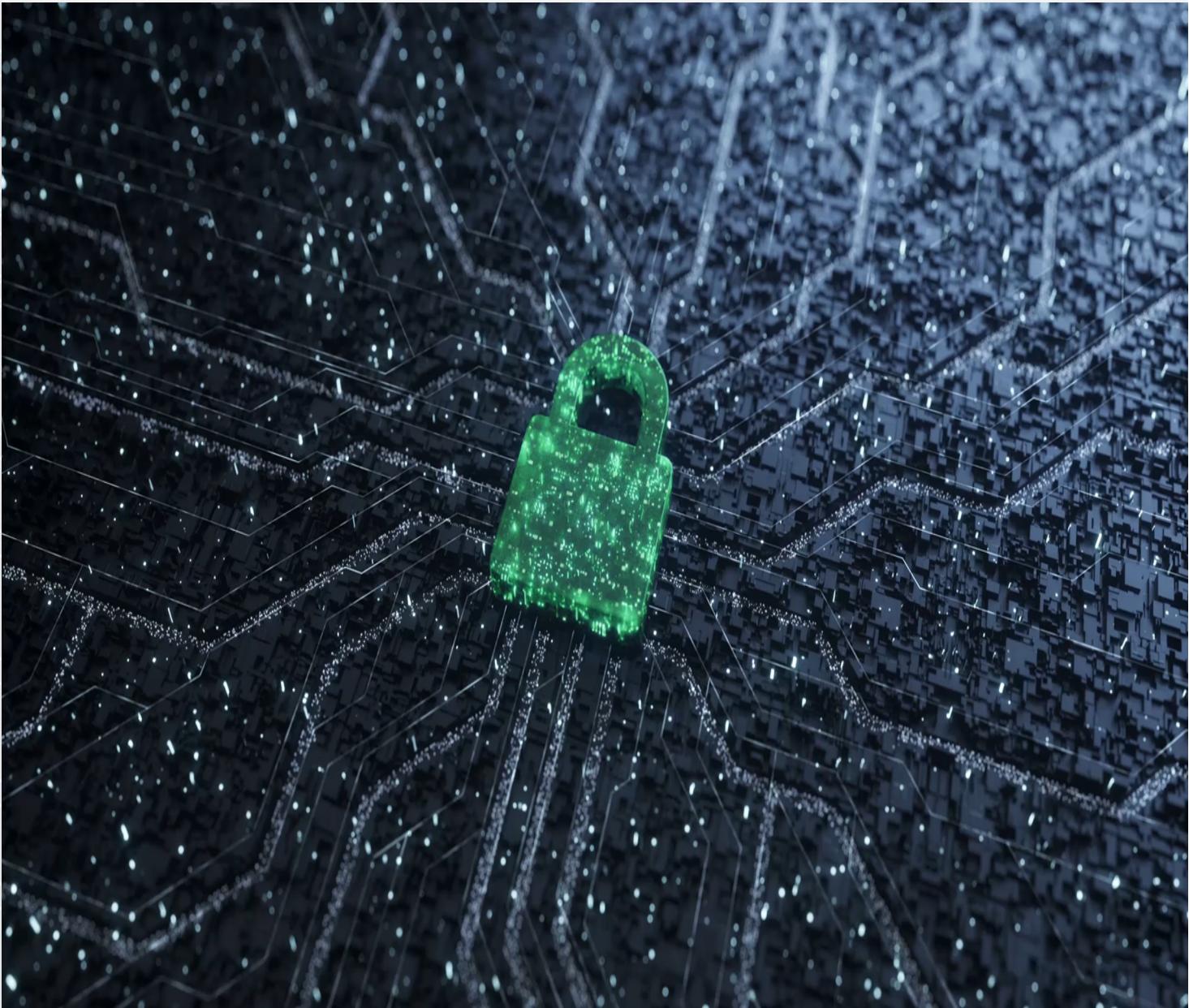


Cas : Fonctionnement d'une équipe de sécurité offensive en entreprise

Cyberconférence Cybereco 2022

Direction Sécurité offensive, Simulation d'adversaires

4 mai 2022



Agenda

- Introduction
- Bâtir une équipe de hacker
- Processus de tests
- Priorisation
- Rapports
- Risques et mitigations
- Conclusion

Présentation



Martin Dubé
Directeur Sécurité offensive,
Simulation d'adversaires

De jour ☀

- ❑ Directeur Sécurité offensive
- ❑ Tente de refaire le monde à coup de rencontres 🤘
- ❑ Raison de me lever le matin
 - ❑ Boire un bon espresso ☕
 - ❑ Innover

De soir 🌙

- ❑ Père de 2 👪
- ❑ Bidouilleur (Hacker) 😈
- ❑ Malware Dev 💀
- ❑ Woodworker 🪚
- ❑ Coureur 🏃

Qu'est-ce que cette image évoque en vous?



**HACKER
ÉTHIQUE**



**CYBER-
CRIMINEL**

Bâtir une équipe de Hacker: Recrutement

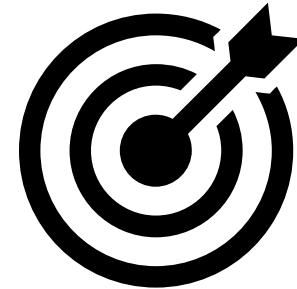
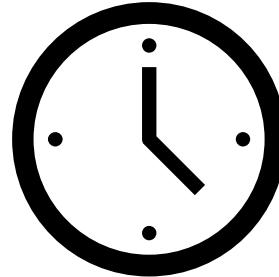
Où?

- Évènements de sécurité
 - Nsec.io (Mtl)
 - Hackfest.ca (Qc)
- Activités Mensuelles
 - Montrehack (Mtl)
 - MtlSec (Mtl)
 - QuébecSec (Qc)
- Réseaux sociaux
 - Discord
 - Slack
 - LinkedIn

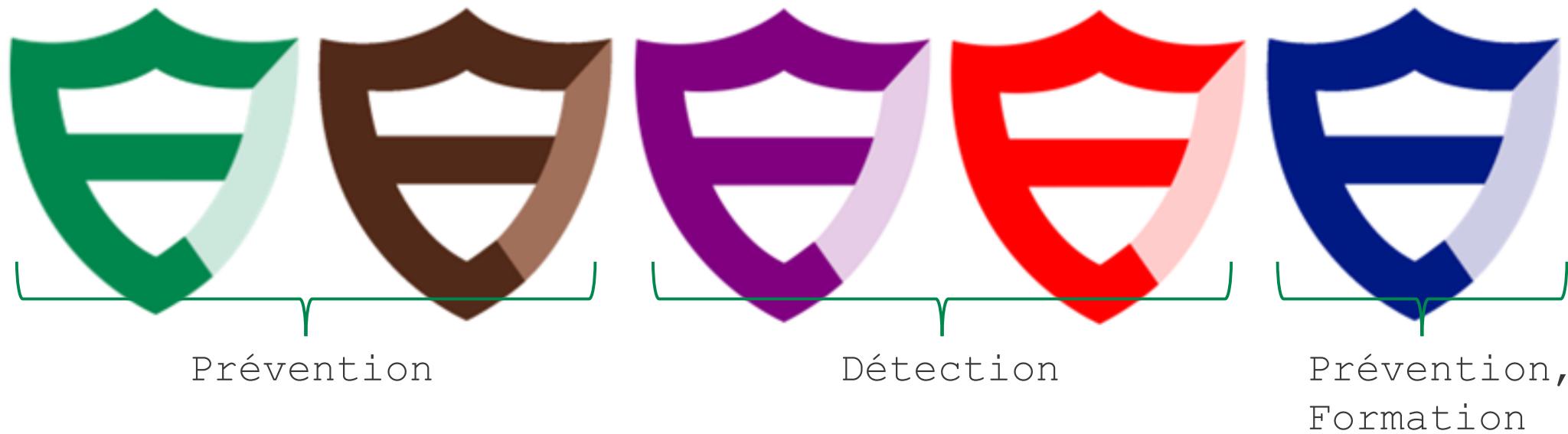
Comment?

- Tests techniques, par exemple :
 - Tests développés maison
 - Plateforme en ligne (ex. HTB)
 - Rédaction d'un rapport
- Entrevues : mises en situation
 - Éviter les questions pièges
 - Éviter les questions clichées
 - Favoriser les mises en situation

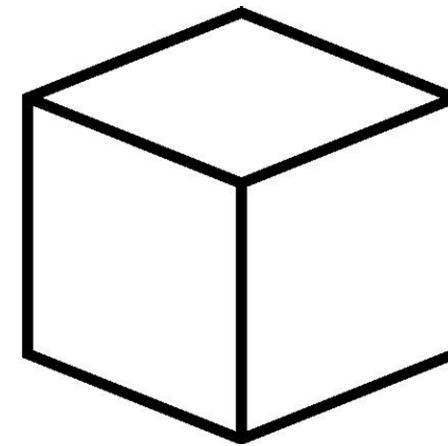
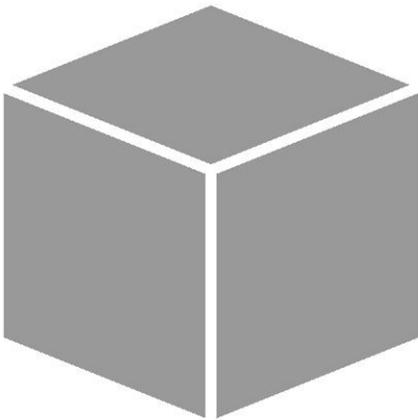
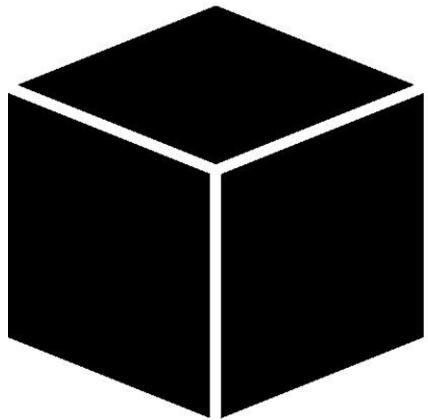
Bâtir une équipe de Hacker: Formation



Bâtir une équipe de Hacker: Focus

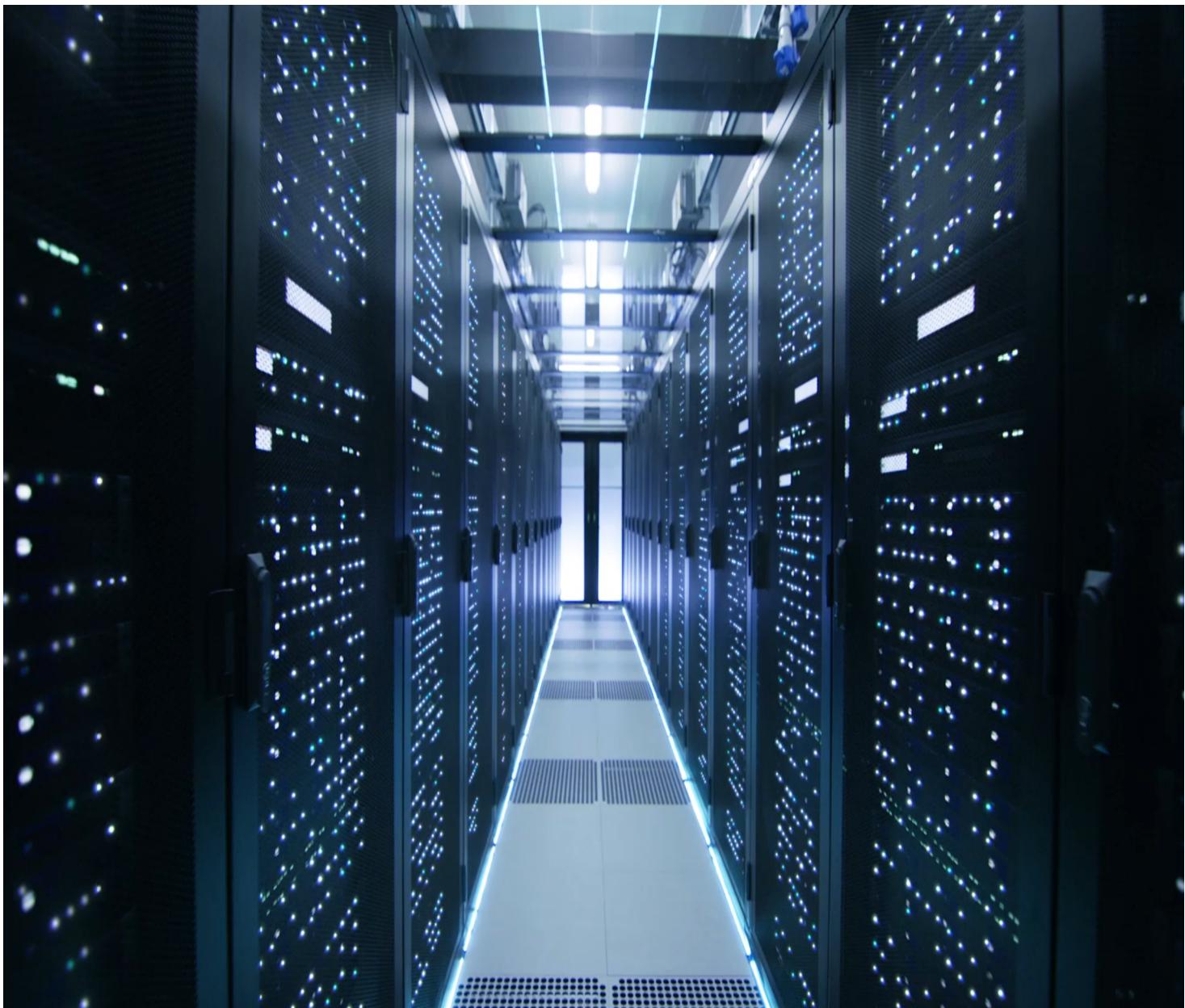


Méthodologies



Catalogue de service

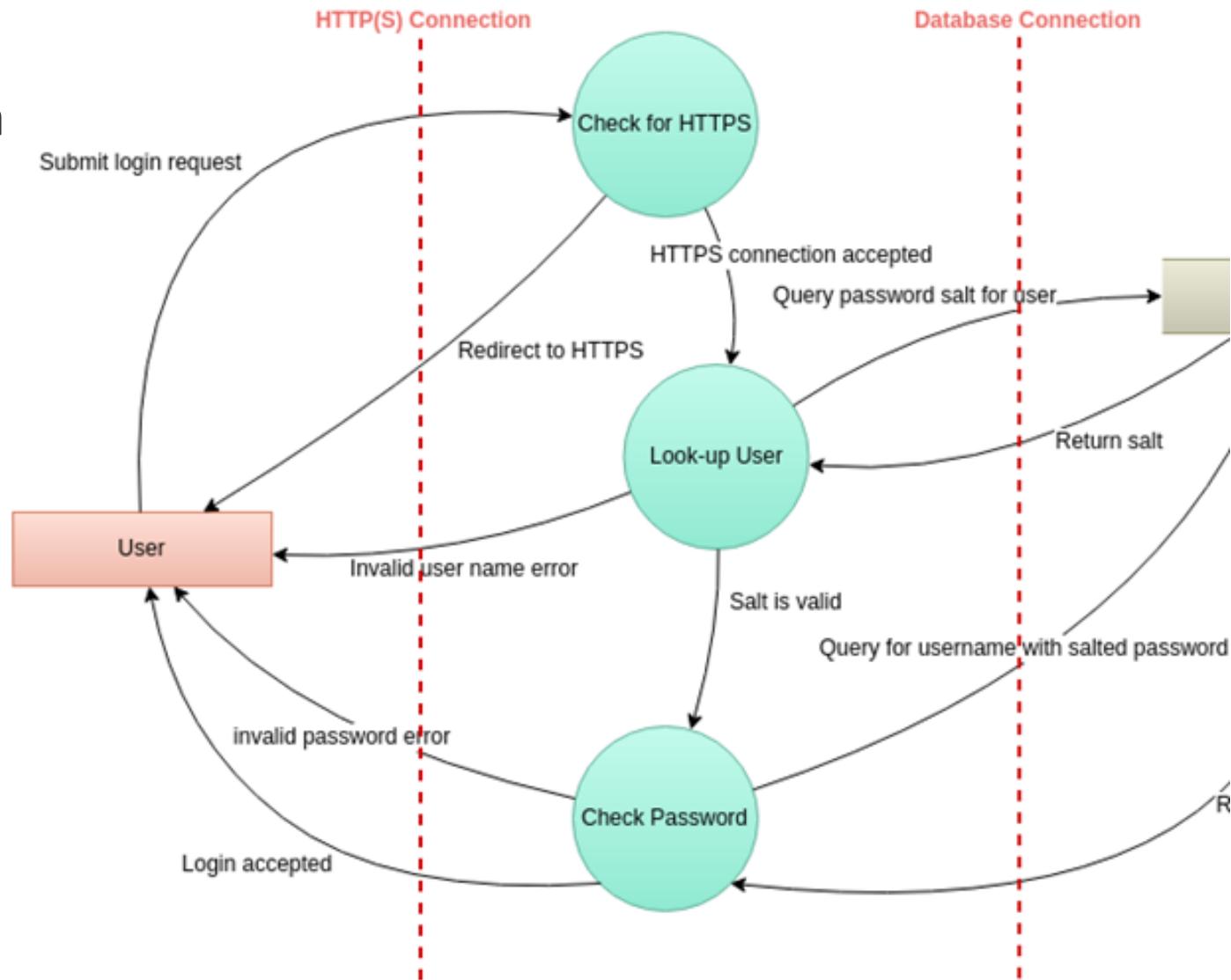
- Test d'intrusion Web
- Test d'intrusion interne
- Test d'intrusion externe
- Test d'intrusion Applications mobiles
- Test d'intrusion Wifi
- Test IoT et Ingénierie Inverse
- Chasse aux vulnérabilités
- Exercice de *Purple Team*
- Simulations d'adversaires
- Et plus (Contributions, Incidents)*



Priorisation

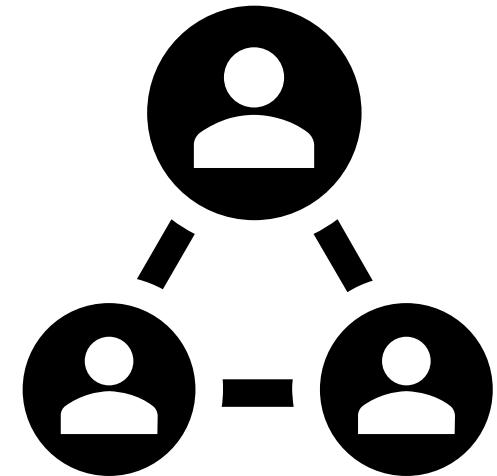
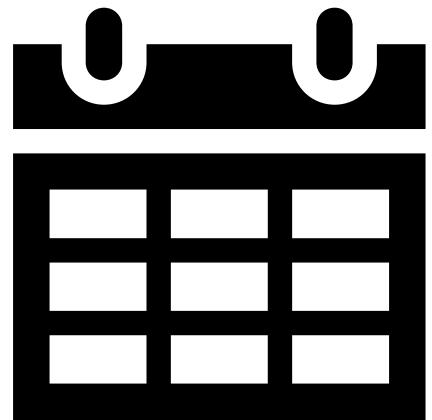
La sécurité débute par la maîtrise de sa surface d'attaque

- Intranet le plus payant : *Threat Model*
 - Identifie les menaces à simuler
 - Identifie les prérequis aux tests
 - Assure une bonne couverture
- Exemple de diagrammes
 - Data flow diagram*
 - Attack Tree*
- OWASP Threat Modeling*



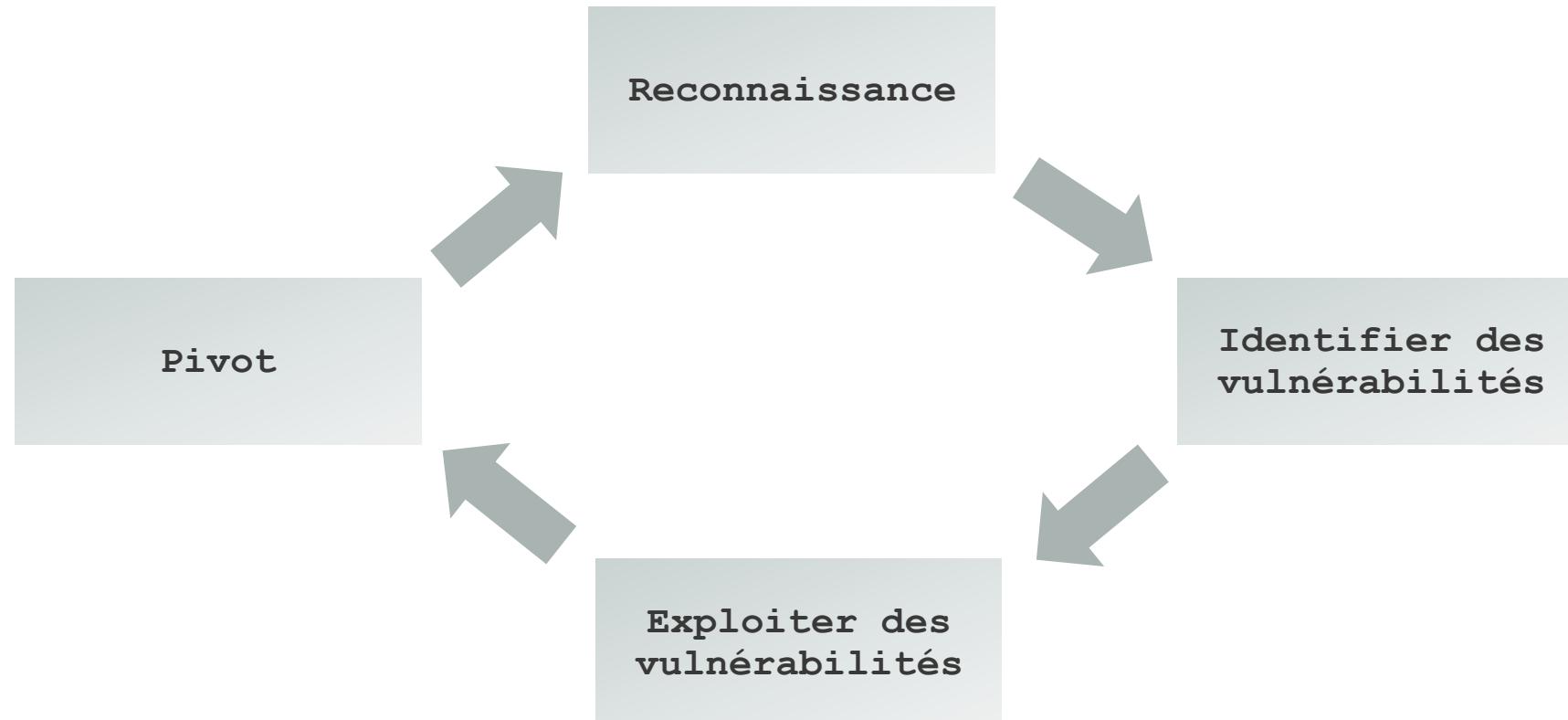
Processus de test

Préparation



Processus de test

Déroulement du test



Processus de test

Rapport

- Sommaire exécutif
- Vulnérabilités: Titre, Description, Risque technique, CVSS, Preuve de concept, Référence
- ! Posture de sécurité
- ! Risques techniques
- ! Menaces concrétisées
- ! Chemins d'attaque

Présentation

- Assure la compréhension
- Opportunité de vulgariser
- Aborder les questions

KPI / Volumétrie

- Produire des tendances pour mieux conseiller la gestion
 - Vulnérabilité - Enjeux
 - Risques
- Contribuer aux orientations de sécurité
 - AoW: *Next best move?*

Rapport

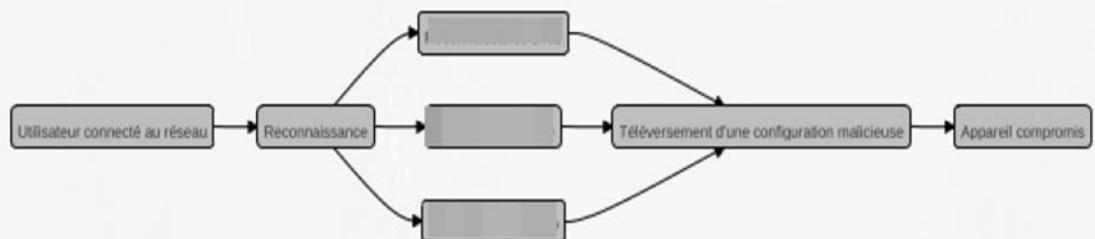
Chaîne d'attaque

- Montrer visuellement la chaîne d'exploitation
- Mettre en évidence le maillon qui briserait la chaîne

Menaces

- Menace interne (ex. employé)
- Poste compromis
- Attaque d'APT

Scénario d'attaque



Exemple de schéma fait avec mermaid.

Sommaire

Accès depuis le réseau intranet

Téléversement de configuration frauduleuse.

Rapport

Posture de sécurité

- ❑ Vulgariser en un seul chiffre la posture de l'actif testé



Risques concrétisés

- ❑ Se baser sur la taxonomie de l'organisation
- ❑ Mieux le risque est compris, meilleur est le correctif



Sophistication

- ❑ Exploitée en 5 minutes par un outil public ou a nécessité 5 jours de développement?



Les risques associés aux tests

Risques

- ❑ Un test d'intrusion peut avoir des impacts négatifs
 - ❑ Actif informationnel
 - ❑ Panique / Incidents
- ❑ Les résultats peuvent être trompeurs si les conditions du test n'étaient pas réalistes
 - ❑ Ex. : réaliser des tests dans un environnement de développement
- ❑ Un testeur pourrait garder des vulnérabilités pour lui
 - ❑ Sujet à débat: Watch the watchers

Mitigations

- ❑ Sensibiliser les testeurs
 - ❑ Règles d'engagement et code de déontologie
 - ❑ Tester les nouvelles attaques en laboratoire
 - ❑ Maîtriser l'impact des attaques (ex. Zerologon CVE-2020-1472)
- ❑ Publier un calendrier de tests
- ❑ S'annoncer aux équipes de défense
- ❑ Documenter et communiquer un bon processus d'escalade
- ❑ Formation
- ❑ Red Team: Cellule Blanche (White-cell)

Conclusion

Leçons apprises

- ❑ Le *ethical hacking* est une profession intellectuelle qui met à profit la curiosité, créativité et débrouillardise.
- ❑ Le *Threat Modeling* est le future de la priorisation des travaux de sécurité
- ❑ Adapter notre langage est important (ex: connecter les vulnérabilités à des risques)
- ❑ On peut faire plus que trouver des vulnérabilités (Contributions, Incidents, Workshop)
- ❑ Comme tout humain, on aime sentir qu'on fait une différence
- ❑ Vive la collaboration: Red  vs Blue 

Merci!



Desjardins