Abilian
CS LAB

OPEN INTEROP

Fiche détaillée, domaine 3 : cybersécurité

Stefane Fermigier (Abilian SAS) · 30 octobre 2026 · DRAFT

Version 0.3
Licence CC BY 4.0

1. État de l'art

1.1 Paysage de la cybersécurité en France

La France dispose d'un écosystème cybersécurité structuré et dynamique :

- **Hexatrust** : groupement d'entreprises françaises et européennes de cybersécurité et de cloud de confiance (plus de 130 membres en 2026).
- **ANSSI** : autorité nationale, définit les référentiels (SecNumCloud, PAMS, etc.) et les exigences de qualification ; elle a publié en mars 2026 le Référentiel Cyber France (ReCyF), destiné aux entités qui seront assujetties à NIS2.
- **Éditeurs français** : Wallix (PAM), Stormshield (firewalls), Olfeo (filtrage web), Mailinblack (anti-phishing), CS Group, Sekoia (XDR/SIEM), Tehtris (XDR), YesWeHack (bug bounty), etc.
- **Intégrateurs et SOC** : nombreux MSSP français (Orange Cyberdefense, Thales, Atos/Eviden, etc.).
- **Projets open source** : Wazuh (SIEM/XDR), MISP (threat intelligence), TheHive (incident response), OpenCTI (threat intelligence), CrowdSec (IPS collaboratif), Coraza (WAF), LeWAF.

Le marché est caractérisé par une **fragmentation des outils** : chaque SOC assemble une mosaïque de solutions (SIEM, EDR, NDR, SOAR, scanner de vulnérabilités, WAF, etc.) dont l'interopérabilité est limitée. Les grands éditeurs américains (CrowdStrike, Palo Alto, Microsoft Sentinel) jouent sur l'intégration propriétaire de leurs suites, créant le même type de lock-in que dans le collaboratif ou le cloud.

1.2 Standards existants par sous-domaine

Threat intelligence et partage d'indicateurs

Standard	Fonction	Maturité	Adoption FR
STIX 2.1 (OASIS)	Format structuré de description de menaces (indicateurs, campagnes, malwares, TTPs)	Mature (OASIS Standard, 2021)	Bonne : utilisé par MISP, OpenCTI, Sekoia
TAXII 2.1 (OASIS)	Protocole de transport pour STIX	Mature (OASIS Standard, 2021)	Bonne, couplé à STIX

Standard	Fonction	Maturité	Adoption FR
MITRE ATT&CK	Base de connaissances des tactiques et techniques adverses	Mature, standard de fait	Très bonne : référence universelle
MISP formats	Formats d'échange d'événements et d'attributs de menaces	Mature (de fait)	Très bonne en Europe ; MISP est un projet luxembourgeois/européen largement déployé

Constat : STIX/TAXII + MITRE ATT&CK forment un socle solide et bien adopté en France. MISP ajoute une couche opérationnelle communautaire très efficace. L'interopérabilité entre plateformes de threat intelligence (TIP) est relativement correcte grâce à STIX.

Détection et réponse (SIEM/XDR/SOAR)

Standard / Format	Fonction	Maturité	Notes
CEF (Common Event Format, ArcSight)	Format de log de sécurité	Mature, de fait	Largement supporté mais propriétaire (Micro Focus)
LEEF (Log Event Extended Format, IBM)	Format de log pour QRadar	Mature, de fait	Spécifique à l'écosystème IBM
Sigma	Langage de règles de détection agnostique au SIEM	En maturation (spécification 2.0, août 2024, avec règles de corrélation)	Très prometteur : permet d'écrire des règles une fois, de les compiler pour tout SIEM (pySigma) ; gouvernance communautaire SigmaHQ
OCSF (Open Cybersecurity Schema Framework)	Schéma normalisé d'événements de sécurité	En maturation (versions 1.x)	Initié par AWS et Splunk en 2022, projet de la Linux Foundation depuis novembre 2024 ; licence Apache 2.0 ; vise à unifier les formats de logs de sécurité
OpenC2 (OASIS)	Commandes standardisées de réponse automatisée	En maturation	Permet d'automatiser la réponse inter-produits
CACAO 2.0 (OASIS)	Playbooks de réponse à incident structurés	En maturation (Committee Specification, novembre 2023)	Standard de playbooks partageables entre SOAR

Constat : C'est le sous-domaine le plus fragmenté. Chaque SIEM/XDR a son propre format de log, son propre langage de requête, ses propres playbooks. **Sigma** et **OCSF** sont les initiatives les plus prometteuses pour normaliser respectivement les règles de détection et les événements de sécurité. L'adoption en France reste limitée.

Sécurité applicative (WAF)

Standard / Ruleset	Fonction	Maturité	Notes
OWASP Core Rule Set (CRS) v4	Ensemble de règles de détection WAF (SQLi, XSS, RCE, etc.)	Mature, standard de fait (branche 4.25 à support long)	Ruleset de référence ; implémenté par Coraza, ModSecurity, LeWAF
OWASP Top 10	Classification des risques applicatifs web	Mature	Référentiel de sensibilisation, pas un protocole
OWASP ASVS (Application Security Verification Standard)	Standard de vérification de sécurité applicative	Mature	Checklist structurée pour les audits

Constat : L'OWASP CRS est un bon exemple de standard d'interopérabilité réussi : un même jeu de règles fonctionne sur plusieurs moteurs WAF. Ce modèle (règles partagées, moteurs interchangeables) devrait inspirer d'autres sous-domaines.

Supply chain logicielle

Standard	Fonction	Maturité	Notes
SPDX 3.0 (Linux Foundation)	SBOM : inventaire des composants logiciels	Mature	La norme ISO/IEC 5962:2021 correspond à SPDX 2.2.1 ; sa révision fondée sur SPDX 3.0 est au stade DIS (2026)
CycloneDX 1.7 (OWASP, Ecma)	SBOM orienté sécurité (vulnérabilités, licences, cryptographie)	Mature	Version 1.6 normalisée par Ecma International (ECMA-424) ; très utilisé dans l'écosystème Java/JS
SLSA	Niveaux de sécurité de la chaîne de build	En maturation	Framework d'évaluation
in-toto	Attestation de chaîne de build	En maturation	Preuve cryptographique des étapes de build
TUF (The Update Framework)	Mise à jour sécurisée de logiciels	Mature	Protection contre les attaques sur les mises à jour
VEX (Vulnerability Exploitability eXchange)	Communication sur l'exploitabilité des vulnérabilités	En maturation	Complément essentiel du SBOM

Constat : Deux standards de SBOM matures (SPDX, CycloneDX) coexistent. Le Cyber Resilience Act impose aux fabricants de produits comportant des éléments numériques d'établir un SBOM à partir du 11 décembre 2027 ; NIS2 pousse dans le même sens par ses exigences sur la sécurité de la chaîne d'approvisionnement. L'enjeu n'est plus la standardisation mais l'**outillage et l'adoption** dans la filière française.

Identité et Zero Trust

Standard	Fonction	Maturité
OIDC + OAuth 2.0 (avec RFC 9700, BCP 240)	Authentification et autorisation	Mature (OAuth 2.1 reste un brouillon IETF)

Standard	Fonction	Maturité
SCIM 2.0	Provisioning d'identités	Mature
SPIFFE	Identité de service (workload identity)	En maturation
Zero Trust Architecture (NIST SP 800-207)	Modèle de sécurité	Mature (principes)
mTLS	Authentification mutuelle service-à-service	Mature

Constat : Les standards d'identité sont matures (cf. fiche transverse, section 1.1). SPIFFE est prometteur pour l'identité de service dans les architectures micro-services.

Cryptographie post-quantique

- Standards NIST finalisés : **ML-KEM** (Kyber), **ML-DSA** (Dilithium), **SLH-DSA** (SPHINCS+)
- **Agilité cryptographique** : principe clé ; les systèmes doivent pouvoir remplacer leurs primitives cryptographiques sans réécriture
- Schémas hybrides (classique + PQC) recommandés en transition
- Pertinent pour les données classifiées ou à durée de vie >10 ans

1.3 Synthèse de maturité

Domaine	Standard existe	Adoption FR	Interopérabilité réelle
Threat intelligence (STIX)	✅	✅	✅ (entre TIPs)
Partage d'IOCs (MISP)	✅ (de fait)	✅	✅
Règles de détection (Sigma)	✅ (spécification Sigma 2.0, SigmaHQ)	⚠️	✕ (chaque SIEM a ses règles)
Format logs de sécurité (OCSF)	✅ (OCSF v1.x, Linux Foundation)	✕	✕ (CEF/LEEF/propriétaire)
Playbooks de réponse (CACAO)	✅ (OASIS CACAO 2.0, CS)	✕	✕ (chaque SOAR a ses playbooks)
Commandes de réponse (OpenC2)	✅ (OASIS OpenC2)	✕	✕
WAF rules (OWASP CRS)	✅	✅	✅ (Coraza, ModSec, LeWAF)
SBOM (SPDX, CycloneDX)	✅	⚠️	⚠️ (adoption en cours)
Identité (OIDC/SCIM)	✅	✅	⚠️ (adoption inégale)
Crypto post-quantique	✅ (NIST FIPS 203/204/205, 2024)	✕	✕ (migration à peine démarrée)

Sigma est **techniquement mature** ; OCSF, CACAO et OpenC2 sont en maturation. Pour tous : les marques « ⚠️ » et « ✕ » signalent une **adoption** insuffisante par les éditeurs et opérateurs français ; elles ne jugent ni l'existence ni la qualité du standard.

2. Analyse des besoins de l'écosystème français

2.1 Pain points identifiés

Les frustrations ci-dessous sont des **retours qualitatifs** issus des échanges du CSF, des discussions Cigref/TOSIT, des consultations ARCEP et de l'étude OPIIEC sur l'interopérabilité (cf. note de vision et état de l'art pour les références). Des retours d'éditeurs de cybersécurité les complètent. Elles n'ont pas fait l'objet d'un sondage quantitatif dédié et seront à corroborer par un travail empirique ultérieur. Le cadrage stratégique général est celui de l'**interopérabilité opposable** (cf. note de positionnement Abilian, novembre 2025 : « *L'interopérabilité, clé de l'efficacité collaborative et de la souveraineté* »), précisé depuis par la doctrine proposée (doctrine).

Côté opérateurs de SOC :

1. « **Chaque produit de sécurité a son propre format de log** » : un SOC qui intègre Stormshield (firewall), Wallix (PAM), Sekoia (XDR) et CrowdSec (IPS) doit écrire des parseurs spécifiques pour chaque source. L'intégration de nouvelles sources est coûteuse et fragile.
2. « **Les règles de détection sont verrouillées dans le SIEM** » : une règle écrite pour Splunk ne fonctionne pas dans Elastic SIEM ou Wazuh. Les équipes de détection réécrivent les mêmes logiques pour chaque outil.
3. « **Les playbooks de réponse ne sont pas portables** » : un playbook SOAR écrit dans Palo Alto XSOAR ne peut pas être réutilisé dans TheHive/Cortex.
4. « **On ne sait pas quels composants open source sont dans nos logiciels** » : le SBOM est encore peu pratiqué par les éditeurs français, alors que le Cyber Resilience Act l'exigera des fabricants à partir du 11 décembre 2027.

Côté éditeurs français de cybersécurité :

5. « **L'intégration avec les autres produits de sécurité nous coûte cher** » : chaque éditeur doit développer des connecteurs N-to-N avec les autres produits du marché.
6. « **Les grands éditeurs américains imposent leur format** » : Microsoft Sentinel, CrowdStrike et Palo Alto imposent leurs formats et APIs, forçant les éditeurs français à s'y adapter plutôt que l'inverse.
7. « **Il n'y a pas de label d'interopérabilité cybersécurité** » : un éditeur ne peut pas prouver facilement que son produit s'intègre de manière standard avec le reste de l'écosystème. La proposition de doctrine (§ 5) y répond par un badge de conformité délivré après essai croisé. Un « compatible OCSF » ou « compatible Sigma » n'y vaut que pour les fonctions déclarées et prouvées.

Côté DSI et RSSI :

8. « **Changer de SIEM, c'est perdre toutes nos règles et nos playbooks** » : la réversibilité est quasi nulle dans le domaine de la détection et de la réponse.

2.2 Besoins structurels

- **Réduire le coût d'intégration des SOC** : permettre aux produits de sécurité français de communiquer entre eux via des interfaces standard plutôt que des connecteurs ad hoc.
- **Constituer une offre SOC souveraine intégrée** : les éditeurs d'Hexatrust doivent pouvoir proposer ensemble une stack de sécurité complète et interopérable, face aux suites intégrées américaines.
- **Préparer la conformité NIS2 / Cyber Resilience Act** : le CRA (règlement (UE) 2024/2847) impose depuis le 11 septembre 2026 la notification des vulnérabilités activement exploitées et des incidents graves (CSIRT désigné, ENISA) ; ses autres obligations, dont le SBOM et la gestion des vulnérabilités, s'appliquent à partir du 11 décembre 2027. La transposition française de NIS2 (projet de loi

« Résilience », adopté par le Sénat en mars 2025) n'est toujours pas votée par l'Assemblée nationale en octobre 2026 ; la Commission a saisi la Cour de justice de l'UE le 8 juillet 2026 et demande des sanctions financières. Ces notifications et ces inventaires circulent entre outils et entre organisations : leur interopérabilité conditionne la conformité.

- **Permettre la portabilité des compétences** : des règles Sigma et des playbooks CACAO portables signifient que les analystes SOC peuvent changer d'outillage sans repartir de zéro.

2.3 Priorisation des besoins

Besoin	Urgence	Impact	Faisabilité
Format normalisé de logs de sécurité (OCSF)	Haute	Très élevé	Moyenne (OCSF existe, adoption à construire)
Règles de détection portables (Sigma)	Haute	Élevé	Haute (Sigma est mature)
SBOM systématique (SPDX/CycloneDX)	Haute	Élevé	Haute (standards matures, outillage existant)
Playbooks de réponse portables (CACAO)	Moyenne	Élevé	Moyenne (CACAO en maturation)
Interopérabilité WAF (OWASP CRS)	Moyenne	Moyen	Haute (déjà fonctionnel)
Indicateur d'interopérabilité cybersécurité (méthode publique, cf. doctrine, § 5.4)	Moyenne	Élevé	Moyenne
Migration post-quantique	Basse (anticipation)	Stratégique	Faible (expertise rare)

3. Propositions concrètes

Prérequis transverses. Les chantiers cybersécurité s'appuient sur les livrables de la fiche transverse :

- **T1 (Identité OIDC/SCIM)** est le socle d'authentification pour les consoles SOC/SIEM/SOAR et l'orchestration des accès des opérateurs ; il s'étend à SPIFFE pour l'identité de service (cf. § 1.2, « Identité et Zero Trust »).
- **T4 (Notifications)** fournit le format CloudEvents réutilisable pour la transmission d'alertes entre composants de la chaîne SOC, en complément des protocoles spécifiques (CACAO pour les playbooks, OpenC2 pour les commandes).
- **CS1 et CL1 (cloud)** partagent la couche d'observabilité : un opérateur de SOC doit pouvoir consommer les logs des clouds via le profil OpenTelemetry de CL1.

Règles communes. Chaque chantier proposé suit la proposition de doctrine : un livrable n'est complet qu'avec une implémentation de référence, une suite de tests de conformité libre et un modèle de déclaration de conformité. La conformité exige 100 % des critères obligatoires, sans compensation ; les autres mesures (taux de détection, couverture, performances) sont publiées à part. Chaque test rend un verdict « conforme » ou « non conforme », à défaut « non applicable » ou « non concluant ». Une suite de tests fournit une preuve technique ; son usage dans un contrat ou un marché public demande une rédaction propre.

3.1 Chantier CS1 : adoption d'OCSF pour les logs de sécurité

Objectif : Les produits de sécurité français émettent des logs dans un schéma normalisé, permettant l'intégration plug-and-play dans n'importe quel SIEM.

Standard : OCSF (Open Cybersecurity Schema Framework, Linux Foundation)

Pourquoi OCSF : C'est le schéma le plus complet et le plus soutenu (AWS, Splunk, IBM, CrowdStrike, Palo Alto ont contribué). Il définit des catégories d'événements normalisées (authentification, réseau, endpoint, fichier, etc.) avec des champs standardisés. Malgré son origine américaine, il est publié sous licence Apache 2.0 et gouverné depuis novembre 2024 par la Linux Foundation. Sa conformité à la définition du standard ouvert retenue par la doctrine proposée (EIF 2004, LCEN art. 4) reste à vérifier formellement, en particulier sur l'ouverture du processus d'évolution.

Actions :

1. **Profil Open Interop OCSF** : définir un profil adapté au contexte français :
   - Sélection des catégories d'événements prioritaires (authentification, réseau, endpoint, WAF)
   - Mapping avec les formats existants des éditeurs Hexatrust
   - Extensions éventuelles pour les besoins spécifiques (qualification ANSSI, etc.)
2. **Pilote Hexatrust** : engager 4-5 éditeurs Hexatrust à émettre leurs logs au format OCSF en parallèle de leur format natif.
3. **Connecteurs SIEM** : développer des parseurs OCSF pour les SIEM open source (Wazuh, OpenSearch Security Analytics) et les intégrer en contribution upstream.
4. **Suite de tests de conformité** : outil validant qu'un flux de logs est conforme au profil OCSF Open Interop, accompagné d'un modèle de déclaration de conformité (classes d'événements et champs pris en charge).

Livrables : Profil OCSF documenté, pilote 4-5 éditeurs, connecteurs SIEM (implémentation de référence), suite de tests, modèle de déclaration.

Délai : 6-9 mois.

3.2 Chantier CS2 : règles de détection portables (Sigma)

Objectif : Les règles de détection sont écrites une fois en Sigma et compilées pour n'importe quel SIEM.

Standard : Sigma

Actions :

1. **Bibliothèque de règles Sigma « France »** : constituer un corpus de règles de détection adaptées au contexte français (menaces sur les administrations, secteurs critiques, TTPs observées par l'ANSSI et les CERT-FR).
2. **Backends Sigma pour les SIEM français** : s'assurer que les compilateurs Sigma couvrent les SIEM utilisés en France (Sekoia, Wazuh, Elastic, Splunk). Contribuer les backends manquants.
3. **Intégration dans les processus Hexatrust** : proposer que les éditeurs Hexatrust fournissent des règles Sigma avec leurs produits (ex. : un éditeur de pare-feu fournirait les règles Sigma qui détectent les événements significatifs de ses produits).
4. **Gouvernance du corpus** : mettre en place un processus de révision et de mise à jour des règles, en lien avec le CERT-FR et les CSIRT sectoriels.

Livrables : Bibliothèque de règles Sigma, backends Sigma, intégration éditeurs, jeu de tests vérifiant qu'un backend traduit correctement les règles de la bibliothèque.

Délai : 6-9 mois.

3.3 Chantier CS3 : SBOM pour la filière française

Objectif : Tout éditeur de logiciel de la filière CSF produit et publie un SBOM à jour pour ses produits.

Standards : SPDX 3.0 et/ou CycloneDX 1.7 (la 1.6 est normalisée ECMA-424) + VEX

Actions :

1. **Guide pratique SBOM** : rédiger un guide adapté aux éditeurs français (PME/ETI), qui couvre le choix du format (SPDX ou CycloneDX) selon le contexte, l'outillage recommandé (Syft, Trivy, cdxgen, etc.), l'intégration dans la CI/CD et la gestion des vulnérabilités via VEX.
2. **Atelier pratique** : organiser un atelier hands-on avec 10-15 éditeurs pour générer leur premier SBOM.
3. **Politique de publication** : proposer un cadre de publication des SBOM (où, comment, fréquence) compatible avec les exigences du Cyber Resilience Act (applicables au 11 décembre 2027) et de NIS2.
4. **Intégration Open Interop** : les SBOM des composants libres produits dans le cadre d'Open Interop seraient systématiquement publiés, servant d'exemple pour la filière.

Livrables : Guide pratique, atelier, modèle de publication, SBOM des composants Open Interop.

Délai : 3-6 mois (quick win).

3.4 Chantier CS4 : playbooks de réponse interopérables

Objectif : Les playbooks de réponse à incident sont partageables entre organisations et entre outils SOAR.

Standard : CACAO 2.0 (OASIS)

Actions :

1. **Évaluation de CACAO** : analyser la spécification CACAO 2.0, évaluer sa couverture par rapport aux besoins des SOC français (gestion de crise, notification ANSSI, conformité NIS2).
2. **Bibliothèque de playbooks** : rédiger 5-10 playbooks CACAO pour les scénarios les plus fréquents en France :
   - Réponse à un ransomware
   - Compromission de compte privilégié
   - Exfiltration de données
   - Incident sur un SI de santé
   - Notification réglementaire (NIS2, RGPD)
3. **Intégration TheHive/Cortex** : contribuer un module d'import/export CACAO dans TheHive (projet open source français de gestion d'incidents).
4. **Exercice de crise** : organiser un exercice inter-organisations utilisant des playbooks CACAO partagés.

Livrables : Évaluation CACAO, bibliothèque de playbooks, module TheHive, retour d'exercice.

Délai : 9-12 mois.

3.5 Chantier CS5 : promotion de l'OWASP CRS et interopérabilité WAF

Objectif : Renforcer l'adoption de l'OWASP CRS comme ruleset de référence dans l'écosystème WAF français et faciliter le remplacement d'un moteur WAF par un autre.

Actions :

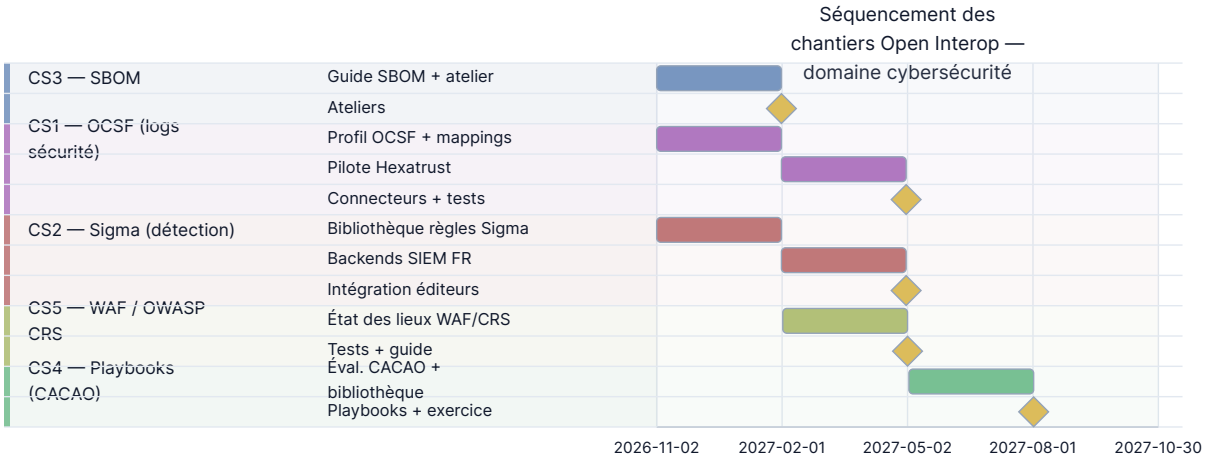
1. **État des lieux** : recenser les moteurs WAF français et européens compatibles CRS (Coraza, LeWAF, etc.) et évaluer le niveau de compatibilité effective.
2. **Tests de conformité CRS** : adapter les tests de régression du projet CRS en une suite vérifiant qu'un moteur WAF implémente correctement le CRS v4. Le verdict de conformité repose sur les critères obligatoires (chargement des règles, comportement attendu sur chaque cas de test) ; le taux de détection et le taux de faux positifs sur un corpus de référence sont publiés séparément et n'entrent pas dans le verdict.
3. **Extensions CRS** : contribuer des règles CRS spécifiques aux menaces observées dans le contexte français/européen.
4. **Documentation** : guide de déploiement CRS adapté aux architectures françaises (reverse proxy, cloud souverain, etc.).

Livrables : État des lieux, suite de tests et modèle de déclaration de conformité, contributions CRS, guide.

Délai : 6-9 mois.

3.6 Vue d'ensemble et séquencement

Les dates sont indicatives : elles supposent un lancement en novembre 2026.



3.7 Articulation avec Hexatrust

Les chantiers cybersécurité gagneraient à être menés avec Hexatrust et ses membres, si le groupement s'y engage :

- **CS1 (OCSF)** et **CS2 (Sigma)** : les éditeurs Hexatrust sont les premiers contributeurs et les premiers bénéficiaires. Leur engagement est critique.
- **CS3 (SBOM)** : Hexatrust peut jouer un rôle de prescripteur auprès de ses membres pour l'adoption systématique du SBOM.
- **CS4 (CACAO)** : les SOC opérés par les membres Hexatrust sont le terrain d'expérimentation naturel.
- **CS5 (CRS)** : les éditeurs WAF d'Hexatrust sont directement concernés.

Le modèle OWASP CRS (un ruleset ouvert implémenté par des moteurs interchangeables) peut servir de modèle aux autres sous-domaines : des règles, schémas et playbooks ouverts et partagés, implémentés par des produits en concurrence.

Références

Standards et spécifications — Threat intelligence

- **STIX 2.1** — OASIS. https://oasis-open.github.io/cti-documentation/stix/intro.html
- **TAXII 2.1** — OASIS. https://oasis-open.github.io/cti-documentation/taxii/intro.html
- **OpenC2** — OASIS. https://openc2.org/
- **MITRE ATT&CK** — Base de connaissances. https://attack.mitre.org/

Standards et spécifications — Détection et réponse

- **OCSF** (Open Cybersecurity Schema Framework) — Linux Foundation. https://schema.ocsf.io/
- **Sigma** — Langage de règles de détection. https://sigmahq.io/
- **CACAO 2.0** — OASIS (playbooks de réponse). https://www.oasis-open.org/committees/cacao/

Standards et spécifications — Sécurité applicative

- **OWASP Core Rule Set (CRS)** — Règles WAF de référence. https://coreruleset.org/
- **OWASP Top 10** — Classification des risques applicatifs. https://owasp.org/www-project-top-ten/
- **OWASP ASVS** — Standard de vérification de sécurité applicative. https://owasp.org/www-project-application-security-verification-standard/

Standards et spécifications — Supply chain logicielle

- **SPDX 3.0** — Linux Foundation (ISO/IEC 5962:2021 pour SPDX 2.2.1, révision 3.0 en cours), Software Bill of Materials. https://spdx.dev/
- **CycloneDX 1.7** — OWASP, ECMA-424, SBOM orienté sécurité. https://cyclonedx.org/
- **SLSA** — Supply-chain Levels for Software Artifacts. https://slsa.dev/
- **in-toto** — Attestation de chaîne de build. https://in-toto.io/
- **TUF** (The Update Framework) — Mise à jour sécurisée. https://theupdateframework.io/
- **VEX** — Vulnerability Exploitability eXchange. https://www.cisa.gov/sbom

Standards et spécifications — Identité et Zero Trust

- **SPIFFE** — Secure Production Identity Framework. https://spiffe.io/
- **Zero Trust Architecture** — NIST SP 800-207. https://csrc.nist.gov/pubs/sp/800/207/final

Standards et spécifications — Cryptographie post-quantique

- **ML-KEM, ML-DSA, SLH-DSA** — NIST PQC Standards. https://csrc.nist.gov/projects/post-quantum-cryptography

Réglementations

- **Cyber Resilience Act** — Règlement (UE) 2024/2847. https://eur-lex.europa.eu/eli/reg/2024/2847
- **NIS2** — Directive (UE) 2022/2555. https://eur-lex.europa.eu/eli/dir/2022/2555

Projets open source

- **Wazuh** — SIEM/XDR open source. https://wazuh.com/
- **MISP** — Plateforme de threat intelligence. https://www.misp-project.org/
- **TheHive** — Gestion d'incidents. https://strangebee.com/thehive/
- **OpenCTI** — Plateforme de cyber threat intelligence. https://www.opencti.io/
- **CrowdSec** — IPS collaboratif. https://www.crowdsec.net/
- **Coraza** — Moteur WAF open source compatible CRS. https://coraza.io/

Écosystème français

- **Hexatrust** — Groupement d'entreprises françaises de cybersécurité. https://www.hexatrust.com/
- **ANSSI** — Agence nationale de la sécurité des systèmes d'information. https://www.ssi.gouv.fr/
- **CERT-FR** — Centre de réponse aux incidents. https://www.cert.ssi.gouv.fr/

Documents Open Interop

- Note de vision Open Interop
- État de l'art des standards d'interopérabilité
- Fiche transverse (chantier T1 = socle identité OIDC/SCIM des consoles SOC, SIEM et SOAR ; T4 = format de notifications réutilisable pour les alertes)
- Fiche collaboratif
- Fiche cloud (CS1 et CL1 partagent la couche d'observabilité)
- Proposition de doctrine pour Open Interop (définitions, niveaux de preuve, badge, autorité technique)