TRAVAILLER DANS LA CYBERSECURITE

SUPPORT PRINCIPAL : TRYHACKME.COM

DELAUTRE BENJAMIN

EQUIPES BLUE, RED ET PURPLE

Blue team

DEFENDERS
Works to keep systems safe

SKILLS
Network monitoring
Data analysis
Risk assessments
Threat detection

Purple team

MEMBERS FROM BOTH TEAMS
Gets blue and red teams to work together to improve the security posture of an organization

SKILLS
Collaboration
Information-sharing
Reporting
Analysis

Red team

ATTACKERS
Works to break into systems

SKILLS
Penetration testing
Social engineering
Vulnerability scanning
Custom tools and software development

TA CARRIERE… ET TOI

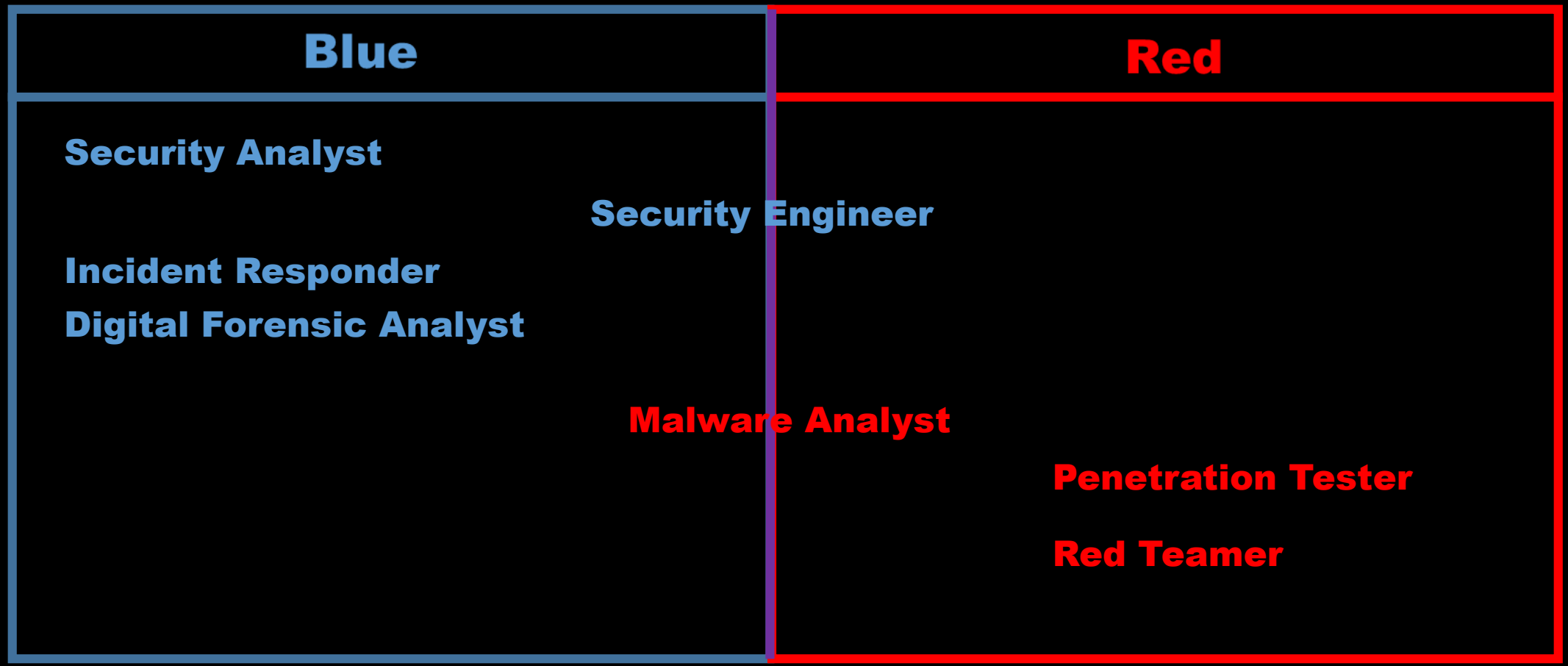
- **Red ou Blue, il faut réfléchir au métier qui mobilisera au mieux vos particularités (compétences, intérêts,…)**

- **Explorez pendant la formation et sondez vos centres d'intérêts…**
  - **« J'ai une passion pour le réseau ! »**
  - **« La programmation est top ! »**
  - **…**

TA CARRIERE… ET TOI

- …et votre personnalité ?
  - « J’aime travailler dans le feu de l’action »
  - « Je préfère analyser les choses tranquillement »
  - …

LES METIERS (EXEMPLES)



SECURITY ANALYST

En tant que *Security Analyst*, vous êtes chargé de protéger le matériel, les logiciels et les réseaux de votre entreprise contre le vol, la perte ou l'accès non autorisé. Les *Security analyst* surveillent le réseau et d'autres opérations pour prévenir et détecter les violations.

Tâches courantes :

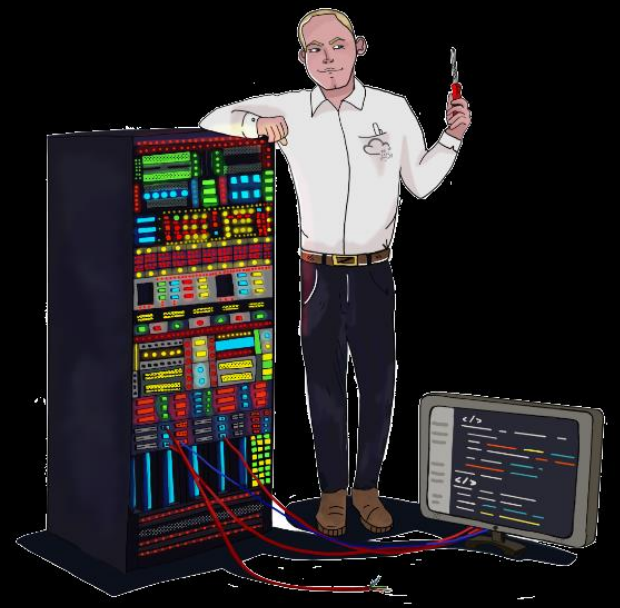
- Surveiller le trafic réseau pour les incidents et événements de sécurité
- Enquêter sur les incidents et réagir aux événements en temps réel
- Installer et faire fonctionner des pare-feu, des programmes de cryptage et d'autres logiciels de sécurité
- Corriger les vulnérabilités
- Développer et promouvoir les meilleures pratiques en matière de sécurité de l'information
- Mener des recherches sur les menaces et développer des plans de sécurité

SECURITY ENGINEER

Pour les différencier des *Security analyst*, les *Security Engineer* conçoivent et implémentent l'architecture de sécurité. Ils cherchent constamment de nouvelles façons de déjouer les tentatives d'obtenir un accès non autorisé aux systèmes et réseaux informatiques d'une entreprise.

Tâches courantes :

- Tester les mesures de sécurité sur l'ensemble des logiciels
- Surveiller les réseaux et les rapports pour mettre à jour les systèmes et atténuer les vulnérabilités
- Identifier et mettre en œuvre les systèmes nécessaires pour une sécurité optimale
- Concevoir et mettre en en place l'architecture de sécurité
- Planifiez les mises à niveau de la sécurité informatique et réseau et testez le matériel et les logiciels



INCIDENT RESPONDER

Les *Incident Responder* répondent de manière productive et efficace aux failles de sécurité. Les responsabilités comprennent la création de plans, de politiques et de protocoles que les organisations doivent adopter pendant et après les incidents.

Tâches courantes :

- Développer et adopter un plan de réponse aux incidents complet et utilisable
- Maintenir de bonnes pratiques en matière de sécurité et soutenir les mesures de réponse aux incidents dans l'organisation
- Rapports post-incidents et préparation aux attaques futures, en tenant compte des enseignements et des adaptations à tirer des incidents

DIGITAL FORENSIC ANALYST

Le *Digital Forensic Analyst* travaille sur l'acquisition de données, l'investigation et l'analyse d'appareils numériques pour recueillir des preuves. A l'aide d'outils numériques, il produit les preuves nécessaires pouvant être utilisées devant un tribunal. Par exemple, il enquête sur les cas liés à une intrusion illégale dans le réseau de votre organisation et suit les empreintes numériques pour retrouver l'attaquant.

Tâches courantes :

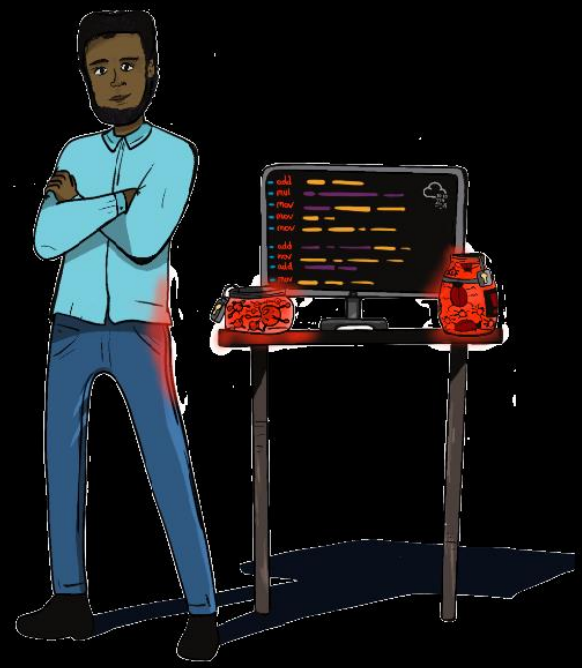
- Recueillir des preuves numériques tout en respectant les procédures légales
- Analyser les preuves numériques pour trouver des réponses liées à l'affaire
- Documentez vos découvertes et faites un rapport

MALWARE ANALYST

Le travail d'un *Malware Analyst* consiste à analyser les programmes suspects, à découvrir ce qu'ils font et à rédiger des rapports sur leurs découvertes. Ils utilisent leur capacité de programmation pour comprendre comment une attaque a été déployée et comment s'en défendre. Ils possèdent les connaissances nécessaires pour disséquer l'exploit et identifier la vulnérabilité cible.

Tâches courantes :

- Effectuer une analyse statique des programmes malveillants : *Reverse engineering*
- Effectuez une analyse dynamique des échantillons de logiciels malveillants en observant leurs activités dans un environnement contrôlé
- Documenter et rapporter toutes les découvertes



PENETRATION TESTER

Les *Penetration Tester* simulent des cyberattaques autorisées afin d'identifier et de signaler les failles de sécurité sur les systèmes informatiques, les réseaux et les infrastructures, y compris les sites Internet.

Tâches courantes :

- Effectuer des tests sur les systèmes informatiques, les réseaux et les applications Web
- Effectuer des évaluations de sécurité, des audits et analyser les politiques
- Évaluer et rendre compte des informations, recommander des actions pour la prévention des attaques

RED TEAMER

Les *Red Teamers* sont mis en place pour tester les capacités de détection et de réponse de l'entreprise. Ce poste nécessite d'imiter les actions des cybercriminels, d'émuler des attaques malveillantes, de conserver l'accès et d'éviter la détection. Les évaluations peuvent durer jusqu'à un mois.

Tâches courantes :

- Émulez le rôle d'un acteur malveillant pour découvrir les vulnérabilités exploitables, maintenir l'accès et éviter la détection
- Évaluer les contrôles de sécurité, les informations sur les menaces et les procédures de réponse aux incidents des organisations
- Évaluez et créez des rapports sur les informations, avec des données exploitables pour que les entreprises évitent les instances du monde réel

TON METIER AVEC UN QUIZ

- **Cliquez sur le lien suivant : https://www.lockheedmartin.com/en-us/news/features/2020/what-cyber-career-is-right-for-you.html**

- **Cliquez sur skip à la fin du questionnaire et découvrez votre métier !**

THE END

SOURCES

- *“Red team vs. blue team vs. purple team: What's the difference?” : https://www.techtarget.com/searchsecurity/tip/Red-team-vs-blue-team-vs-purple-team-Whats-the-difference*
- *“Careers in Cyber” : https://tryhackme.com/room/careersincyber*
- *“What cyber career is right for you ?” : https://www.lockheedmartin.com/en-us/news/features/2020/what-cyber-career-is-right-for-you.html*
- *« 5 CyberSecurity career paths (and how to get started) » : https://www.coursera.org/articles/cybersecurity-career-paths*
- *« Security Engineer vs. Security Analyst: What’s the Difference?” : https://online.maryville.edu/online-bachelors-degrees/computer-science/careers/security-engineer-vs-security-analyst/#:~:text=Generally%20speaking%2C%20security%20engineers%20design,to%20prevent%20and%20detect%20breaches*.
- *« How to become a malware analyst: A complete career guide” : https://cybersecurityguide.org/careers/malware-analyst/*