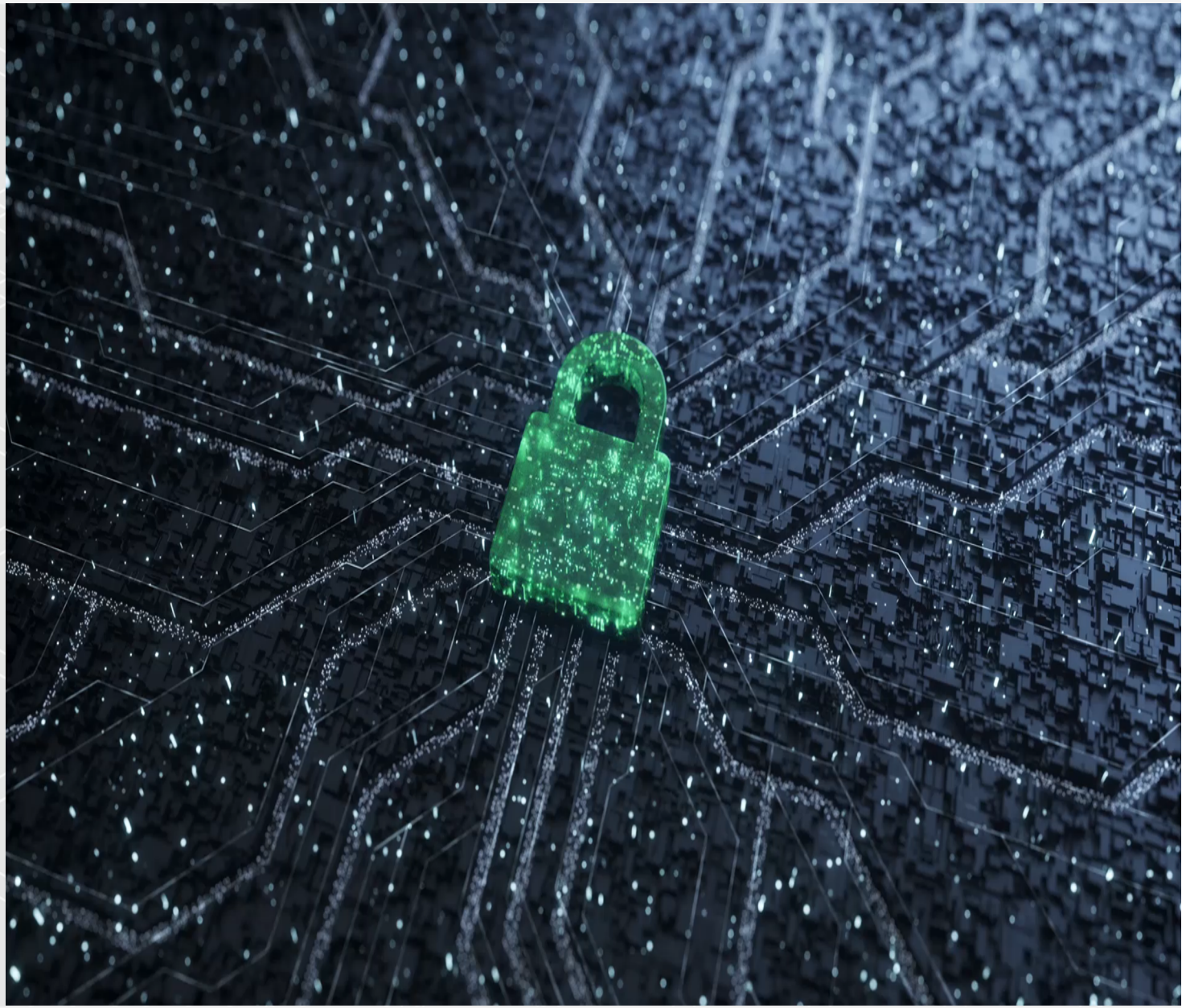
Bleu + Rouge = Mauve
1 seul objectif!

Cyberconférence Cybereco 2023

18 avril 2023

Desjardins



Agenda

1. Qui sommes-nous?
2. Qu’est-ce que « Purple Teaming »
3. Outils
4. Conclusion

Bio: Martin Dubé

Martin Dubé
Directeur Sécurité offensive,
Simulation d'adversaires

De jour

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

De soir

- Père de 2
- Bidouilleur (Hacker)
- *Malware Dev*
- Apprenti DevOps
- *Woodworker*
- Coureur

Bio: Dany Lafrenière

De jour

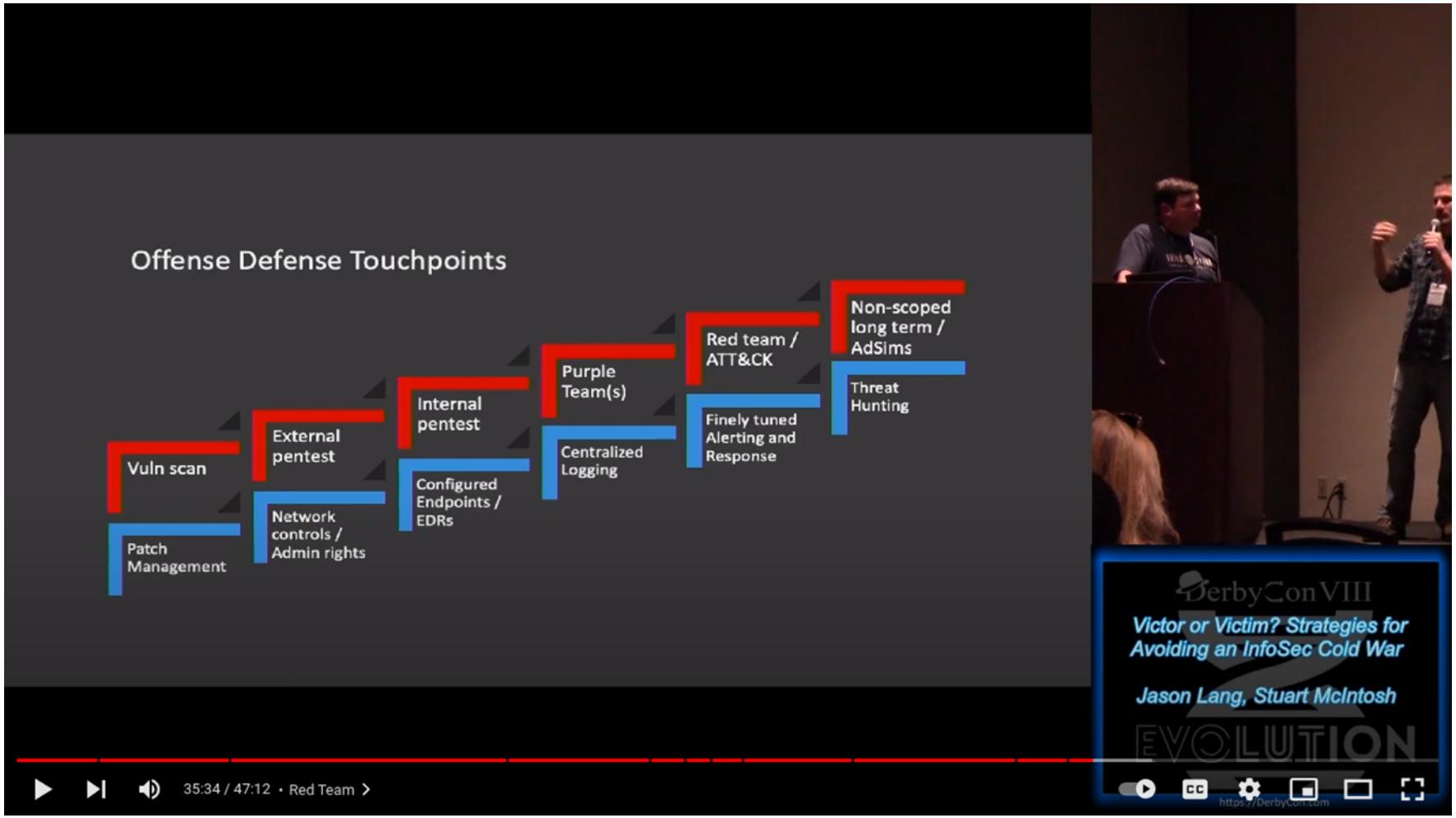
- Maitrise du jeu Tetris Agenda
- Fervent du « tierless SOC »
- Raisons de me lever le matin
  - Alarme à 5 AM
  - Défendre, avec un groupe de passionnés, nos membres et clients
  - Brainstormer avec Martin …

De soir

- Marcher
- Méditer
- Écouter de la musique
- Lectures et recherches
- « Binger » une série télé …

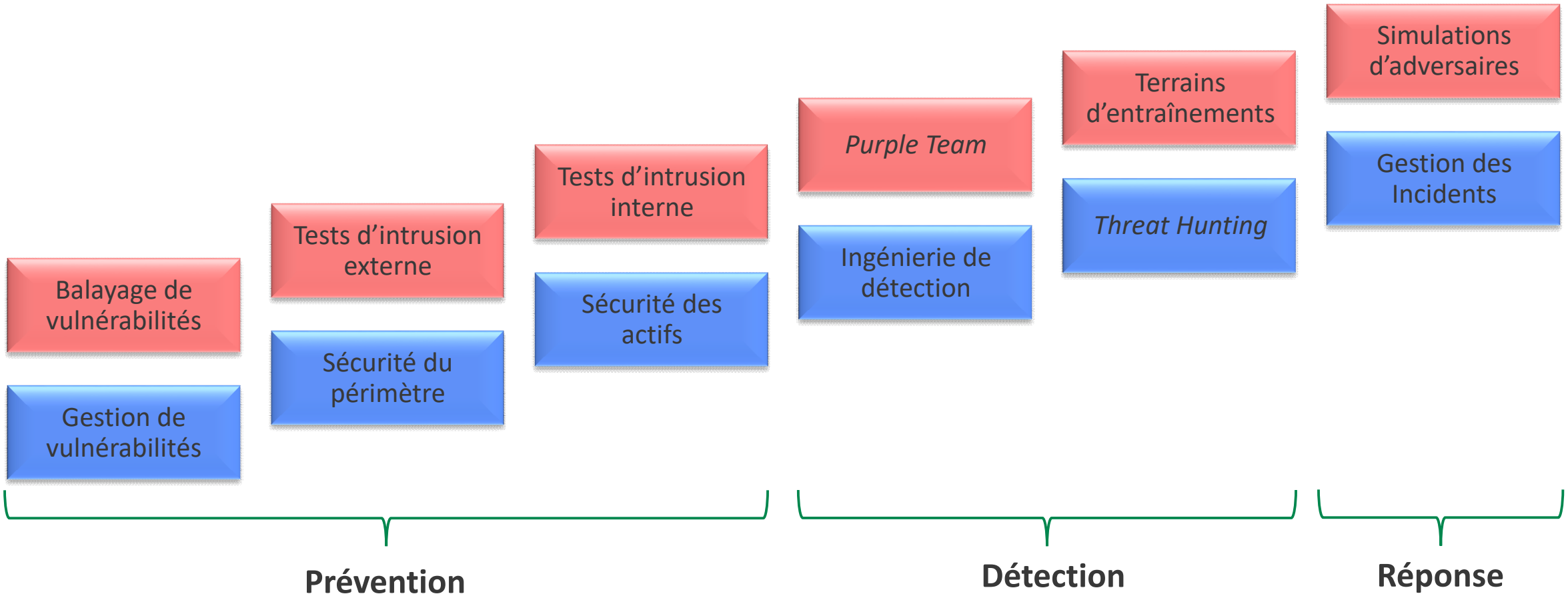
Dany Lafrenière
Directeur Investigation de Sécurité de l'information

Inspiration pour cette présentation



Source: https://www.youtube.com/watch?v=9_cZ5xn-huc

Points de rencontre entre l'attaque et la défense



Qu’est-ce que le purple teaming?

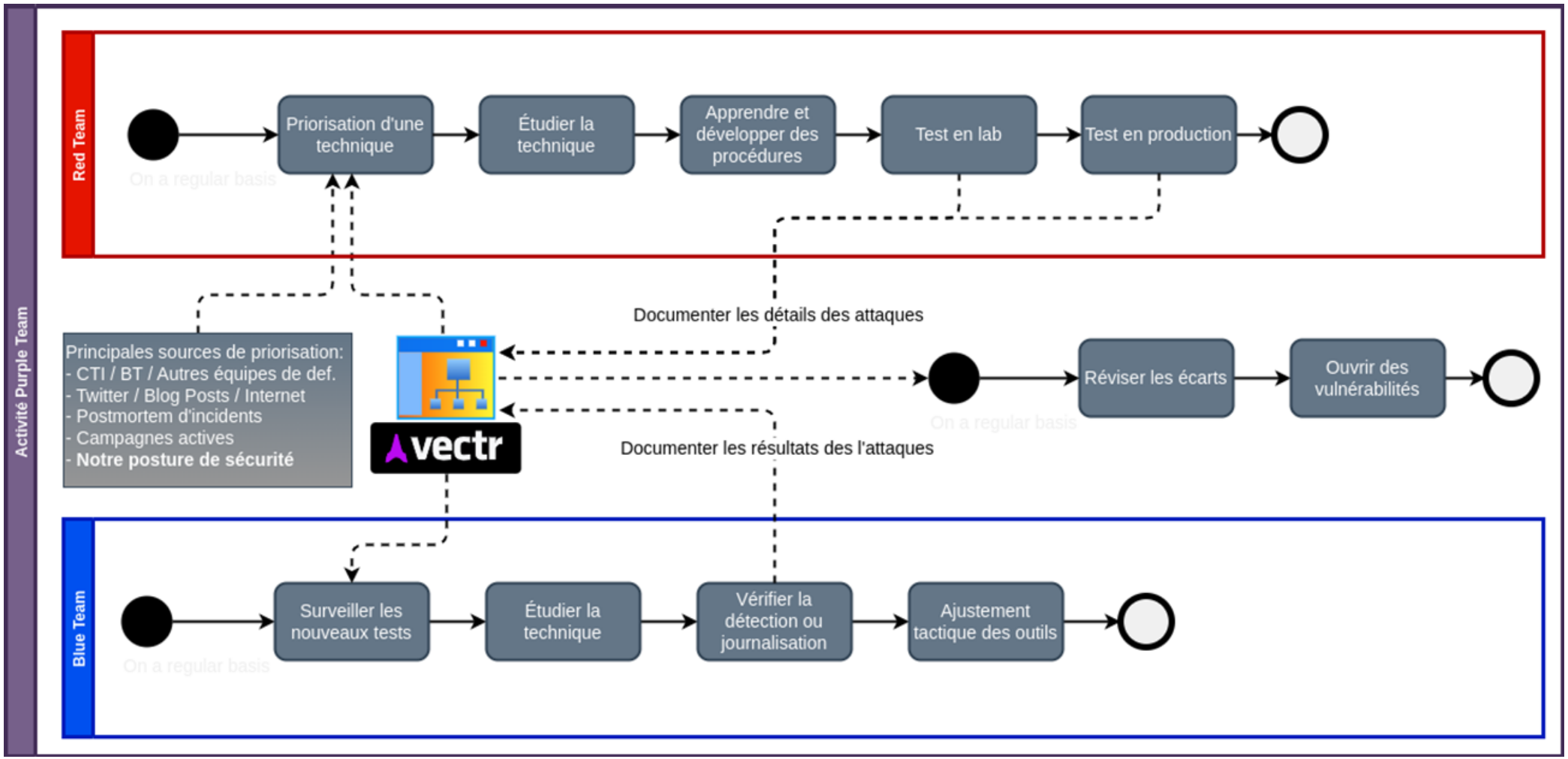
La genèse de l'arc-en-ciel :rainbow:

Le *purple teaming* est un état d'esprit coopératif entre les attaquants et les défenseurs travaillant du même côté. Il doit être pensé comme une fonction plutôt que comme une équipe.

Activités des *Blue Teams*	Activités des *Purple ~~Teams~~*	Activités des *Red Teams*
Objectif: Défendre	Objectif: Améliorer la posture	Objectif: Tester la résilience
Requiert: Autonomie	Requiert: Collaboration	Requiert: Un incident (surprise)
Vélocité: Élevé	Vélocité: Élevé	Vélocité: Faible

https://danielmiessler.com/study/red-blue-purple-teams/

Processus *Purple*



Risques et mitigations

Risques

- Un tests peuvent 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
  - Ne pas prioriser les bonnes techniques
- Un débalancement dans la charge de travail des 2 équipes peut avoir des effets pervers
  - Volume de test
  - Disponibilité des équipes

Mitigations

- Encadrer les tests
  - Règles d'engagement et code de déontologie
  - Tester les nouvelles attaques en laboratoire
  - Maîtriser l'impact des attaques (ex. Zerologon CVE-2020-1472)
  - S'annoncer aux équipes de défense
  - La priorisation doit être basé sur les risques et menaces
- Structurer les tests dans des plages
- Les activités doivent être asynchrones
- Documenter et communiquer un bon processus de prise en charge des résultats

Équipe ou Équipes?

- Qu’est-ce qui distingue une équipe d’un groupe de personnes?
  - L’équipe a un **objectif commun**

- Une équipe mauve est une équipe virtuelle, composée de plusieurs équipes
  - Un objectif commun et clair
  - Autonome
  - Maître de son art

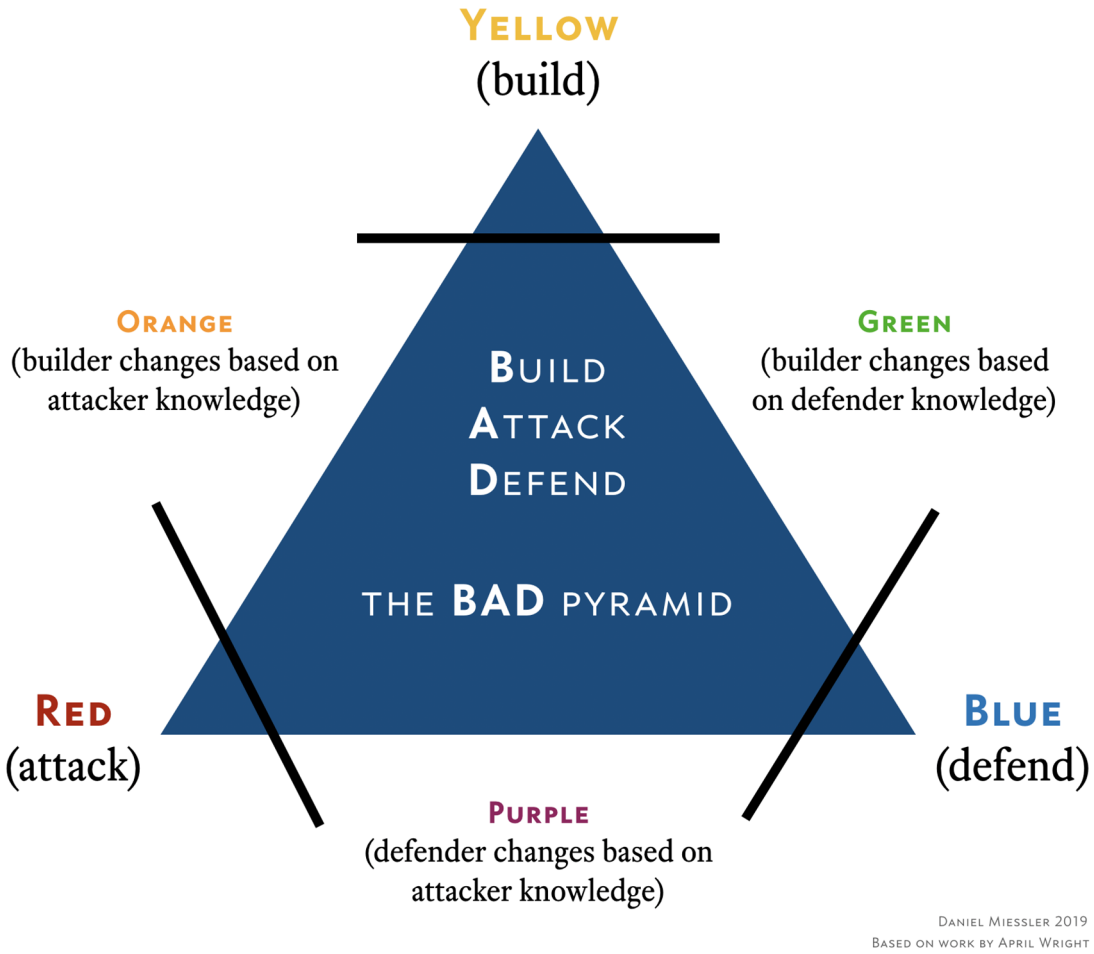
Cohésions !

- La confiance est un élément fondamental dans toutes les relations
  - Consistance
  - Communication
  - Temps

- Accueillir les différences entre les 2 équipes
  - Une journée typique: Déluge constant d'évènements vs Développer des *POC* en laboratoire
  - Sentiment d'accomplissement: Défendre l'organisation vs Proactivement identifier des vulnérabilités
    - Les 2 équipes **protègent** l'organisation… à leurs façons!
    - Les 2 équipes vont célébrer leurs victoires… la victoire!

Le triangle chromatique

- Le *Blue Team* est souvent en charge d'augmenter toutes les défenses
  - Est-ce réaliste?
- Honorons la mission de chaque équipe
  - Rouge: Identifier des augmentations de défenses
  - Bleu: Défendre l'organisation
  - Jaune: Augmenter les défenses
- Collaboration!

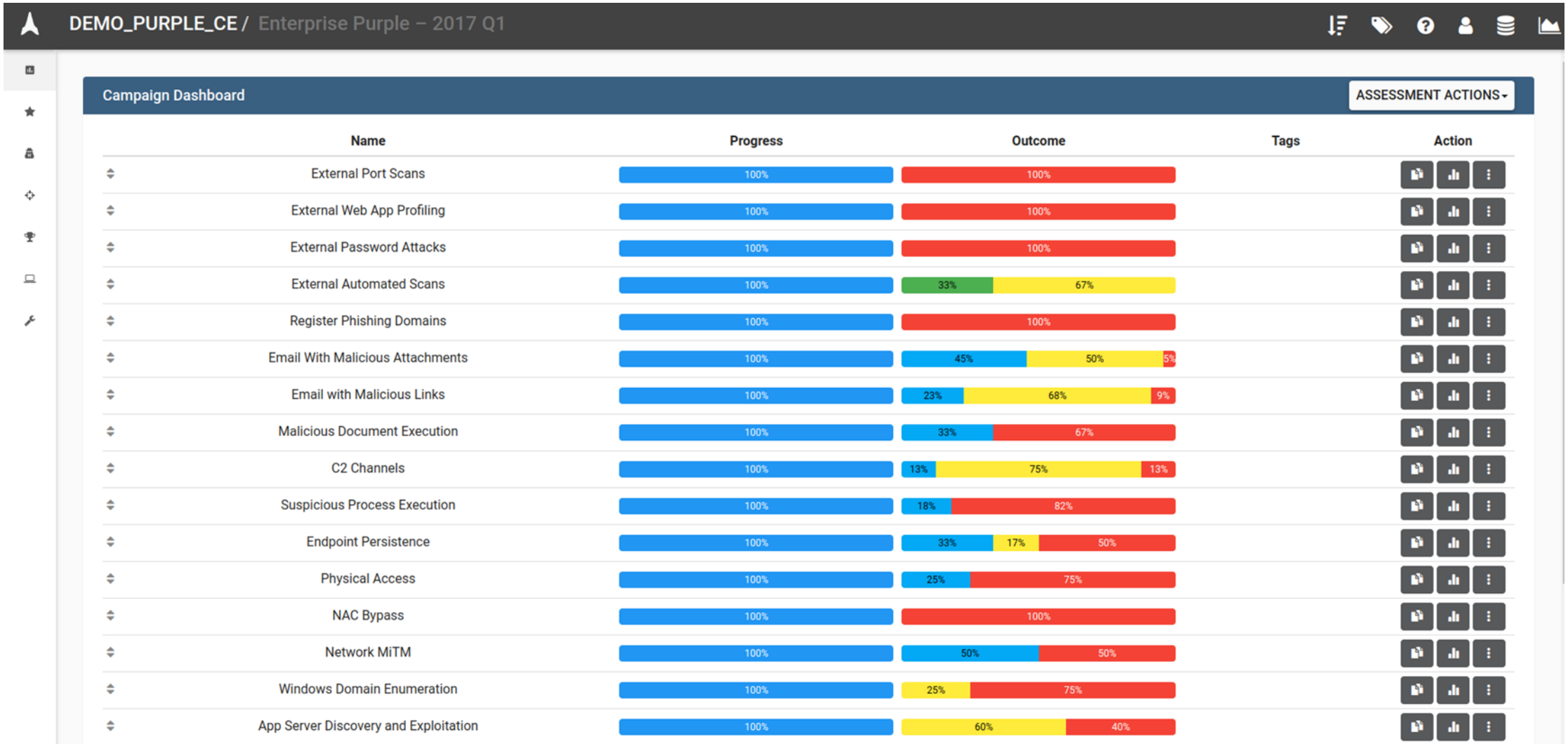


The BAD pyramid: https://danielmiessler.com/study/red-blue-purple-teams/

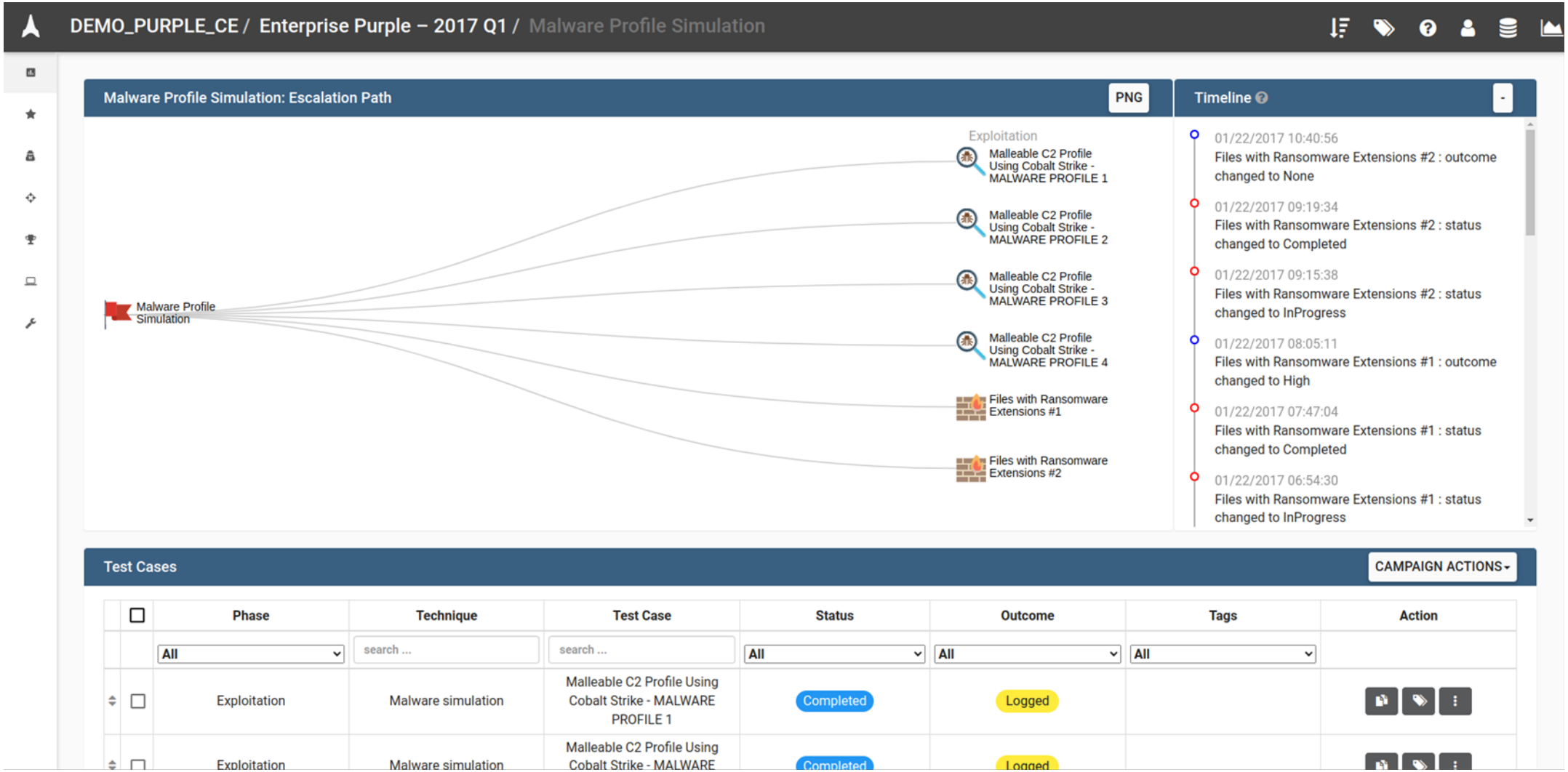
Outils

Alternatives à des chiffriers Excel…

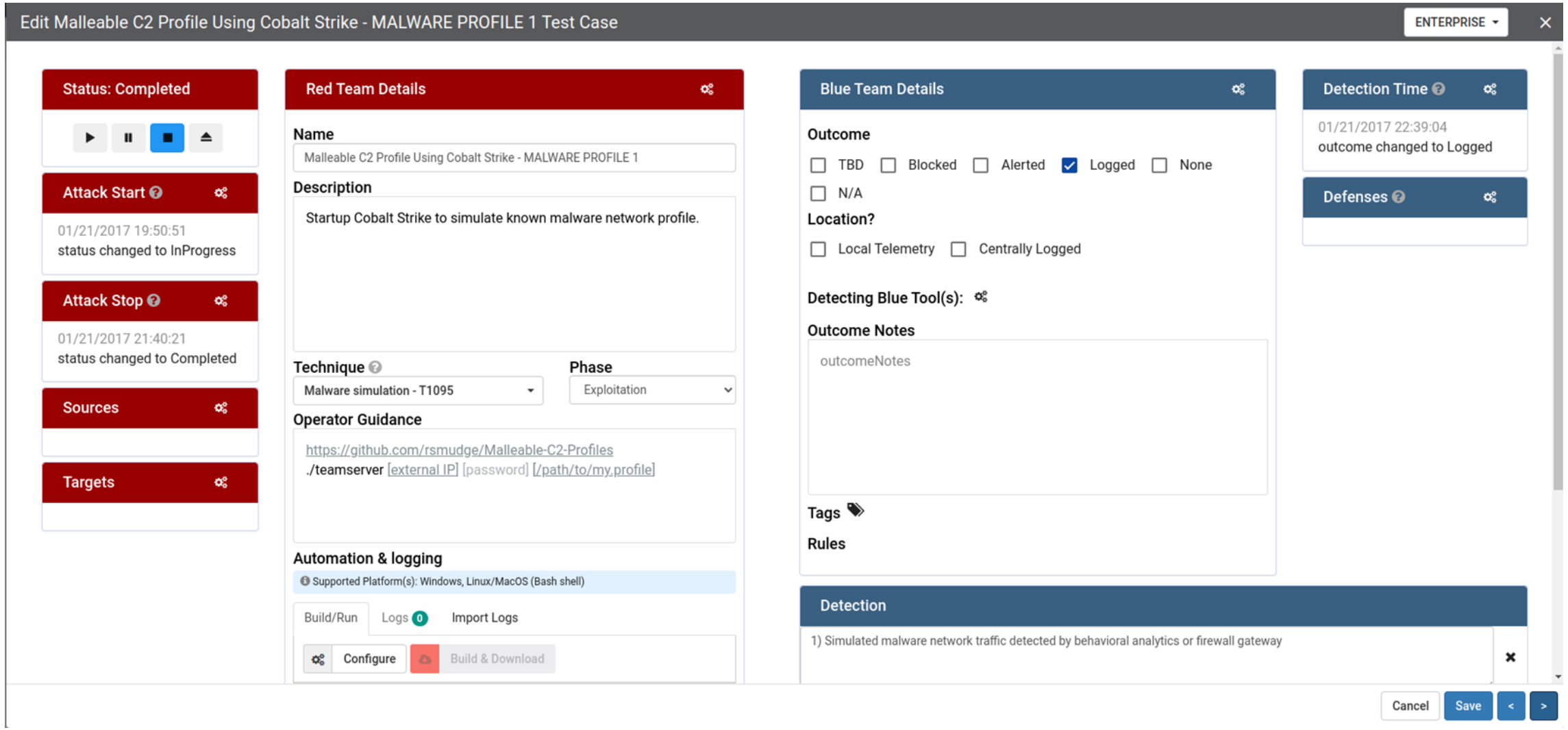
Outils: Vectr



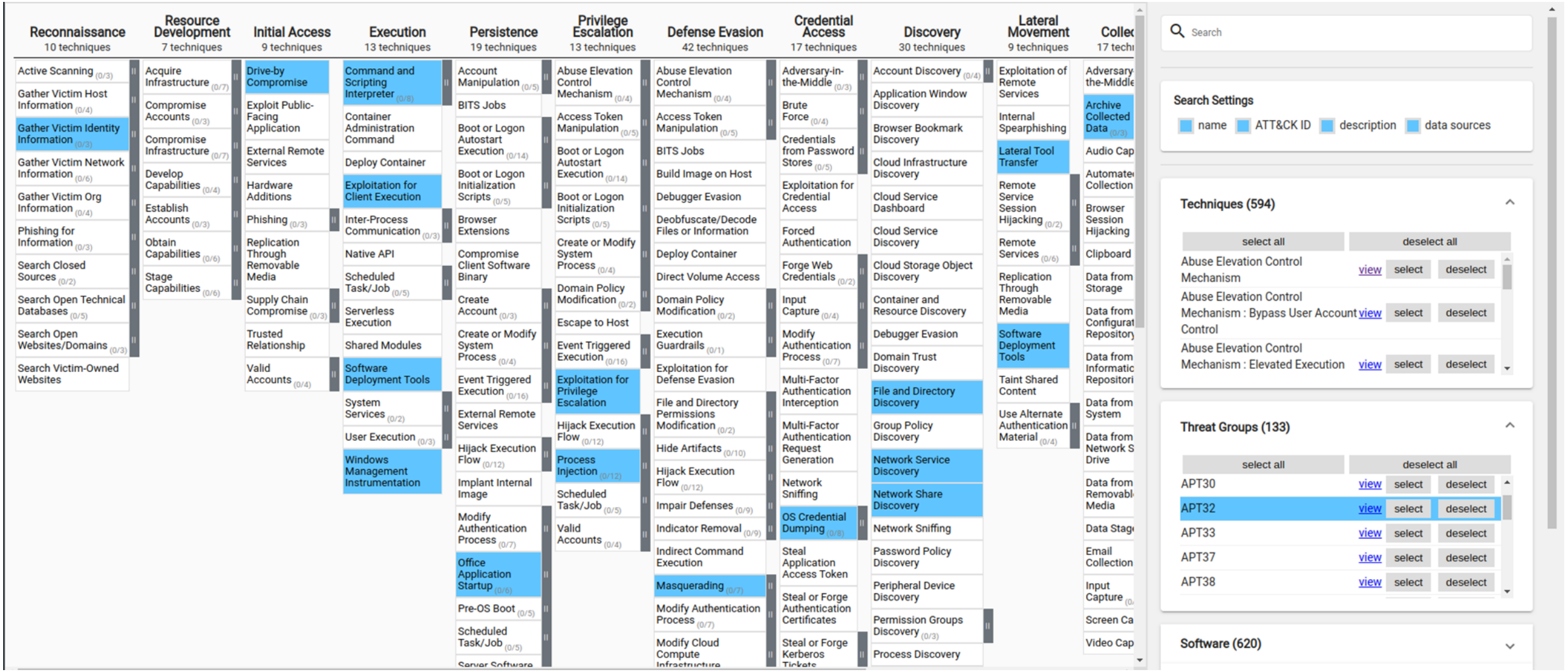
Outils: Vectr



Outils: Vectr



Outils: MITRE ATT&CK Navigator



En conclusion

Conclusion

Leçons apprises

- Le *purple teaming* est une activité très efficace pour se préparer contre des cyberattaques
  - À condition d'être prêt: Gestion de vulnérabilités, Tests d'intrusion réguliers, Cyber-hygiène, etc.
  - **Toutes entreprises** devraient faire du Purple Team avant de faire du Red Team.
  - La fonction purple doit se métamorphoser en continue.
- Il existe d'excellents outils publiquement accessibles pour faire cette activité
- Comme tout humain, on aime sentir qu'on fait une différence
- Priorisation, priorisation, priorisation!
- Vive la collaboration: Red ❤️ vs Blue 💙

Merci!

Desjardins