Luxgap

DATA PRIVACY PARTNER

CYBERSECURITY & GOVERNANCE

# Luxgap CISO: Definition & Mission

The **Chief Information Security Officer** (CISO) is the central pillar of information systems security. At Luxgap, this function is reimagined as an outsourced service — an agile, expert, and structured model for organizations that want to **master cyber risk without compromise**.


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

# 01 — Luxgap CISO: Definition & Mission

The CISO (Chief Information Security Officer) manages **end-to-end ICT security**: from strategy definition to technical architecture, including daily operations and crisis management. They ensure a coherent, measurable, and business-aligned security posture for the organization.

## CISO-as-a-Service

At Luxgap, the CISO is designed as an outsourced service: **senior expertise**, structured governance, equipped execution, and knowledge transfer to your internal teams. A flexible model that adapts to your maturity and constraints.

## Risk Reduction

The central objective is to **reduce risk** in all its forms — financial, operational, legal, and reputational — by covering external, internal, cloud, and human factors.

## Defense-in-Depth & Zero Trust

The philosophy is based on defense-in-depth security coupled with the **Zero Trust** model and continuous improvement. Each layer of defense strengthens the next.

**Constant Deliverables:** risk register, security roadmap, policies and standards, operational controls, audit evidence, reporting to management — a comprehensive framework for long-term security management.

# 02 — Why a CISO is Critical

Cybersecurity is not a one-time project with a beginning and an end: it's a permanent **management system**, consisting of processes, clearly defined roles, documented evidence, and performance indicators. Without a CISO to orchestrate this whole, security efforts remain fragmented and reactive.

## What a CISO Brings

### Strategic Prioritization

Identify **what truly matters** among hundreds of potential risks. Arbitrate budget investments based on real impact and not media hype.

### Technical → Business Translation

Transform technical vulnerabilities into **understandable business risks**: revenue loss, production downtime, regulatory sanctions, customer disputes, damage to brand and trust.

### Alignment Management / IT / Business Units

Bridge the gap between corporate governance and technical teams so that security decisions are understood, accepted, and applied at all levels.

## Ongoing Challenges

The CISO maintains a consistent level of security despite increasing complexity factors:

- **Organic growth** and M&A operations that alter the scope
- **Widespread remote work** and BYOD that dissolve the network perimeter
- **Massive SaaS adoption** and multi-cloud without governance
- **Subcontracting** and outsourcing of critical processes

Finally, the CISO establishes a real **crisis capability**: scenario anticipation, regular exercises, structured response, and systematic feedback to strengthen organizational resilience.

# 03 — Luxgap Scope: all ICT + human risks

The Luxgap approach covers the **entire spectrum of risks** faced by a modern organization. No blind spots are tolerated: each threat vector is identified, evaluated, and treated proportionally.

## External Risks

Opportunistic and targeted attacks, volumetric and application DDoS, sophisticated phishing campaigns, supply chain compromise, brand abuse. These threats come from various actors — cybercriminals, hacktivists, competitors — and require constant monitoring.

## Cloud Risks

Inadvertent public exposure of resources, failing IAM with overly permissive roles, incomplete logs preventing investigation, unprotected or unrotated access keys, missing or unapplied security baselines.

## Third-Party Risks

Service providers, IT outsourcing, software vendors, digital supply chain, and business partners — each interconnection represents a potential entry point for attackers.

## Internal Risks

Human errors, misconfigurations, unreviewed excessive privileges, proliferating shadow IT, risk of sabotage or intentional data leakage. The human factor remains the primary vector of compromise in 85% of incidents.

## Physical Risks

Insufficient access control to premises, theft of equipment, confidentiality of exchanges in meeting rooms, management of visitors and sensitive areas.

## Compliance Risks

Sector-specific requirements (NIS2, DORA, financial regulations), contractual security obligations, data breach notification obligations, potential penalties for non-compliance.

# 04 — Operational Model: From Risk to Action

The Luxgap operational model transforms risk analysis into concrete and measurable actions, following a **six-phase** cycle that ensures comprehensive coverage and continuous improvement.

1 Understand

Map critical assets, identify sensitive data, analyze essential business processes, evaluate relevant threats, and identify existing vulnerabilities. This phase forms the foundation of any informed decision.

2 Decide

Define risk appetite with management, establish investment priorities, allocate the security budget, and build a realistic **30/60/90-day action plan** with measurable milestones.

3 Deploy

Implement technical controls (firewalls, EDR, MFA), organizational controls (policies, procedures, governance), and human controls (awareness, training, security culture) in a coordinated manner.

4 Monitor

Ensure continuous detection via SOC/SIEM, conduct proactive threat hunting operations, leverage cyber threat intelligence (CTI), and track relevant operational metrics.

5 React

Manage incidents according to proven playbooks: forensic investigation, service restoration, internal and external communication, preservation of the chain of evidence.

6 Improve

Conduct systematic post-mortems, apply systemic corrections (not just ad hoc), harden configurations, and enhance detection capabilities.

# 05 — Governance: Who Decides What (Without Friction)

Effective security governance relies on **clear decision-making structures**, well-defined roles, and transparent arbitration mechanisms. The goal is to integrate security into existing corporate governance, without creating paralyzing bureaucracy.

1

### Security Committee

Brings together Management, IT, key business units, HR, and legal/DPO. This strategic decision-making body validates priorities, budgets, and risk acceptances.

2

### Role Clarification

**Asset owners**, application managers, administrators, SOC, and vendors: everyone understands their responsibilities, reporting obligations, and limits of action.

3

### Arbitration Rules

Security vs. cost vs. time vs. user experience: formalized criteria with **complete traceability** of decisions made, including risk acceptances.

4

### Documentary Framework

Policies, standards, operational procedures, exception management, and evidence collection — a living and auditable documentation corpus.

**Governance Calendar:** monthly operational reviews + quarterly risk committees + annual security strategy review. This rhythm ensures constant vigilance without overburdening stakeholders.

# 06 — Asset Mapping & Dependencies

THE FOUNDATION OF EVERYTHING

You can only protect what you know. Asset mapping is the **indispensable foundation** of any serious security initiative. Without it, investments are blind and risks are invisible.

## Exhaustive Inventory

- Workstations, physical and virtual servers
- Containers, networks, active equipment
- Connected objects (IoT), SaaS applications
- Service accounts, API keys, certificates

## Flow Mapping

- Data flows between systems
- APIs and interconnections
- VPNs and partner links
- Automated file exchanges

## Crown Jewels

Identification of assets whose **loss or alteration stops activity**: customer databases, production systems, intellectual property, financial data. These "crown jewels" receive a priority level of protection.

## Shadow IT

Proactive detection of undeclared SaaS, uncontrolled external shares, and collaborative tools adopted without security validation. Shadow IT represents an invisible and growing attack surface.

## Deliverables

"Pragmatic" CMDB (focused on usefulness), updated architecture diagrams, asset criticality matrix with scoring.

# 07 — Data Classification & Usage Rules

Data classification is the prerequisite for applying **proportionate protection measures** to information sensitivity. Without classification, everything is treated the same way — either overprotected (friction) or underprotected (risk).

### Public

Information intended for free sharing. No specific distribution restrictions.

### Internal

Internal use only. Controlled sharing, no external distribution without authorization.

### Confidential

Restricted access. Encryption required, access logging, sharing on a strict need-to-know basis.

### Secret

Maximum protection. End-to-end encryption, named access, complete traceability.

## Rules per Level

For each level: authorized storage, sharing conditions, export and print restrictions, retention period, and encryption requirements. These rules are translated into **"do/don't" sheets** per business use case.

## Associated Controls

DLP targeted at risky channels, systematic encryption of sensitive data, automatic tagging, granular access rights management, and exhaustive logging of operations on classified data.

# 08 — Risk Analysis: Luxgap Method

DECISION-ORIENTED

The Luxgap risk analysis does not produce theoretical reports that end up in a drawer. It is designed to **directly feed decisions** for management and operational teams.

## Identified Threats

- **Cybercriminals**: ransomware, fraud
- **Insiders**: error, malice
- **Competition**: industrial espionage
- **Hacktivism**: reputational damage
- **Human error**: misconfiguration
- **Outages**: system failures

## Priority Scenarios

### Ransomware

Massive encryption, production halt, ransom demand, data loss

### Payment Fraud

CEO identity theft, supplier bank detail modification, fraudulent transfer

### M&A Leak

Exfiltration of strategic documents during a confidential operation

### Email Compromise

Email account takeover, lateral movement, access to sensitive data

**Evaluation:** probability × impact (financial / operational / legal / reputational). **Measures:** prevention, detection, response, transfer (insurance) or documented acceptance. **Deliverables:** living risk register, prioritized treatment plan, residual risks validated by management.

# 09 — Target Architecture: Zero Trust

PRACTICAL, NOT MARKETING

Zero Trust is not a product to buy: it's an **architectural paradigm shift.** The fundamental principle is simple — *"Never trust, always verify"* — but its implementation requires a methodical approach.

## Continuous Verification

Every access is verified across four dimensions: user **identity**, request **context**, **device status**, and real-time **risk level**.

## Segmentation

Network, applications, data, and accounts are compartmentalized to **limit lateral movement**. An attacker who compromises one segment cannot pivot freely.

## Least Privilege

Systematic MFA, conditional access, short sessions, periodic rights reviews. Each user only accesses what they strictly need.

## Visibility & Resilience

Centralized logs, event correlation, business-oriented alerting. Immutable backups and restoration procedures **regularly tested**.

# 10 — Perimeter Security: Network & External Access

The network perimeter remains an **essential first line of defense**, even in a Zero Trust world. This involves rigorously controlling what enters and exits the infrastructure.

1

## NGFW Firewall

Advanced application filtering, integrated IPS/IDS, reasoned geo-blocking, and **"deny by default"** rules. Only explicitly authorized traffic is accepted — all other traffic is blocked and logged.

2

## VPN / ZTNA

Remote access **segmented by role** with device posture verification, mandatory MFA, and detailed access logs. ZTNA is progressively replacing classic VPN for more granular control.

3

## DDoS Protection

Upstream defense via ISP/CDN, automatic failover mechanisms, and tested response runbooks. The objective: maintain availability even under volumetric attack.

4

## Egress Filtering

Limit data exfiltration by controlling outbound ports, authorized destinations, web proxy, and DNS. An attacker who has penetrated the network must be **unable to communicate** with the outside.

**Continuous Testing:** external exposure scans, firewall rule reviews, network opening audits, and iterative hardening. Perimeter security degrades without active maintenance.

# 11 — Web, API & Exposed Applications

Applications exposed on the Internet represent the **most visible attack surface** of the organization. Each web service, each API, each customer portal is a potential entry point for attackers.

## WAF & Application Protection

Deployment of a Web Application Firewall covering OWASP Top 10 vulnerabilities, anti-bot protection, intelligent rate limiting, and custom rules adapted to business context. The WAF is a dynamic shield, not a static solution.

## API Securing

Strong authentication (OAuth2/OIDC), granular scopes, call quotas, strict input validation, and centralized secret management. Poorly secured APIs have become the **primary attack vector** for modern applications.

## Certificates & TLS

Comprehensive certificate inventory, automated renewal, modernized TLS (1.2+ minimum), HSTS enabled. An expired certificate or weak TLS configuration is an invitation to attackers.

## CMS Security

Systematic updates, plugin and extension audits, hardening of administrator accounts, regular backups. Unmaintained CMS represent a major risk of compromise.

**Deliverables:** web security baseline, pre-production publication checklist, targeted penetration tests on critical applications.

# 12 — Email, Collaboration & Fraud

Email remains the **number 1 attack vector** — over 90% of cyberattacks start with a malicious email. Securing messaging and collaboration tools is an absolute priority.

## Email Protection

### Advanced Anti-phishing

SPF, DKIM, and DMARC configured in strict mode, multi-layered filtering, sandbox for analyzing suspicious attachments before delivery to users.

### BEC Protection

Rules for detecting CEO fraud (Business Email Compromise), alerts for unusual transfer requests, **mandatory double validation** for all payments, targeted awareness for finance teams.

## Secure Collaboration

### M365 / Google Workspace

Secure tenant configuration, generalized MFA, conditional access, strict control over external shares and connected third-party applications.

### Teams / SharePoint / Drive

Access rights governance, removal of unnecessary public links, limited sharing duration, guest control, and periodic review of external accesses.

# 13 — DNS & brand protection

REDUCE THE ATTACK BEFORE THE ATTACK

Brand and DNS protection is an often overlooked **proactive defense layer**. It allows you to detect and neutralize threats before they reach your users or customers.

01

## Secure DNS

Advanced DNS filtering, automatic blocking of known malicious domains, strict control of resolvers used by workstations and servers. DNS is the first layer of filtering — fast and non-intrusive.

02

## Typosquatting

Continuous monitoring of similar domain registrations: homographs, TLD variations, common typos. Automatic detection and rapid response (takedown, blocking).

03

## CT Certificates

Monitoring Certificate Transparency logs to identify fraudulently issued certificates for domains close to your brand — a precursor sign of a phishing campaign.

04

## Impersonation Detection

Identification of fake websites, fake social media profiles, and phishing campaigns exploiting your brand identity. Coordinated response with legal teams and registrars.

**Deliverables:** brand protection plan, takedown playbook, legal action procedures with registrars and hosts.

# 14 — Segmentation & Network Access Control

Network segmentation is one of the most effective controls against the **propagation of attacks**, especially ransomware. A "flat" network is an ideal playground for attackers.

### Security Zones

Strict separation: users, servers, administration, OT/IoT, guests, and meeting rooms. Each zone has specific access rules.

### NAC

Network Access Control: only compliant devices (patch, EDR, config) access company resources. Non-compliant devices are redirected to a remediation network.

### Secure Wi-Fi

SSIDs separated by usage, WPA2/3 Enterprise with RADIUS authentication, regular key rotation, guest network completely isolated from the corporate network.

### Micro-segmentation

Limitation of ransomware propagation at the application level. Each workload communicates only with the services strictly necessary for its operation.

**Deliverables:** detailed network mapping, documented segmentation rules, progressive "no-break" migration plan to minimize operational impact.

# 15 — Endpoints & Servers: EDR/XDR Protection

Workstations and servers are the **primary targets** for attackers — it's where data lives, users work, and compromises materialize. Modern protection goes far beyond traditional antivirus.

## EDR Deployed Everywhere

Real-time behavioral detection, immediate isolation capability for compromised machines, automatic collection of forensic artifacts for rapid investigation.

## Workstation Hardening

Full disk encryption, USB device control, default blocking of Office macros, whitelisting of approved applications. Each workstation is a fortress.

## Server Protection

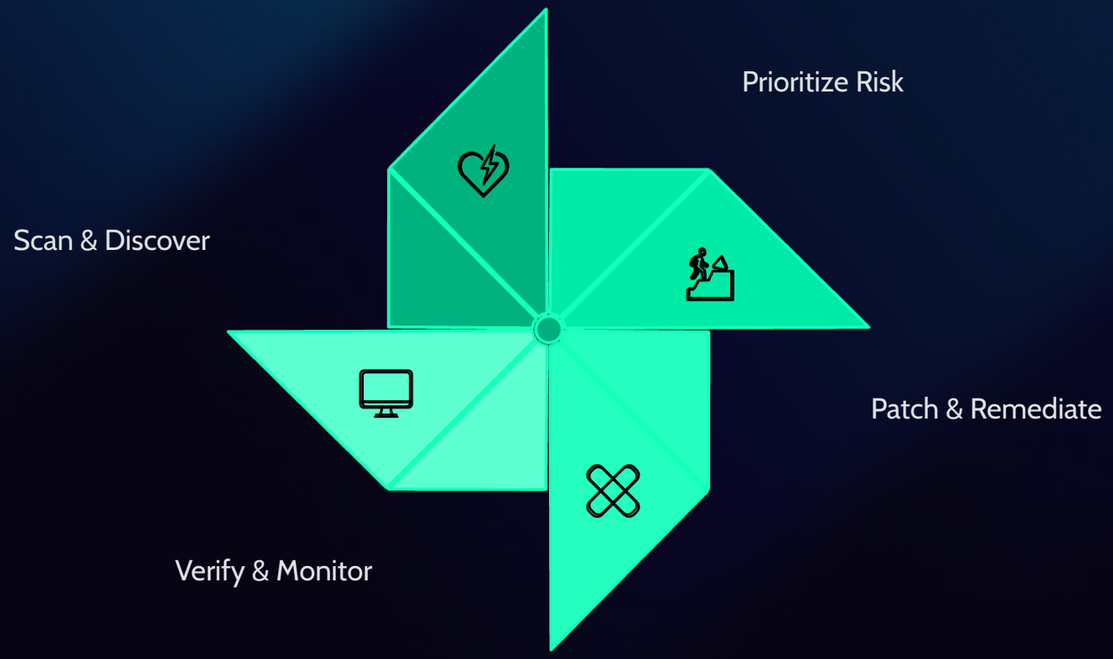
Dedicated security agents, application whitelisting, strict management of active services, monitoring of critical system file integrity.

## Mobile (MDM/MAM)

Separation of professional/personal data, remote wipe in case of loss/theft, compliance verification before accessing corporate resources.

# 16 — Vulnerabilities & Patches: Industrializing the Process

Vulnerability management is a **continuous industrial process**, not a one-time activity. Every day, new vulnerabilities are discovered — the ability to identify, prioritize, and quickly fix them is a major differentiator in security maturity.




This industrialized cycle ensures that critical vulnerabilities are handled as a priority, with contractual and measurable deadlines.

### Comprehensive Inventory

Internal, external, and cloud posture management (CSPM) scanners combined for a 360° view of vulnerabilities. No asset should escape detection.

### Intelligent Prioritization

CVSS criticality × actual exposure × active exploitation in the wild × business value of the asset. No "first-in-first-out" treatment — **real risks come first**.

### Patch Management

Defined deployment cycles, documented and validated exceptions, KPI deadlines (patch SLA: critical < 48h, high < 7d, medium < 30d).

### Zero-days

Accelerated evaluation and response process, temporary workarounds (virtual patching, WAF rules, isolation), emergency communication to teams.

# 17 — Hardening & Configuration: The 80/20 of Risk

Configuration hardening is the security lever offering the **best effort/impact ratio**. The majority of compromises exploit default configurations or undetected deviations — not sophisticated zero-day vulnerabilities.

- ## CIS Standards

  Application of CIS (Center for Internet Security) baselines and vendor guides. Systematic deactivation of unnecessary services, obsolete protocols, and unrequired default functionalities.

- ## Drift Control

  Continuous verification that the configuration remains compliant with the standard (drift detection). Configurations naturally drift — without monitoring, security silently degrades.

- ## Secret Management

  Centralized vault (Vault, KMS), automatic rotation, removal of hardcoded secrets in scripts and CI/CD pipelines. An exposed secret = a compromised access.

- ## Logging

  Activation of critical logs on all systems, synchronized NTP timestamp, protection of log integrity, retention compliant with regulatory and investigation requirements.

# 18 — IAM: Identity, MFA, SSO, Conditional Access

Identity is the **new security perimeter**. In a cloud and mobile world, controlling identities and access has become the fundamental pillar of any modern security architecture.

### Widespread MFA

Priority deployment on admin accounts, remote access, and critical SaaS. MFA blocks **99.9% of password compromise attacks**.

### Centralized SSO

Reduced attack surface through centralized authentication. Better access governance and simplified user experience.

### Conditional Access

Geolocation, device compliance, session risk, blocking legacy protocols. Each access is evaluated in context.

### Joiners / Movers / Leavers

Robust identity lifecycle management process: creation, modification, and departure with immediate and complete access revocation.

**Deliverables:** comprehensive IAM policy, roles/rights matrix per application, periodic access reviews (quarterly for privileged access, semi-annually for standard access).

# 19 — PAM: Mastering Privileges

WHERE EVERYTHING IS AT STAKE

Privileged accounts are the **ultimate target** for attackers. A compromised administrator account provides access to the entire infrastructure. Privileged Access Management (PAM) is therefore a critical control.

## Admin vault

Sessions fully recorded, automatic rotating passwords, **"just-in-time"** access: privilege is granted only for the duration strictly necessary for the operation.

## Separation of duties

Admin ≠ daily user. Mandatory separate accounts, dedicated administration bastion. No admin account browses the Internet or receives email.

## Active Directory / Entra ID

AD hardening with tiering model, dedicated admin workstations (PAW), protection of critical objects (AdminSDHolder, Protected Users, LAPS).

## Vendor control

Temporary access, fully logged, immediately revocable. No vendor has permanent access to production systems.

# 20 — Public Cloud: Posture, Identities, Logs

The public cloud transforms the security model. The **shared responsibility** between the provider and the client must be perfectly understood — and client-side controls rigorously implemented.

## Shared Responsibility

Formal clarification of what falls under the cloud provider (physical infrastructure, hypervisor) and what remains under your responsibility (configurations, identities, data, applications). This sharing is often misunderstood and a source of vulnerabilities.

## CSPM

Cloud Security Posture Management: automated detection of risky configurations — accidental public storage, overly open security groups, exposed access keys, disabled encryption.

## Cloud IAM

Strict application of the principle of least privilege, granular roles and policies, systematic rotation of access keys, strict prohibition of long-term keys.

## Cloud Logging

Audit logs, flow logs, and alerts activated on all critical resources, exported to the central SIEM for correlation and investigation.

**Deliverables:** secure landing zone (cloud foundation), automated guardrails preventing deviations, cloud best practices repository specific to your environment.

# 21 — Private / Hybrid Cloud: Virtualization, Storage, Network

On-premise and hybrid infrastructure requires special attention — it often hosts the **most critical workloads** and the most sensitive data of the organization.

## Hypervisor Security

Regular hypervisor patching, strict isolation between virtual machines, enhanced administrative access controls, logging of all management operations. A compromised hypervisor = all VMs compromised.

## Secure Storage

Systematic encryption at rest, restricted and logged access, regular snapshots, immutability enabled where possible to protect against ransomware.

## Datacenter Network

Rigorous segmentation, east-west firewalling (between internal zones), isolated administration bastions. Internal traffic is monitored as closely as incoming traffic.

## Resilient Backups

Separation of backup accounts and networks, immutability of copies, documented regular restoration tests. Backups are the last line of defense.

# 22 — SaaS: CASB, Shadow IT & Governance

The massive adoption of SaaS has created a **new risk perimeter** largely invisible to traditional IT teams. On average, an organization uses 3 to 5 times more SaaS applications than it realizes.

## CASB / Visibility

Cloud Access Security Broker or equivalent solution to gain **complete visibility** into SaaS usage, control sessions in real-time, and detect abnormal behavior (mass data extraction, connection from a suspicious country).

## Sharing Governance

Control of external guests, deletion of unnecessary public links, automatic expiration of shares, restriction of downloads for sensitive data.

## Third-party Apps & OAuth

Regular review of permissions granted via OAuth, deletion of unapproved applications, limitation of authorized scopes by default.

## SaaS Contracts

Security requirements must be integrated from the contractual phase:

- Formalized **Security Requirements**
- Data **Reversibility** Clauses
- Access to **Audit Logs**
- Data **Location**
- Transparency on **Subcontractors**
- Right of periodic **Audit**

**Deliverables:** exhaustive SaaS register, sharing rules, quarterly controls and reviews.

# 23 — Encryption, Keys & Pragmatic DLP

Data protection relies on three inseparable pillars: **encryption** to render data unreadable in case of a leak, **key management** to control who can decrypt, and **DLP** to prevent data from leaving its authorized perimeter.

## Encryption

TLS 1.2+ for transit, AES-256 encryption at rest for disks, databases, and backups. No sensitive data circulates or rests in plain text.

## Key Management

KMS/HSM with strict separation of roles (who manages keys ≠ who accesses data). Automatic rotation, audited access, secure destruction of obsolete keys.

## Targeted DLP

Focus on real risk channels: outgoing email, web uploads, shared cloud drives. **"Business"** rules rather than generic policies that generate false positives.

## Traceability

Logging of all access to sensitive data, automatic alerts for massive extraction or unusual access. Investigation capability in case of incident.

# 24 — Anti-ransomware: Immutable Backups

Ransomware is the #1 threat to organizations. Attackers now **systematically target backups** before encrypting the production environment. A robust backup strategy is your ultimate safety net.

### 3-2-1+ Rule

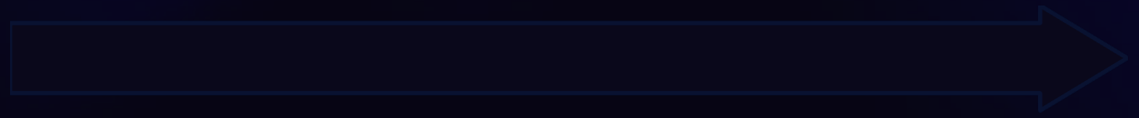
At least 3 copies, on 2 distinct media, with 1 offline or immutable, and complete separation of administrative identities between production and backups.

### Protected Backups

Dedicated accounts with MFA, isolated network inaccessible from production, real-time integrity monitoring. An attacker must **never be able to reach** backups.

### Restoration Tests

Monthly or quarterly exercises including disaster scenarios: "we lost AD", "we lost the cloud". Each test is documented with actual measured times.



### Minimum Viable Company

Definition of services to be restored with absolute priority, with recovery time objectives (RTO) and data loss objectives (RPO) validated by management.

# 25 — DevSecOps & Secure SDLC

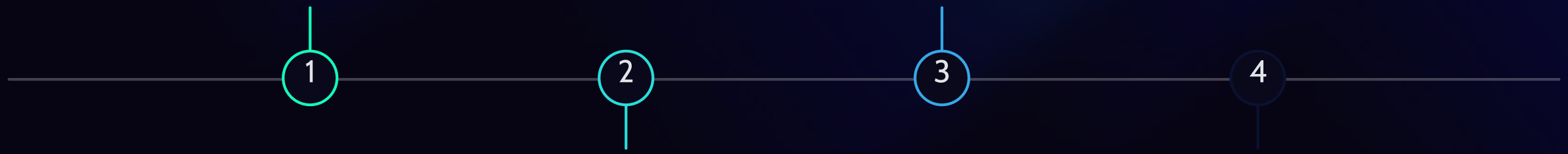
Application security can no longer be an afterthought — it must be natively integrated into the Software Development Life Cycle (SDLC). DevSecOps makes security a shared responsibility between developers, operations, and security.

### Design

**Threat modeling** from the design phase. Identification of attack surfaces, sensitive data flows, and security requirements before writing the first line of code.

### CI/CD Pipeline

Automated security gates: no deployment if critical vulnerability detected. Strict separation of environments (dev/staging/prod), artifact signatures.




### Development

SAST (static analysis), automated secret scanning, open-source dependency control (SBOM), secure coding rules applied in the IDE.

### Production

Continuous DAST/IAST, dependency monitoring for new vulnerabilities, up-to-date SBOM, formalized **"go/no-go"** criteria for each release.

**Deliverables:** DevSecOps policy, phase-specific security checklists, security acceptance criteria, code vulnerability dashboard.

# 26 — SOC / SIEM: Centralized Monitoring

AND USEFUL

A SOC (Security Operations Center) without intelligence is a noise factory. The challenge is not to collect the maximum number of logs, but to detect **relevant signals** and react effectively — avoiding "alert fatigue" which neutralizes teams.

## Collection & Correlation

Critical logs are collected from all layers: **identity** (AD, Entra ID, SSO), **endpoints** (EDR), **firewall**, **cloud** (AWS/Azure/GCP), **email**, **servers**, and **business applications**.

Correlation cross-references these sources to detect complex scenarios: multi-stage fraud, suspicious admin behavior, progressive exfiltration, early ransomware signals.

## SOC Operations

**Structured Playbooks:** each alert type has an associated triage, escalation, containment, and communication procedure.

**Quality:** continuous rule tuning, alert prioritization, establishment of behavioral baselines to reduce false positives. An effective SOC generates **actionable alerts**, not noise.

**Deliverables:** documented SIEM use cases, log dictionary, SOC procedures, MTTD/MTTR metrics.

# 27 — Advanced Detection: UEBA, XDR & Hunting

Beyond rule-based detection, advanced techniques identify threats that **evade signatures** — sophisticated attackers who blend into legitimate traffic.

## UEBA

User & Entity Behavior Analytics: anomaly detection through machine learning — connections from unusual locations, massive data exfiltration, administrator behavior deviating from their baseline.

## XDR

Extended Detection & Response: cross-referencing endpoint + network + identity + cloud signals to **reduce detection time** (MTTD) and build a unified view of the attack.

## Threat Hunting

Proactive search based on targeted hypotheses: "is an attacker already in our network?". Focus on critical assets and weak signals that automatic rules do not detect.

## Purple Teaming

Joint red/blue team exercises to test detection under real conditions, without disrupting production. Each exercise enhances detection capabilities.

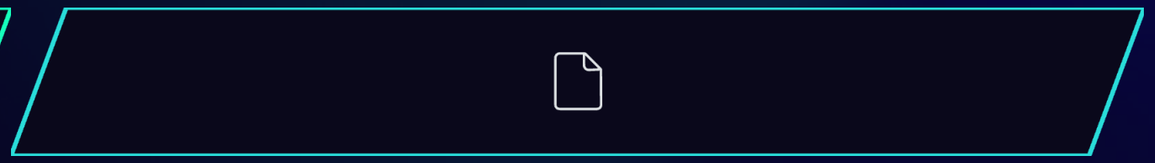
**Deliverables:** annual hunting plan, investigation reports, "detect/stop" improvements integrated into the SOC backlog after each exercise.

# 28 — CTI: Decision-Oriented Cyber Intelligence

Cyber Threat Intelligence transforms raw threat information into **actionable intelligence** that guides security decisions at all levels of the organization.

## Multiple Sources

OSINT, national and sectoral CERT/CSIRT, specialized providers, sharing communities (MISP, ISACs), alerts on actively exploited CVEs. The diversity of sources enhances the quality of intelligence.



## Two-Tier Production

"Executive" notes (risk/impact in business language) for management + detailed technical sheets (IOC, TTP, detection rules) for IT/SOC teams.

## Operational Alignment

CTI directly informs patching prioritization, SOC rule enrichment, configuration hardening, and targeted awareness campaigns.

## Sectoral Monitoring

Typical adversary profiles for your sector, analysis of the most used TTPs (tactics, techniques, and procedures), identification of emerging trends.

# 29 — Dark web monitoring

SECURED & LEGALLY CONTROLLED

Dark web monitoring allows for the **early detection** of compromise signals before they escalate into a major incident. It is a proactive, legally framed intelligence capability.

## Objective

Early detection of **compromised credentials** (credentials leaks), internal data breaches, mentions of your brand in malicious forums, and the sale of initial access to your infrastructure on marketplaces.

## Monitored Scope

Corporate emails, domain names, identities of executives and sensitive individuals, keywords related to confidential projects (M&A, R&D), IP addresses, and brands.

## Alert Processing

Systematic validation and qualification (true positive vs. false positive), followed by immediate actions: password reset, MFA enforcement, in-depth investigation if necessary.

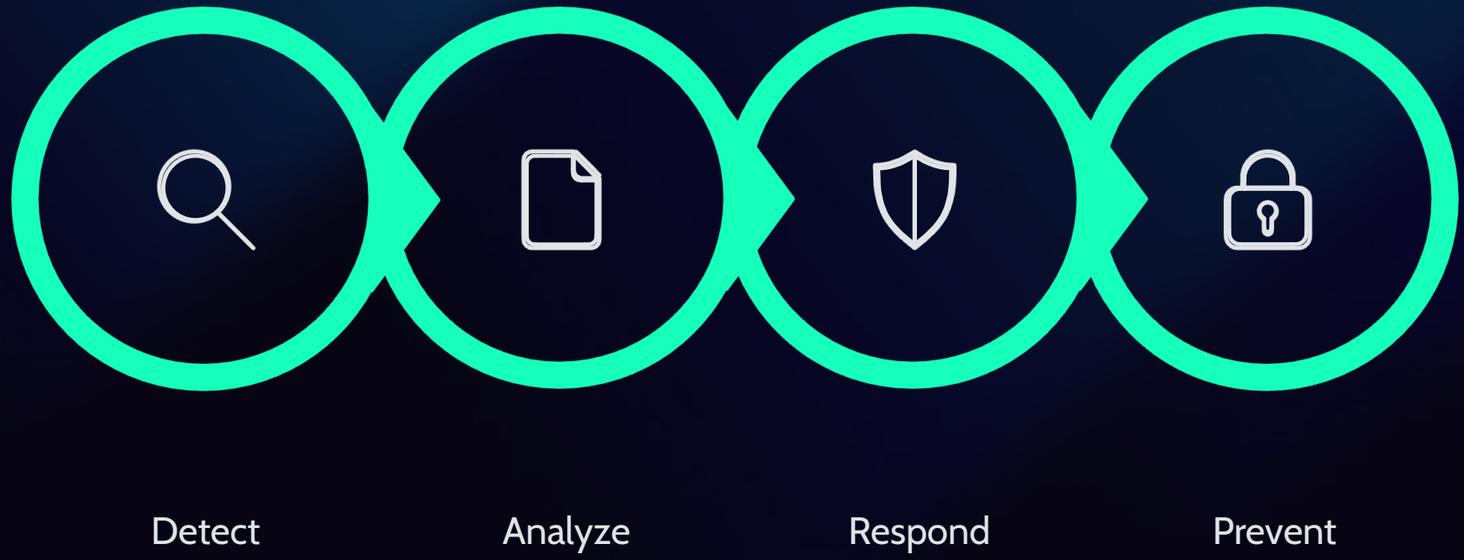
## Strict Governance

Minimization of collected data, access traceability, limited and supervised retention, preservation of chain of custody in case of transmission to authorities.

**Deliverables:** real-time actionable alerts, summary dashboards, playbooks for responding to credential leaks.

# 30 — Domain Name Monitoring

Typosquatting and domain name impersonation are frequently used techniques by attackers to **deceive your employees, customers, and partners**. Active monitoring allows these threats to be neutralized before they cause damage.




This continuous loop process ensures permanent coverage against attempts to impersonate your digital identity.

**Proactive prevention:** defensive registration of similar domains, DMARC hardening in "reject" mode, continuous monitoring of new threats. **Deliverables:** up-to-date "lookalikes" registry, documented response process, monthly monitoring reports.

# 31 — Attack Preparation Signals

EARLY WARNING

Attackers never strike without preparation. The **reconnaissance** phase always precedes the attack — and it is during this phase that detectable signals appear, offering a window for preventive action.

## Involuntary Exposure

Detection of new publicly exposed ports or services, misconfigured cloud buckets, accessible Git repositories containing source code or secrets. Each exposure is an immediate call to action.

## Active Reconnaissance

Intensive port scans, brute force attempts, targeted 404 errors on administration paths, WAF anomalies revealing application mapping by an attacker.

## Exploitation in Progress

IOCs (indicators of compromise) correlated with exploitation attempts of CVEs actively used in the wild. Near real-time detection through CTI integration.

## Pre-Incident Targeting

Increase in compromise attempts on VIP accounts, specific targeting of finance and HR teams (attackers' preferred targets for fraud and initial access).

**Deliverables:** continuously updated exposure table, automated alerting system, documented and measured rapid preventive actions.

# 32 — Physical Security: Access, Visitors & Equipment

Physical security is the **essential complement** to cybersecurity. An attacker with physical access to your premises can bypass most logical protections in minutes.

## Access Control

- **Named badges** with differentiated access zones
- Logging of all entries
- Immediate revocation in case of departure or incident
- Temporary rights for occasional contractors

## Visitor Management

- Mandatory escort in sensitive areas
- Visually distinct visitor badges
- NDA if accessing confidential information
- Clearly marked restricted areas

## Equipment Protection

- Automatic workstation locking
- Privacy screen filters in open areas
- Strict clean desk policy
- Secure destruction of storage media

## Inventory & Traceability

- Exhaustive inventory and labeling of all equipment
- Loss/theft procedure with immediate notification
- Mandatory encryption on all mobile devices
- Periodic physical audits of premises

# 33 — Meeting Rooms: Confidentiality & Countermeasures

STRICT FRAMEWORK

Meeting rooms are places where the most sensitive information of the organization circulates: M&A, strategy, HR discussions, R&D. Protecting the **confidentiality of these exchanges** against eavesdropping, indiscretion, and leakage is an obligation.

## Organizational Measures ("soft")

Formalized rules for sensitive meetings: strict control of room access, guest management, prohibition of unauthorized recording, personal phones in silent mode or outside depending on the sensitivity level.

## Technical Measures ("tech")

Complete inventory of equipment (videoconferencing, microphones, audio bars), regular firmware updates, hardening of configurations, dedicated network segmentation for room equipment.

## Inspection Measures

Periodic audits of the room and its equipment, search for technical anomalies (without resorting to illegal intrusive practices), verification of the integrity of cabling and devices.

**Deliverables:** "sensitive room" standard defining protection levels, checklists before and after each sensitive meeting, periodic audit reports.

# 34 — Awareness: Changing Behaviors

Technology is not enough — employees are both the **weakest link and the first line of defense**. An effective awareness program does not merely inform: it durably transforms behaviors.

## Program by Profiles

Content adapted to each audience: management (strategic risks), finance (payment fraud), HR (personal data), IT (technical threats), sales (social engineering on the go).

## Phishing Simulations

Regular exercises with personalized coaching — never "name & shame". The goal is learning, not punishment. Click-through rates decrease by **60 to 70%** after 12 months of the program.

## "Stop & Check" Culture

Simple and accessible reporting channel, rewarding good reflexes (reporting a suspicious email), positive communication. Security becomes a collective reflex, not a suffered constraint.

**Deliverables:** annual awareness plan, measured KPIs (phishing click-through rate, reporting rate, maturity score), personalized internal training materials.

# 35 — Internal Risk: Insiders (Intentional or Unintentional)

Internal risk is one of the most challenging threats to manage because it comes from individuals with **legitimate access** to systems and data. It covers a wide spectrum: from unintentional error to deliberate sabotage.

### Error & Negligence

Misconfiguration, sending data to the wrong recipient, loss of equipment, use of unapproved tools. The majority of internal incidents are not malicious.

### Privilege Abuse

Access to out-of-scope data, extraction for personal use, circumvention of controls, misuse of administrator rights.

### Exfiltration & Sabotage

Theft of intellectual property, data destruction, deliberate compromise — the rarest but most destructive cases.

## Technical Controls

- Strict least privilege and access reviews
- Exhaustive logging of actions
- UEBA alerts on atypical behaviors
- Temporary, tracked, validated, and expiring exceptions

## HR Processes

- Secure onboarding with initial awareness training
- Strict offboarding: access revoked **immediately**
- Contractual clauses and reminder of obligations
- Proactive management of sensitive departure situations

# 36 — Third-Party Security: Vendors & Partners

Every vendor, service provider, or partner connected to your systems represents an **extension of your attack surface.** Supply chain attacks are growing exponentially — SolarWinds, Kaseya, MOVEit are just the most publicized examples.

1

## Pre-contractual Evaluation

Structured security questionnaire, request for evidence (ISO 27001, SOC2 certifications, audit reports), definition of non-negotiable minimum requirements before signing.

2

## Contractual Clauses

Incident notification within 24 hours, transparency on subcontracting, data location, access to logs, authorization for security tests, reversibility, **right to audit**.

3

## Operational Monitoring

Annual compliance reviews, continuous monitoring of granted accesses, rotation of shared keys, dedicated network segmentation per partner.

4

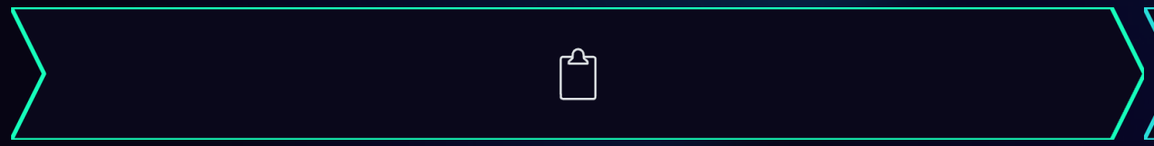
## Software Supply Chain

Evaluation of critical dependencies, identification of risky publishers, control of maintenance accesses, monitoring of updates.

**Deliverables:** comprehensive TPRM (Third Party Risk Management) program, risk scoring per vendor, remediation plans and corrective action tracking.

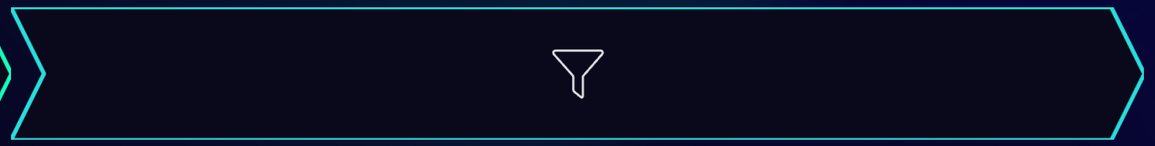
# 37 — Incident Response: contain quickly, investigate properly

The incident response capability determines whether a compromise remains a **manageable incident** or turns into a major crisis. Every minute counts — preparation makes the difference.



## Preparation

Playbooks per scenario (ransomware, BEC, leak, cloud compromise, insider), emergency contact list, 24/7 on-call, pre-deployed forensic tools.



## Detection & Triage

Real-time severity classification, prioritization of impacted critical services, activation of the appropriate response level according to the incident's scale.

## Containment

Isolate compromised systems, revoke tokens and sessions, force resets, apply blocks — **without destroying evidence** necessary for investigation.

## Forensics

Artifact collection, construction of the attack timeline, identification of root causes, assessment of impact perimeter, preservation of the chain of custody.

**Deliverables:** formalized IR plan, detailed operational procedures per incident type, post-incident reports with recommendations, improvement plan integrated into the security backlog.

# 38 — Business Continuity & Crisis: BCP/DR + Communication

Business continuity and crisis management are the **ultimate safety net** when all other layers of defense have been breached. The goal: maintain vital functions and communicate effectively under pressure.

## BIA (Business Impact Analysis)

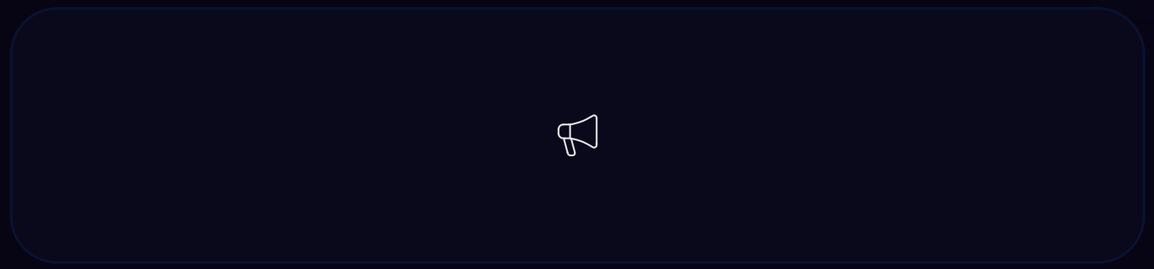
Identification of critical business processes, evaluation of financial and operational impacts of an interruption, definition of interruption tolerances (RTO/RPO) validated by management.

## DR Strategy

Redundancy of critical systems, tested restoration procedures, "clean room" environment in case of ransomware to rebuild on a healthy and verified basis.

## Exercises

Tabletop exercises with management (crisis simulation), technical restoration tests, internal and external communication exercises. Each exercise generates concrete improvements.



## Crisis Communication

Pre-written and validated messages, defined spokesperson roles, coordination with legal and cyber insurance. In a crisis, improvisation is the enemy — everything must be **prepared in advance**.

# 39 — Steering: KPI/KRI, Evidence & Continuous Improvement

What cannot be measured cannot be improved. Security steering relies on **objective indicators**, tangible evidence, and rigorous governance that transforms data into decisions.

## Operational KPIs

**99%**

MFA Coverage

Target on all critical accounts

**<48h**

Critical Patching Time

SLA for critical vulnerabilities

**100%**

EDR Deployment

Deployment on all endpoints

**<15min**

Detection Time

Target MTTD for critical incidents

## KRIs (Key Risk Indicators)

- **Excessive Privileges**: number of accounts with rights greater than needed
- **Public Exposure**: services and data accessible from the Internet
- **Orphan Accounts**: active identities without an identified owner
- **Missing Logs**: critical systems without active logging

## Audit Evidence

Signed policies, documented access reviews, restoration test reports, closed remediation tickets, formalized risk decisions — a complete corpus for any internal or external audit.

**Deliverables:** interactive CISO cockpit, ready-to-use audit pack, updated quarterly roadmap, monthly executive dashboard.

# 40 — Luxgap CISO Offering: What You Get

The Luxgap CISO offering is structured in **progressive phases** to maximize value from day one and build sustainable maturity. Each phase produces concrete and measurable results.

### 📋 Diagnosis — 30 days

Complete mapping of your environment, identification of priority risks, implementation of immediate impact quick wins, construction of the 90-day action plan. You know exactly where you are and where to go.

### 🛡️ Control Implementation — 90 days

IAM/MFA deployed, initial network segmentation, EDR on all endpoints, centralized log collection, immutable backups operational, IR playbooks activated. The **critical foundations** are in place.

### 🚀 Maturity Program — 6 to 12 months

ISO 27001/NIST maturity uplift, deployment of advanced SOC use cases, TPRM vendor program, DevSecOps integration, cloud posture hardening. Your security reaches a **certifiable level**.

### 👁️ Continuous Monitoring — ongoing

Brand/dark web/domain monitoring, external exposure surveillance, real-time alerting, executive reporting. Security lives, evolves, and adapts continuously.

**Operating Mode:** Shared "ownership" — Luxgap drives strategy, governance, and expertise, your teams execute with constant support and continuous skill transfer. The goal is your **long-term autonomy**, not dependence.

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