CYBERSECURITY | EXTERNAL EXPOSURE MONITORING

Luxgap External Exposure Monitoring (EEM)

Luxgap
DATA PRIVACY PARTNER

Detect what your teams don't see: data leaks, compromised credentials, malicious domains, and exposed services on your external perimeter.

With evolving threats, companies can no longer settle for protecting their internal network perimeter. The real attack surface extends far beyond: open web, public cloud, criminal marketplaces, encrypted messaging, DNS and Certificate Transparency logs, code repositories, underground forums... Luxgap EEM provides a **continuous monitoring** of this "*invisible exterior*" to identify critical exposures before they are exploited.

Detection

Multi-source collection and automated analysis

Qualification

Sorting, contextualization, and noise elimination

Prioritization

Criticality, exploitability, business impact

Remediation

Correction, timestamped proof, and reporting

Ultimate goal: reduce risk *before* the incident — whether it's extortion, Account Takeover, fraud, ransomware, or reputational damage. An end-to-end managed service, designed for demanding security teams.

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

⚠ THE OBSERVATION

The Problem: The Company is Leaking... Outside the Perimeter

The most critical exposures often occur **outside** the "controlled" information system — where your traditional monitoring tools have no visibility.

Ubiquitous and Invisible Leaks

Misconfigured cloud storages (S3, Azure Blob, GCS), public Git repositories containing secrets, forgotten file shares, Shadow IT instances deployed by business teams, data transmitted to providers without sufficient control... The vectors of exposure multiply as the company's digital ecosystem expands.

Attackers have understood this well and are **industrializing** their approach: automated reconnaissance of the external attack surface, massive collection of credentials via stealers, brand and domain impersonation, resale of data on criminal marketplaces. The time between the discovery of an exposure and its exploitation is reduced to a few hours.

The visibility paradox: internal scans, EDR, SIEM, and firewalls protect what you know. But they are blind to what happens *outside* your perimeter. **External visibility** combining Digital Risk Protection and Attack Surface Management is needed to fill this blind spot.

PRODUCT VISION

Our "Managed External Perimeter"

A comprehensive **Managed External Perimeter**: everything that can expose your assets, identities, data, and brand, continuously monitored, qualified, and managed.

Faster, Deeper

Our approach is based on a unique technological and human combination. We deploy detection capabilities that cover the entire external spectrum: open web, deep web, dark web, cloud, DNS, Certificate Transparency logs, marketplaces, and closed forums.

The fundamental difference: a **drastic reduction of noise** through expert qualification and business contextualization of each alert. Every signal is enriched, correlated, and prioritized before reaching your teams.

Risk-Driven Management

Each detected exposure is evaluated according to four key dimensions to ensure your resources are focused on what truly matters:

Criticality

Nature and sensitivity of exposed data or assets

Exploitability

Ease of exploitation by an attacker

Business Impact

Operational, financial, and legal consequences

Compliance

Implications of GDPR, NIS2, DORA, and sectoral obligations

EEM OVERVIEW

3 Families of Risks to Cover

External Exposure Monitoring is structured around three complementary pillars, covering the entire spectrum of external digital risks your organization faces.

Digital Risk Protection

Brand and domain protection, impersonation detection, fight against online fraud, and prevention of Account Takeovers. This family covers risks that exploit the **trust** that your customers and partners place in your brand.

- Brand & domain monitoring
- Phishing and typosquatting detection
- Fraud monitoring (CEO fraud, fake suppliers)

External Attack Surface

Discovery and management of the external attack surface, reduction of technical exposures, assessment of risks related to the supply chain and M&A operations. This family targets **technical vulnerabilities** exploitable from the outside.

- Asset discovery & inventory
- Shadow services & exposed vulnerabilities
- Third-party risk and technical due diligence

Threat Intelligence

Targeted intelligence, proactive hunting, vulnerability management enrichment, and third-party risk monitoring. This family transforms **weak signals** into actionable intelligence to anticipate attacks.

- Contextualized IoC/IoA
- Multi-source correlation
- SIEM/SOAR/EDR integration

These three pillars work in synergy: a data leak (Digital Risk) correlated with compromised credentials (Threat Intelligence) targeting an exposed service (Attack Surface) constitutes an imminent compromise scenario that only a unified vision can detect and address in time.

MODULE 1

Data Leakage Detection & Breach Prevention

Detect and secure publicly accessible sensitive data before it is exploited by a malicious actor.

Detection Scope

Our Data Leakage Detection module continuously scans the most critical exposure sources: cloud buckets and objects (AWS S3, Azure Blob Storage, Google Cloud Storage), databases accessible without authentication (MongoDB, Elasticsearch, Redis), search engine indexes referencing internal documents, and misconfigured storage on SaaS or FTP platforms.

Identified Indicators

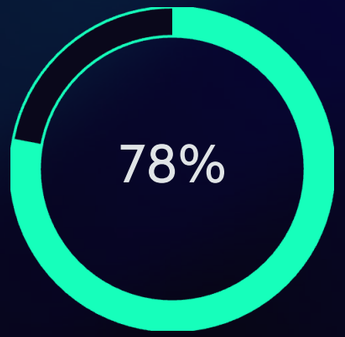
- **PII (Personal Identifiable Information)**: names, emails, social security numbers, banking data, medical records
- **Technical Secrets**: API keys, access tokens, certificates, sensitive configurations
- **Internal Documents**: contracts, strategic plans, HR documents, intellectual property
- **Customer Exports & Backups**: database dumps, CRM exports, unencrypted backups

Deliverables & Outputs

For each identified exposure: **timestamped proof**, precise affected perimeter, prioritized remediation recommendations, and post-remediation validation confirming effective securing.

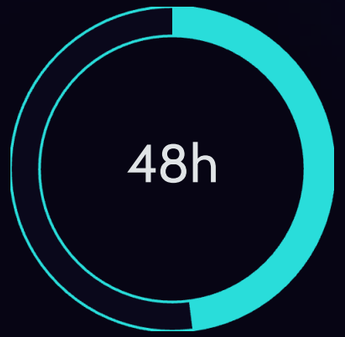
Key Value

Reduction of GDPR risk through control of confidentiality and proactive minimization of the data exposure surface. Each detection is documented to feed your processing records and impact assessments (DPIAs).



Cloud Leaks

Data leaks originate from cloud misconfigurations



Critical Window

Average time between exposure and exploitation by an attacker

MODULE 2

Credential Intelligence

Detect credential leaks before they lead to a compromise of your critical accounts and systems.

Detection Sources

Compromised credentials represent the most exploited attack vector. Our monitoring covers the entire leak ecosystem:

Public Leaks

Stolen databases made public (historical and recent breaches)

Paste sites

Pastebin, GitHub Gists, and similar platforms where credentials are published

Stealer logs

Results from credential-stealing malware (RedLine, Raccoon, Vidar…)

Criminal Marketplaces

Resale of access and sessions on dark web markets

Monitoring Scope

We monitor your **corporate emails**, domains, brands, critical applications (VPN, SSO, business portals), and **VIP accounts** (executives, administrators, developers). Each detected credential is correlated with its exposure context to assess the real risk.

Remediation Actions

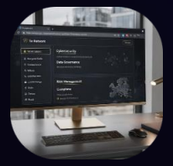
- **Targeted reset** of compromised passwords with user notification
- **MFA / conditional access activation** on at-risk accounts
- **Invalidation of active sessions and tokens** potentially compromised
- **SSO hardening**: review of access policies and federation rules

Value: significant reduction in Account Takeovers, direct prevention of fraud and ransomware that exploit stolen credentials as an initial entry point.

MODULE 3

Dark Web Monitoring

Detect and mitigate attacks in preparation: underground forums, encrypted messaging, and closed communities.



Monitored Sources

Our coverage extends to the main channels used by malicious actors: Tor forums and .onion sites, specialized boards (XSS, Exploit, BreachForums), historical IRC channels, private Telegram groups, and Discord servers. Each source is continuously monitored by specialized agents and automated crawlers.

Proactive Detection

We identify **mentions of your brand**, internal projects, resold access (initial access brokers), data for sale, and extortion signals before they materialize. Each mention is captured with its full context: author, channel, timestamp, and associated content.

Expert Qualification

Each signal is qualified according to its **credibility** (actor's profile, history, reputation), the **stage of the attack** (reconnaissance, preparation, execution), and its **correlation** with other indicators (compromised credentials, already exposed data, malicious infrastructure).

Ethical and Legal Safeguards: Our monitoring is conducted with a **strictly defensive purpose**. No data "purchases", no inducement to obtain information, no interaction with malicious actors. All evidence is collected passively and in compliance with the applicable legal framework.

MODULE 4

Brand & Domain Protection

Monitor and neutralize similar domains, typosquatting, phishing, and all forms of digital identity theft.

Multi-source Detection

Our detection engine continuously cross-references multiple data streams to identify malicious domains and their associated infrastructures: **Passive DNS** (historical and real-time resolutions), **zone files** (new domain registrations), and **Certificate Transparency logs** (SSL certificates issued for domains mimicking yours).

Covered Impersonation Cases

- **Fake HR/Finance portals**: login pages mimicking your internal tools to steal your employees' credentials
- **Fake IT support**: sites claiming to offer technical assistance related to your products or services
- **CEO fraud & BEC**: domains used to impersonate executives in 'president fraud' campaigns
- **Fake suppliers**: portals mimicking your partners to intercept payments or data
- **Fraudulent applications**: mobile or web apps using your brand without authorization

Actions & Neutralization

01

Scoring & Analysis

Assessment of the risk of each suspicious domain (similarity, content, infrastructure, activity)

02

Evidence Gathering

Timestamped screenshots, WHOIS, DNS records, hosted content

03

Contact Registrar & Hosting

Suspension requests to relevant registrars and hosts

04

Takedown & Blocking

Takedown and blocking procedures (where applicable), follow-up until resolution

Value: fraud reduction targeting your customers and employees, lasting brand protection, and preserved business continuity.

MODULE 5

External Attack Surface & Shadow Services

Reduce exploitable technical exposure before an attacker discovers and uses it as an entry point.

Detection of Exposed Services

An organization's external attack surface evolves daily. Services are deployed, forgotten, or misconfigured — often without security teams being informed. Our module continuously identifies exposed and vulnerable services accessible from the internet:

Exposed RDP

Ransomware Compromise Vector #1

TeamViewer / VNC

Insecure Remote Access

Telnet / SSH

Legacy Protocols without Adequate Encryption

Docker / APIs

Exposed Containers and Administration Interfaces

Focus: Vulnerable RDP

RDP services exposed on the Internet remain one of the most exploited attack vectors by ransomware groups and initial access brokers. Our specialized detection identifies these services **before compromise**, with a qualification of the risk level (authentication, version, geographical exposure, correlation with leaked credentials).

Deliverables

- **Complete Inventory** of exposed services with technical fingerprinting
- **Exposure Level**: classification by criticality and exploitability
- **Recommendations**: access restriction, VPN implementation, MFA activation, network segmentation, patch application

MODULE 6

Contextualized Threat Intelligence

Actionable intelligence, not noise. Enriched, correlated compromise indicators directly integratable into your security stack.

Contextualized IoC/IoA

Our Threat Intelligence feed provides enriched and contextualized Indicators of Compromise (IoC) and Indicators of Attack (IoA): malicious IP addresses, phishing and command & control URLs, impersonation domains, identified payloads, and malicious files. Each indicator is accompanied by its **origin context**, its **trustworthiness**, and its **relevance** to your specific perimeter.

Multi-dimensional Correlation

The true power lies in correlation: a detected **data exposure** is cross-referenced with associated **compromised credentials**, **dark web mentions** referencing your organization, and an **impersonation infrastructure** targeting your brand. This correlated view transforms isolated signals into actionable threat scenarios.

Native Integrations

Indicators and alerts integrate directly into your existing security ecosystem based on your technical stack: **SIEM/SOAR** (Splunk, Sentinel, QRadar), **EDR** (CrowdStrike, SentinelOne, Defender), **ticketing** (ServiceNow, Jira), and **IAM** (Azure AD, Okta). Standard formats (STIX/TAXII, CEF, syslog) are supported.

The goal is not to drown you in data, but to provide you with the **decision-making elements** that allow your analysts to prioritize, investigate, and respond more quickly to real threats.

METHODOLOGY

« Zero noise » : Our Qualification Method

Too many alerts kill the alert. Our commitment: you only receive **qualified, contextualized, and actionable signals**.

1 Broad Detection

Maximum coverage of external sources — open web, deep web, dark web, cloud, DNS, CT logs — to leave no blind spots. The breadth of collection ensures that critical exposures do not slip through the net.

2 Human Qualification & Sorting Rules

Each alert undergoes a qualification process combining automated rules and human expertise. False positives are eliminated, weak signals are enriched, and only true risks are escalated to your teams.

3 Business Alignment

Prioritization integrates three dimensions: **legal impact** (personal data, regulatory obligations), **operational impact** (critical services, business continuity), **reputational impact** (brand, customer trust).

4 Prioritization Indicators

Each qualified alert is scored according to: criticality, exploitability, affected surface, temporal urgency, and identified remediation owner — for an immediate and targeted response.

Our promise: reduce false positives through a « managed perimeter » model where each alert is contextual, enriched, and ready for action. Your SOC focuses on remediation, not triage.

PROCESS

From signal to correction: remediation workflow

A structured 6-step process to ensure that each detected exposure is handled end-to-end, with complete traceability and actionable evidence.

Discovery Qualification Prioritization Action Plan Remediation

This workflow ensures **complete traceability** of each exposure, from discovery to resolution. Each step is documented and timestamped to meet audit and compliance requirements.

Deliverables at each step

Tickets & tracking

Each qualified alert generates a ticket with associated status, owner, and SLA

Timestamped evidence

Screenshots, logs, IOCs and technical elements dated and digitally signed

Recommendations

Prioritized corrective actions, adapted to the technical and organizational context

Exec & ops reports

Summaries for management and detailed reports for operational teams

COMPLIANCE

Designed for « Security + Privacy by Design »

Our EEM service is designed from its conception to comply with the strictest European regulatory requirements, while maximizing detection efficiency.

GDPR — Compliance Framework

01

Security of Processing (Art. 32)

Our approach falls within the obligation to implement technical and organizational measures appropriate to the risk. Proactive detection of exposures constitutes a preventive security measure within the meaning of GDPR.

02

Legal Basis & Minimization

Legitimate interest (Art. 6.1.f) is generally the most relevant legal basis for detecting compromised identifiers and data. We support the implementation of rigorous governance including documented balance tests (LIA).

ĆĊ

Subcontracting (Art. 28)

Formalized DPA, documented instructions, confidentiality commitments, described technical and organizational measures, and guaranteed auditability.

04

Incident Management (Art. 33–34)

Support for timely notification and complete traceability of evidence to document each incident.

NIS2 & DORA

Depending on your organization's scope of activity, the EEM service directly contributes to the obligations imposed by the European NIS2 and DORA directives:

Detection

Threat and external exposure detection capability, compliant with continuous monitoring requirements

Surface Reduction

Measurable reduction of the external attack surface, with documented evidence

Reporting & Management

Structured processes and evidence for incident reporting and crisis management

PACKAGING

From "Quick Win" to Continuous Monitoring

Our delivery options adapt to your context, maturity, and business needs — from ad-hoc audits to permanent monitoring.

Continuous Annual Monitoring

Recommended — Permanent monitoring of your entire external perimeter with continuous detection, qualification, and remediation. Executive monthly reports, operational dashboards, and quarterly security posture reviews. The most comprehensive option for sustainable risk reduction.

Short-Term Monitoring

Targeted monitoring during a defined period: major marketing campaign, corporate event, ongoing merger-acquisition, or crisis management. Typical duration of 1 to 6 months with clearly defined scope and objectives.

One-Off Audit

One-time evaluation of your external exposure: comprehensive technical audit, M&A due diligence, digital supply chain assessment. Deliverable: detailed report with exposure mapping, risk scoring, and prioritized action plan.

Incident Response & Remediation

Post-detection acceleration: when an incident is identified (internal or external), our teams intervene to quickly qualify, contain, and remediate. Investigation, evidence collection, coordination with third parties, and complete documentation for notification obligations.

LET'S TAKE ACTION

Business Model: Modular, Scalable, Value-Oriented

Transparent & Predictable Pricing

Our pricing model is based on two simple axes:

1

Number of Modules

Select the modules relevant to your context (Credentials, Brand/Domain, Dark Web, Data Leakage, Attack Surface, Threat Intel) and compose your customized coverage.

2

Company Size

Pricing adapts to your employee bracket to ensure a cost proportionate to your actual scope.

Partnership Models

Resale

Distribution of the service to your clients under your brand

MSSP

Integration into your managed security services offering

Why Luxgap?

Luxgap's differentiation is based on a **unique combination** of skills rarely found in a single partner:

External DPO

Integrated privacy expertise for documented compliance from detection

External CISO

Strategic security vision aligned with your business challenges

Governance

Faster remediation, actionable evidence, structured reporting

🚀 Call-to-action: Launch a **"Proof of Value"** of 2 to 4 weeks on 2 modules — **Credentials + Brand/Domain** — to concretely measure the value of the service within your scope. Tangible results guaranteed, then progressive extension to other modules according to your priorities.

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