BEYOND THE FIREWALL : LA RÉALITÉ DES MÉTIERS DE LA CYBERSÉCURITÉ

Conférence de Christian QUIVY à Centrale Nantes, Directeur Conseil Expert Sécurité à CGI

Cet article a été l'objet d'une Conférence sur le thème de la cybersécurité à l'occasion du Week-End Nantralien en décembre 2023.

La cybersécurité est un domaine consistant à prévoir, anticiper et protéger les systèmes d'information, les réseaux et les programmes contre les violations numériques. Ces cyberattaques visent généralement à obtenir des informations sensibles, à les détruire ou les transformer, à extorquer des fonds, ou à interrompre les processus normaux dans une entreprise par exemple.

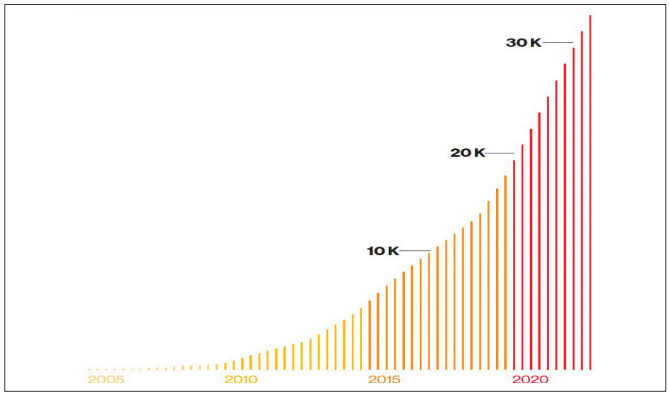
Une cyberattaque peut se traduire par différentes infractions: vol d'identité, tentative d'extorsion, perte de données importantes, mise en danger d'infrastructures essentielles comme les centrales, les hôpitaux ou les entreprises.

La mise en œuvre de mesures efficaces de cybersécurité est complexe aujourd'hui, en raison des nombreux équipements variés et des hackers qui suivent et parfois précèdent la technologie.

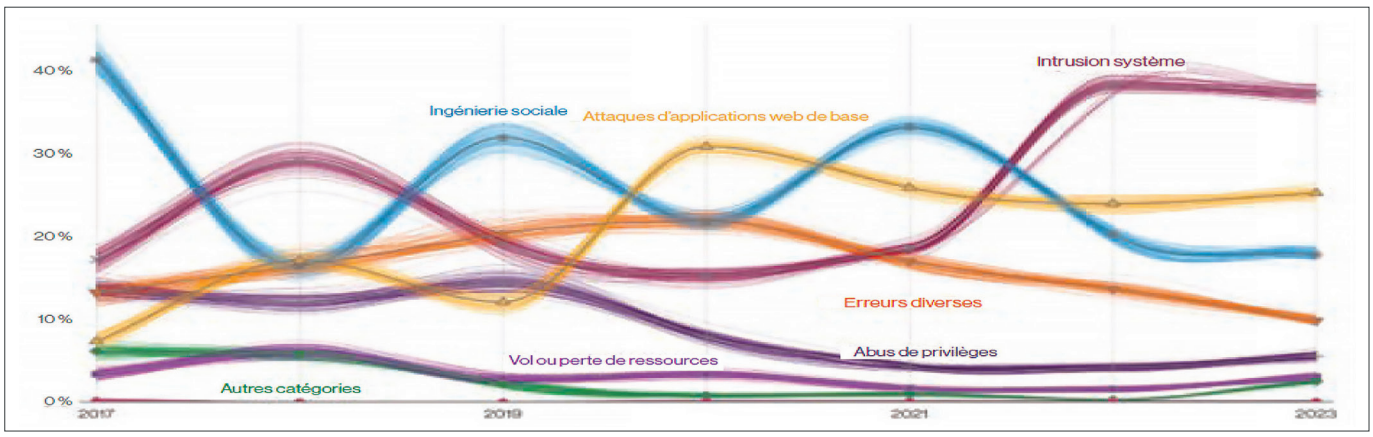
Pour être efficace la cybersécurité doit proposer différents étages de protection sur les ordinateurs, les stations, les réseaux, les programmes et toutes données à sécuriser.

Dans les années 80 différents appareils de communication existaient : clavier numérique, enregistreur cassettes, minitel, téléphone à cadrans, qui nécessitaient déjà de la vigilance pour la sécurité des informations.

L'émission, la modification, le vol ou l'utilisation non autorisée de données sensibles (par exemple de clés, de métadonnées, de codes ou d'autres informations de sécurité) ou la modification intempestive d'un système, ou d'un processus lié à la sécurité afin d'obtenir un accès illégal est une compromission.



Evolution chronologique du nombre de cas de compromission.
Source : Verizon.



Évolution chronologique des typologies de compromission.
Source : Verizon.

La progression de la technologie de l'information a crée un ensemble de métiers regroupés dans la **Cybersécurité**.

LES GRANDES FAMILLES DES MÉTIERS DE LA CYBERSÉCURITÉ

- Gestion de la sécurité et pilotage des projets de sécurité.
- Conception et maintien d'un Système d'information (SI) sécurisé.
- Gestion des incidents et des crises de sécurité.
- Conseil, services et recherche.

Gestion de la sécurité et pilotage des projets de sécurité

- **Le Directeur Cybersécurité**
  Executive security director, Directeur de la Sécurité des Systèmes d'Information (DSSI), Group Chief Information Security Officer.
  Il est en charge de la définition de la stratégie de cybersécurité dans de grandes organisations.

- **Le Responsable de la Sécurité des Systèmes d'Information (RSSI)**
  Chief Information Security Officer (CISO). Il assure le pilotage de la démarche de cybersécurité sur un périmètre organisationnel et/ou géographique au sein de l'organisation, selon la taille de l'organisation. Dans les PME/TPE, ce poste peut ne pas être dédié et être porté par le DSI ou autre.

- **Le Coordinateur sécurité**
  Il apporte un support aux équipes opérationnelles pour la réalisation des actions de sécurité et assure le suivi des plans d'action.

- **Le Directeur de programme de sécurité**
  Il pilote l'ensemble des projets de sécurité dans le cadre d'un programme de transformation de la sécurité des SI.

- **Le Responsable de projet de sécurité**
  Il définit, met en œuvre et conduit des projets de déploiement de solutions et d'outils de sécurité.

Conception et maintien d'un SI sécurisé

- **Le Chef sécurité de projet / Spécialiste en développement sécurisé**
  Il s'assure de la bonne prise en compte des aspects de sécurité des SI dans les projets informatiques ou métier.
- **L'Architecte sécurité**
  Il s'assure que les choix techniques et technologiques des projets IT et métiers respectent les exigences de sécurité de l'organisation. Il a l'Autorité technique sur les architectures de sécurité.
- **Le Spécialiste sécurité d'un domaine technique**
  Il possède une expertise sur la sécurité d'un domaine technique particulier (système, réseau, Cloud, IAM, Active Directory…).
- **Le Cryptologue**
  Expert sur la spécification, l'utilisation et la mise en œuvre opérationnelle de moyens cryptographiques, notamment au sein de laboratoires de recherche.
- **L'Administrateur de solutions de sécurité**
  Il installe et exploite des solutions de sécurité diverses (Antivirus, sondes, firewalls, IAM…).
- **L'Auditeur de sécurité organisationnelle**
  Il réalise des audits et contrôles de conformité des processus de sécurité.
- **Auditeur de sécurité technique**
  Il réalise des évaluations techniques de la sécurité d'environnements informatiques.

Gestion des incidents et des crises de sécurité

- **Le Responsable du SOC (Security Operation Center)**
  Il planifie et organise les opérations quotidiennes du SOC et le plan d'amélioration des services du SOC.
- **L'Opérateur analyste SOC**
  Il assure la supervision du système d'information afin de détecter des activités suspectes ou malveillantes.
- **Le Responsable du CSIRT**
  CSIRT (Computer Security Incident Response Team) ou CERT (Computer Emergency Response Team).
  Responsable d'une équipe de réponse aux incidents de sécurité du système d'information de l'organisation.
- **L'Analyste réponse aux incidents de sécurité**
  Il analyse les symptômes et réalise les analyses techniques sur le SI. Identifie le mode opératoire de l'attaquant et qualifie l'étendue de la compromission.
- **Le Gestionnaire de crise de cybersécurité**
  L'Analyste de la menace cybersécurité
  Il étudie l'évolution des motivations et des modes opératoires des attaquants. Fournit aux CERT/CSIRT et SOC des renseignements contextualisés leur permettant d'adapter et d'améliorer leurs moyens de prévention, de détection et de réponse à incident interne.

Conseil, services et recherche

- **Le Consultant en cybersécurité**
  Il intervient au sein d'une société de services. Il apporte son expertise aussi bien sur des sujets méthodologiques que techniques.
- **Le Formateur en cybersécurité**
  Il assure la formation et/ou la sensibilisation sur les volets réglementaires, techniques ou opérationnels de la cybersécurité.
- **L'Évaluateur de la sécurité des technologies de l'information**
  Il Intervient au sein de laboratoires d'évaluation. Il vérifie la conformité d'un produit ou système selon une méthode et des critères normalisés, réglementaires ou privés.
- **Le Développeur de solutions de sécurité**
  Il intervient au sein de sociétés d'éditions de produits informatiques.
- **L'Intégrateur de solutions de sécurité**
  Au sein d'une société d'intégration de solutions, il contribue au choix de l'architecture de la solution de sécurité et en assure l'assemblage au sein du SI. Il peut également assurer l'exploitation et le maintien en conditions opérationnelles.
- **Le Chercheur en sécurité des systèmes d'information**
  Il mobilise des connaissances expertes pour contribuer à l'émergence de technologies novatrices et de savoirs inédits.

LES MÉTIERS EN COULEUR

Dans le monde de la cybersécurité, il est courant d'utiliser les couleurs.

Red, Blue et Purple pour faire référence à des équipes spécifiques.

Red Team : Imite les attaquants en utilisant leurs techniques.

Blue team : Utilise ses compétences pour se défendre.

Purple team : Prépare des scénarios d'attaque et prend en compte les résultats dans le but d'améliorer la défense.

L'origine des couleurs bleues et rouge viendrait du domaine militaire dans les années 60. Le DoD (département de la défense américain) les aurait utilisées pour décrire une simulation dans laquelle l'équipe bleue (États-Unis) travaillait sur un traité de contrôle des armements avec l'équipe rouge (Union Soviétique). Le terme Purple est apparu récemment, comme étant un mélange des couleurs bleues et rouges, qu'il vise à combiner au mieux.

RED TEAM

La Red Team représente les attaquants, c'est l'équipe offensive.

L'équipe rouge peut être un groupe externe de pentesters (tests d'intrusion) ou une équipe au sein de l'organisation. Son but est d'émuler un **acteur réellement malveillant** et de tenter de pénétrer le système, afin d'en tester la sécurité.
Une Red Team peut mettre en œuvre des moyens comme la falsification d'une carte d'accès d'un employé, ou de l'ingénierie sociale, afin de pénétrer physiquement dans les locaux de l'entreprise.

Méthodes standards de l'équipe rouge

- Reconnaissance initiale et renseignement en source ouverte (OSINT) pour recueillir des informations sur la cible.
- Ingénierie sociale et hameçonnage.
- Tests de pénétration physiques et numériques, utilisation de vulnérabilités.
- Utilisation de leurres pour masquer les actions aux défenseurs.

Tableau comparatif Red team/pentest

La notion de Red Team est fréquemment assimilée aux tests de pénétration, pourtant il existe des différences significatives entre les deux. Dans une prestation de pentest, un périmètre précis est défini et des accès initiaux sont souvent donnés aux auditeurs. Le pentest doit couvrir un maximum du périmètre établi. En Red Team, l'équipe Blue n'est en général pas informée de l'exercice et aucun accès n'est donné aux auditeurs. On introduira ici la notion de **White Team**, équipe restreinte au courant de l'exercice ainsi que des actions réalisées, qui va guider si besoin ou limiter les actions de la Red Team.

Si la Blue Team détecte un exercice Red Team, l'exercice peut se transformer en Assume Breach (l'exercice se poursuit en partant du principe qu'un attaquant a pu accéder au réseau interne), qui peut être considéré comme du Purple Team.

Comparatif (Source les différences entre Red Team et Pentest)	**Red Team**	**Pentest**
La Blue Team est-elle au courant de l'exercice ?	Non	Oui
Le périmètre durant l'exercice est ?	Plus grand	Plus petit
Comment sont remontées les vulnérabilités ?	Remontées en allant d'un point A à un point B	Remontées sur tout le scope défini
L'exercice a t'il besoin d'ingénierie sociale sur les réseaux sociaux ?	Oui	Non
Une White Team est-elle nécessaire à tout l'exercice ?	Oui	Non

Outils du Pentesteur

Les pentesteurs disposent d'un grand nombre d'outils, parfois des suites complètes, pour automatiser leurs tests et augmenter leurs capacités de traitement. Parmi ceux-ci, on peut citer :

Kali Linux : Système d'exploitation Linux optimisé pour l'attaque, livré avec un grand nombre d'outils.

Nmap (network mapper) : scan réseau, scan de ports.

Metasploit : référence un grand nombre d'exploit, directement utilisables depuis le logiciel après paramétrage des informations de la cible. Cet outil permet d'automatiser un grand nombre de tâches fastidieuses.

Wireshark : analyseur de protocole. Permet d'étudier en détail le trafic réseau.

John the Ripper : Craqueur de mot de passe hors ligne.

Hydra : Craqueur de mot de passe en ligne.

Burp Suite : Scanner de vulnérabilités web.

Nessus : Scanner de vulnérabilités.

OWASP **ZAP** (Zed Attack Proxy) **:** test de pénétration sur les applications web.

Sqlmap : automatisation des attaques par injection SQL.

Shodan : recherche d'appareils connectés à Internet.

OpenVAS : Scanner de vulnérabilités.

Scapy : interpréteur Python permettant de travailler sur les paquets réseau.

Impaquet : construction de paquets à partir de zéro, analyse de données brutes.

BLUE TEAM

La Blue Team représente les défenseurs.

Il s'agit de l'équipe SSI chargée d'assurer la sécurité du système d'information, et comprend généralement des membres de **SOC et/ou CERT/CSIRT, ainsi que les gestionnaires de crise**.
Son rôle est de comprendre chaque phase d'un incident et agir de manière appropriée.

Les méthodes

- Examen et analyse des données des logs.
- Utilisation d'une plateforme de gestion des informations et événements de sécurité (SIEM) pour la détection des intrusions et le triage des alarmes en temps réel.
- Analyse du trafic et des flux de données.
- Collecte de nouvelles informations sur les menaces et mise en œuvre des actions appropriées en fonction des risques.

Outils et techniques Blue Team

La Blue Team a un panel très large d'outils et techniques de surveillance.

Des **EDR** *(Endpoint Detection and Response)*, permettant de surveiller et agir notamment sur :

- Injections suspicieuses dans un processus.
- Modifications dans le registre Windows.
- Mise en place de moyens de persistance (tâches planifiées par exemple).
- Modifications suspectes de fichiersDumps de mémoire.
- Enchaînement de comportements suspects sur le poste

Des **IPS** *(Intrusion Prevention System)* et **IDS** (*Intrusion Detection System)* permettant la surveillance du réseau.

Un **SIEM** (Security Information and Event Management), qui permet de collecter et agréger des données, majoritairement des logs (journaux d'événements) des équipements réseaux, postes de travail et serveurs. Cet outil permet de faire des recherches et de mettre en place des règles de détection, souvents basées sur les **TTPs** (Tactics, techniques and procedures) des acteurs malveillants, par exemple :

- Scans réseaux offensifs.
- Utilisation d'exploits publics et connus.
- Comptes compromis ou tentatives de compromission.
- Mise en place de moyens de persistance.
- Élévation de privilèges.
- Contournement de permissions.
- Mouvement latéral.
- Communication vers un **C2** (ou C&C, *Command and Control*).

PURPLE TEAM

Une **Purple team** n'est **pas nécessairement une équipe à part entière**. L'objectif est de réunir les équipes rouge et bleue pour travailler ensemble et créer une boucle de rétroaction solide.

La Purple Team va faire intervenir des **analystes de la menace** *(CTI Cyber Threat Intelligence)* de manière à contextualiser au maximum les scénarios des exercices, en fonction de la menace réelle sur l'entreprise, des techniques associées et de la défense en place.

Les méthodes

Modélisation : Prise de contexte (environnement, stratégie de défense…) et définition des scénarios d'attaque.

Réalisation : Réalisation de l'exercice et génération d'une chronologie d'événements.

Collaboration : Échange avec la Red Team et la Blue Team et comparaison des écarts de détection.

Capitalisation : Documentation et amélioration des règles de détection et des procédures de réponse sur incident.