Etat de la cyber sécurité

m2iformation.fr

SOMMAIRE

Définition et importance de la cybersécurité

La cybersécurité est la pratique consistant à protéger les systèmes, les réseaux et les programmes contre les attaques numériques. Ces attaques visent généralement à accéder, modifier ou détruire des informations sensibles, à extorquer de l'argent aux utilisateurs ou à interrompre les opérations normales des entreprises.

- **Protection des données sensibles :** Les données personnelles, financières et confidentielles doivent être protégées contre les accès non autorisés.
- **Continuité des activités :** Les cyberattaques peuvent paralyser les opérations des entreprises, causant des pertes financières et de la réputation.
- **Respect des réglementations :** De nombreuses lois et réglementations imposent des obligations strictes en matière de protection des données (GDPR, HIPAA, etc.).
- **Prévention des fraudes :** Les entreprises doivent se protéger contre les fraudes financières et les vols d'identité.
- **Confiance des clients :** Une bonne sécurité renforce la confiance des clients et des partenaires commerciaux.

Menaces et risques courants

1. **Malware (logiciel malveillant) :**
   - **Types de malware :** Virus, vers, chevaux de Troie, ransomware, spyware, adware.
   - **Fonctionnement :** Ces logiciels peuvent voler des données, endommager des systèmes ou prendre le contrôle des ordinateurs.
2. **Phishing :**
   - **Techniques :** Emails frauduleux, sites web contrefaits, SMS trompeurs.
   - **Objectif :** Tromper les utilisateurs pour qu'ils divulguent des informations sensibles telles que des identifiants de connexion et des informations financières.
3. **Attaques par déni de service (DoS) et déni de service distribué (DDoS) :**
   - **Technique :** Surcharger un serveur ou un réseau avec un trafic massif pour le rendre indisponible.
   - **Impact :** Interruption des services en ligne, pertes financières et de réputation.
4. **Intrusions et exploitations de vulnérabilités :**
   - **Technique :** Exploiter des failles de sécurité dans les logiciels et les systèmes.
   - **Impact :** Accès non autorisé aux systèmes, vol de données, perturbation des opérations.
5. **Menaces internes :**
   - **Sources :** Employés actuels ou anciens, contractuels, partenaires commerciaux.
   - **Impact :** Vol de données, sabotage, divulgation de secrets commerciaux.

Acteurs principaux de la menace

1. Hackers :

- **White Hat :** Hackers éthiques qui testent les systèmes pour trouver et corriger les vulnérabilités.
- **Black Hat :** Hackers malveillants qui exploitent les vulnérabilités pour des gains personnels ou financiers.
- **Grey Hat :** Hackers qui agissent sans autorisation mais sans intention malveillante, souvent pour alerter sur des failles de sécurité.

2. Groupes APT (Advanced persistent threat) :

- **Définition :** Groupes organisés, souvent soutenus par des États, qui mènent des campagnes de cyberespionnage ou de sabotage à long terme.
- **Caractéristiques :** Attaques ciblées, discrétion, utilisation de techniques sophistiquées pour rester indétectés.
- **Objectifs :** Vol de propriété intellectuelle, espionnage industriel, déstabilisation politique.

3. Cybercriminels :

- **Motivations :** Gains financiers par le biais de ransomware, de fraudes en ligne, de vente de données volées.
- **Techniques :** Piratage de comptes bancaires, escroqueries par phishing, mise en place de marchés noirs sur le dark web.
- **Organisations :** Souvent organisés en réseaux criminels, opérant à l'échelle internationale.

Analyse des incidents majeurs de l'Année Passée

1.Attaque sur SolarWinds (Sunburst)

- **Date :** Décembre 2020
- **Description :** Une attaque sophistiquée qui a compromis le logiciel de gestion de réseau Orion de SolarWinds. Les hackers ont inséré une porte dérobée dans une mise à jour logicielle, affectant des milliers d'organisations à travers le monde, y compris des agences gouvernementales et des entreprises privées.
- **Technique Utilisée :** Supply Chain Attack (attaque de la chaîne d'approvisionnement).
- **Impact :** Accès non autorisé à des réseaux sensibles, vol potentiel de données confidentielles, coûts de remédiation élevés.

2. Ransomware sur colonial pipeline

- **Date :** Mai 2021
- **Description :** L'attaque de ransomware par le groupe DarkSide a paralysé le plus grand pipeline de carburant des États-Unis, provoquant des pénuries d'essence et une augmentation des prix.
- **Technique Utilisée :** Ransomware.
- **Impact :** Interruption des services de pipeline, paiement d'une rançon de 4,4 millions de dollars, perturbation économique significative.

Analyse des incidents majeurs de l'année passée

3. Violation de données chez facebook

- **Date :** Avril 2021
- **Description :** Les données personnelles de plus de 530 millions d'utilisateurs de Facebook ont été exposées en ligne, y compris des numéros de téléphone, des noms complets, des emplacements, des dates de naissance et des adresses email.
- **Technique Utilisée :** Scraping de données à partir de profils publics.
- **Impact :** Risques accrus de fraude, d'hameçonnage et de vols d'identité pour les utilisateurs concernés.

4. Cyberattaque contre JBS USA

- **Date** : Juin 2021
- **Description :** JBS, le plus grand producteur de viande au monde, a été victime d'une attaque de ransomware qui a forcé la fermeture de plusieurs usines aux États-Unis, au Canada et en Australie.
- **Technique Utilisée :** Ransomware.
- **Impact :** Perturbation de la chaîne d'approvisionnement alimentaire, paiement d'une rançon de 11 millions de dollars.

Tendances Actuelles dans les Cyberattaques

1. Phishing

- **Description :** Technique où les attaquants envoient des emails frauduleux pour tromper les utilisateurs et leur faire révéler des informations sensibles telles que des identifiants de connexion ou des informations financières.
- **Évolution :** Les attaques de phishing sont de plus en plus sophistiquées, utilisant des techniques de spear phishing (ciblage de victimes spécifiques) et de business email compromise (compromission d'emails professionnels).

2. Ransomware

- **Description :** Les attaquants chiffrent les données de la victime et demandent une rançon pour fournir la clé de déchiffrement.
- **Évolution :** Augmentation des attaques de double extorsion, où les attaquants menacent non seulement de ne pas déchiffrer les données, mais aussi de les divulguer publiquement. Les groupes de ransomware en tant que service (RaaS) rendent ces attaques plus accessibles aux cybercriminels.

3. Attaques par déni de service distribué (DDoS)

- **Description :** Surcharger un serveur ou un réseau avec un trafic massif pour le rendre indisponible.
- **Évolution :** Les attaques DDoS deviennent plus fréquentes et puissantes, utilisant des botnets massifs et des techniques de réflexion/amplification pour maximiser l'impact. L'Internet des objets (IoT) est souvent exploité pour créer ces botnets.

Tendances actuelles dans les cyberattaques

4. Exploitation de vulnérabilités

- **Description :** Les attaquants exploitent des failles de sécurité dans les logiciels et les systèmes pour obtenir un accès non autorisé.
- **Évolution :** Augmentation des attaques zero-day (exploitant des vulnérabilités non corrigées), et une plus grande exploitation des vulnérabilités dans les technologies cloud et IoT.

5. Menaces internes

- **Description :** Menaces posées par des personnes ayant un accès légitime aux systèmes de l'organisation, telles que des employés ou des partenaires.
- **Évolution :** Les menaces internes deviennent plus sophistiquées, avec des insiders exploitant des accès privilégiés pour voler des données sensibles ou saboter des systèmes. La surveillance et la gestion des accès deviennent cruciales.

Responsabilités et missions analyste SOC

1. **Surveillance continue**

   L'analyste SOC est chargé de la surveillance en continu des réseaux, des systèmes et des applications afin de détecter les activités suspectes et les incidents de sécurité potentiels. Cette surveillance est cruciale pour identifier rapidement les menaces et minimiser les dommages potentiels. L'analyste utilise des outils de gestion des informations et des événements de sécurité (SIEM) pour collecter, analyser et corréler les logs provenant de diverses sources.

   Exemple :

   - **Situation :** L'analyste SOC utilise un SIEM comme Splunk pour surveiller les journaux d'activité des serveurs, des pare-feu, des systèmes de détection d'intrusion (IDS), et des applications.
   - **Action :** Il configure des règles et des alertes pour identifier les comportements anormaux, comme des tentatives de connexion multiples échouées ou des transferts de données inhabituels.
   - **Résultat :** Lorsqu'une alerte est déclenchée, l'analyste enquête immédiatement pour déterminer si l'activité est malveillante et prendre les mesures nécessaires.

Responsabilités et missions analyste SOC

2. **Analyse et détection des menaces**

   L'analyste SOC analyse les alertes générées par les outils de sécurité pour distinguer les vraies menaces des faux positifs. Cette analyse implique une compréhension approfondie des menaces actuelles, des vulnérabilités et des techniques d'attaque courantes.

   Exemple :

   - **Situation :** Une alerte SIEM indique plusieurs tentatives de connexion échouées depuis une adresse IP inconnue.
   - **Action :** L'analyste examine les journaux de connexion pour voir si les tentatives proviennent d'une adresse IP malveillante connue ou si elles correspondent à un comportement utilisateur légitime.
   - **Résultat :** Si l'adresse IP est suspecte, l'analyste peut bloquer l'IP au niveau du pare-feu et déclencher une enquête plus approfondie pour comprendre l'étendue de la menace.

Responsabilités et missions analyste SOC

3. **Réponse aux incidents**

   Lorsque des incidents de sécurité sont détectés, l'analyste SOC prend des mesures immédiates pour contenir et mitiger l'incident. Cela peut inclure l'isolement des systèmes compromis, la suppression des logiciels malveillants et la restauration des systèmes à partir de sauvegardes.

   Exemple :

   - **Situation :** Un poste de travail est infecté par un ransomware qui commence à chiffrer les fichiers.
   - **Action :** L'analyste isole immédiatement le poste de travail du réseau pour empêcher la propagation du ransomware. Ensuite, il utilise des outils de détection et de suppression des malwares pour nettoyer le système infecté.
   - **Résultat :** Après la suppression du ransomware, l'analyste restaure les fichiers chiffrés à partir de sauvegardes et enquête sur la source de l'infection pour renforcer les mesures de sécurité.

Responsabilités et missions analyste SOC

4. **Gestion des alertes et des événements**

   L'analyste SOC doit gérer et prioriser les alertes de sécurité pour s'assurer que les menaces les plus critiques sont traitées en premier. Cela implique de classifier les alertes en fonction de leur gravité et de leur impact potentiel sur l'organisation.

   Exemple :

   - **Situation :** Le SIEM génère des centaines d'alertes par jour.
   - **Action :** L'analyste configure des filtres et des priorités pour se concentrer sur les alertes les plus critiques, telles que celles impliquant des tentatives de compromission de données sensibles.
   - **Résultat :** Cela permet de traiter rapidement les incidents à haut risque et de minimiser les interruptions pour l'organisation.

Responsabilités et missions analyste SOC

5. **Documentation et reporting**

   L'analyste SOC doit documenter tous les incidents de sécurité, les actions prises et les résultats obtenus. La documentation est essentielle pour les audits de sécurité, l'amélioration continue des processus et la communication avec les parties prenantes.

   Exemple :

   - **Situation :** Après la réponse à une attaque de phishing réussie, l'analyste documente l'incident.
   - **Action :** Il rédige un rapport détaillant comment l'attaque a été détectée, les mesures prises pour contenir l'incident, et les recommandations pour éviter de futures attaques similaires.
   - **Résultat :** Le rapport est partagé avec l'équipe de gestion pour informer des actions correctives et des améliorations possibles des politiques de sécurité.

Compétences nécessaires

1. **Connaissances techniques :**

   Un analyste SOC doit posséder une solide compréhension des réseaux informatiques, des systèmes d'exploitation (Windows, Linux), et des protocoles de communication pour identifier et analyser les menaces de sécurité.

   Exemple :

   - **Situation :** Une alerte indique un trafic anormal sur un réseau.
   - **Action :** L'analyste utilise ses connaissances en protocoles réseau pour analyser les paquets et identifier si le trafic est légitime ou une attaque.
   - **Résultat :** L'analyste peut rapidement déterminer la nature du trafic et agir en conséquence.

Compétences nécessaires

2. **Analyse et résolution de problèmes :**

   Les analystes SOC doivent être capables de diagnostiquer rapidement les problèmes de sécurité et de trouver des solutions efficaces sous pression.

   Exemple :

   - **Situation :** Une application critique cesse de fonctionner après une mise à jour de sécurité.
   - **Action :** L'analyste examine les journaux d'erreurs, identifie le problème et propose une solution pour corriger la mise à jour sans compromettre la sécurité.
   - **Résultat :** L'application est remise en service rapidement avec des mesures de sécurité intactes.

Compétences nécessaires

3. **Connaissance des menaces et vulnérabilités :**

   Les analystes doivent rester informés des dernières menaces, vulnérabilités et techniques d'attaque pour protéger efficacement leur organisation.

   Exemple :

   - **Situation :** Une nouvelle vulnérabilité zero-day est annoncée pour un logiciel utilisé par l'organisation.
   - **Action :** L'analyste évalue l'impact potentiel, met en place des mesures de mitigation temporaires et planifie une mise à jour de sécurité.
   - **Résultat :** L'organisation est protégée contre l'exploitation de la vulnérabilité avant qu'un correctif officiel ne soit disponible.

Compétences nécessaires

4. **Communication :**

   Une communication claire et efficace est essentielle pour documenter les incidents, collaborer avec les équipes et informer les parties prenantes.

   Exemple :

   - **Situation :** Après une tentative d'intrusion, l'analyste doit informer la direction.
   - **Action :** Il prépare un rapport clair et concis, expliquant l'incident, les actions prises et les mesures de prévention futures.
   - **Résultat :** La direction est bien informée et peut prendre des décisions éclairées sur les mesures de sécurité supplémentaires.

Compétences nécessaires

5. **Utilisation des Outils de Sécurité :**

   Les analystes SOC doivent maîtriser les outils de sécurité couramment utilisés, tels que les SIEM, les IDS/IPS et les outils de gestion des vulnérabilités.

   Exemple :

   - **Situation :** L'analyste reçoit une alerte de compromission potentielle via le SIEM.
   - **Action :** Il utilise les fonctionnalités du SIEM pour enquêter sur l'alerte, corréler les événements et comprendre la portée de l'incident.
   - **Résultat :** L'incident est rapidement analysé et les mesures appropriées sont prises pour atténuer la menace.

Outils et Technologies Utilisés

1. **SIEM (Security Information and Event Management)**

   Les SIEM collectent, analysent et corrèlent les logs de divers systèmes pour détecter les anomalies et les incidents de sécurité. Ils permettent une visibilité centralisée et facilitent la détection des menaces.

   Exemple :

   - **Outil :** Splunk
   - **Fonction :** Collecte des logs de différents systèmes (serveurs, pare-feu, IDS/IPS) et génère des alertes en cas d'activités suspectes.

Outils et Technologies Utilisés

2. **IDS/IPS (Intrusion Detection/Prevention Systems)**

   Les IDS/IPS surveillent le trafic réseau pour détecter et/ou prévenir les activités malveillantes. Les IDS détectent les intrusions tandis que les IPS prennent des mesures pour les empêcher.

   Exemple :

   - **Outil :** Snort
   - **Fonction :** Analyse le trafic réseau en temps réel et déclenche des alertes ou bloque les paquets suspects.

Outils et Technologies Utilisés

3. **Firewalls**

   Les pare-feu contrôlent le trafic réseau entrant et sortant en appliquant des règles de sécurité prédéfinies pour protéger les réseaux contre les accès non autorisés.

   Exemple :

   - **Outil :** Cisco ASA
   - **Fonction :** Filtre le trafic réseau en fonction de règles configurées pour empêcher les accès non autorisés.

4. **Outils d'Analyse Forensique**

   Description :
   Ces outils sont utilisés pour l'analyse approfondie des incidents de sécurité et la collecte de preuves numériques.

   Exemple :

   - **Outil :** EnCase
   - **Fonction :** Permet l'analyse des disques et des systèmes compromis pour identifier l'origine et l'impact des incidents de sécurité.

Outils et Technologies Utilisés

5. **Outils de Gestion des Vulnérabilités**

   Description :
   Les outils de gestion des vulnérabilités identifient, classifient et gèrent les vulnérabilités présentes dans les systèmes et les réseaux.

   Exemple :

   - **Outil :** Nessus
   - **Fonction :** Scanne les réseaux et les systèmes pour identifier les vulnérabilités et propose des recommandations pour les corriger.

Composants d'un SOC

1. **SIEM (Security Information and Event Management) :**
   - **Fonction :** Un SIEM collecte, corrèle et analyse les journaux et les événements de sécurité provenant de diverses sources. Il fournit une vue centralisée des événements de sécurité, permettant une détection rapide des menaces et des incidents.
   - **Exemples :** Splunk, ArcSight, QRadar.
2. **IDS/IPS (Intrusion Detection/Prevention Systems) :**
   - **IDS (Intrusion Detection Systems) :** Ces systèmes surveillent le trafic réseau pour détecter des activités suspectes ou malveillantes. Ils génèrent des alertes lorsqu'une menace potentielle est détectée.
   - **IPS (Intrusion Prevention Systems) :** En plus de détecter les intrusions comme l'IDS, un IPS peut également prendre des mesures pour prévenir ces intrusions, telles que bloquer le trafic suspect.
   - **Exemples :** Snort (IDS), Suricata (IDS), Cisco Firepower (IPS).
3. **Firewalls :**
   - **Fonction :** Les pare-feux contrôlent le trafic entrant et sortant du réseau de l'organisation selon des règles de sécurité prédéfinies. Ils forment la première ligne de défense contre les attaques.
   - **Exemples :** Palo Alto Networks, Fortinet, Check Point.

Composants d'un SOC

4. **Endpoint Detection and Response (EDR) :**
   - **Fonction :** Les solutions EDR surveillent et analysent les activités sur les endpoints (ordinateurs, serveurs, appareils mobiles) pour détecter et répondre aux menaces de manière proactive.
   - **Exemples :** CrowdStrike, Carbon Black, SentinelOne.
5. **Threat Intelligence Platforms :**
   - **Fonction :** Ces plateformes collectent et analysent des informations sur les menaces provenant de diverses sources pour aider à identifier des indicateurs de compromission (IoC) et anticiper les attaques.
   - **Exemples :** ThreatConnect, Recorded Future.
6. **Security Orchestration, Automation, and Response (SOAR) :**
   - **Fonction :** Les solutions SOAR intègrent diverses technologies et processus pour automatiser les réponses aux incidents, coordonner les actions entre différents outils et améliorer l'efficacité des opérations de sécurité.
   - **Exemples :** Phantom, Demisto, Siemplify.

Processus et workflows typiques

1. **Surveillance continue :** Le SOC surveille en permanence les réseaux, systèmes et données de l'organisation pour détecter des activités suspectes ou anormales.
   - **Outils :** SIEM, IDS/IPS, EDR.
2. **Détection des incidents :** Lorsqu'un événement de sécurité suspect est détecté, il est analysé pour déterminer s'il constitue un incident de sécurité réel.
   - **Outils :** SIEM, Threat Intelligence, IDS/IPS.
3. **Analyse et investigation :** Les analystes de sécurité examinent les incidents détectés pour comprendre la nature et l'ampleur de la menace, ainsi que son impact potentiel.
   - **Outils :** SIEM, EDR, Threat Intelligence.
4. **Réponse aux incidents :** Le SOC prend des mesures pour contenir, éradiquer et récupérer des incidents de sécurité. Cela inclut l'isolation des systèmes compromis, la suppression des logiciels malveillants et la restauration des systèmes affectés.
   - **Outils :** SOAR, EDR, IPS.

Processus et workflows typiques

5. **Remédiation et récupération :** Après la réponse initiale, des actions correctives sont mises en place pour prévenir de futures occurrences de l'incident et restaurer les opérations normales.
   - **Outils :** Backup and Recovery solutions, Patch Management.
6. **Rapports et amélioration continue :**
   - **Description :** Des rapports sur les incidents et les performances du SOC sont générés pour informer la direction et améliorer continuellement les processus et les technologies.
   - **Outils :** SIEM, Reporting Tools.

Méthodologies de détection et de réponse

1. **Détection basée sur les signatures :** Utilise des signatures de menaces connues pour détecter les attaques. Efficace pour les menaces déjà documentées.
   - **Exemples :** Antiviruses, IDS basés sur des signatures.
2. **Détection basée sur les anomalies :** Identifie les activités anormales par rapport à un comportement normal prédéfini. Efficace pour détecter des menaces inconnues.
   - **Exemples :** SIEM avec détection des anomalies, solutions de Machine Learning.
3. **Détection basée sur l'heuristique :** Utilise des règles heuristiques pour détecter des comportements potentiellement malveillants. Combine des éléments de signatures et d'anomalies.
   - **Exemples :** Outils EDR, certains IDS/IPS.

Méthodologies de détection et de réponse

4. **Réponse automatisée :** Utilise des solutions SOAR pour automatiser les réponses aux incidents, réduisant ainsi le temps de réaction et limitant l'impact des incidents.
    - **Exemples :** Automatisation des quarantaines d'endpoint, déploiement automatique de correctifs.
5. **Approche de la chasse aux menaces (Threat Hunting) :** Implique la recherche proactive de menaces cachées dans l'environnement de l'organisation, souvent sans alerte préalable.
    - **Exemples :** Analyse manuelle des journaux, utilisation d'outils de Threat Intelligence pour identifier des comportements suspects.

TP 1

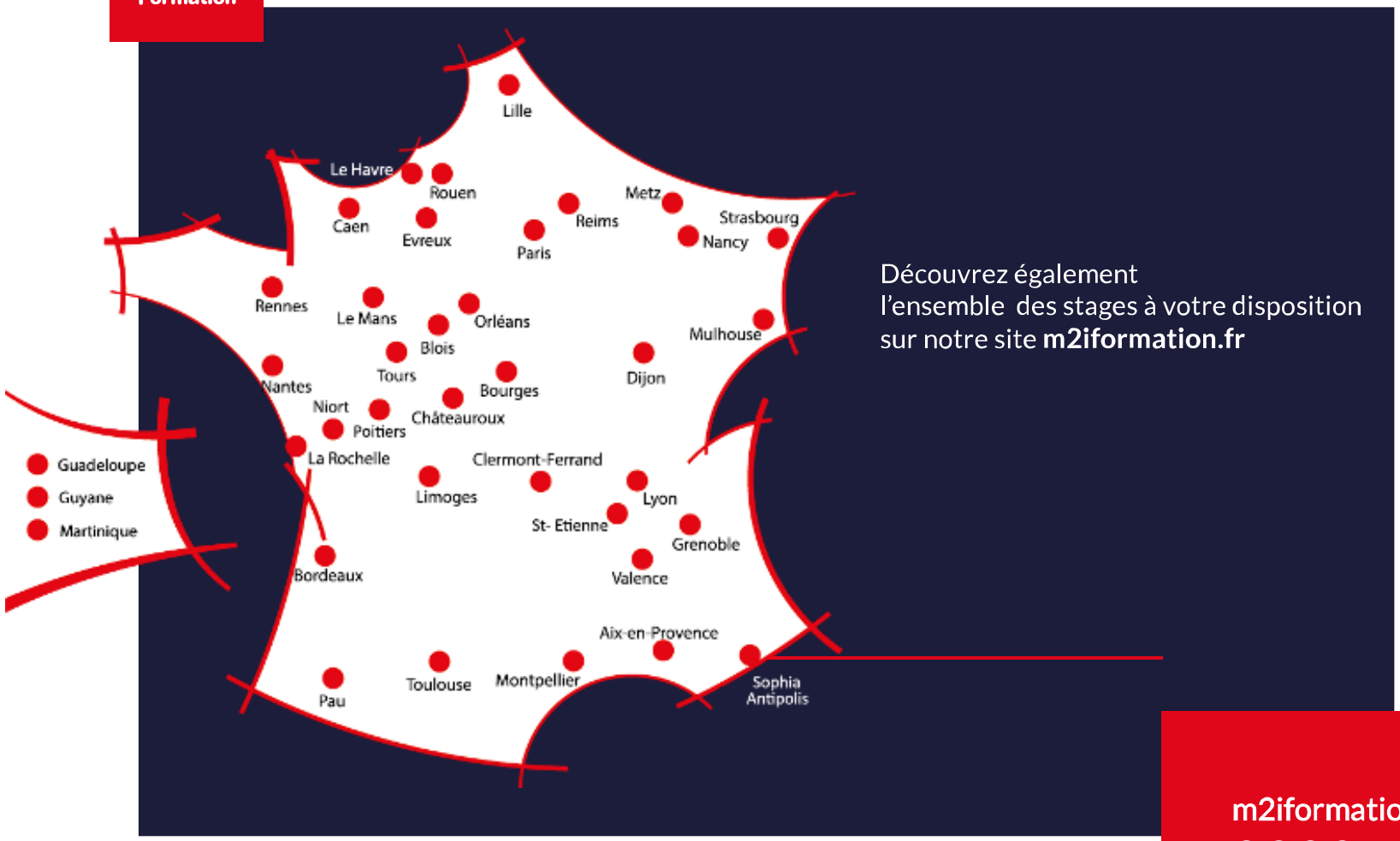
Objectif: Le but de ce TP est de vous familiariser avec les vulnérabilités de sécurité majeures des cinq dernières années qui ont fait la une des médias, comprendre comment elles ont été exploitées, et quelles solutions ont été mises en place pour les résoudre.

1. **Sélection des Vulnérabilités Majeures**:
   - Identifiez au moins cinq vulnérabilités majeures qui ont fait la une des médias au cours des cinq dernières années.
   - Pour chaque vulnérabilité, documentez les informations de base : date de découverte, description de la faille, produits ou services affectés.
2. **Analyse de l'Exploitation**:
   - Recherchez comment chaque vulnérabilité a été exploitée. Utilisez des rapports d'incidents, des analyses de sécurité, et des articles de presse pour trouver des détails sur les attaques réelles.
   - Décrivez les méthodes d'exploitation, les acteurs impliqués (si connus), et les impacts des attaques (ex. : vol de données, interruptions de service, etc.).

TP 1

3. **Solutions et Mesures de Mitigation**:
    - Identifiez les mesures de mitigation et les solutions qui ont été mises en place pour chaque vulnérabilité. Cela peut inclure des patchs logiciels, des mises à jour de sécurité, des recommandations de configuration, etc.
    - Documentez les actions prises par les entreprises ou les développeurs pour résoudre les problèmes et protéger les utilisateurs.
4. **Présentation des Résultats**:
    - Compilez vos résultats dans un rapport structuré.
    - Utilisez des graphiques et des tableaux pour illustrer les données de manière claire.
    - Préparez une présentation résumant les points clés de votre recherche et analyse.

Bonne recherche et analyse !



Découvrez également
l'ensemble des stages à votre disposition
sur notre site **m2iformation.fr**

m2iformation.fr