RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LEAD A SECURITY SUPERVISION PROJECT

Cyril Poirret
Agence Nationale de la Sécurité des Systèmes d'Information

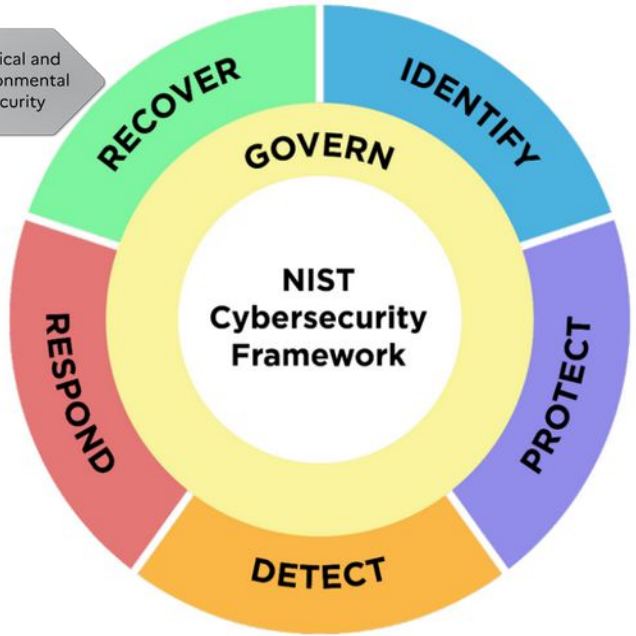
Preamble

- Who am I?
- What is security supervision?
  - It helps to know if IS (information systems) is under attack
  - At first, let’s consider security supervision ≈ detection ≈ SOC (security operation center)
  - This definition will be clarified during the presentation
- What is NOT security supervision?
  - ≠ IT monitoring, that helps to know if IS works, and if it delivers expected services
  - ≠ IT operation monitoring, IT services monitoring, relating to IT monitoring

Summary

An essential function of cybersecurity…

- **Governance**
  - Risk management framework
  - Manage ecosystem
  - Monitor vulnerabilities and threat
  - Assess and monitor security level
  - Manage human factor
- **Protection**
  - Information system architecture security
  - Data protection
  - Information system administration security
  - Identitiy and acces management
  - Maintain in operational and security condition
  - Physical and environmental security
- **Defense**
  - Sensors
  - Detection
  - Alert management and qualification
  - Incident response
- **Resilience**
  - Organize crisis management
  - Organize business continuity
  - Organize disaster recovery



…about which so much has been written

- Cybersecurity frameworks distinguish between:
  - Log management and analysis (NIST 800-92, CIS control 8, LPM rules 5 and 6, NIS rule 19)
  - Network detection (NIST 800-94, CIS control 13, LPM rule 7, NIS rule 18)
- Or deal with the whole incident lifecycle:
  - SIM3 (Security Incident Management Maturity Model): in terms of maturity
  - NIST 800-61r3 (Incidents Response Recommandations and…): in terms of risk management
- PDIS (prestataires de détection d'incidents de sécurité) requirements reference framework
  - cover logs, detection and analysis, but in terms of requirements
- Many articles cover technical aspects
- A strong commercial concern:
  - a wide range of offers, of concepts, and possible combinations
  - It sometimes creates gaps between needs and procurements

Summary

PREAMBLE

SECURITY SUPERVISION LANDSCAPE

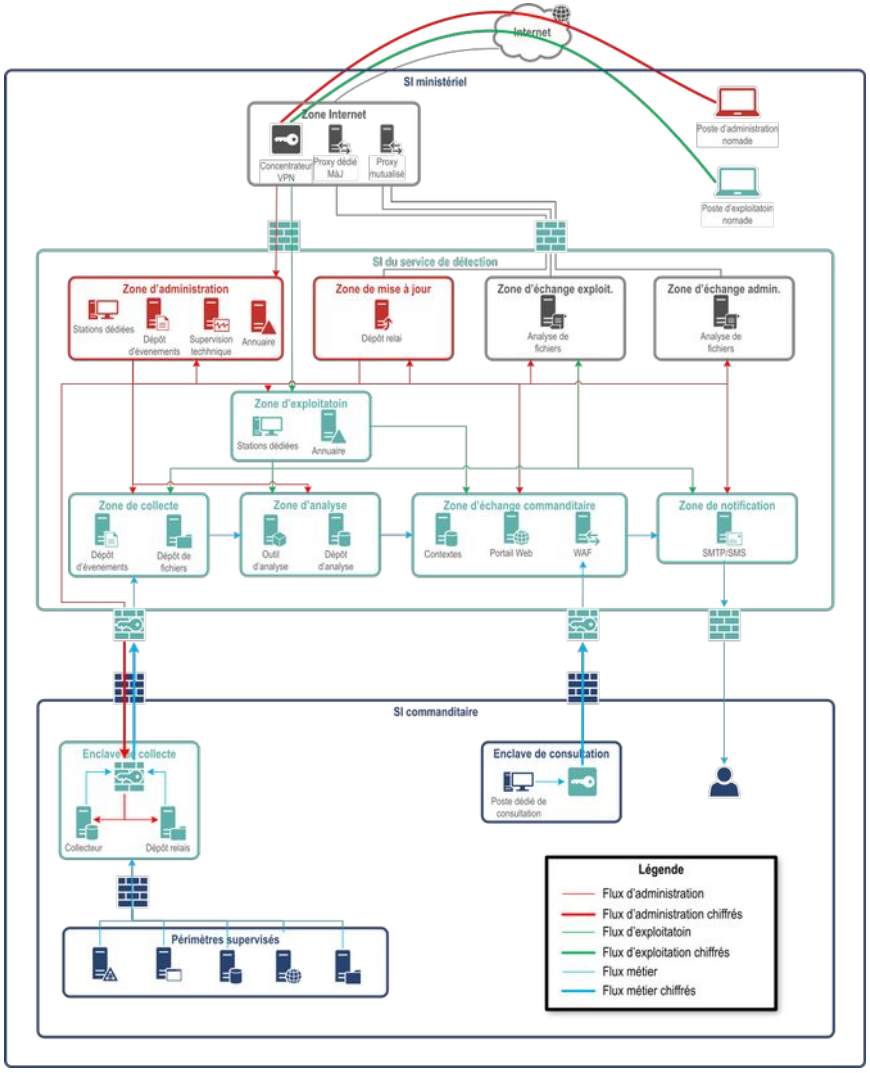
WORK ORIENTATIONS

GUIDE OVERVIEW

FOLLOW-UP

High expectations from the French ecosystem

- Service providers, editors, end users request changes
  - On the one hand, the PDIS framework improves cyber maturity
  - On the other hand, it is no longer suited to its environment
- First reaction: what about simplifying the PDIS framework?

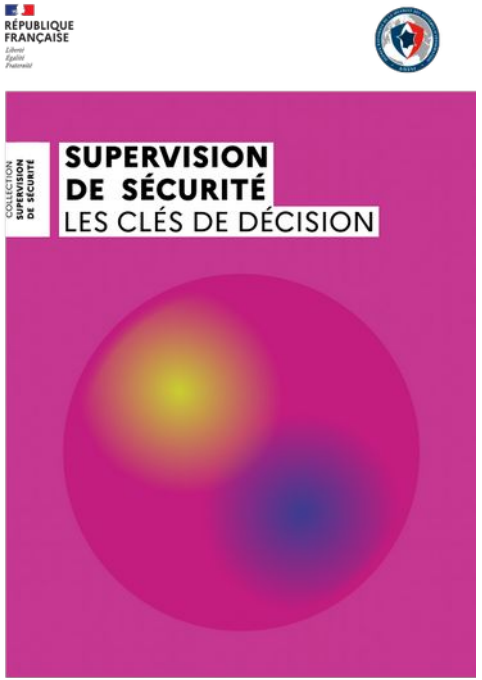

Internet
SI ministériel
Zone Internet
Concentrateur VPN
Proxy dédié MàJ
Proxy mutualisé
Poste d'administration nomade
Poste d'exploitatoin nomade
SI du service de détection
Zone d'administration
Stations dédiées
Dépôt d'évenements
Supervision techhnique
Annuaire
Zone de mise à jour
Dépôt relai
Zone d'échange exploit.
Analyse de fichiers
Zone d'échange admin.
Analyse de fichiers
Zone d'exploitatoin
Stations dédiées
Annuaire
Zone de collecte
Dépôt d'évenements
Dépôt de fichiers
Zone d'analyse
Outil d'analyse
Dépôt d'analyse
Zone d'échange commanditaire
Contextes
Portail Web
WAF
Zone de notification
SMTP/SMS
SI commanditaire
Enclave de collecte
Collecteur
Dépôt relais
Enclave de consultation
Poste dédié de consultation
Périmètres supervisés
Légende
Flux d'administration
Flux d'administration chiffrés
Flux d'exploitatoin
Flux d'exploitation chiffrés
Flux métier
Flux métier chiffrés

High expectations from French ecosystem

- Service providers, editors, end users request changes
  - On the one hand, the PDIS framework improves cyber maturity
  - On the other hand, it is no longer suited to its environment
- First reaction: what about simplifying the PDIS framework?
- A better choice: describe what security supervision should be
  - The raw material comes from 2.5 years of discussions
  - Internally: detection service, detection research laboratory, qualification advisors, architects, reviewers
  - Externally: qualified service providers, editors, end users, reviewers

High expectations from French ecosystem

- Service providers, editors, end users request changes
  - On the one hand, the PDIS framework improves cyber maturity
  - On the other hand, it is no longer suited to its environment
- First reaction: what about simplifying the PDIS framework?
- A better choice: describe what security supervision should be
  - The raw material comes from 2.5 years of discussions
  - Internally: detection service, detection research laboratory, qualification advisors, architects, reviewers
  - Externally: qualified service providers, editors, end users, reviewers
- Bonus: provide arguments to help obtain budgets



Summary

PREAMBLE

SECURITY SUPERVISION LANDSCAPE

WORK ORIENTATIONS

GUIDE OVERVIEW

FOLLOW-UP

Project management-oriented content

- Table of contents:
  - Definitions
  - Sub-objectives
  - Challenges/risks
  - Recommendations
- Possible uses:
  - Ease project leader’s work in a capacity building context
  - Establish a statement of requirements for service providers
  - Assess an existing service

Security supervision definition

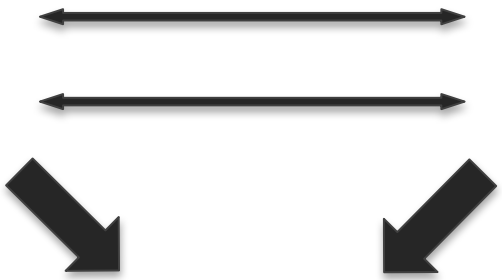
- All ressources and activities committed for,
- *as soon as possible*,

- **detect** and **qualify** a security incident on a supervised perimeter,
- and **choose the appropriate response** when the incident is confirmed.

- It involves human, organisational, technical and financial resources.

Security supervision strategy

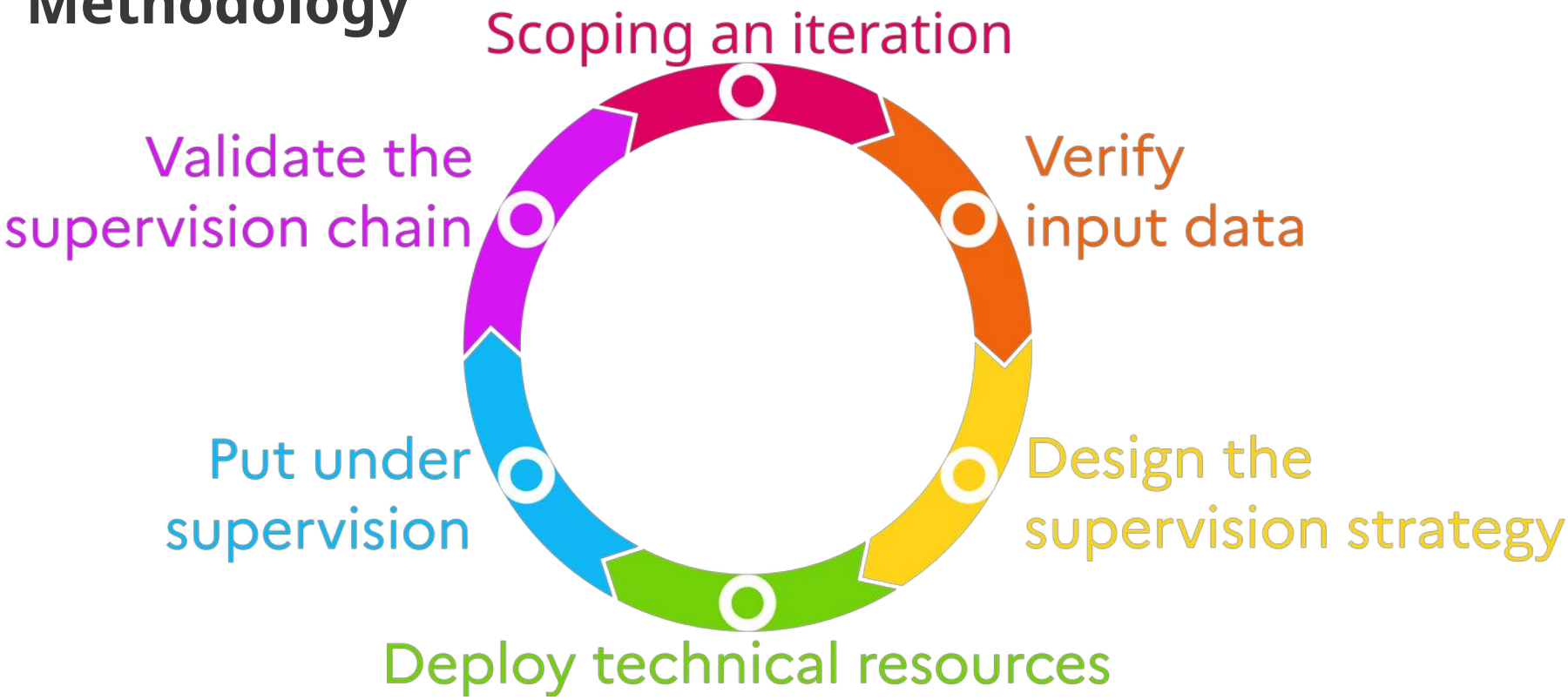
- Risk analysis
  - Identify feared events
  - Identify matching operational scenarios
  - Identify data produced by operational scenarios



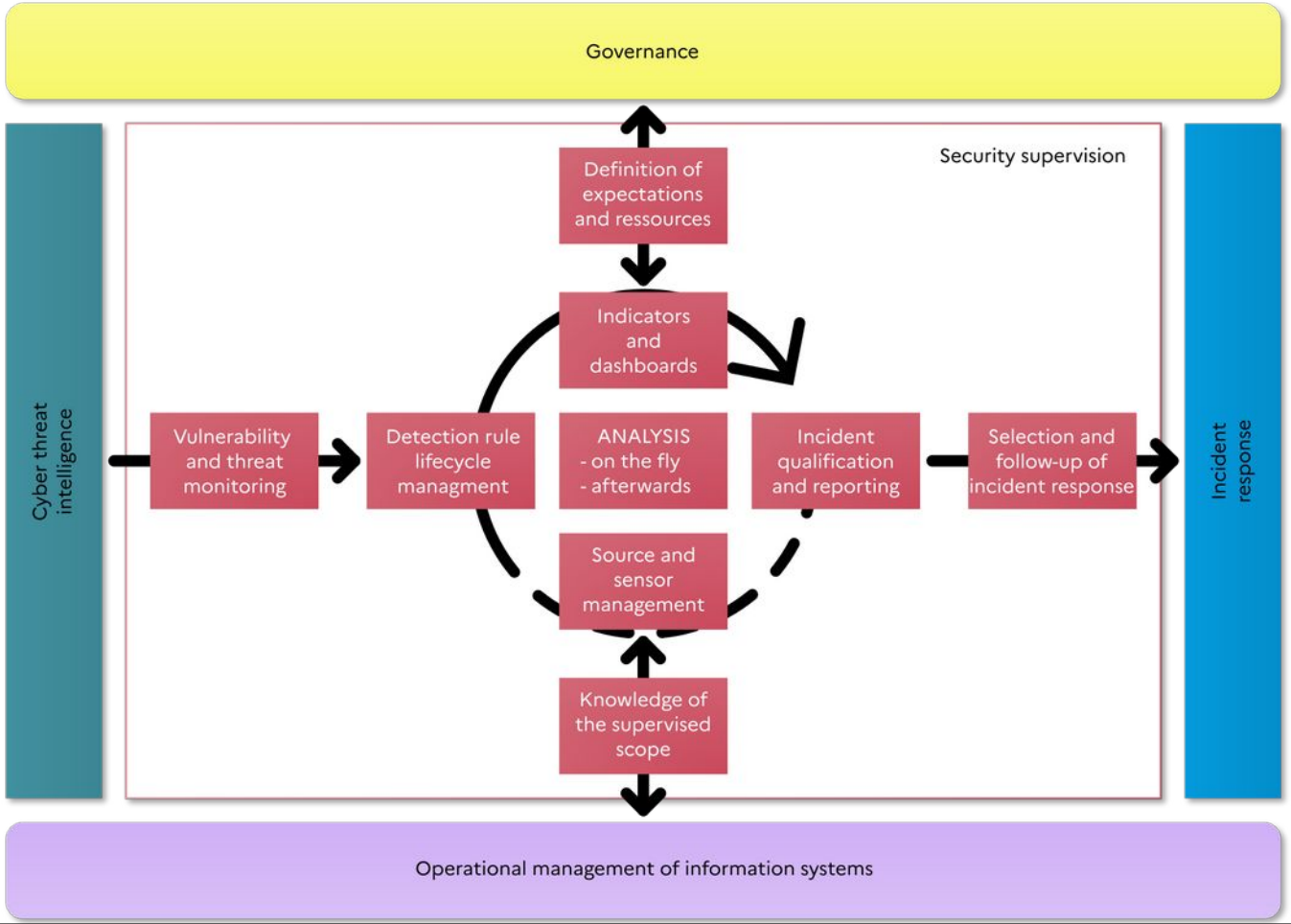
- Knowledge of the supervised scope
  - Family of data available or retrievable
  - Relevant collection point to detect feared events
  - Detection rules that take advantage of this data to detect feared events

- Align expectations with resources:
  - Prioritize scopes to cover
  - Prioritize data to collect for each scope
  - Prioritize technical ressources to deploy

Methodology



Process


Governance
Security supervision
Definition of expectations and ressources
Indicators and dashboards
Cyber threat intelligence
Vulnerability and threat monitoring
Detection rule lifecycle managment
ANALYSIS
- on the fly
- afterwards
Incident qualification and reporting
Selection and follow-up of incident response
Incident response
Source and sensor management
Knowledge of the supervised scope
Operational management of information systems

In summary

- Make security supervision and limit complex IT or governance tasks
  - As soon as possible
  - Even if it’s not perfect
- Allow analysts to gain experience
  - Understanding supervised scope
  - Starting process
- After that, improve supervision
  - Iteratively
  - In a process of continuous improvement

Summary

PREAMBLE

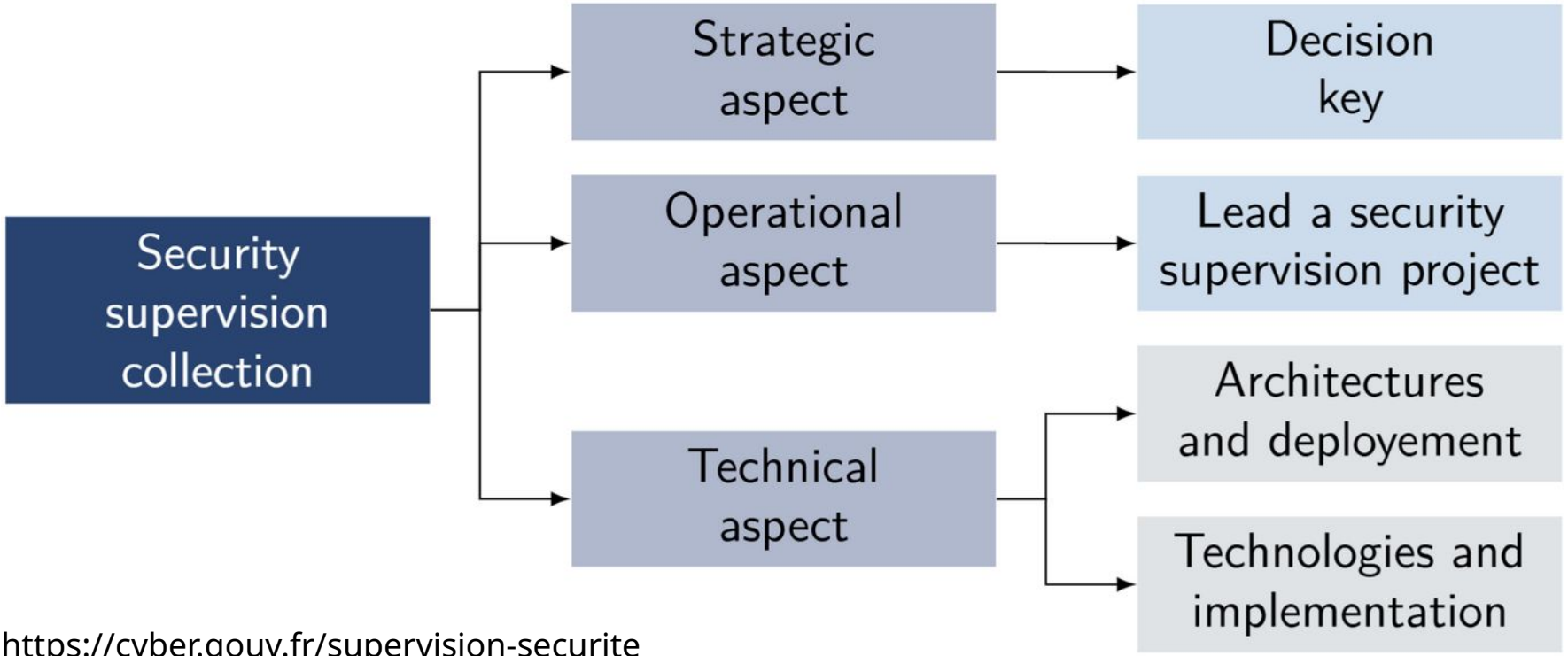
SECURITY SUPERVISION LANDSCAPE

WORK ORIENTATIONS

GUIDE OVERVIEW

FOLLOW-UP

Productions to come



https://cyber.gouv.fr/supervision-securite

Thank you for listening!

ANY QUESTIONS?