Module 1 – Fondamentaux techniques et règlementaires

Fondamentaux de la sécurité des SI et réseaux

Séquence 6 : Veille technologique et règlementaire

OIDANEOS

Présentation de la séquence
Objectifs et notions abordées

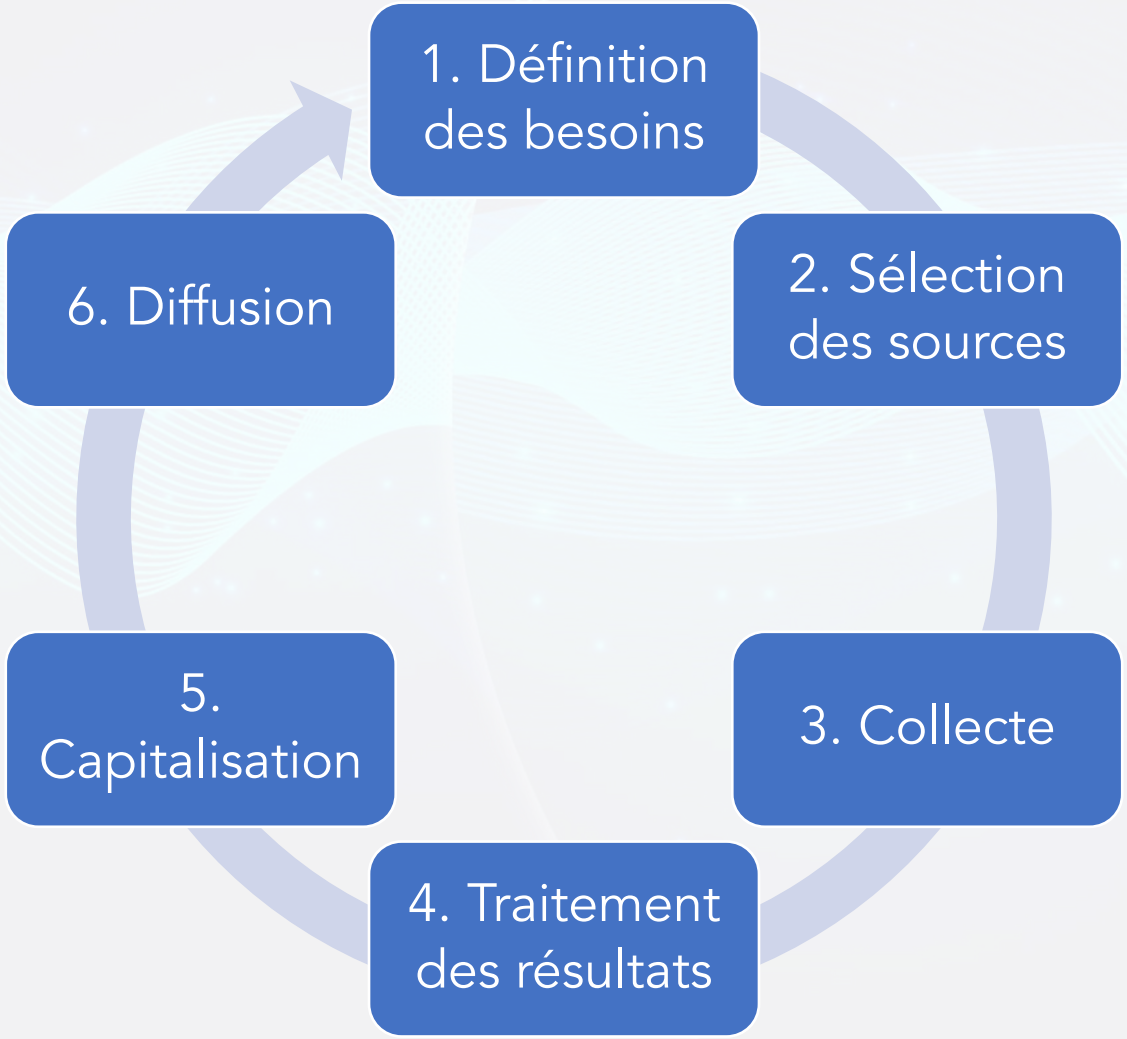
Identifier les sources fiables et mettre en place une veille cyber

- Objectifs et cadre de la veille cyber
- Réalisation de la veille cyber
- Exploitation et diffusion des résultats

Objectifs et cadre de la veille cyber

Objectifs et cadre de la veille cyber

Le cycle de la veille



Objectifs et cadre de la veille cyber

L'importance de la veille cyber

- Anticipation des menaces et des risques cyber
- Place à part entière dans la stratégie de protection des systèmes d'information des entreprises
- Réaction adaptée et efficace en cas d'incidents cyber
- Évolution constante des technologies
- Dynamique géopolitique ayant un impact majeur sur la sécurité numérique

Objectifs et cadre de la veille cyber
Particularités de la veille en cybersécurité

- Flux d'information exponentiel
- Durée de vie limitée pour chacune des informations
- Rapidité de la collecte d'informations
- Règles strictes en matière de partage et d'utilisation

Objectifs et cadre de la veille cyber

Catégories de veille en cybersécurité

Menaces

Risques

Géopolitique

Concurrentielle

Règlementaire

Technologique

Réputationnelle

Objectifs et cadre de la veille cyber

Prérequis d'une veille en cybersécurité

- **Curiosité et patience**
- **Recherche et tri des informations**
- **Accès aux outils de veille**
- **Expertise technique**
- **Maîtrise des langues**

Objectifs et cadre de la veille cyber

Les niveaux de veille

Opérationnel	Tactique	Stratégique
Appuyer les professionnels dans la gestion opérationnelle des systèmes et des données d'une organisation	Avoir une bonne connaissance de la nature des menaces cyber connues et émergentes pour renforcer sa posture de sécurité	Comprendre les motivations et les intentions des attaquants et contextualiser les menaces
• Identifier les comportements suspects de manière précoce • Détecter des incidents de sécurité • Réagir rapidement et efficacement aux vulnérabilités exploitées	• Identifier les risques cyber en collectant des informations essentielles • Améliorer ses connaissances des modes opératoires des acteurs malveillants • Ajuster les mécanismes de défense pour s'adapter aux menaces connues et émergentes • Définir des mesures de protection complémentaires à mettre en place	• Comprendre les motivations des attaquants • Évaluer les risques spécifiques à un métier, un secteur d'activité ou d'une région • Cartographier le panorama des menaces • Savoir détecter des signaux faibles parmi les informations recueillis

Objectifs et cadre de la veille cyber

Le cadrage de la veille en cybersécurité

Destinataire de la veille	• Conseil d'administration et membres de la direction • Équipes internes de cybersécurité • DSI / RSSI • Analystes SOC
Contenu et fréquence de diffusion	• Quelles informations inclure dans les remontées de veille ? Quelles informations ou sujets omettre ? • A quelle fréquence sera transmise la veille ?
Mise en forme	• Rapports écrits • Tableaux de bord en ligne • Présentations • Newsletters
Fréquence de la veille	• En fonction de l'actualité, de la criticité, de votre disponibilité

Réalisation de la veille cyber

Réalisation de la veille cyber

Les différentes sources d'informations en cybersécurité

Agences de cybersécurité

Réalisation de la veille cyber

Les différentes sources d'informations en cybersécurité

Les centres de partages sectoriels (Information Sharing and Analysis Center – ISAC)

- Critical Infrastructure Information Sharing & Analysis Centre (CI-ISAC) en Australie
- Global Mining and Metals Information Sharing & Analysis Centre (MM-ISAC) au Canada
- European Energy – Information Sharing & Analysis Centre (EE-ISAC) en Europe

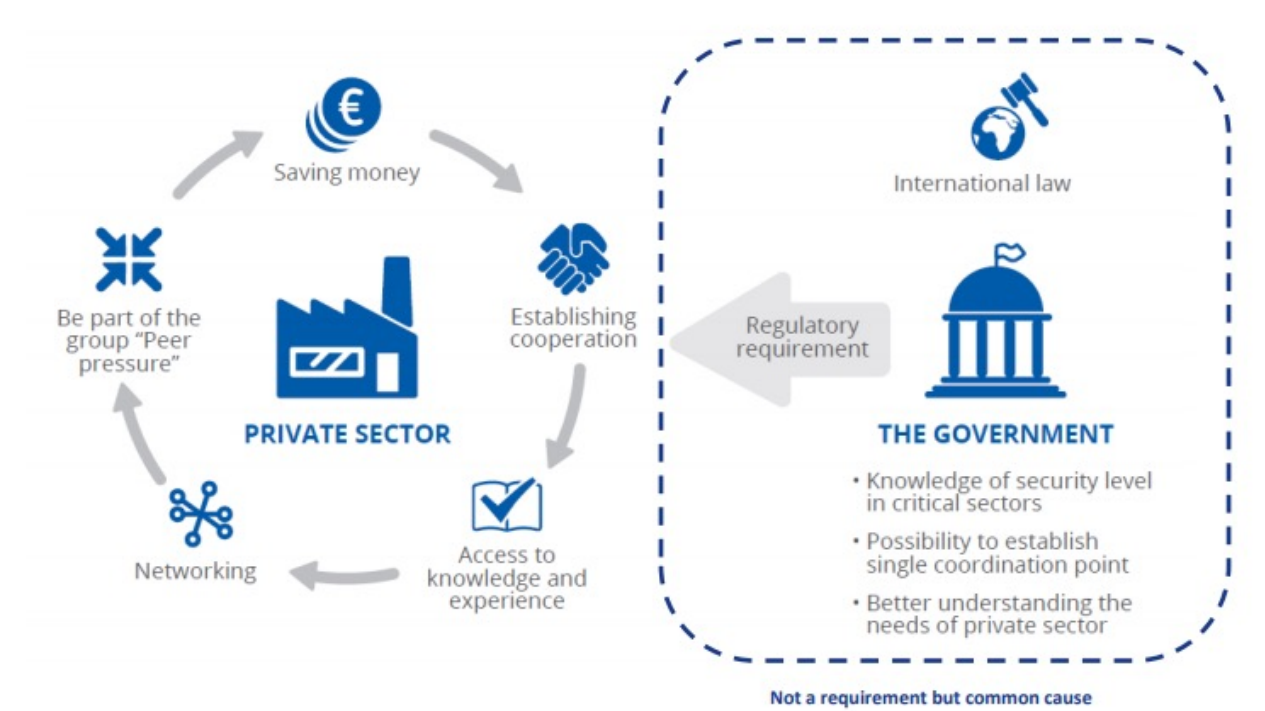


Figure 1: Reasons for the creation of ISACs

Réalisation de la veille cyber

Les différentes sources d'informations en cybersécurité

CERT Santé

FRANCE CYBER MARITIME M-CERT

CERT Aviation France

CERT-FR

Les équipes de réponse aux incidents

InterCERT FRANCE

Réalisation de la veille cyber

Les différentes sources d'informations en cybersécurité

Sources communautaires et réseaux professionnels

CESIN

CLUSIF

CDSE CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES

Cigref RÉUSSIR LE NUMÉRIQUE

OSINT-FR OPEN SOURCE INTELLIGENCE ASSOCIATION LOI 1901

{M} {82}

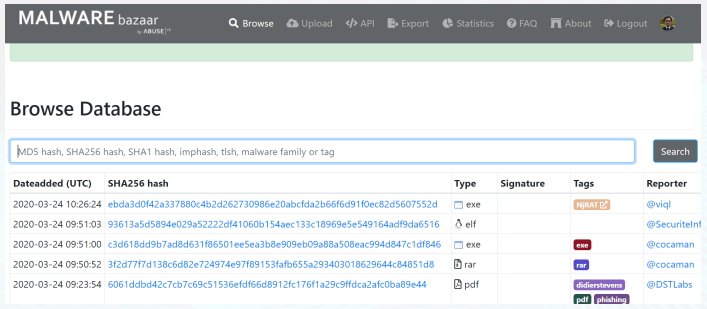
CLUB 27001

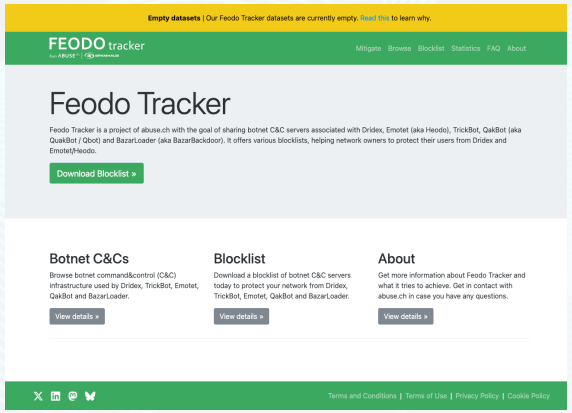
CLUBEBIOS

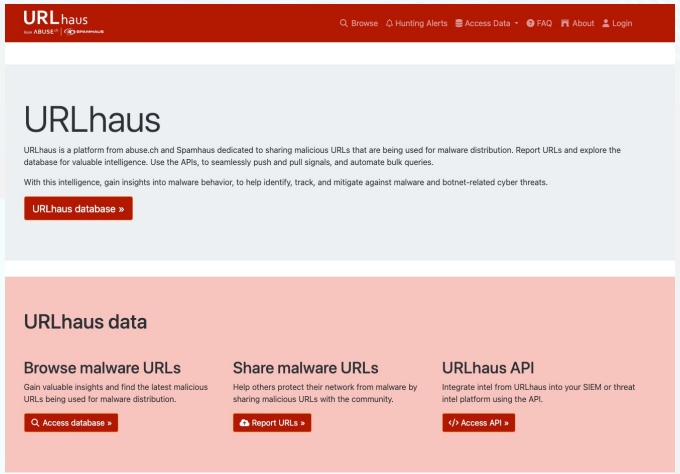
Réalisation de la veille cyber

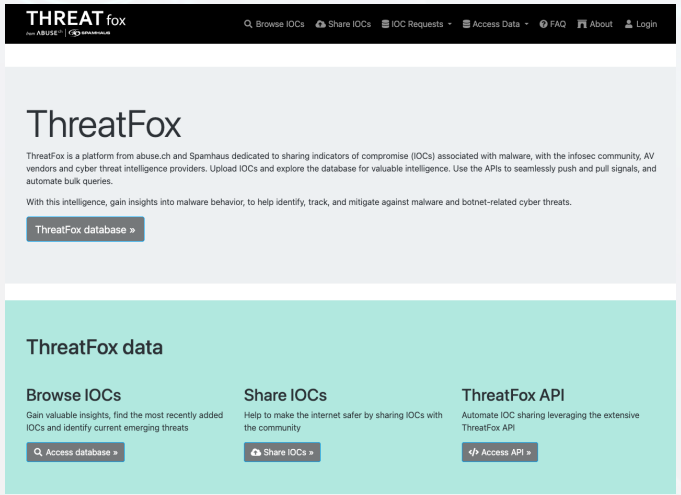
Les différentes sources d'informations en cybersécurité

Les feeds communautaires









Réalisation de la veille cyber

Les différentes sources d'informations en cybersécurité

- Écosystème des partenaires
- Médias spécialisés
- Éditeurs de cybersécurité
- Réseaux sociaux
- Publications universitaires et de recherches
- Forums, marketplace cybercriminels, darkweb

Réalisation de la veille cyber
Les ressources disponibles

- **Articles de blogs**
  - Krebsonsecurity
  - Risk-Insight de Wavestone
- **Rapports**
  - Panorama sur les menaces du CERT-FR, de l'ANSSI ou de Cybermalveillance
- **Newsletters**
  - VeilleCyber
  - SANS CyberSecurity Newsletter
- **Podcasts et émissions**
  - NoLimitSecu
- **Webinaires**

Réalisation de la veille cyber
Les ressources disponibles

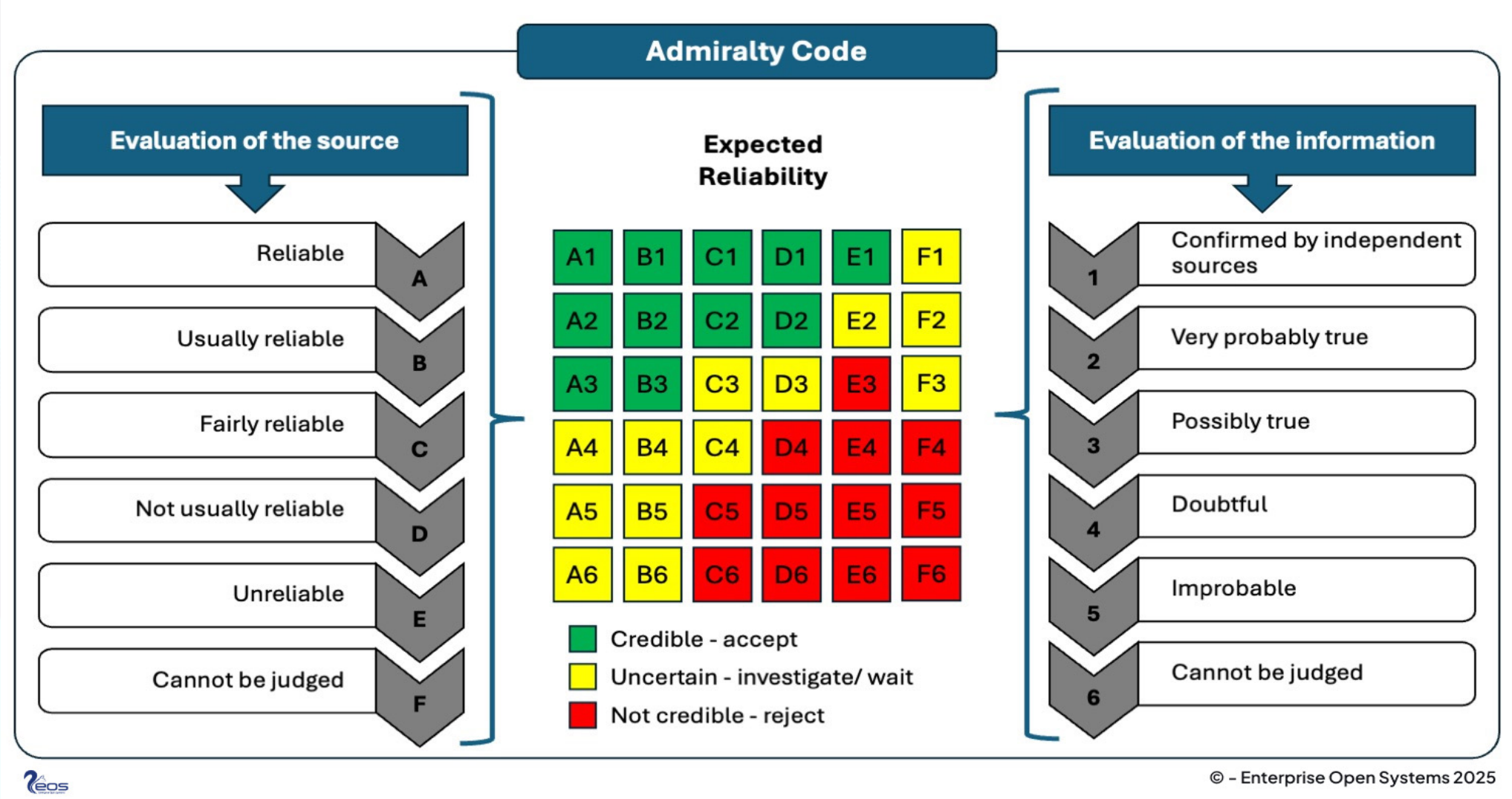
- **Articles, communiqués et conférences de presse**
- **Journaux**
  - ZATAZ
- **Événements et conférences sur la cybersécurité**
  - Forum International de la Cybersécurité (FIC)
  - LeHack
  - DEFCON
  - Blackhat
- **Forums spécialisés**
- **Actualité législative**

Réalisation de la veille cyber

La qualification des sources d'information

- **Crédibilité**
- **Actualité**
- **Transparence**
- **Analyse critique**
- **Indépendance**
- **Cohérence**

Réalisation de la veille cyber
La qualification des sources d'information



Réalisation de la veille cyber

La qualification des sources d'information

Réalisation de la veille cyber
Structuration de la veille cyber

Opérationnel	Tactique	Stratégique
Surveillance en temps réel des éléments cruciaux pour la sécurité informatique	Analyse approfondie des menaces et des attaquants pour leur compréhension approfondie et l'élaboration de contre-mesures	Examen des enjeux de cybersécurité pour prendre des décisions éclairées pour protéger l'organisation à long terme
• Suivi des flux d'indicateurs de compromission (IoC) • Suivi de nouvelles vulnérabilités et correctifs associés • Suivi des fuites de données et des revendications des victimes par les groupes d'attaquants	• Tendances relatives aux risques et menaces cyber • Techniques d'attaque adoptées par les acteurs de la menace • Arsenal des attaquants • Apparition et évolution des outils malveillants	• Motivation des attaquants • Liens entre les campagnes d'attaque et les intérêts étatiques • Règlementations nationales et internationales • Géopolitique et enjeux internationaux

Ces niveaux peuvent être interconnectés et met en évidence la complexité de la veille en cybersécurité. Il est nécessaire d'avoir une approche globale pour assurer une protection efficace.

Réalisation de la veille cyber
Classification de la veille

- Priorité et importance
- Type de source
- Fiabilité et crédibilité
- Thématique
- Critères géographiques ou linguistiques
- Type de média collecté

Réalisation de la veille cyber
Traitement et analyse de l'information

- **Analyse des résultats de veille**
  - Analyse des tendances pour l'identification des modèles émergents
  - Évaluation des risques associés à différentes vulnérabilités ou menaces
  - Formulation de recommandations

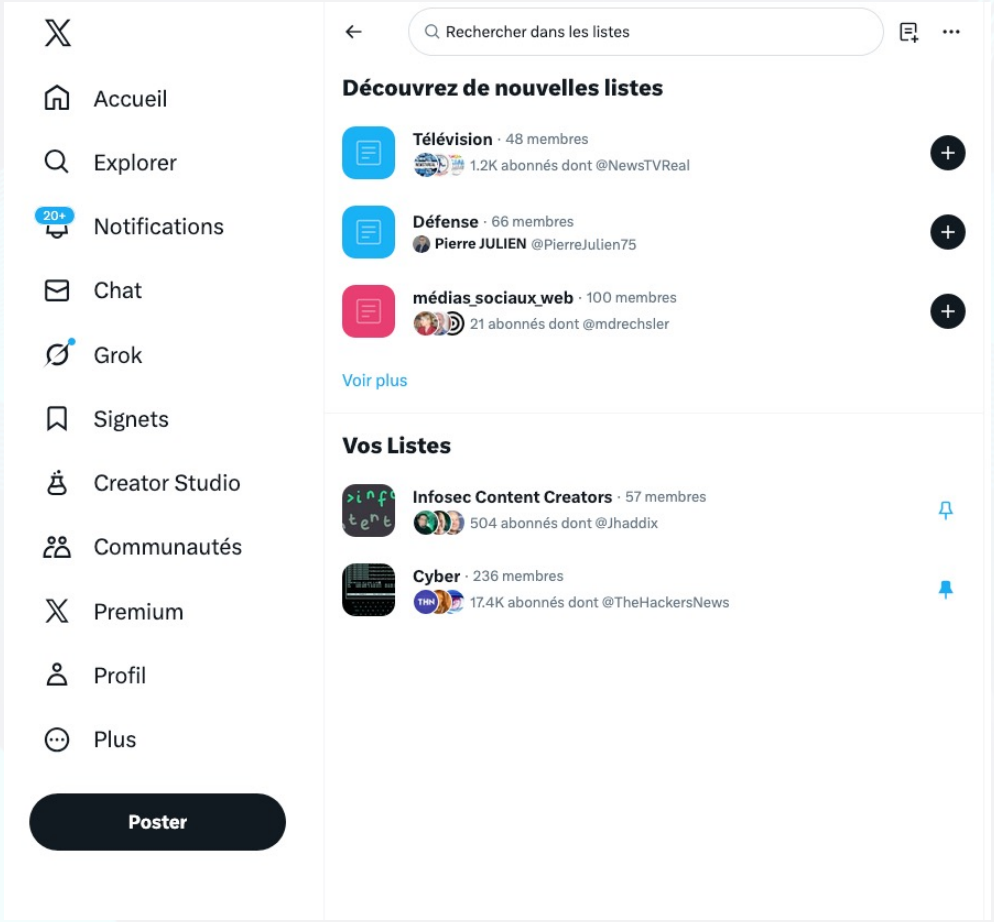
Réalisation de la veille cyber

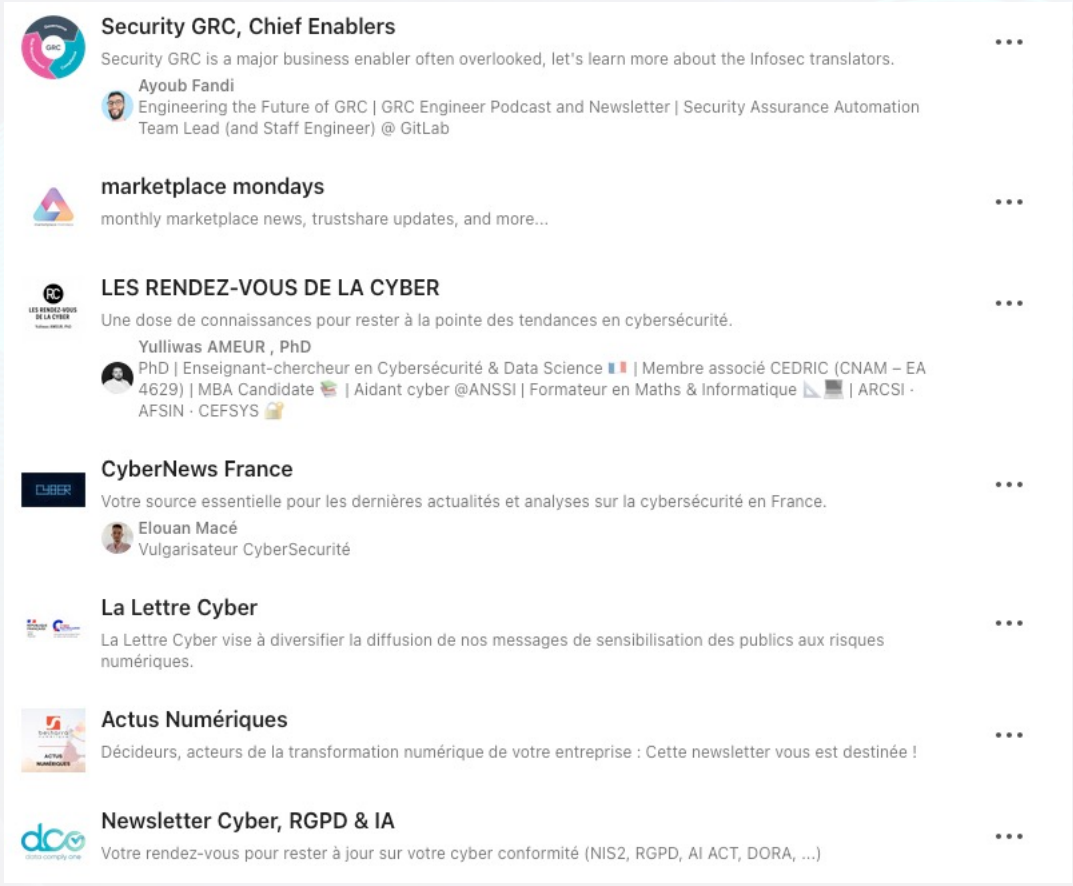
Outils pour collecter, traiter et analyser les données

- **Threat Intelligence Platforms (TIP)**
  - OpenCTI
  - MISP
- **Gestionnaires de favoris**
  - RainDrop
  - Zotero
- **Agrégateurs de flux RSS**
  - Start.me
  - Flipboard
  - Inoreader
- **Plateformes de veille**
  - Feedly
- **Tableurs**
  - Excel, Google Sheets…

Réalisation de la veille cyber

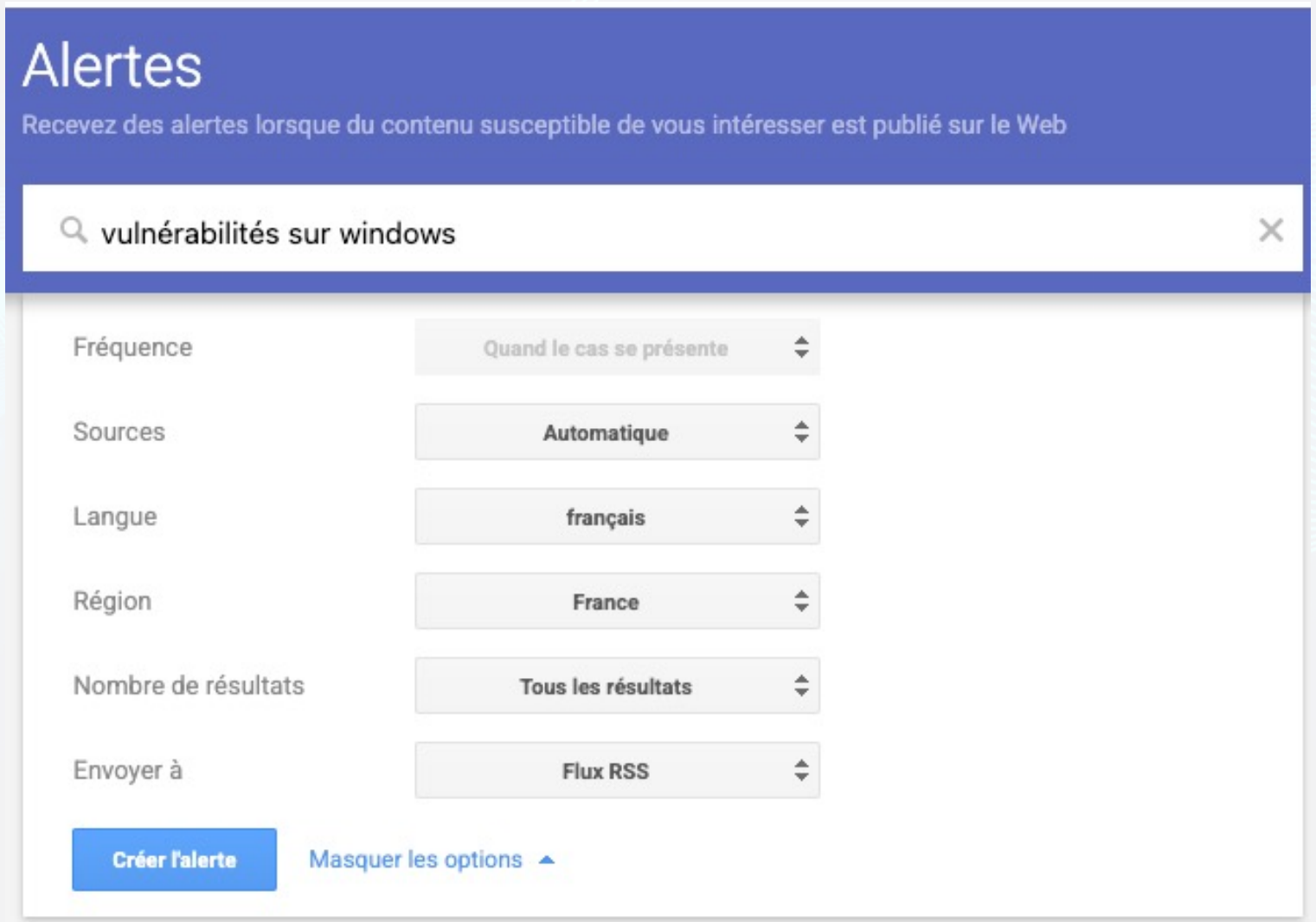
Outils pour collecter, traiter et analyser les données





Réalisation de la veille cyber

Outils pour collecter, traiter et analyser les données



Réalisation de la veille cyber

Outils pour collecter, traiter et analyser les données

Exploitation et diffusion des résultats

Exploitation et diffusion des résultats

Diffusion des résultats de la veille

- Destinataires
- Contenu
- Fréquence de diffusion
- Mise en forme des résultats de votre veille

Exploitation et diffusion des résultats

Respect des protocoles d'utilisation et de diffusion de l'information

- Normalisation de l'échange et de l'utilisation des informations
- Convergence des pratiques de traitement de l'information
- Consolidation des liens de confiance entre différentes communautés
- Protection des systèmes d'information

Exploitation et diffusion des résultats

Respect des protocoles d'utilisation et de diffusion de l'information

Interprétation opérationnelle des différents niveaux de TLP applicables aux informations partagées par l'ANSSI	
TLP:RED	**Diffusion limitée au seul périmètre interne d'une entité juridique, sur la base du besoin d'en connaître.** Par exemple : • un bénéficiaire peut partager à tout ou partie d'une équipe interne bien identifiée et sur la base du besoin d'en connaître mais le repartage au-delà de l'entité juridique est interdit ; • un bénéficiaire peut partager avec ses prestataires en régie qui ont le besoin d'en connaître.
TLP:AMBER	**Diffusion limitée à quelques entités identifiées, liées par un engagement (*ex: une communauté fermée*).** Par exemple : • un bénéficiaire peut partager avec ses prestataires en régie et externes, ses filiales et son groupe ; • un prestataire peut partager avec, ou utiliser au profit de tous ses clients.
TLP:GREEN	**Diffusion libre au sein d'une communauté (ouverte ou fermée) bien identifiée, repartage libre au sein de ces communautés (prestataires inclus).** Par exemple : • un bénéficiaire peut partager avec ses prestataires, son groupe, ses filiales, ses partenaires et les pairs de sa communauté sans pour autant diffuser l'information publiquement ; • un prestataire peut partager avec ses clients, son groupe, ses filiales, et les pairs de son secteur sans pour autant diffuser l'information publiquement.
TLP:CLEAR	**Diffusion publique, sans restriction, partage libre entre les différentes communautés, y compris sur Internet.**

Interprétation opérationnelle des différents niveaux de PAP applicables aux informations partagées par l'ANSSI	
PAP:RED	**Utilisation limitée aux investigations numériques ou à la détection, sur des infrastructures dédiées :** • seules les personnes ayant le besoin d'en connaître ont accès à ces infrastructures ; • ces infrastructures sont protégées des réseaux publics (ex.: Internet) et des infrastructures communes du système d'information (ci-après « SI ») de l'entité ; • afin de ne rien révéler des capacités de détection, seules des actions non visibles par un potentiel attaquant sont autorisées, telles que par exemple des recherches hors production sur des éléments collectés préalablement ; • les interactions directes ou indirectes, ainsi que les requêtes sur des services tiers, ne sont pas autorisées. Par exemple : • après collecte d'éléments réseaux/systèmes/évenementiels, remontés sur un réseau maîtrisé et isolé depuis lequel un bénéficiaire peut surveiller ses infrastructures pour confirmer l'absence d'une menace spécifique ou détecter son apparition ; • un prestataire peut exploiter l'information sur un SI d'investigation / de détection pour le compte de ses clients (nécessite l'export d'information du SI client vers son SI dédié). L'usage de services IaaS/SaaS spécialisés en la matière est autorisé si le contrat permet de garantir la confidentialité des données manipulées.
PAP:AMBER	**Utilisation limitée à une exploitation passive de la donnée, c'est-à-dire aux seules actions non directement visibles des sources malveillantes.** Par exemple: • un bénéficiaire peut faire de la recherche en source ouverte ou consulter une base de connaissance en ligne, pour mieux qualifier l'information ; • un bénéficiaire peut utiliser l'information au sein d'une infrastructure compromise pour identifier un élément malveillant (*ex. : détecter la présence d'un code malveillant lors d'une chasse sur parc*) Les interactions, même indirectes, avec le système ou l'infrastructure de l'attaquant sont interdites.
PAP:GREEN	**Utilisation encadrée autorisant les interactions non intrusives avec des sources malveillantes.** Par exemple : • un bénéficiaire peut bloquer, au niveau d'un pare-feu, du trafic malveillant entrant en provenance d'une adresse IP ; • un bénéficiaire peut bloquer, au niveau d'un serveur mandataire, du trafic malveillant sortant à destination d'une adresse Web.
PAP:CLEAR	**Utilisation libre dans le respect des licences et de la loi, pas de contrainte relative à l'exploitation ou à la manipulation de l'information.**

Exploitation et diffusion des résultats

Respect des protocoles d'utilisation et de diffusion de l'information

	PAP:RED	PAP:AMBER	PAP:GREEN	PAP:CLEAR
TLP:RED	P1	P2	N/A	N/A
TLP:AMBER	P3	P4	P5	N/A
TLP:GREEN	N/A	P6	P7	NA
TLP:CLEAR	N/A	N/A	N/A	P8

Exploitation et diffusion des résultats

Amélioration continue

Exploitation des résultats de la veille

Valeur ajoutée de la veille

Prise en compte des feedbacks

Préparation du prochain cycle de veille