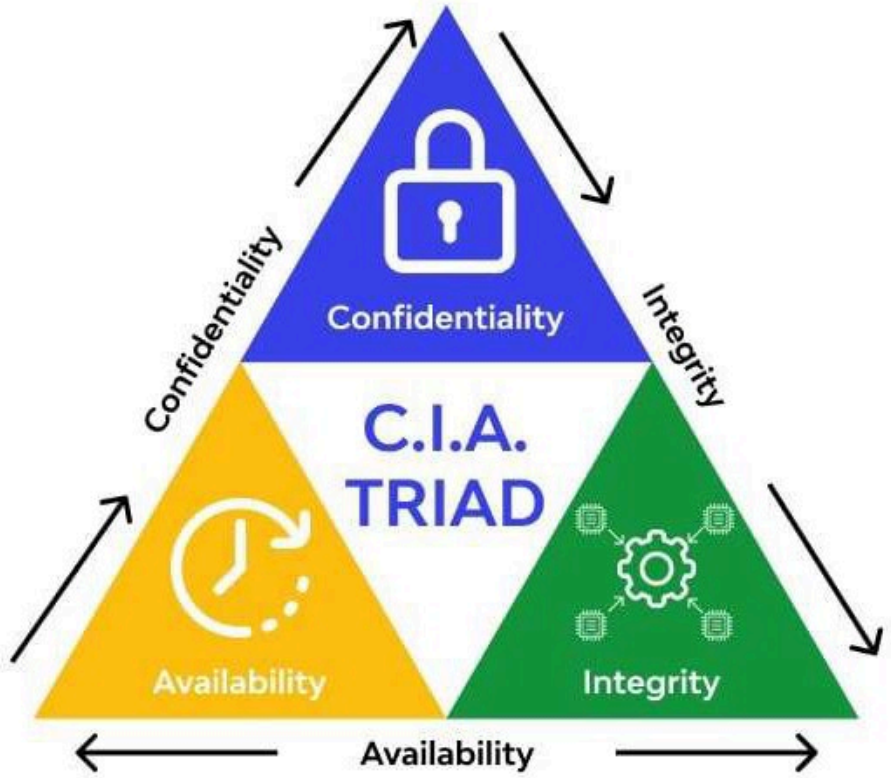
S'assurer que l'information est accessible uniquement par les ayants droit.

L'intégrité

S'assurer que l'information n'a pas été altérée ou modifiée par une entité non autorisée.

La disponibilité (Availability)

S'assurer que l'information reste disponible peu importe le moment de sa consultation.



BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Les principes complémentaires

La Traçabilité

S’assurer et remonter à l’origine de l’action.

L’authentification

S’assurer que uniquement les entités autorisées ont accès aux ressources.

La non-répudiation

S’assurer qu’une entité ne peut nier son implication dans une action.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Les principes complémentaires

La prévention

Appliquer le concept de la défense en profondeur.

La détection

Mettre en place un système de détection fiable et performant.

La réaction

Réagir de manière ordonnée en cas d’incident.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Les sources d’attaques

White Hat (hacker bien intentionné)

- Expert dans la sécurité des systèmes d’information et qui a pour but d’aider les organisations ou les entreprises à améliorer leur sécurité.
- Chercheur / conférencier / Développeur…

Gray Hat (hacker intentionné mais!)

- Expert qui peut parfois agir pour le bien.
- Il est prêt à dépasser les limites pour défendre une philosophie/idéologie.

Black Hat (hacker mal intentionné)

- Communément connu sous le nom du pirate informatique
- Il a comme objectif de nuire et détruire.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Les sources d’attaques

Script-Kiddies (hacker ?)

- Avec des connaissances très limitées dans le domaine de la sécurité informatique.
- Utiliser uniquement des outils existants dans le but de défacer un site web.
- Existe de plus en plus.

Les sources d’attaques

Motivation des hackers :

- **Curiosité** : Certains hackers sont motivés par la simple volonté de comprendre comment les systèmes fonctionnent et d'explorer de nouvelles technologies.
- **Politique** : D'autres hackers, souvent appelés "hacktivistes", sont motivés par des causes politiques ou sociales. Leur objectif peut être de perturber un gouvernement ou une organisation pour attirer l'attention sur une question particulière.
- **Profit** : Les hackers malveillants peuvent être motivés par l'appât du gain. Cela inclut le vol de données sensibles pour les vendre, ou l'implantation de ransomwares pour demander des paiements en échange de l'accès aux données volées.
- **Sabotage** : Certains hackers cherchent à nuire à une organisation pour des raisons personnelles ou professionnelles, par exemple en provoquant des perturbations dans les opérations ou en détruisant des données critiques.

L’origine des cyberattaques

Attaque ciblée	Attaque classique
• Grand impact sur la cible. • Basé sur une stratégie et une cible bien déterminée. • Avec de très bonnes compétences techniques. • Utilisation de techniques sophistiquées et furtivité. • Le gain financier ou industriel n’est pas immédiat. • Le coût est non négligeable.	• Impact faible ou moyen • La cible est découverte d’une façon opportuniste. • Variation des compétences (d’un script kiddie au hacker). • Les systèmes ciblés sont souvent non ou partiellement patchés. • Le gain rapide. • Recherche de la reconnaissance.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Les phases d'une attaque ciblée - La préparation

Définition des objectifs

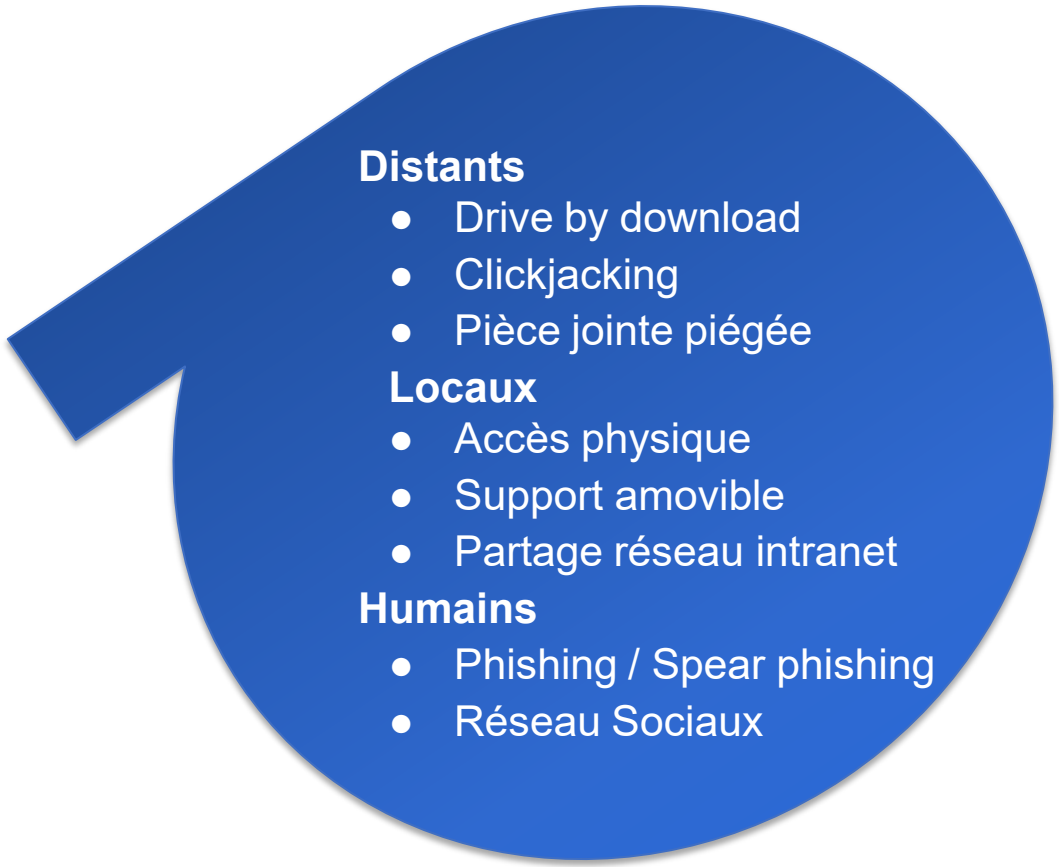
- L'espionnage industriel
- L'élimination de la concurrence
- Le profit
- La vengeance
- Cyberguerre

Préparation de l'attaque

- Prise d'empreintes (Reconnaissance)

Elaboration de la stratégie

- Les vecteurs d'attaque



BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Les phases d’une attaque ciblée - L’Intrusion

Repérage de l’infrastructure et des points d’entrées

- Organigramme de la structure.
- Identification de personnels.
- D’un site web à une non vérification de personnes habiles (port de badge obligatoire).

Intrusion furtive dans l’infrastructure de la cible

- La discrétion est la clé de la durée d’infiltration.
- Ciblage du facteur humain.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Les phases d’une attaque ciblée - Compromission

Compromission des systèmes d’information

- Prise de contrôle
- Récupération des identifiants…

Déploiement d’outils malveillants

- Backdoors, Remote Administration Tools (RAT)...
- Clé usb malveillante (Rubber Ducky…)

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Les phases d’une attaque ciblée - Extension

Elévation de privilèges

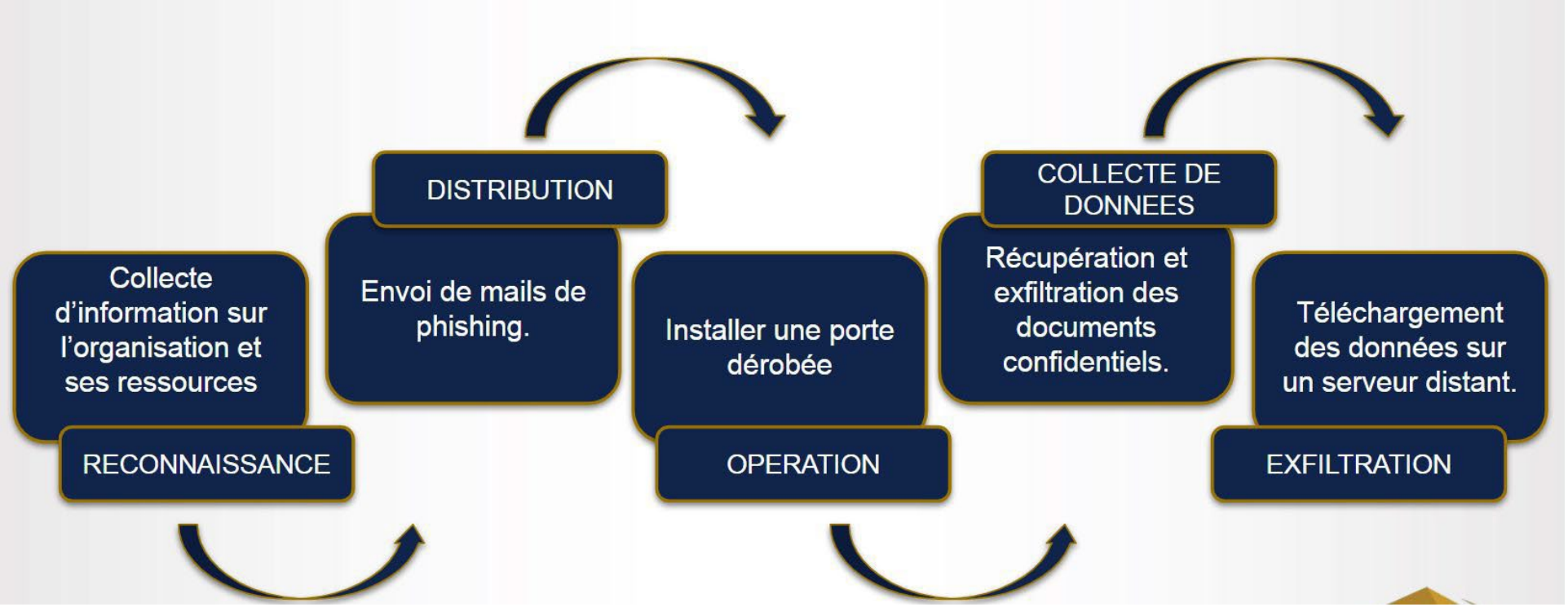
- Accroître les droits d’accès sur les systèmes compromis

Exfiltration de données

- Command & Control
- Revente sur la black market...

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Cyberkill Chain



BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

APT - Advanced Persistent Threat

- Acronyme créé dans les années 2000.
- Utilise tout un arsenal de techniques d'attaques pour atteindre l'objectif.
- La combinaison de différentes méthodes et outils en font une attaque avancée.
- Le but d'une APT est de rester le plus longtemps possible sans éveiller les soupçons (furtivité).
- Les attaquants sont dotés de compétences techniques très avancées.

Classification des malwares

Virus

- Ancien terme pour dire malware.
- Généralement caché dans un autre programme anodin.
- Il produit des copies de lui-même et les insère dans d'autres programmes.

Vers

- Généralement petit et autonome.
- Se réplique et se propage via le réseau.
- A pour but de détruire.

Spyware/adware (keylogger)

- Installé à l'insu de l'utilisateur et transmet des informations sur son activité.
- Fournit aux annonceurs des informations sur les habitudes de navigation.

Classification des malwares

Rootkit

- Un kit permettant de dissimuler l'activité malveillante.
- Il interagit souvent avec des fonctionnalités bas niveau du système.

Botnet (C&C)

- Réseau de machines zombies.
- Envoie des commandes pour DOS/DDOS...

Ransomware

- Chiffre les documents personnels et demande une rançon en échange.

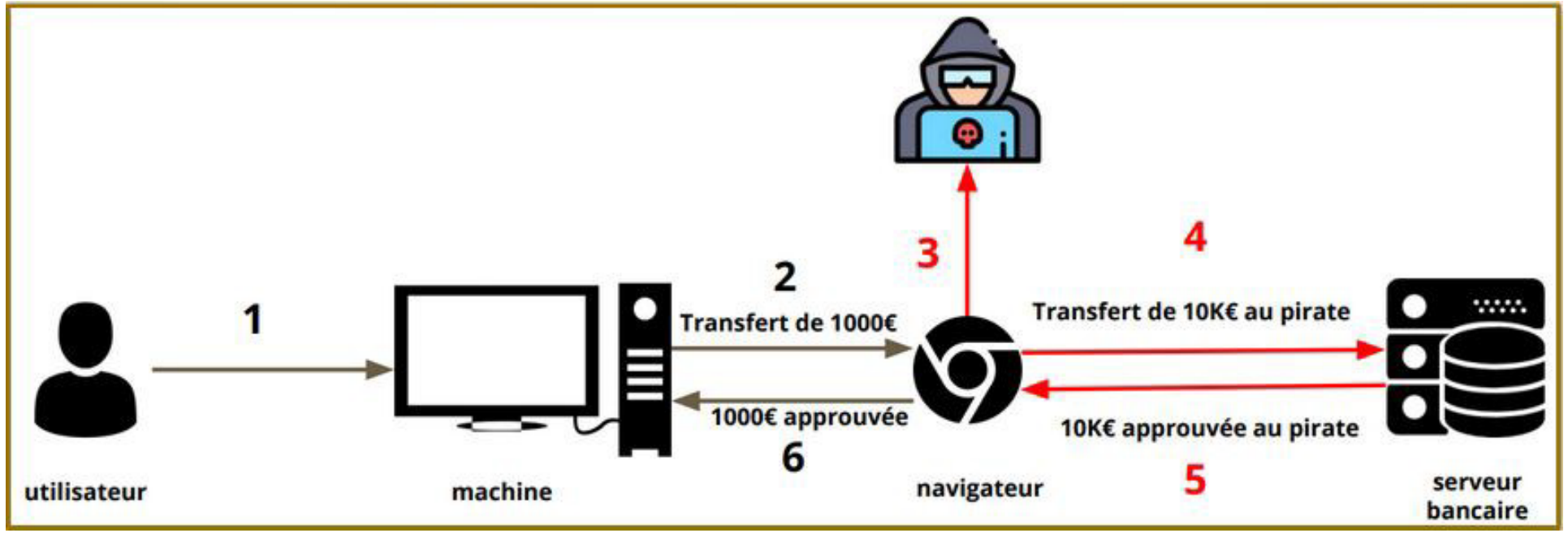
Crypto-mineurs

- Utilise les ressources de la machine pour miner des crypto-monnaies.

Symptômes d’infection

Changement des mots de passes

- Extension malveillante dans le navigateur (MITB).



BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Symptômes d’infection

Demande de rançon

- Causé par un ransomware qui prend en otage la machine.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Symptômes d’infection

Ralentissement du système (crypto-mineurs)

- Utilisation épuisante des ressources de la machine.
- Processeur en surchauffe continue.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Symptômes d’infection

Dans la majorité des cas aucun symptôme n'apparaît !

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Impossible de me faire pirater , ça n’arrive qu’aux autres !

Il existe deux types d’entreprises :

- Celles qui se sont fait piratées.
- Celles qui ne le savent pas encore.

Les cyberattaques évoluent chaque jour et peuvent être désastreuses

- Saint-Gobain (250 M€ de dégâts à cause de NotPetya).

La cible finale d’une cyberattaque est bel et bien les terminaux finaux

- PC, serveurs, mobile, tablette...

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Appliquer une sécurité optimale

Maintenir à jour les systèmes

- Solutions de protection de poste d'utilisateur (Antivirus…).
- Les systèmes (bulletins de sécurité, CVE…).
- Les applications (Java, Adobe…).

Sensibilisation et formation du personnel

- S'informer sur les attaques de bases des pirates informatiques.
- Ne pas être à la merci de l'attaquant.

Sensibilisation et formation particulière des administrateurs

- Les personnes les plus critiques pour une entreprise.
- Détiennent des accès admins sur tout le parc.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Questions a se poser

- Quel est le but de la cyberattaque ?
- Comment j'ai pu être une cible ?
- Quelle est la source qui nous prend pour cible ?
- Sont-ils très compétents ?
- Qu'est ce qu'ils ont volé ?
- Depuis combien de temps suis-je infecté ?
- Quels sont les équipements infectés ?
- Comment puis-je le savoir ?
- Comment puis-je me prémunir pour l'éviter dans l'avenir ?

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Panorama des solutions de Cybersécurité

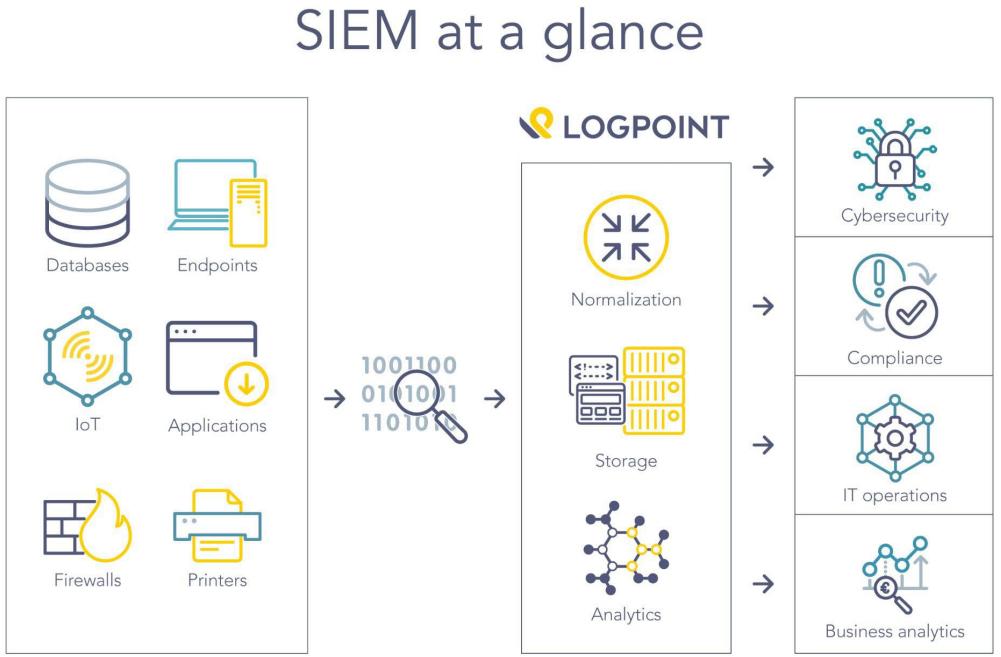
Les solutions Endpoint

Une catégorie d’outils et de solutions qui mettent l’accent sur la détection d’activités suspectes directement sur les hôtes du système d'information.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

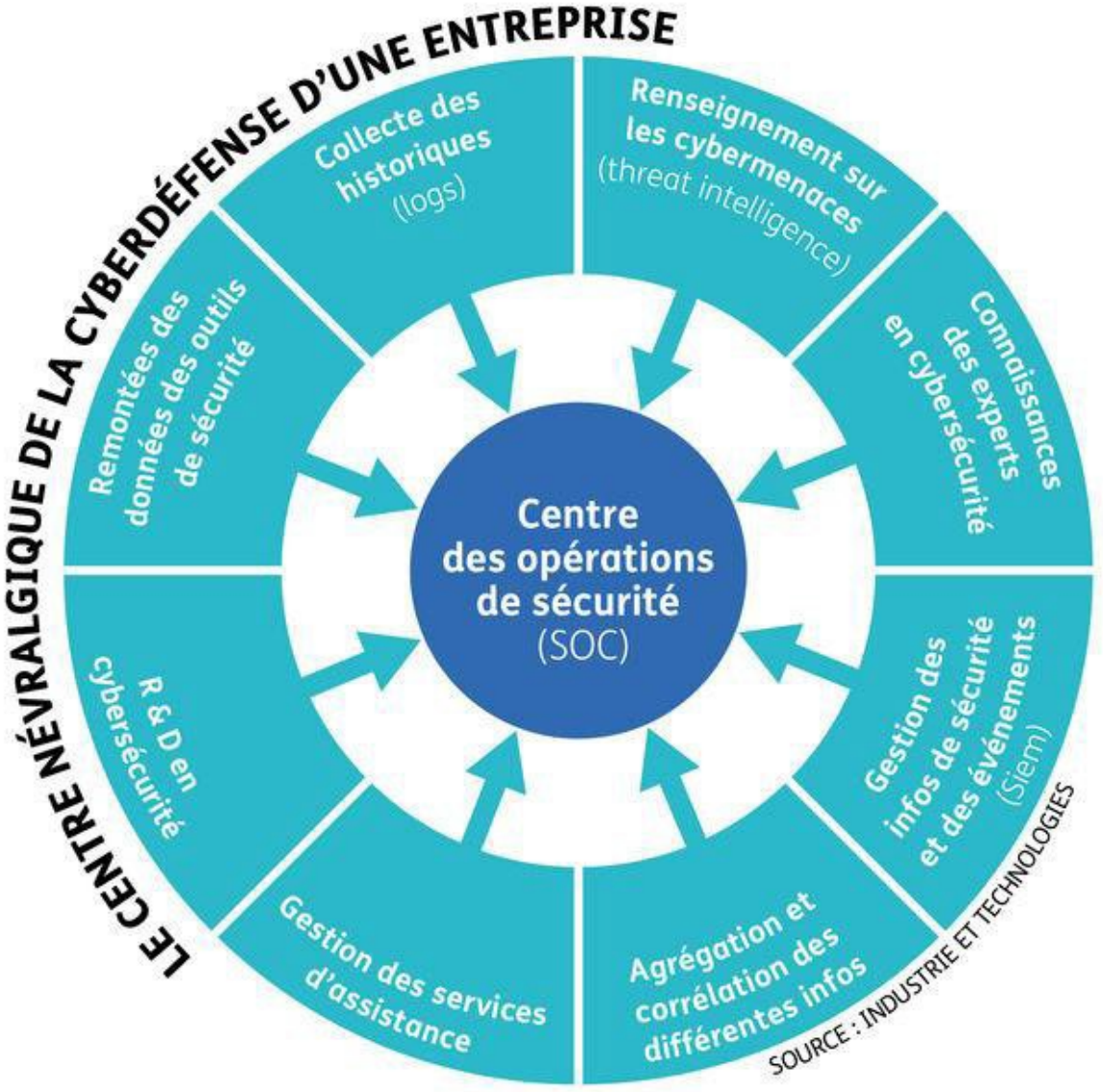
Les solutions SIEM

- L‘intégration avec d’autres contrôles.
- L’intelligence artificielle.
- Le flux d’informations quant aux menaces.
- Un rapport de conformité robuste.
- Capacités judiciaires.



BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Security Operation Center (SOC)



BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Le guide d’hygiène de l’ANSSI (1/10)

Sensibiliser et former

- Former les équipes opérationnelles à la sécurité des systèmes d’information.
- Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique.
- Maîtriser les risques de l’infogérance.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Le guide d’hygiène de l’ANSSI (2/10)

Connaître le système d’information

- Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau.
- Disposer d’un inventaire exhaustif des comptes privilégiés et le maintenir à jour.
- Organiser les procédures d’arrivée, de départ et de changement de fonction des utilisateurs.
- Autoriser la connexion au réseau de l’entité aux seuls équipements maîtrisés.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Le guide d’hygiène de l’ANSSI (3/10)

Authentifier et contrôler les accès

- Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur.
- Attribuer les bons droits sur les ressources sensibles du système d’information.
- Définir et vérifier des règles de choix et de dimensionnement des mots de passe.
- Protéger les mots de passe stockés sur les systèmes.
- Changer les éléments d’authentification par défaut sur les équipements et services.
- Privilégier lorsque c’est possible une authentification forte.

Le guide d’hygiène de l’ANSSI (4/10)

Sécuriser les postes

- Mettre en place un niveau de sécurité minimal sur l’ensemble du parc informatique
- Se protéger des menaces relatives à l’utilisation de supports amovibles
- Utiliser un outil de gestion centralisée afin d’homogénéiser les politiques de sécurité
- Activer et configurer le pare-feu local des postes de travail
- Chiffrer les données sensibles transmises par voie Internet.

Le guide d’hygiène de l’ANSSI (5/10)

Sécuriser le réseau

- Segmenter le réseau et mettre en place un cloisonnement entre ces zones.
- S’assurer de la sécurité des réseaux d’accès Wi-Fi et de la séparation des usages.
- Utiliser des protocoles réseaux sécurisés dès qu’ils existent. ○ Mettre en place une passerelle d’accès sécurisé à Internet.
- Cloisonner les services visibles depuis Internet du reste du système d’information.
- Protéger sa messagerie professionnelle.
- Sécuriser les interconnexions réseau dédiées avec les partenaires.
- Contrôler et protéger l’accès aux salles serveurs et aux locaux techniques.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Le guide d’hygiène de l’ANSSI (6/10)

Sécuriser l’administration

- Interdire l’accès à Internet depuis les postes ou serveurs utilisés pour l’administration du système d’information.
- Utiliser un réseau dédié et cloisonné pour l’administration du système d’information.
- Limiter au strict besoin opérationnel les droits d’administration sur les postes de travail.

Le guide d’hygiène de l’ANSSI (7/10)

Gérer le nomadisme

- Prendre des mesures de sécurisation physique des terminaux nomades.
- Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable.
- Sécuriser la connexion réseau des postes utilisés en situation de nomadisme.
- Adopter des politiques de sécurité dédiées aux terminaux mobiles.

Le guide d’hygiène de l’ANSSI (8/10)

Maintenir le système d’information à jour

- Définir une politique de mise à jour des composants du système d’information.
- Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Le guide d’hygiène de l’ANSSI (9/10)

Superviser, auditer, réagir

- Activer et configurer les journaux des composants les plus importants.
- Définir et appliquer une politique de sauvegarde des composants critiques.
- Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées.
- Désigner un référent en sécurité des systèmes d’information et le faire connaître auprès du personnel.
- Définir une procédure de gestion des incidents de sécurité.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Le guide d’hygiène de l’ANSSI (10/10)

Mener une analyse de risque formelle

- Le recours aux bonnes pratiques de sécurité informatique.
- Une analyse de risque systématique fondée sur les retours d’expérience des utilisateurs.
- Une gestion structurée des risques formalisée par une méthodologie dédiée.
- La méthode EBIOS est recommandée.

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Keepass

- Logiciel open source permettant la gestion des mots de passe (coffre-fort)
- Il suffit de retenir un seul mot de passe (passphrase)
- La base de données des mots de passe est chiffrée
    - Keepass 1.x : AES (256 bits) et Twofish (256 bits).
    - Keepass 2.x : AES (256 bits) et ChaCha20 (256 bits).

- Certifié par l'ANSSI
- https://www.ssi.gouv.fr/entreprise/certification_cspn/keepass-version-2-10-portable/
- https://keepass.fr/

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

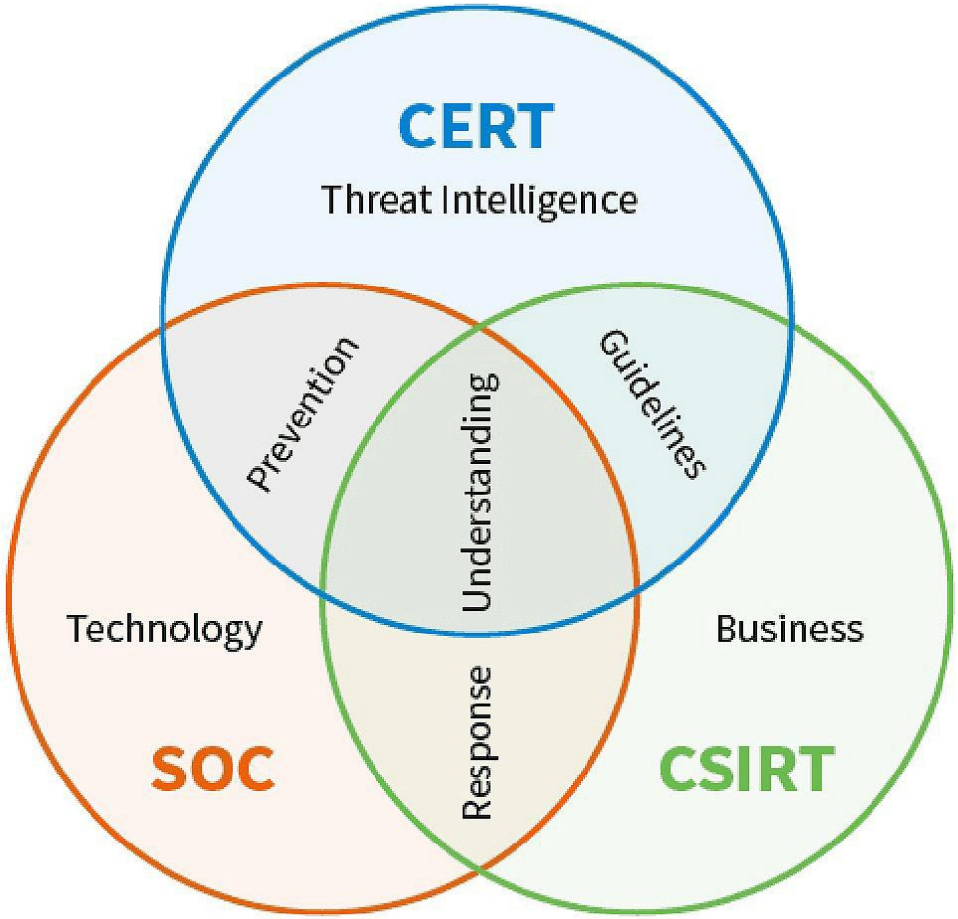
Les événements de hacking à ne pas rater !

CYBER MOIS

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

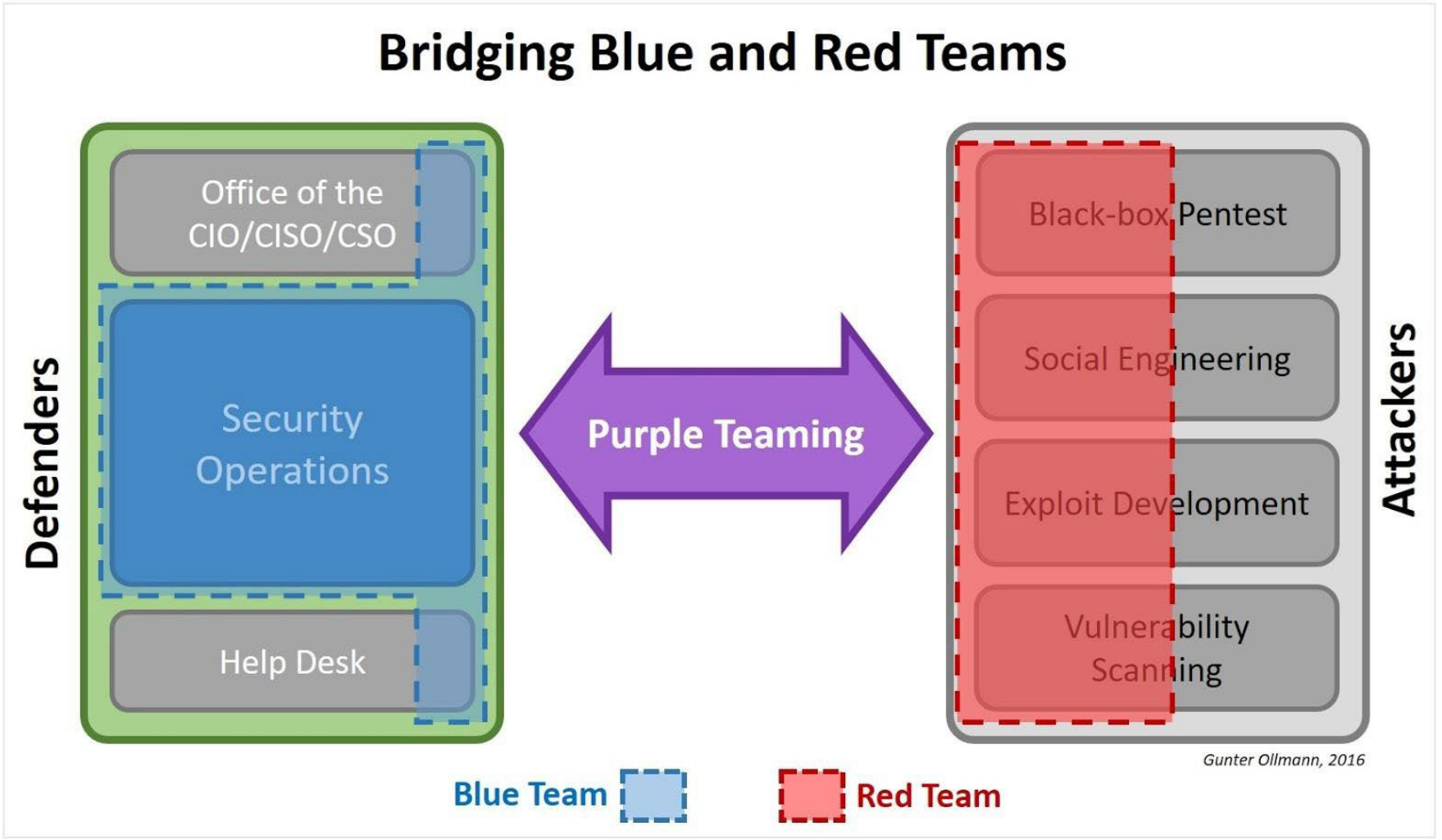
CERT / CSIRT / SOC

- **CSIRT**:
- Dès la réception d'une alerte de sécurité de la part du SOC, le CSIRT est chargé de mener les investigations relatives à l'incident de sécurité. Quand un CSIRT obtient l'autorisation de la part du SEI d'utiliser la marque CERT, celui-ci devient un CERT et intègre la communauté mondiale des CERT.



BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

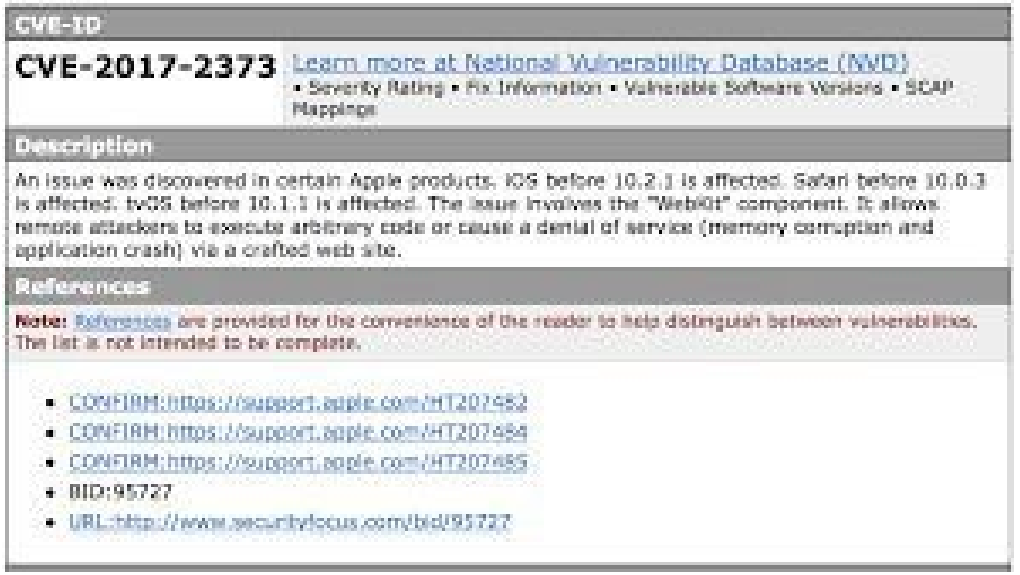
Red Team / Blue Team / Purple Team



BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

CVE : Common Vulnerabilities and Exposures

- Maintenue par MITRE (@CVEnew).
- Un dictionnaire qui recense des vulnérabilités en cybersécurité connues du grand public.
- L'objectif est d'identifier de manière unique et divulguer publiquement les vulnérabilités relatives à des versions spécifiques de logiciels.
- Possède la forme CVE-AAAA-NNNN (Année et numéro d'ID unique).



BCOPIN
CYBERSÉCURITÉ & SYSTÈMES

Questions ?

Formateur : Bertrand Copin
Linkedin : https://www.linkedin.com/in/bertrand-copin/
Site : https://www.bcopin.com
Mail : conseils@bcopin.com
Tél : 07 63 53 46 81

BCOPIN
CYBERSÉCURITÉ & SYSTÈMES