CYBERSÉCURITÉ | EXTERNAL EXPOSURE MONITORING

Luxgap External Exposure Monitoring (EEM)

Luxgap
DATA PRIVACY PARTNER

Détectez ce que vos équipes ne voient pas : fuites de données, identifiants compromis, domaines malveillants et services exposés sur votre périmètre externe.

Avec les menaces en constante évolution, les entreprises ne peuvent plus se contenter de protéger leur périmètre réseau interne. La surface d'attaque réelle s'étend bien au-delà : web ouvert, cloud public, marketplaces criminelles, messageries chiffrées, logs DNS et Certificate Transparency, dépôts de code, forums souterrains… Luxgap EEM assure une **surveillance continue** de cet « extérieur invisible » pour identifier les expositions critiques avant qu'elles ne soient exploitées.

Détection

Collecte multi-sources et analyse automatisée

Qualification

Tri, contextualisation et élimination du bruit

Priorisation

Criticité, exploitabilité, impact business

Remédiation

Correction, preuve horodatée et reporting

Objectif ultime : réduire le risque *avant* l'incident — qu'il s'agisse d'extorsion, d'Account Takeover, de fraude, de ransomware ou d'atteinte à la réputation. Un service managé de bout en bout, pensé pour les équipes sécurité exigeantes.

Julien Winkin – Julien.winkin@luxgap.com +352 621 583 116

⚠ LE CONSTAT

Le problème : l'entreprise fuit… hors du périmètre

Les expositions les plus critiques se produisent souvent **en dehors** du système d'information « maîtrisé » — là où vos outils de surveillance traditionnels n'ont aucune visibilité.

Des fuites omniprésentes et invisibles

Stockages cloud mal configurés (S3, Azure Blob, GCS), dépôts Git publics contenant des secrets, partages de fichiers oubliés, instances Shadow IT déployées par des équipes métier, données transmises à des prestataires sans contrôle suffisant… Les vecteurs d'exposition se multiplient à mesure que l'écosystème numérique de l'entreprise s'étend.

Les attaquants l'ont bien compris et **industrialisent** leur approche : reconnaissance automatisée de la surface d'attaque externe, collecte massive d'identifiants via des stealers, usurpation de marques et domaines, revente de données sur les marketplaces criminelles. Le temps entre la découverte d'une exposition et son exploitation se réduit à quelques heures.

Le paradoxe de la visibilité : les scans internes, EDR, SIEM et firewalls protègent ce que vous connaissez. Mais ils sont aveugles à ce qui se passe *en dehors* de votre périmètre. Il faut une **visibilité externe** combinant Digital Risk Protection et Attack Surface Management pour combler cet angle mort.

Cloud public

Buckets, bases, APIs exposées sans authentification

Dépôts & Shadow IT

Secrets dans le code, services non inventoriés

Attaquants industrialisés

Reconnaissance, stealers, revente, extorsion

Angle mort EDR/SIEM

Outils internes incapables de voir l'extérieur

VISION PRODUIT

Notre « périmètre externe managé »

Un **Managed External Perimeter** complet : tout ce qui peut exposer vos actifs, identités, données et marque, surveillé, qualifié et piloté en continu.

Plus rapide, plus profond

Notre approche repose sur une combinaison technologique et humaine unique. Nous déployons des capacités de détection qui couvrent l'ensemble du spectre externe : web ouvert, deep web, dark web, cloud, DNS, Certificate Transparency logs, marketplaces et forums fermés.

La différence fondamentale : une **réduction drastique du bruit** grâce à une qualification experte et une contextualisation métier de chaque alerte. Chaque signal est enrichi, corrélé et priorisé avant d'atteindre vos équipes.

Pilotage par le risque

Chaque exposition détectée est évaluée selon quatre dimensions clés pour garantir que vos ressources sont concentrées sur ce qui compte vraiment :

Criticité

Nature et sensibilité des données ou actifs exposés

Exploitabilité

Facilité d'exploitation par un attaquant

Impact business

Conséquences opérationnelles, financières et juridiques

Conformité

Implications RGPD, NIS2, DORA et obligations sectorielles

PANORAMA EEM

3 familles de risques à couvrir

L'External Exposure Monitoring s'articule autour de trois piliers complémentaires, couvrant l'intégralité du spectre des risques numériques externes auxquels fait face votre organisation.

Digital Risk Protection

Protection de la marque et des domaines, détection d'usurpation d'identité (impersonation), lutte contre la fraude en ligne et prévention des Account Takeovers. Cette famille couvre les risques qui exploitent la **confiance** que vos clients et partenaires placent dans votre marque.

- Brand & domain monitoring
- Détection de phishing et typosquatting
- Surveillance des fraudes (CEO fraud, faux fournisseurs)

External Attack Surface

Découverte et gestion de la surface d'attaque externe, réduction des expositions techniques, évaluation des risques liés à la supply chain et aux opérations M&A. Cette famille cible les **vulnérabilités techniques** exploitables depuis l'extérieur.

- Asset discovery & inventory
- Shadow services & vulnérabilités exposées
- Risque tiers et due diligence technique

Threat Intelligence

Renseignement ciblé, hunting proactif, enrichissement du vulnerability management et surveillance des risques tiers. Cette famille transforme les **signaux faibles** en renseignements exploitables pour anticiper les attaques.

- IoC/IoA contextualisés
- Corrélation multi-sources
- Intégration SIEM/SOAR/EDR

Ces trois piliers fonctionnent en synergie : une fuite de données (Digital Risk) corrélée à des identifiants compromis (Threat Intelligence) ciblant un service exposé (Attack Surface) constitue un scénario de compromission imminent que seule une vision unifiée peut détecter et traiter à temps.

MODULE 1

Data Leakage Detection & Breach Prevention

Détecter et sécuriser les données sensibles accessibles publiquement avant qu'elles ne soient exploitées par un acteur malveillant.

Périmètre de détection

Notre module de Data Leakage Detection scanne en continu les sources d'exposition les plus critiques : buckets et objets cloud (AWS S3, Azure Blob Storage, Google Cloud Storage), bases de données accessibles sans authentification (MongoDB, Elasticsearch, Redis), index de moteurs de recherche référençant des documents internes, et stockages mal configurés sur des plateformes SaaS ou FTP.

Indicateurs recherchés

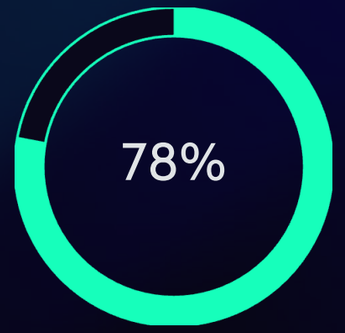
- **PII (données personnelles)** : noms, emails, numéros de sécurité sociale, données bancaires, dossiers médicaux
- **Secrets techniques** : clés API, tokens d'accès, certificats, configurations sensibles
- **Documents internes** : contrats, plans stratégiques, documents RH, propriété intellectuelle
- **Exports clients & backups** : dumps de bases, exports CRM, sauvegardes non chiffrées

Livrables & sorties

Pour chaque exposition identifiée : **preuve horodatée**, périmètre précis touché, recommandations de correction priorisées, et validation post-remédiation confirmant la sécurisation effective.

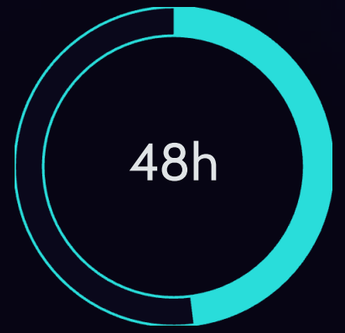
Valeur clé

Réduction du risque RGPD grâce à une maîtrise de la confidentialité et une minimisation proactive de la surface d'exposition des données. Chaque détection est documentée pour alimenter vos registres de traitement et vos analyses d'impact (AIPD).



Fuites cloud

Des fuites de données proviennent de mauvaises configurations cloud



Fenêtre critique

Délai moyen entre exposition et exploitation par un attaquant

MODULE 2

Credential Intelligence

Détecter les fuites d'identifiants avant qu'elles ne mènent à une compromission de vos comptes et systèmes critiques.

Sources de détection

Les identifiants compromis représentent le vecteur d'attaque le plus exploité. Notre surveillance couvre l'ensemble de l'écosystème de fuite :

Fuites publiques

Bases de données volées rendues publiques (breaches historiques et récentes)

Paste sites

Pastebin, GitHub Gists et plateformes similaires où des credentials sont publiés

Stealer logs

Résultats de malwares voleurs d'identifiants (RedLine, Raccoon, Vidar…)

Marketplaces criminelles

Revente d'accès et sessions sur les marchés du dark web

Périmètre de surveillance

Nous surveillons vos **emails corporate**, domaines, marques, applications critiques (VPN, SSO, portails métier) et **comptes VIP** (dirigeants, administrateurs, développeurs). Chaque identifiant détecté est corrélé à son contexte d'exposition pour évaluer le risque réel.

Actions de remédiation

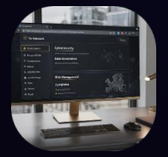
- **Reset ciblé** des mots de passe compromis avec notification utilisateur
- **Activation MFA / conditional access** sur les comptes à risque
- **Invalidation des sessions et tokens** actifs potentiellement compromis
- **Durcissement SSO** : revue des politiques d'accès et des règles de fédération

Valeur : baisse significative des Account Takeovers, prévention directe de la fraude et du ransomware qui exploitent les identifiants volés comme point d'entrée initial.

MODULE 3

Dark Web Monitoring

Détecter et atténuer les attaques en préparation : forums souterrains, messageries chiffrées et communautés fermées.



Sources surveillées

Notre couverture s'étend aux principaux canaux utilisés par les acteurs malveillants : forums Tor et sites .onion, boards spécialisés (XSS, Exploit, BreachForums), canaux IRC historiques, groupes Telegram et serveurs Discord privés. Chaque source est monitorée en continu par des agents spécialisés et des crawlers automatisés.

Détection proactive

Nous identifions les **mentions de votre marque**, projets internes, accès revendus (initial access brokers), données mises en vente, et signaux d'extorsion avant qu'ils ne se concrétisent. Chaque mention est capturée avec son contexte complet : auteur, canal, horodatage et contenu associé.

Qualification experte

Chaque signal est qualifié selon sa **crédibilité** (profil de l'acteur, historique, réputation), le **stade de l'attaque** (reconnaissance, préparation, exécution) et sa **corrélation** avec d'autres indicateurs (identifiants compromis, données déjà exposées, infrastructure malveillante).

Garde-fous éthiques et juridiques : notre surveillance est menée à **finalité strictement défensive**. Aucun « achat » de données, aucune incitation à l'obtention d'informations, aucune interaction avec les acteurs malveillants. Toutes les preuves sont collectées passivement et dans le respect du cadre légal applicable.

MODULE 4

Brand & Domain Protection

Surveiller et neutraliser les domaines similaires, le typosquatting, le phishing et toute forme d'usurpation de votre identité numérique.

Détection multi-sources

Notre moteur de détection croise en permanence plusieurs flux de données pour identifier les domaines malveillants et leurs infrastructures associées : **DNS passif** (résolutions historiques et en temps réel), **zone files** (nouveaux enregistrements de domaines), et **Certificate Transparency logs** (certificats SSL émis pour des domaines imitant le vôtre).

Cas d'usurpation couverts

- **Faux portails RH/Finance** : pages de connexion imitant vos outils internes pour voler les identifiants de vos collaborateurs
- **Faux support IT** : sites prétendant offrir une assistance technique liée à vos produits ou services
- **CEO fraud & BEC** : domaines utilisés pour usurper l'identité de dirigeants dans des campagnes de fraude au président
- **Faux fournisseurs** : portails imitant vos partenaires pour intercepter des paiements ou des données
- **Applications frauduleuses** : apps mobiles ou web reprenant votre marque sans autorisation

Actions & neutralisation

01

Scoring & analyse

Évaluation du risque de chaque domaine suspect (similarité, contenu, infrastructure, activité)

ĆČ

Constitution de preuves

Captures d'écran horodatées, WHOIS, enregistrements DNS, contenu hébergé

03

Contact registrar & hosting

Demandes de suspension auprès des registrars et hébergeurs concernés

04

Takedown & blocage

Procédures de retrait et blocage (lorsque applicable), suivi jusqu'à résolution

Valeur : réduction de la fraude ciblant vos clients et collaborateurs, protection durable de votre marque, et continuité commerciale préservée.

MODULE 5

External Attack Surface & Shadow Services

Réduire l'exposition technique exploitable avant qu'un attaquant ne la découvre et ne l'utilise comme point d'entrée.

Détection des services exposés

La surface d'attaque externe d'une organisation évolue quotidiennement. Des services sont déployés, oubliés ou mal configurés — souvent sans que les équipes sécurité en soient informées. Notre module identifie en continu les services exposés et vulnérables accessibles depuis Internet :

RDP exposé

Vecteur #1 de compromission ransomware

TeamViewer / VNC

Accès distants non sécurisés

Telnet / SSH

Protocoles legacy sans chiffrement adéquat

Docker / APIs

Conteneurs et interfaces d'administration exposés

Focus : Vulnerable RDP

Les services RDP exposés sur Internet restent l'un des vecteurs d'attaque les plus exploités par les groupes de ransomware et les initial access brokers. Notre détection spécialisée identifie ces services **avant compromission**, avec une qualification du niveau de risque (authentification, version, exposition géographique, corrélation avec des credentials leakés).

Livrables

- **Inventaire complet** des services exposés avec fingerprinting technique
- **Niveau d'exposition** : classification par criticité et exploitabilité
- **Recommandations** : restriction d'accès, mise en place de VPN, activation MFA, segmentation réseau, application de correctifs

MODULE 6

Threat Intelligence contextualisée

Du renseignement exploitable, pas du bruit. Des indicateurs de compromission enrichis, corrélés et directement intégrables dans votre stack de sécurité.

IoC/IoA contextualisés

Notre flux de Threat Intelligence fournit des indicateurs de compromission (IoC) et d'attaque (IoA) enrichis et contextualisés : adresses IP malveillantes, URLs de phishing et de command & control, domaines d'usurpation, payloads identifiés et fichiers malveillants. Chaque indicateur est accompagné de son **contexte d'origine**, de sa **confiance** et de sa **pertinence** pour votre périmètre spécifique.

Corrélation multi-dimensionnelle

La véritable puissance réside dans la corrélation : une **exposition de données** détectée est croisée avec des **identifiants compromis** associés, des **mentions dark web** évoquant votre organisation, et une **infrastructure d'usurpation** ciblant votre marque. Cette vision corrélée transforme des signaux isolés en scénarios de menace actionnables.

Intégrations natives

Les indicateurs et alertes s'intègrent directement dans votre écosystème de sécurité existant selon votre stack technique : **SIEM/SOAR** (Splunk, Sentinel, QRadar), **EDR** (CrowdStrike, SentinelOne, Defender), **ticketing** (ServiceNow, Jira) et **IAM** (Azure AD, Okta). Les formats standards (STIX/TAXII, CEF, syslog) sont supportés.

L'objectif n'est pas de vous noyer sous les données, mais de vous fournir les **éléments décisionnels** qui permettent à vos analystes de prioriser, investiguer et répondre plus rapidement aux menaces réelles.

MÉTHODOLOGIE

« Zero noise » : notre méthode de qualification

Trop d'alertes tuent l'alerte. Notre engagement : vous ne recevez que des **signaux qualifiés, contextualisés et actionnables.**

1 Détection large

Couverture maximale des sources externes — web ouvert, deep web, dark web, cloud, DNS, CT logs — pour ne laisser aucun angle mort. L'étendue de la collecte garantit que les expositions critiques ne passent pas entre les mailles du filet.

2 Qualification humaine & règles de tri

Chaque alerte passe par un processus de qualification combinant règles automatisées et expertise humaine. Les faux positifs sont éliminés, les signaux faibles sont enrichis, et seuls les vrais risques remontent à vos équipes.

3 Alignement métier

La priorisation intègre trois dimensions : **impact juridique** (données personnelles, obligations réglementaires), **impact opérationnel** (services critiques, continuité d'activité), **impact réputation** (marque, confiance clients).

4 Indicateurs de priorisation

Chaque alerte qualifiée est scorée selon : criticité, exploitabilité, surface touchée, urgence temporelle, et responsable de remédiation identifié — pour une réponse immédiate et ciblée.

Notre promesse : réduire les faux positifs grâce à un modèle de « périmètre managé » où chaque alerte est contextuelle, enrichie et prête à l'action. Votre SOC se concentre sur la remédiation, pas sur le tri.

PROCESSUS

Du signal à la correction : workflow de remédiation

Un processus structuré en 6 étapes pour garantir que chaque exposition détectée est traitée de bout en bout, avec traçabilité complète et preuves exploitables.

Découverte Qualification Priorisation Plan d'action Remédiation

Ce workflow garantit une **traçabilité complète** de chaque exposition, de sa découverte à sa résolution. Chaque étape est documentée et horodatée pour répondre aux exigences d'audit et de conformité.

Livrables à chaque étape

Tickets & suivi

Chaque alerte qualifiée génère un ticket avec statut, responsable et SLA associés

Preuves horodatées

Captures, logs, IOC et éléments techniques datés et signés numériquement

Recommandations

Actions correctives priorisées, adaptées au contexte technique et organisationnel

Rapports exec & ops

Synthèses pour la direction et rapports détaillés pour les équipes opérationnelles

CONFORMITÉ

Conçu pour « Security + Privacy by Design »

Notre service EEM est architecturé dès sa conception pour respecter les exigences réglementaires européennes les plus strictes, tout en maximisant l'efficacité de la détection.

RGPD — Cadre de conformité

01

Sécurité du traitement (art. 32)

Notre approche s'inscrit dans l'obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées au risque. La détection proactive d'expositions constitue une mesure de sécurité préventive au sens du RGPD.

02

Base légale & minimisation

Le **légitime intérêt** (art. 6.1.f) est généralement la base légale la plus pertinente pour la détection de compromission d'identifiants et de données. Nous accompagnons la mise en place d'une gouvernance rigoureuse incluant des tests de balance (LIA) documentés.

03

Sous-traitance (art. 28)

DPA formalisé, instructions documentées, engagements de confidentialité, mesures techniques et organisationnelles décrites, et auditabilité garantie.

ÇÇ

Gestion d'incidents (art. 33–34)

Appui à la notification dans les délais requis et traçabilité complète des éléments de preuve pour documenter chaque incident.

NIS2 & DORA

Selon le périmètre d'activité de votre organisation, le service EEM contribue directement aux obligations imposées par les directives européennes NIS2 et DORA :

Détection

Capacité de détection des menaces externes et des expositions, conforme aux exigences de surveillance continue

Réduction de surface

Réduction mesurable de la surface d'attaque externe, avec preuves documentées

Reporting & gestion

Processus et preuves structurés pour le reporting d'incidents et la gestion de crise

PACKAGING

Du « quick win » au monitoring continu

Nos options de délivrance s'adaptent à votre contexte, votre maturité et vos besoins métier — de l'audit ponctuel au monitoring permanent.

Monitoring annuel continu

Recommandé — Surveillance permanente de l'ensemble de votre périmètre externe avec détection, qualification et remédiation en continu. Rapports mensuels exécutifs, tableaux de bord opérationnels, et revues trimestrielles de la posture de sécurité. L'option la plus complète pour une réduction durable du risque.

Monitoring court terme

Surveillance ciblée pendant une période définie : campagne marketing majeure, événement corporate, fusion-acquisition en cours, ou gestion de crise. Durée typique de 1 à 6 mois avec périmètre et objectifs clairement définis.

Audit one-off

Évaluation ponctuelle de votre exposition externe : audit technique complet, due diligence M&A, évaluation de la supply chain numérique. Livrable : rapport détaillé avec cartographie des expositions, scoring des risques et plan d'action priorisé.

Incident response & remédiation

Accélération post-détection : lorsqu'un incident est identifié (interne ou externe), nos équipes interviennent pour qualifier, contenir et remédier rapidement. Investigation, collecte de preuves, coordination avec les tiers et documentation complète pour les obligations de notification.

PASSONS À L'ACTION

Modèle commercial : modulaire, scalable, orienté valeur

Pricing transparent & prévisible

Notre modèle de tarification repose sur deux axes simples :

1

Nombre de modules

Sélectionnez les modules pertinents pour votre contexte (Credentials, Brand/Domain, Dark Web, Data Leakage, Attack Surface, Threat Intel) et composez votre couverture sur mesure.

2

Taille de l'entreprise

Le pricing s'adapte à votre band d'employés pour garantir un coût proportionné à votre périmètre réel.

Modèles de partenariat

Resale

Distribution du service à vos clients sous votre marque

MSSP

Intégration dans votre offre de services managés de sécurité

Pourquoi Luxgap ?

La différenciation de Luxgap repose sur une **combinaison unique** de compétences rarement réunies chez un même partenaire :

DPO externe

Expertise privacy intégrée pour une conformité documentée dès la détection

CISO externe

Vision sécurité stratégique alignée sur vos enjeux business

Gouvernance

Remédiation plus rapide, preuves exploitables, reporting structuré

🚀 Call-to-action : Lancez une **« Proof of Value »** de 2 à 4 semaines sur 2 modules — **Credentials + Brand/Domain** — pour mesurer concrètement la valeur du service sur votre périmètre. Résultats tangibles garantis, puis extension progressive aux autres modules selon vos priorités.

Julien Winkin – Julien.winkin@luxgap.com +352 621 583 116