Certificate Transparency : surveillance phishing et typosquatting

> Exploitez les CT logs pour surveiller en temps réel les certificats suspects sur vos domaines : Certstream, crt.sh, détection typosquatting et intégration...

Chaque jour, des milliers de certificats TLS sont émis par les autorités de certification et enregistrés dans des journaux publics immuables appelés CT logs (Certificate Transparency logs). Ce mécanisme, conçu à l'origine pour détecter les certificats frauduleux émis par des CA compromises, est devenu en 2026 l'un des outils de veille les plus puissants pour les équipes de sécurité : il permet de surveiller en quasi-temps réel l'émission de tout nouveau certificat sur votre domaine ou sur des domaines imitant votre marque. Les attaquants utilisent les CT logs depuis des années pour la reconnaissance passive : un scan leur révèle vos sous-domaines oubliés, vos nouvelles infras, vos prestataires cloud et vos projets en développement. Ce guide vous explique comment retourner cet avantage informationnel en faveur des défenseurs : surveiller Certstream, interroger crt.sh, détecter automatiquement le typosquatting et les domaines de phishing imitant votre marque, et intégrer ces alertes dans votre SOC ou votre workflow d'investigation forensique. En 2024, plus de 3 000 nouveaux domaines imitant des marques françaises ont été détectés chaque mois via CT monitoring — sans cette surveillance proactive, la plupart de ces campagnes de phishing auraient eu le temps de piéger des centaines de victimes avant d'être détectées et signalées.

À RETENIR

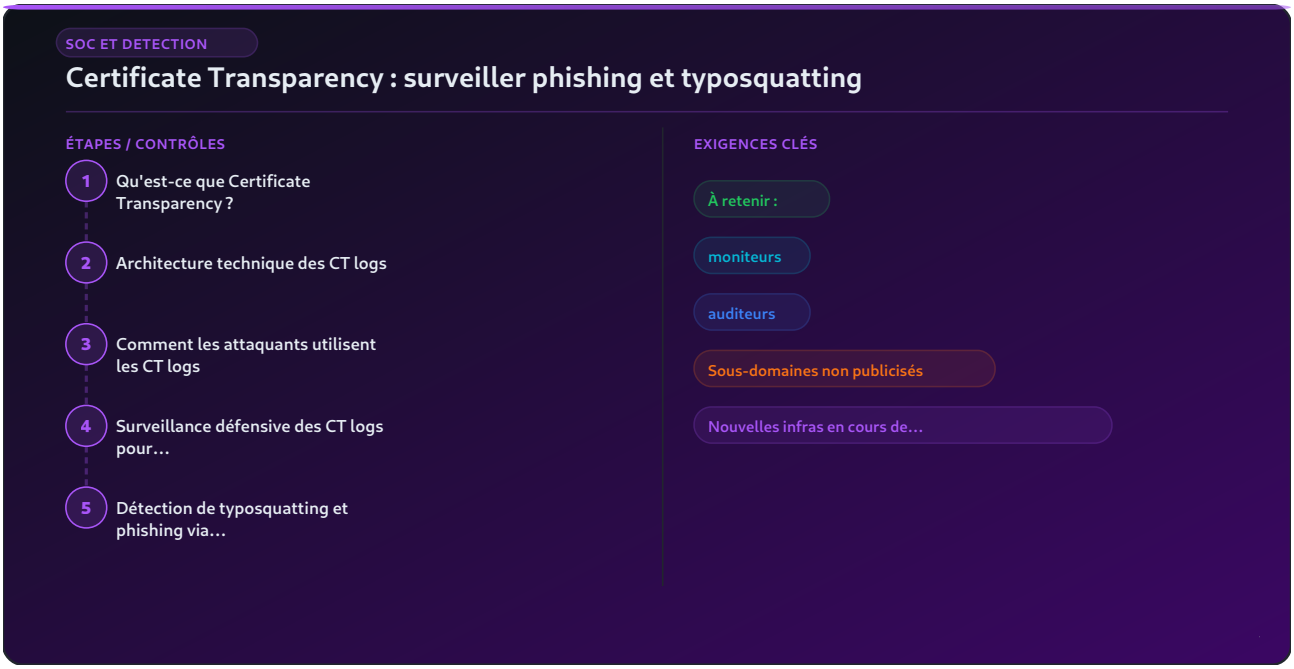
À retenir :

Depuis 2018, Chrome exige que tout certificat TLS de confiance soit loggé dans au moins deux CT logs approuvés — il existe aujourd'hui plus de 100 CT logs actifs dans le monde.

Certstream permet de consommer le flux de tous les nouveaux certificats en temps réel via WebSocket — environ 10 à 20 certificats par seconde.

La détection de typosquatting via CT logs filtre sur les homoglyphes, les variations orthographiques et les combinaisons marque+action (votreentreprise-facture.com).

Les CT logs permettent de retrouver des domaines C2 historiques dans les investigations forensiques — même si le domaine a expiré depuis.



Qu'est-ce que Certificate Transparency ?

Certificate Transparency (CT) est un framework ouvert de journalisation et d'audit des certificats TLS, défini par la RFC 6962 (Google, 2013) et son successeur RFC 9162. L'idée centrale : chaque autorité de certification (DigiCert, Let's Encrypt, Sectigo, etc.) doit soumettre les certificats qu'elle émet dans des journaux publics, cryptographiquement intègres et append-only (on ne peut qu'ajouter des entrées, jamais en supprimer ou modifier).

En 2011, la CA DigiNotar a été compromise et a émis des certificats frauduleux pour google.com et des agences gouvernementales iraniennes. En 2012, Trustwave a admis avoir émis un certificat intermédiaire permettant de signer des certificats pour n'importe quel domaine. Ces incidents ont

révélé qu'il était impossible de détecter les certificats frauduleux sans registre public. CT résout ce problème : si un certificat n'est pas dans les logs, les navigateurs modernes le rejettent.

Depuis avril 2018, Google Chrome exige que tout certificat TLS de confiance soit accompagné de SCT (Signed Certificate Timestamps) prouvant son inclusion dans au moins deux CT logs approuvés. Un certificat sans SCT valides est rejeté avec l'erreur NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED. Apple Safari a une politique similaire depuis 2017.

Architecture technique des CT logs

Un CT log est une structure de données Merkle tree (arbre de hachage binaire). Chaque certificat soumis est haché et ajouté comme feuille de l'arbre. La racine (Merkle Tree Hash) est publiée périodiquement et signée par la clé privée du log operator. Cette signature (STH, Signed Tree Head) permet à tout auditeur de vérifier l'intégrité du log.

⚡ **Retour terrain**

Dans les SOC que j'accompagne, le principal problème n'est pas le manque d'alertes mais l'excès : 'alert fatigue' systématique, analysts qui désactivent des règles jugées trop bruyantes sans documentation, et faux positifs récurrents qui masquent les vrais incidents. J'ai développé un tableau de bord simple — 3 métriques : taux de faux positifs par règle, MTTD (mean time to detect) sur incidents réels, et ratio alertes/analyst — qui permet en une réunion hebdomadaire de 30 minutes d'identifier les règles à tuner en priorité.

SCT (Signed Certificate Timestamp)

Quand une CA soumet un certificat à un CT log, elle reçoit en retour un SCT : une promesse cryptographique signée que ce certificat sera inclus dans le log dans un délai Maximum Merge Delay (MMD, généralement 24h). Le SCT est ensuite embarqué dans le certificat (extension X.509) ou envoyé via TLS handshake — c'est ce SCT que Chrome vérifie pour autoriser l'affichage de la page.

Moniteurs et auditeurs

L'architecture CT distingue deux types d'acteurs : les **moniteurs** qui consomment les CT logs et vérifient leur contenu (détectent les certificats frauduleux, surveillent des domaines spécifiques — c'est le rôle que vous allez jouer), et les **auditeurs** qui vérifient la cohérence cryptographique des logs (aucune entrée supprimée ou modifiée). Le navigateur Chrome fait office d'auditeur léger via Expect-CT headers.

Comment les attaquants utilisent les CT logs

Les équipes offensives et les APT utilisent les CT logs depuis des années pour la reconnaissance passive. C'est une technique OSINT légale et indétectable car elle n'implique aucune interaction avec les systèmes cibles. En interrogeant crt.sh ou en consommant Certstream, un attaquant peut découvrir :

Sous-domaines non publicisés : `staging.votreentreprise.fr`, `dev.votreentreprise.fr`, `vpn.votreentreprise.fr` — chaque sous-domaine HTTPS est dans les CT logs.

Nouvelles infras en cours de déploiement : un certificat émis pour `nouveau-erp.votreentreprise.fr` révèle qu'un projet est en cours, potentiellement avec une configuration de sécurité pas encore durcie.

Prestataires cloud : un certificat Let's Encrypt pour `votreentreprise.s3.amazonaws.com` révèle l'usage d'AWS S3, potentiellement avec des buckets mal configurés.

Historique complet : tous les certificats émis depuis 2013 sont disponibles — y compris pour des infras abandonnées qui pourraient encore être accessibles.

Surveillance défensive des CT logs pour votre domaine

crt.sh : interrogation manuelle et API

crt.sh (opéré par Sectigo) est le moteur de recherche CT le plus connu. Il agrège la quasi-totalité des CT logs publics et expose une interface web et une API REST.

```
 # Chercher tous les certificats pour votreentreprise.fr et sous-domaines
curl -s "https://crt.sh/?q=%.votreentreprise.fr&output=json" | \
  python3 -c "import json,sys; data=json.load(sys.stdin); [print(d['name_value']) for d in data]"
  sort -u
```

Cette requête retourne tous les sous-domaines pour lesquels un certificat a été émis — y compris des sous-domaines que vous n'avez peut-être pas référencés dans vos inventaires d'actifs.

Certstream : flux temps réel

Certstream est un service open source (CaliDog Security) qui consomme en continu tous les CT logs publics et expose un flux WebSocket de tous les nouveaux certificats. Le débit est d'environ 10 à 20 certificats par seconde en permanence. En filtrant ce flux sur votre domaine, vous recevez une alerte dans les secondes suivant l'émission d'un nouveau certificat.

```
 # Installation
pip3 install certstream

# Test simple
python3 -c "import certstream; certstream.listen(lambda m,c: print(m['data']['leaf_cert']['all_do
```

Facebook CT Monitor

Facebook propose un service gratuit de surveillance CT qui envoie un email à l'adresse enregistrée dans le WHOIS chaque fois qu'un nouveau certificat est émis pour votre domaine. C'est la solution la plus simple pour une surveillance basique sans infrastructure.

Détection de typosquatting et phishing via CT logs

La détection de domaines imitant votre marque est le cas d'usage le plus précieux de la surveillance CT. Un attaquant préparant une campagne de phishing va émettre un certificat TLS pour son domaine frauduleux — et ce certificat va apparaître dans les CT logs.

Patterns à surveiller

Homoglyphes : remplacement de caractères par des similaires visuels (l → I, o → 0, rn → m). Ex. : `ayinedjimi-consultants.fr` → `ayinedjim1-consultants.fr`.

Additions de mots : `votreentreprise-facture.fr`, `votreentreprise-paiement.fr`, `secure-votreentreprise.fr`.

TLD alternatifs : votre domaine .fr en .com, .net, .io, ou avec un nouveau TLD suspect.

Insertions de caractères : `votre-entreprise.fr`, `votreentreprisee.fr`.

Algorithme de similarité pour la détection

```
 import certstream
from Levenshtein import distance as levenshtein_distance
import unicodedata

WATCHED_DOMAIN = "votreentreprise"
ALERT_THRESHOLD = 3  # distance de Levenshtein max

def normalize(domain):
    # Normalise les homoglyphes Unicode
    return unicodedata.normalize('NFKD', domain).encode('ascii', 'ignore').decode()

def callback(message, context):
    if message['message_type'] != 'certificate_update':
        return
    domains = message['data']['leaf_cert']['all_domains']
    for domain in domains:
        parts = domain.replace('*.', '').split('.')
        if len(parts) < 2:
            continue
        apex = parts[-2]
        normalized = normalize(apex)
        dist = levenshtein_distance(WATCHED_DOMAIN, normalized)
        if 0 < dist <= ALERT_THRESHOLD:
            print(f"[ALERTE] Domaine suspect: {domain} (distance={dist})")
            # Ici: envoyer alerte Slack/webhook

certstream.listen(callback)
```

Implémentation d'un monitor CT avec alerting Slack

Pour une intégration opérationnelle dans un workflow SOC, voici un script complet de surveillance avec alerting Slack via webhook :

```
 import certstream
import requests
import json
from datetime import datetime

WATCHED_DOMAINS = ["votreentreprise.fr", "ayinedjimi.fr"]
SLACK_WEBHOOK = "https://hooks.slack.com/services/XXXXX/YYYYY/ZZZZZ"
KEYWORDS = ["votreentreprise", "ayinedjimi", "nedjimi"]

def send_slack_alert(domain, cert_info):
    payload = {
        "text": ":rotating_light: *Nouveau certificat suspect détecté*",
        "attachments": [{
            "color": "danger",
            "fields": [
                {"title": "Domaine", "value": domain, "short": True},
                {"title": "Émetteur", "value": cert_info.get('issuer', {}).get('O', 'N/A'), "shor
                {"title": "Date", "value": datetime.utcnow().isoformat(), "short": True},
            ]
        }]
    }
    requests.post(SLACK_WEBHOOK, data=json.dumps(payload))

def callback(message, context):
    if message['message_type'] != 'certificate_update':
        return
    all_domains = message['data']['leaf_cert']['all_domains']
    cert_info = message['data']['leaf_cert']
    for domain in all_domains:
        clean = domain.lower().replace('*.', '')
        for keyword in KEYWORDS:
            if keyword in clean and clean not in WATCHED_DOMAINS:
                print(f"[{datetime.now()}] Suspect: {clean}")
                send_slack_alert(clean, cert_info)
                break

print("Démarrage surveillance CT logs...")
certstream.listen(callback)
```

CT logs en investigation forensique

Les CT logs conservent tous les certificats émis depuis 2013 — une mine d'or pour l'investigation forensique. Cas d'usage :

Retrouver des domaines C2 historiques : en cherchant les certificats associés à une infrastructure malveillante connue, on peut découvrir tous les domaines C2 utilisés dans une campagne APT.

Pivot sur un IOC : un domaine malveillant identifié peut être le point d'entrée pour trouver d'autres domaines de la même infrastructure (même CA, même organisation dans le Subject).

Timeline de l'infrastructure attaquante : les dates d'émission des certificats révèlent quand l'attaquant a préparé son infrastructure — souvent plusieurs semaines avant l'attaque.

Attribution : les erreurs des attaquants dans les champs Subject (nom d'organisation, localité) fournissent parfois des indices d'attribution.

```
# Chercher les certificats d'un domaine C2 suspect via crt.sh API
curl -s "https://crt.sh/?q=suspecte-infra.com&output=json" | \
  python3 -m json.tool | grep "name_value\|not_before\|issuer_name"
```

Limites des CT logs

La surveillance CT n'est pas infaillible. Ses limites :

Wildcards : un certificat wildcard (`*.votreentreprise.fr`) couvre tous les sous-domaines sans les révéler. Un attaquant qui obtient un wildcard frauduleux peut créer des sous-domaines indétectables via CT monitoring.

Délai de publication : le Maximum Merge Delay (MMD) est de 24h. En pratique, la plupart des CAs publient les certificats en quelques minutes, mais le délai existe.

Certificats privés : les certificats émis par une CA privée interne ne sont pas dans les CT logs publics.

DV vs OV vs EV : les certificats Domain Validation (DV, Let's Encrypt) sont émis en quelques secondes sans vérification d'identité — un attaquant peut créer un domaine de phishing certifié TLS en moins de 5 minutes.

Intégration dans un SOC : enrichissement IOC et threat intel

Dans un SOC mature, le monitoring CT s'intègre dans le flux d'enrichissement des indicateurs de compromission. Les domaines suspects détectés peuvent être soumis à des services de réputation (VirusTotal, URLscan), corrélés avec les logs proxy pour vérifier si des utilisateurs internes ont déjà visité le domaine suspect, ajoutés aux blocklists DNS (RPZ) préventives avant même que le domaine soit actif en phishing, et partagés sur des plateformes de threat intel (MISP, OpenCTI).

Notre article sur les règles Sigma et la détection décrit comment transformer ces indicateurs CT en règles de détection dans votre SIEM. La détection proactive des domaines de phishing complète notre article sur le quishing et phishing AiTM. Pour la corrélation dans un SOC, notre guide sur la détection des attaques AD avec Wazuh propose des intégrations similaires. Les attaques BEC détectables via CT monitoring sont analysées dans notre article sur les fraudes BEC et leur défense.

FAQ — Questions fréquentes

Certificate Transparency révèle-t-il les sous-domaines internes de mon organisation ?

Oui, si ces sous-domaines utilisent des certificats TLS émis par une CA publique de confiance. Tout certificat émis par ces CAs doit être loggé dans les CT logs — il n'y a pas de mécanisme d'exclusion pour les sous-domaines "privés". C'est pourquoi les équipes de sécurité recommandent d'utiliser une CA privée interne (PKI interne) pour les services internes. Pour les services accessibles depuis Internet avec des certificats publics, leur présence dans les CT logs

est inévitable — l'enjeu est de surveiller ces certificats pour détecter les émissions non autorisées. Un enregistrement DNS CAA correctement configuré (`votreentreprise.fr. CAA 0 issue "letsencrypt.org"`) restreint quelles CAs peuvent émettre des certificats pour votre domaine et est une défense complémentaire.

Certstream est-il fiable pour une utilisation en production ?

Certstream est un service gratuit opéré par CaliDog Security (open source sur GitHub). La fiabilité pour une utilisation en production a des limites : le service public peut subir des interruptions. Pour une utilisation en production critique, il est recommandé de déployer sa propre instance Certstream ou d'utiliser des solutions commerciales comme DomainTools Iris ou Recorded Future qui agrègent les CT logs avec des SLA de disponibilité. Pour une PME ou une équipe sécurité avec des ressources limitées, le service public Certstream combiné avec crt.sh est suffisant. Les ressources officielles sont disponibles sur certificate.transparency.dev et le moteur de recherche CT de référence sur crt.sh.

Comment réagir si je détecte un domaine de phishing imitant mon organisation via CT monitoring ?

La détection précoce via CT est un avantage majeur car le domaine peut ne pas encore être actif. Les actions recommandées : 1) Vérifier si le domaine est déjà actif (DNS lookup, URLscan.io). 2) Bloquer préventivement le domaine dans votre proxy et vos solutions de filtrage DNS. 3) Signaler le domaine à l'hébergeur (abuse contact WHOIS) et à la CA émettrice. 4) Déposer le domaine sur Google Safe Browsing et PhishTank. 5) Si votre marque est protégée, contacter votre service juridique pour une procédure de récupération via l'AFNIC (pour les .fr) ou l'ICANN. 6) Alerter vos clients si le domaine est déjà actif. Cette réactivité transforme le CT monitoring en outil de protection de marque proactif, complémentaire à la défense anti-BEC.

Environnement de test et laboratoire pratique

La maîtrise des techniques de sécurité offensive et défensive requiert un environnement de pratique dédié. L'installation d'un laboratoire virtuel sur votre poste (VMware Workstation, VirtualBox, ou Proxmox pour une infrastructure plus élaborée) permet de tester les concepts présentés dans cet article sans risque pour les systèmes de production.

Configuration recommandée du lab

Pour reproduire les scénarios décrits, une configuration minimale comprend : un hyperviseur disposant d'au moins 16 Go de RAM et 4 cœurs CPU, un réseau virtuel isolé (host-only ou internal network sans accès Internet pour les VMs malveillantes), et un snapshot de base avant chaque manipulation pour faciliter le retour arrière. Les distributions spécialisées Kali Linux (offensive) et Parrot OS Security Edition couvrent l'ensemble des outils nécessaires sans configuration manuelle. Pour l'aspect défensif, Security Onion déploie en une seule VM un stack complet (Zeek, Suricata, Elasticsearch, Kibana) qui permet de visualiser l'impact des techniques testées.

Ressources de formation complémentaires

Les plateformes d'entraînement permettent de consolider la pratique dans des environnements légaux et structurés. HackTheBox et TryHackMe proposent des machines virtuelles sur lesquelles appliquer les techniques décrites, avec des difficultés progressives adaptées aux débutants comme aux experts. Pour les scénarios d'entreprise (Active Directory, Cloud, applications web complexes), les labs Pro de HackTheBox ou les modules DFIR/SOC de Blue Team Labs Online offrent des cas réalistes. Les CTF compétitifs (Hack The Box CTF, DEFCON CTF, PicoCTF) développent la créativité et l'adaptabilité face à des challenges inédits. La régularité de pratique (1-2 heures hebdomadaires minimum) prime sur l'intensité ponctuelle pour développer des réflexes durables.

Indicateurs de maturité et métriques de sécurité

Mesurer l'efficacité des mesures de sécurité implémentées est indispensable pour justifier les investissements et guider les priorités. Les métriques suivantes constituent un tableau de bord de sécurité applicable aux organisations de toutes tailles.

Métriques de couverture et de détection

Les indicateurs clés à suivre mensuellement : taux de couverture MITRE ATT&CK (pourcentage des techniques adversariales couvertes par des règles de détection actives) ; Mean Time To Detect (MTTD) pour les incidents de sécurité confirmés ; Mean Time To Respond (MTTR) depuis l'alerte jusqu'à la résolution ; taux de faux positifs sur les alertes SIEM (objectif : moins de 5% pour les règles de haute priorité) ; pourcentage de systèmes avec agents EDR installés et actifs (objectif : 100% des endpoints gérés). Ces métriques, compilées dans un rapport mensuel pour la direction, permettent de démontrer la valeur des investissements sécurité et d'identifier les domaines nécessitant des ressources supplémentaires.

Amélioration continue par les exercices

Les organisations les plus matures en matière de cybersécurité organisent régulièrement des exercices pour tester et améliorer leurs capacités. Les exercices tabletop (simulation de crise sur table, sans activation des systèmes techniques) développent la coordination des équipes et valident les procédures de communication de crise. Les tests de pénétration (pentest) annuels fournissent une évaluation objective de la résistance technique de l'infrastructure. Les exercices Red/Blue/Purple Team (1-2 fois par an pour les organisations matures) permettent d'aligner les équipes offensive et défensive autour d'objectifs communs d'amélioration. Chaque exercice doit donner lieu à un plan d'action formalisé avec des jalons de correction mesurables, intégré dans la feuille de route sécurité de l'organisation.

Synthèse et perspectives 2026

Les techniques et recommandations présentées dans ce guide s'inscrivent dans un contexte de menaces en constante évolution. La cybersécurité offensive et défensive sont deux faces d'une même médaille : comprendre les mécanismes d'attaque est indispensable pour construire des défenses robustes et résilientes face aux acteurs malveillants les plus sophistiqués.

Pour les équipes sécurité, l'enjeu de 2026 est double : maintenir une veille continue sur les nouvelles techniques publiées par la communauté de recherche (CVE, exploit-db, GitHub, Secrech, SSTIC) tout en assurant le durcissement progressif de l'infrastructure existante. Le référentiel MITRE ATT&CK reste le fil conducteur le plus efficace pour structurer un programme de détection et de réponse face aux tactiques, techniques et procédures des groupes APT ciblant les secteurs critiques.

La formation continue des équipes, la simulation régulière d'incidents (exercices tabletop, exercices Red/Blue/Purple Team), et l'automatisation des tâches répétitives via des outils SOAR constituent les piliers d'une organisation cyber mature. Les organisations qui investissent dans ces trois axes démontrent systématiquement de meilleures métriques de détection et de réponse (MTTD et MTTR réduits de 40% en moyenne selon les benchmarks sectoriels) face aux incidents de sécurité.

Sources et références

MITRE ATT&CK — Matrice de détection

ANSSI — Guide du SOC

CISA — Cybersecurity Incident & Vulnerability Response Playbooks

Pour aller plus loin

Les concepts présentés dans cet article constituent une base solide pour approfondir le sujet. Ces ressources complémentaires permettent d'aller plus loin dans la compréhension et la mise en pratique.

Ressources officielles de référence

ANSSI — Guides et recommandations techniques — La bibliothèque technique de l'ANSSI publie régulièrement des guides à jour sur tous les aspects de la sécurité des systèmes d'information. Disponibles gratuitement sur ssi.gouv.fr.

NIST Cybersecurity Framework — Référentiel international structurant la gestion des risques cyber en 6 fonctions. Version 2.0 publiée en 2024, disponible sur nist.gov.

MITRE ATT&CK — Base de connaissances des techniques adversariales, régulièrement mise à jour avec les nouvelles menaces observées dans le monde réel.

Formation continue

Certifications professionnelles reconnues : CISSP, CISM (management), OSCP, CEH (technique)

Plateformes de formation pratique : HackTheBox, TryHackMe, Hack The Box Academy

Veille quotidienne : bulletins CERT-FR, alertes CISA, flux RSS NVD

Mise en réseau professionnel

La communauté cybersécurité française est active et ouverte : les clubs RSSI, l'OSSIR, le CLUSIF, et les conférences comme le FIC (Forum International de la Cybersécurité) et les SSTIC sont des points de rencontre essentiels pour les professionnels du secteur. Ces échanges permettent de rester à jour sur les menaces émergentes et les bonnes pratiques réelles.

