LES FICHES PRATIQUES CLOUD TEMPLE

Cyber threat intelligence, en clair

DEFINITION

La Cyber Threat Intelligence (CTI) désigne l'ensemble des processus, outils et données permettant de collecter, analyser et partager des informations sur les menaces informatiques.

QUI ? COMMENT ? POURQUOI ?

L'objectif est de répondre à ces questions pour anticiper les actions malveillantes et de renforcer la défense des systèmes d'information.

- Identifier les acteurs de la menace
- Reconnaître les techniques d'attaque
- Anticiper le vulnérabilités exploitées et les campagnes malveillantes
- Renforcer les mesures de prévention, détection et réponse
- Aide à la prise de décision stratégique et opérationnelle en cybersécurité

LES CARACTÉRISTIQUES DE LA CYBER THREAT INTELLIGENCE

Types de renseignements	**Tactique** : Informations sur les techniques, tactiques et procédures (TTP) | **Opérationnel** : Détails sur des événements spécifiques en cours ou passés | **Stratégique** : Analyse de haut niveau sur les menaces, leurs motivations et objectifs | **Technique** : Données brutes et indicateurs exploitables directement par des outils
Sources de CTI	**OSINT** | **Sources commerciales** : fournisseurs de Threat Intelligence |**Partage communautaire** : ISACs, projets open-source, échanges entre CERTs | **Sources internes** : logs, incidents passés, analyses de malware ou de réseau
Outils et plateformes CTI	**MITRE ATT&CK** : base de données des TTP utilisées par les attaquants | **MISP** : plateforme de partage de threat intelligence | **STIX/TAXII** : formats normalisés d'échange de renseignements | **Outils de veille** : VirusTotal, Shodan, ThreatConnect...

L'ANALYSE

Giuliano Ippoliti,
directeur cybersécurité de
Cloud Temple

« Pour rivaliser avec les grandes puissances mondiales, en particulier les États-Unis et la Chine, les États membres de l'Union européenne ont tout intérêt à mutualiser leurs compétences en matière de cybersécurité et à renforcer leur coopération. Ce texte s'inscrit dans cette dynamique en prévoyant notamment le renforcement des prérogatives de l'ENISA, la promotion de schémas de certification à l'échelle européenne et la consolidation des synergies entre États membres.»

LE CYCLE DE VIE DU CTI

- La planification : quels besoins, quelles menaces surveiller ?
- La collecte d'informations (outils, veille, sources) Le traitement des données collectées
- Processus d'analyse : corrélation, tri, contextualisation
- La diffusion : partage avec les bonnes personnes ou outils
- Retour d'expérience : évaluation de la pertinence et amélioration continue

Pour être pertinente, la threat intelligence doit être contextualisée, partagée et exploitée efficacement dans l'organisation. De même la manipulation de données ne doit pas porter sur des données confidentielles et personnelles.

CLOUD TEMPLE
Innovative by design