Red Team, Blue Team en cybersécurité

1. Définitions générales

En cybersécurité, ces termes désignent des équipes spécialisées aux rôles différents, qui collaborent pour renforcer la sécurité d'une organisation.

2. Red Team (Équipe rouge)

- **Rôle :** Simuler des attaques réelles contre le système informatique pour tester sa résistance.
- **Objectif :** Trouver les failles de sécurité avant les vrais attaquants (hackers).
- **Techniques :** Pentesting (test d'intrusion), exploitation de vulnérabilités, phishing simulé, social engineering.
- **Exemple :** Une Red Team va essayer de pirater le réseau d'une entreprise comme un hacker pour identifier les points faibles.

3. Blue Team (Équipe bleue)

- **Rôle :** Défendre, surveiller et protéger les systèmes informatiques contre les attaques.
- **Objectif :** Détecter, analyser et répondre aux menaces en temps réel.
- **Techniques :** Configuration de pare-feux, surveillance des logs, gestion des incidents, mise en place de systèmes de détection (IDS/IPS).
- **Exemple :** Une Blue Team analyse les alertes générées par les systèmes pour bloquer une attaque en cours.

4. Purple Team (Équipe pourpre)

- **Rôle :** Faciliter la collaboration entre Red Team et Blue Team.
- **Objectif :** Améliorer continuellement la sécurité en partageant les découvertes de la Red Team avec la Blue Team pour mieux se défendre.
- **Fonctionnement :** Travaille sur des scénarios conjoints, des formations croisées, et optimise les outils et stratégies.

5. Autres équipes

- **Green Team** : Souvent chargée du développement sécurisé (DevSecOps), intègre la sécurité dès la conception des logiciels.
- **Yellow Team** : Spécialisée dans l'analyse de risques et la conformité réglementaire.

6. Ces termes sont-ils techniques ?

- Ces termes sont devenus des **jargon professionnel en cybersécurité** pour désigner des rôles précis.
- Ils sont couramment utilisés dans les entreprises, les formations, et les certifications.

Types d'alertes et priorités (Niveaux 1, 2, 3, ...)

1. Qu'est-ce qu'une alerte en sécurité ?

- Une **alerte** est un message généré par un système de sécurité (pare-feu, IDS, antivirus...) pour signaler un événement suspect ou malveillant.
- L'alerte informe les administrateurs qu'il faut investiguer et peut déclencher une action immédiate.

2. Pourquoi classifier les alertes par priorité ?

- Les systèmes génèrent souvent beaucoup d'alertes, il faut savoir lesquelles traiter en premier.
- La priorité aide à organiser la réponse en fonction de la gravité et l'urgence.
- Cela évite de perdre du temps sur des alertes mineures quand une menace critique est présente.

3. Types de priorité d'alerte

Priorité	Nom / Niveau	Description	Action recommandée
1	**Critique / Urgent**	Attaque confirmée, impact immédiat grave	Intervention immédiate nécessaire
2	**Haute**	Activité suspecte probable	Analyse rapide et réponse rapide
3	**Moyenne**	Comportement anormal, mais pas urgent	Surveillance et enquête
4	**Basse**	Informations ou événements peu risqués	Suivi périodique ou rapport
5	**Info / Notification**	Simple information ou succès d'opération	Pas d'action immédiate nécessaire

4. Exemples :

- **Priorité 1 (Critique)** : Détection d'un malware en train de s'exécuter, ou d'une backdoor activée.
- **Priorité 2 (Haute)** : Tentative de connexion SSH multiple échouée suspecte.
- **Priorité 3 (Moyenne)** : Modification non autorisée d'un fichier système.
- **Priorité 4 (Basse)** : Scan de port provenant d'une IP externe.
- **Priorité 5 (Info)** : Service démarré avec succès.

Comprendre la priorité des alertes permet une gestion efficace de la sécurité. L'objectif est de traiter en priorité les incidents critiques qui peuvent causer des dommages importants. Les alertes faibles doivent être surveillées pour détecter des tendances ou préparer des actions futures.