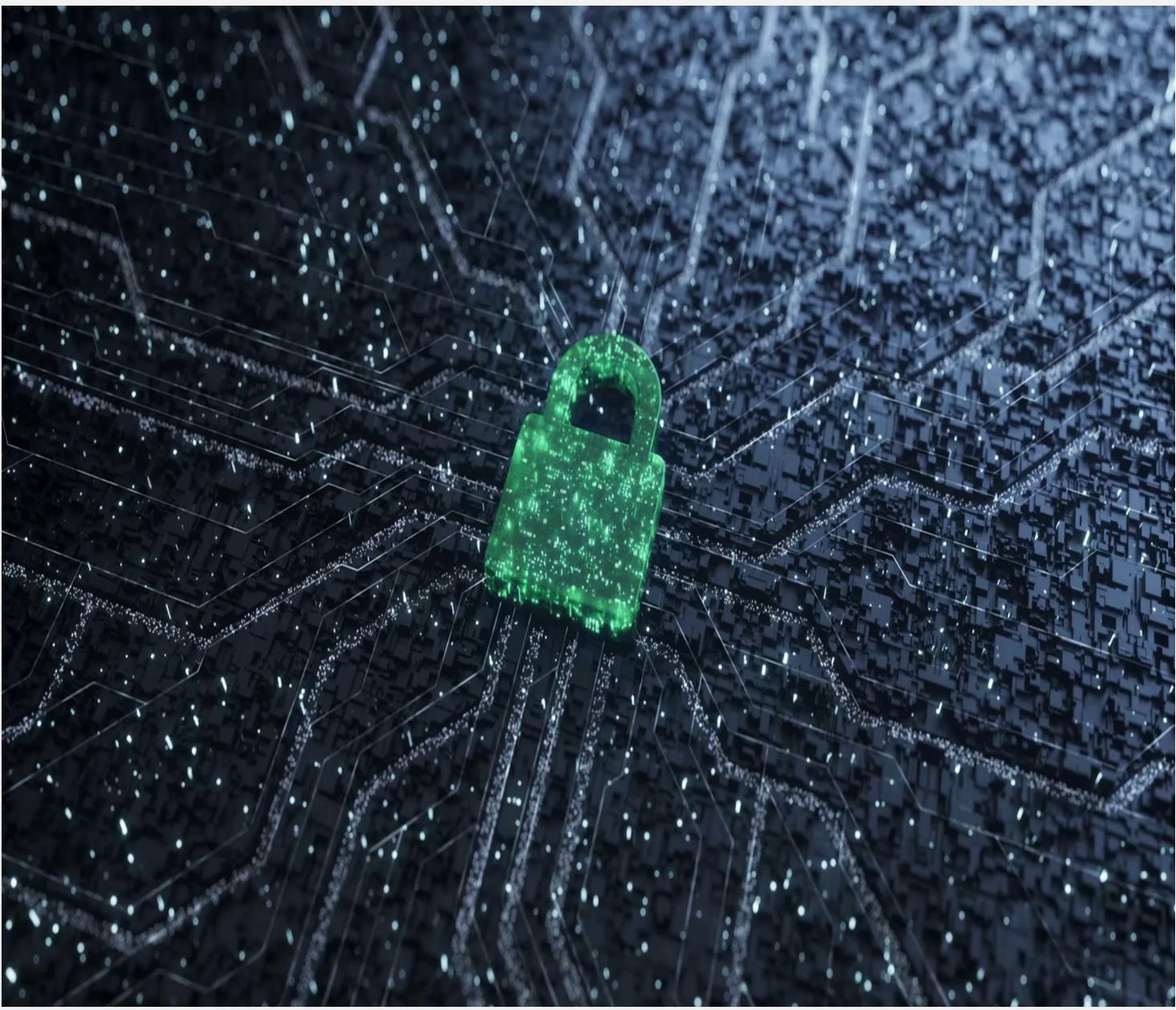




Bleu + Rouge = Mauve 1 seul objectif!

Cyberconférence Cybereco 2023

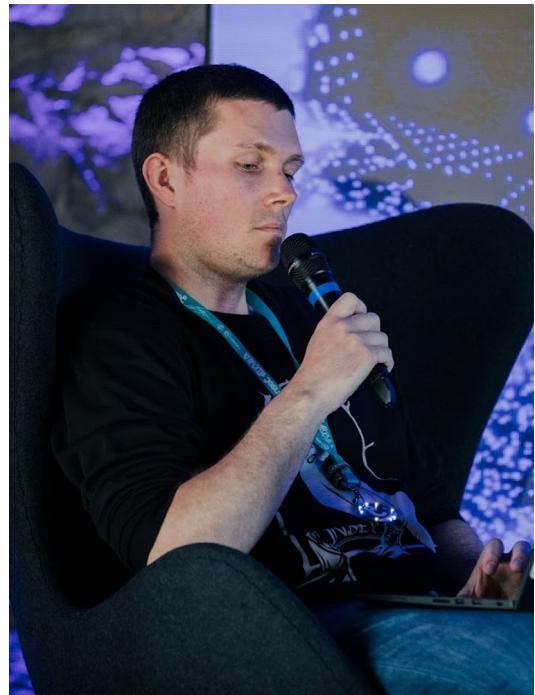
18 avril 2023



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 🏃

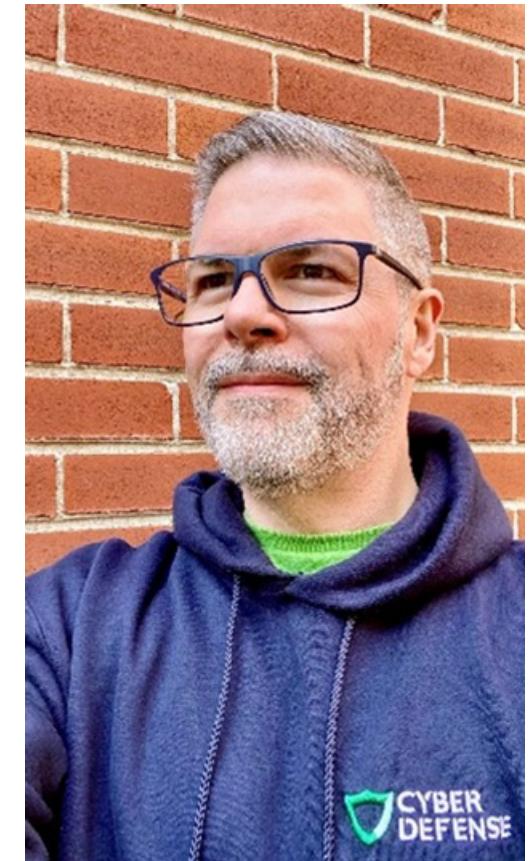
Bio: Dany Lafrenière

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 ...

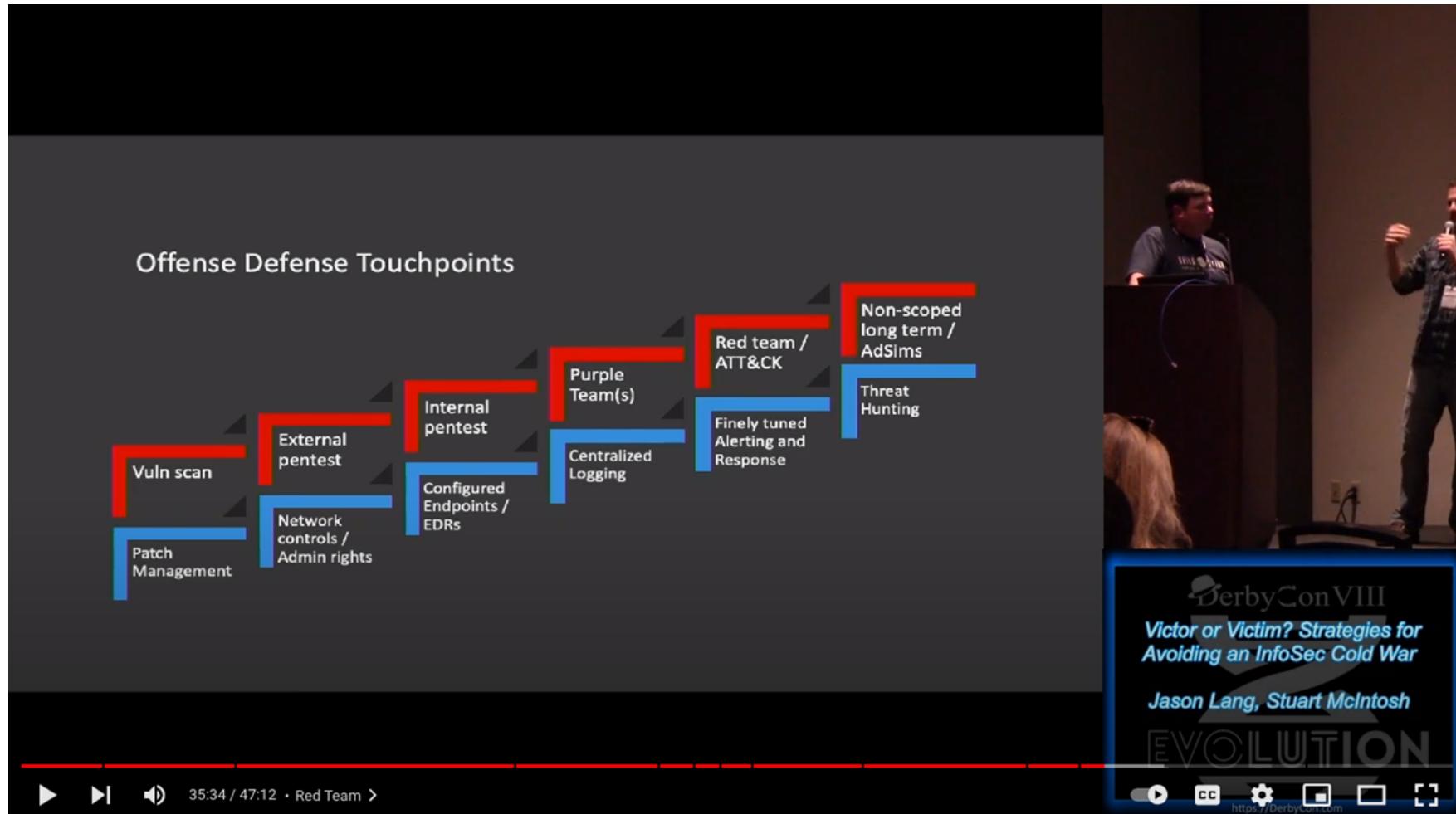
De soir 🌙

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



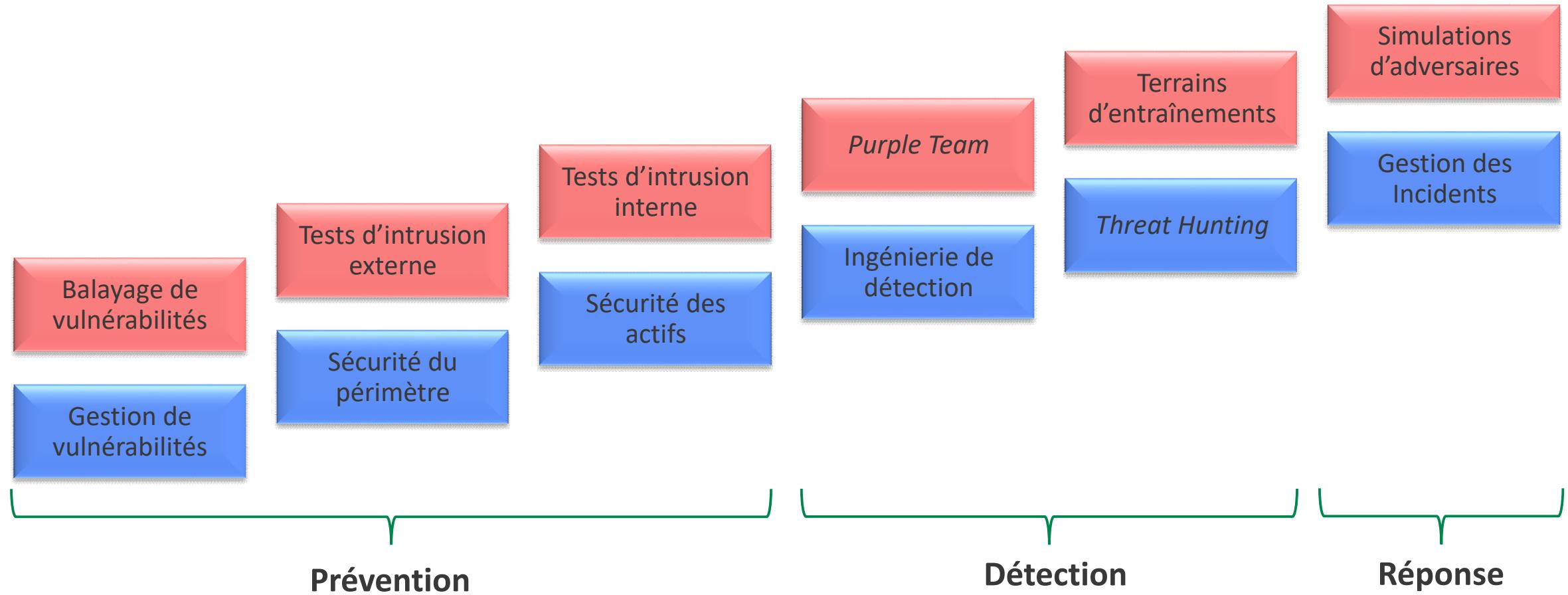
Dany Lafrenière
Directeur Investigation de
Sécurité de l'information

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?



7

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*

Objectif: Défendre

Requiert: Autonomie

Vélocité: Élevé

Activités des *Purple Teams*

Objectif: Améliorer la posture

Requiert: Collaboration

Vélocité: Élevé

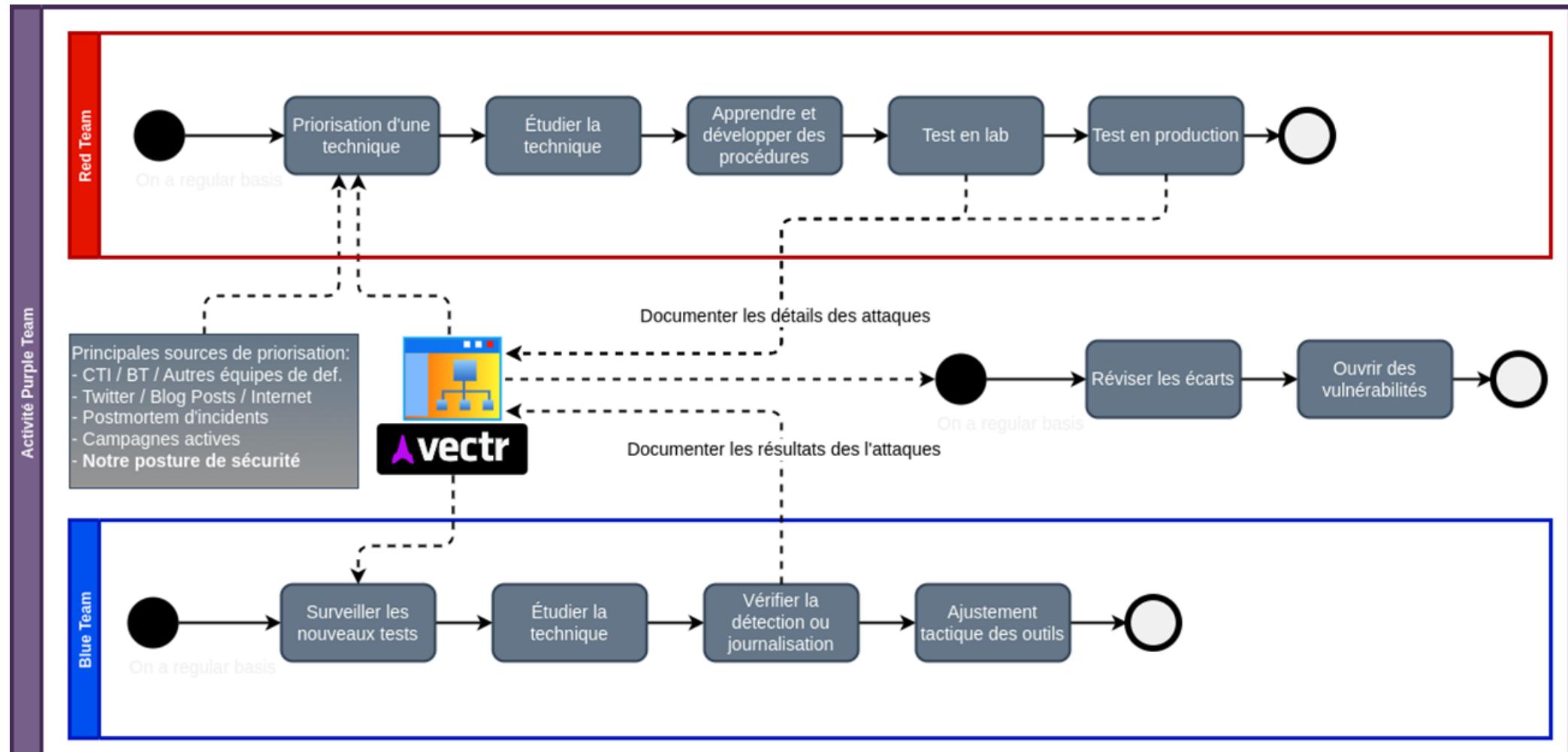
Activités des *Red Teams*

Objectif: Tester la résilience

Requiert: Un incident (surprise)

Vélocité: Faible

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

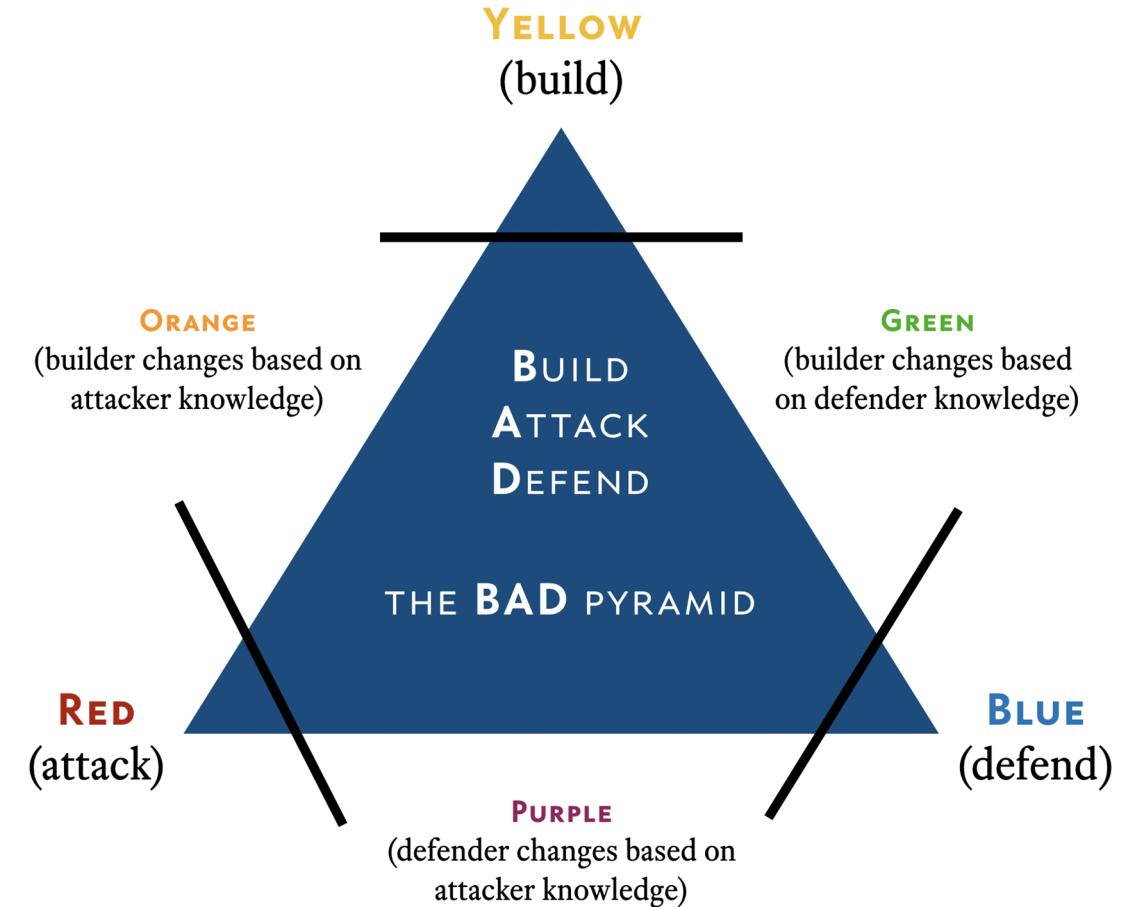
Cohésions !

- ❑ 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!



DANIEL MIESSLER 2019
BASED ON WORK BY APRIL WRIGHT

Outils

Alternatives à des chiffriers Excel...

Outils: Vectr

DEMO_PURPLE_CE / Enterprise Purple – 2017 Q1

Campaign Dashboard ASSESSMENT ACTIONS

Name	Progress	Outcome	Tags	Action
External Port Scans	<div style="width: 100%;">100%</div>	<div style="width: 100%;">100%</div>		
External Web App Profiling	<div style="width: 100%;">100%</div>	<div style="width: 100%;">100%</div>		
External Password Attacks	<div style="width: 100%;">100%</div>	<div style="width: 100%;">100%</div>		
External Automated Scans	<div style="width: 100%;">100%</div>	<div style="width: 33%; background-color: #28a745;">33%</div> <div style="width: 67%; background-color: #ffc107;">67%</div>		
Register Phishing Domains	<div style="width: 100%;">100%</div>	<div style="width: 100%;">100%</div>		
Email With Malicious Attachments	<div style="width: 100%;">100%</div>	<div style="width: 45%; background-color: #28a745;">45%</div> <div style="width: 50%; background-color: #ffc107;">50%</div> <div style="width: 5%;">#ff6363</div>		
Email with Malicious Links	<div style="width: 100%;">100%</div>	<div style="width: 23%; background-color: #28a745;">23%</div> <div style="width: 68%; background-color: #ffc107;">68%</div> <div style="width: 9%;">#ff6363</div>		
Malicious Document Execution	<div style="width: 100%;">100%</div>	<div style="width: 33%; background-color: #28a745;">33%</div> <div style="width: 67%;">#ff6363</div>		
C2 Channels	<div style="width: 100%;">100%</div>	<div style="width: 13%; background-color: #ffc107;">13%</div> <div style="width: 75%;">#ffc107</div> <div style="width: 13%;">#ff6363</div>		
Suspicious Process Execution	<div style="width: 100%;">100%</div>	<div style="width: 18%; background-color: #ff6363;">18%</div> <div style="width: 82%;">#ff6363</div>		
Endpoint Persistence	<div style="width: 100%;">100%</div>	<div style="width: 33%; background-color: #28a745;">33%</div> <div style="width: 17%; background-color: #ffc107;">17%</div> <div style="width: 50%;">#ff6363</div>		
Physical Access	<div style="width: 100%;">100%</div>	<div style="width: 25%; background-color: #28a745;">25%</div> <div style="width: 75%;">#ff6363</div>		
NAC Bypass	<div style="width: 100%;">100%</div>	<div style="width: 100%;">100%</div>		
Network MiTM	<div style="width: 100%;">100%</div>	<div style="width: 50%; background-color: #28a745;">50%</div> <div style="width: 50%;">#ff6363</div>		
Windows Domain Enumeration	<div style="width: 100%;">100%</div>	<div style="width: 25%; background-color: #ffc107;">25%</div> <div style="width: 75%;">#ff6363</div>		
App Server Discovery and Exploitation	<div style="width: 100%;">100%</div>	<div style="width: 60%;">#ffc107</div> <div style="width: 40%;">#ff6363</div>		

Outils: Vectr

DEMO_Purple_CE / Enterprise Purple – 2017 Q1 / Malware Profile Simulation

Malware Profile Simulation: Escalation Path

PNG

Timeline ?

Timeline:

- 01/22/2017 10:40:56: Files with Ransomware Extensions #2 : outcome changed to None
- 01/22/2017 09:19:34: Files with Ransomware Extensions #2 : status changed to Completed
- 01/22/2017 09:15:38: Files with Ransomware Extensions #2 : status changed to InProgress
- 01/22/2017 08:05:11: Files with Ransomware Extensions #1 : outcome changed to High
- 01/22/2017 07:47:04: Files with Ransomware Extensions #1 : status changed to Completed
- 01/22/2017 06:54:30: Files with Ransomware Extensions #1 : status changed to InProgress

Test Cases

CAMPAIGN ACTIONS ▾

<input type="checkbox"/>	Phase	Technique	Test Case	Status	Outcome	Tags	Action
<input type="checkbox"/>	All	search ...	search ...	All	All	All	
<input type="checkbox"/>	Exploitation	Malware simulation	Malleable C2 Profile Using Cobalt Strike - MALWARE PROFILE 1	Completed	Logged		
<input type="checkbox"/>	Exploitation	Malware simulation	Malleable C2 Profile Using Cobalt Strike - MALWARE	Completed	Logged		

Outils: Vectr

Edit Malleable C2 Profile Using Cobalt Strike - MALWARE PROFILE 1 Test Case ENTERPRISE ▾ X

Status: Completed

▶ ⏸ ⏹ ▲

Attack Start ⓘ

01/21/2017 19:50:51
 status changed to InProgress

Attack Stop ⓘ

01/21/2017 21:40:21
 status changed to Completed

Sources ⓘ

Targets ⓘ

Red Team Details

Name
 Malleable C2 Profile Using Cobalt Strike - MALWARE PROFILE 1

Description
 Startup Cobalt Strike to simulate known malware network profile.

Technique ⓘ
 Malware simulation - T1095

Phase
 Exploitation

Operator Guidance
<https://github.com/rsmudge/Malleable-C2-Profiles>
 ./teamserver [external IP] [password] [/path/to/my.profile]

Automation & logging
Supported Platform(s): Windows, Linux/MacOS (Bash shell)

Build/Run

Logs 0

Import Logs

⚙️

Configure

⬇️

Build & Download

Blue Team Details

Outcome
 TBD Blocked Alerted Logged None
 N/A

Location?
 Local Telemetry Centrally Logged

Detecting Blue Tool(s): ⓘ

Outcome Notes
 outcomeNotes

Tags ⚡

Rules

Detection

1) Simulated malware network traffic detected by behavioral analytics or firewall gateway

Cancel Save ◀ ▶

Outils: MITRE ATT&CK Navigator

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
10 techniques	7 techniques	9 techniques	13 techniques	19 techniques	13 techniques	42 techniques	17 techniques	30 techniques	9 techniques	17 techniques
Active Scanning (0/3) Gather Victim Host Information (0/4) Gather Victim Identity Information (0/3) Gather Victim Network Information (0/6) Gather Victim Org Information (0/4) Phishing for Information (0/3) Search Closed Sources (0/2) Search Open Technical Databases (0/5) Search Open Websites/Domains (0/3) Search Victim-Owned Websites	Acquire Infrastructure (0/7) Compromise Accounts (0/3) Compromise Infrastructure (0/7) Develop Capabilities (0/4) Establish Accounts (0/3) Obtain Capabilities (0/6) Stage Capabilities (0/6)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (0/3) Replication Through Removable Media Supply Chain Compromise (0/3) Trusted Relationship Valid Accounts (0/4)	Command and Scripting Interpreter (0/8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (0/3) Native API Scheduled Task/Job (0/5) Serverless Execution Create or Modify System Process (0/4) Create Account (0/3) Domain Policy Modification (0/2) Escape to Host Event Triggered Execution (0/16) Exploitation for Privilege Escalation External Remote Services Hijack Execution Flow (0/12) Process Injection (0/12) Implant Internal Image Modify Authentication Process (0/7) Office Application Startup (0/6) Pre-OS Boot (0/5) Scheduled Task/Job (0/5) Server Software	Account Manipulation (0/5) BITS Jobs Boot or Logon Autostart Execution (0/14) Boot or Logon Initialization Scripts (0/5) Browser Extensions Compromise Client Software Binary Create or Modify System Process (0/4) Create Account (0/3) Domain Policy Modification (0/2) Escape to Host Event Triggered Execution (0/16) Exploitation for Privilege Escalation External Remote Services Hijack Execution Flow (0/12) Process Injection (0/12) Implant Internal Image Modify Authentication Process (0/7) Office Application Startup (0/6) Pre-OS Boot (0/5) Scheduled Task/Job (0/5) Server Software	Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) Boot or Logon Autostart Execution (0/14) Build Image on Host Boot or Logon Initialization Scripts (0/5) Debugger Evasion Deobfuscate/Decode Files or Information Create or Modify System Process (0/4) Deploy Container Direct Volume Access Domain Policy Modification (0/2) Execution Guardrails (0/1) Exploitation for Defense Evasion File and Directory Permissions Modification (0/2) Hide Artifacts (0/10) Hijack Execution Flow (0/12) Impair Defenses (0/9) Indicator Removal (0/9) Indirect Command Execution Masquerading (0/7) Modify Authentication Process (0/7) Modify Cloud Compute Infrastructure	Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) BITS Jobs Build Image on Host Boot or Logon Initialization Scripts (0/5) Debugger Evasion Deobfuscate/Decode Files or Information Create or Modify System Process (0/4) Deploy Container Direct Volume Access Domain Policy Modification (0/2) Execution Guardrails (0/1) Exploitation for Defense Evasion File and Directory Permissions Modification (0/2) Hide Artifacts (0/10) Hijack Execution Flow (0/12) Impair Defenses (0/9) Indicator Removal (0/9) Indirect Command Execution Masquerading (0/7) Modify Authentication Process (0/7) Modify Cloud Compute Infrastructure	Adversary-in-the-Middle (0/3) Brute Force (0/4) Credentials from Password Stores (0/5) Exploit for Credential Access Forced Authentication Forge Web Credentials (0/2) Input Capture (0/4) Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing OS Credential Dumping (0/8) Steal Application Access Token Steal or Forge Authentication Certificates Steal or Forge Kerberos Tickets	Account Discovery (0/4) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Debugger Evasion Domain Trust Discovery File and Directory Discovery Group Policy Discovery Network Service Discovery Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (0/3) Process Discovery	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (0/2) Replication Through Removable Media Data from Configuration Repository Data from Informatic Repository Data from System Data from Network S Drive Data from Removable Media Data Stage Email Collection Input Capture (0/1) Screen Capture Video Cap	Adversary-in-the-Middle (0/3) Archive Collected Data (0/3) Audio Cap Automated Collection Browser Session Hijacking Clipboard Data from Storage Data from Configurable Repository Data from Informatic Repository Data from System Data from Network S Drive Data from Removable Media Data Stage Email Collection Input Capture (0/1) Screen Capture Video Cap

Search:

Search Settings:

- name
- ATT&CK ID
- description
- data sources

Techniques (594)

Technique	Action
Abuse Elevation Control Mechanism	view select deselect
Abuse Elevation Control Mechanism : Bypass User Account	view select deselect
Abuse Elevation Control Mechanism : Elevated Execution	view select deselect

Threat Groups (133)

Threat Group	Action
APT30	view select deselect
APT32	view select deselect
APT33	view select deselect
APT37	view select deselect
APT38	view select deselect

Software (620)

Software	Action
APT30	view select deselect
APT32	view select deselect
APT33	view select deselect
APT37	view select deselect
APT38	view select deselect



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