Consultant Cybersécurité

16/10/2025

Rémi ROMMELARD

Qui suis-je ?

ROMMELARD Rémi
Consultant (ACTEAM-IT)

Parcours Professionnel:

Formation initiale:

- BAC +3 Licence Science humaine Psychologie
- BAC +2 BTS informatique de gestion
- BAC +5 Chargé de projet en système informatique appliqué

Présentation du domaine métier

Qui s'imagine « défense » (blue), « attaque » (red), « gouvernance » (GRC) ?

Notre Objectif : démystifier le métier, donner des pistes concrètes pour débuter, répondre à toutes les questions.

La Sécurité est un moyen, pas une fin

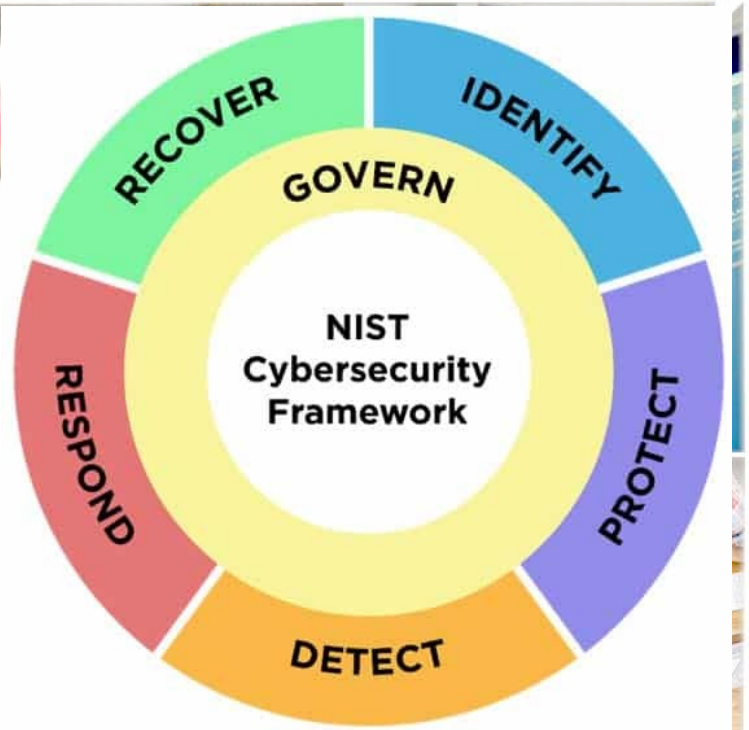
Présentation du domaine métier

Consultant cybersécurité
aider une organisation à réduire ses risques en alignant
méthodes, contrôles et techniques avec ses enjeux métier.

Terrain (tech) **et** gouvernance (risque/compliance).

Indépendance d'esprit, éthique stricte.

Présentation du domaine métier



LES 5 Fonctions : NIST CSF comme fil rouge

- Identify : carto des actifs, menaces, risques, exigences.
- Protect : IAM, durcissement, segmentation, sensibilisation.
- Detect : journaux, SIEM/XDR, use cases, chasse aux menaces.
- Respond : procédures, playbooks, cellules de crise, forensics.
- Recover : sauvegardes, PRA, amélioration continue.

À quoi ressemble une mission ?

- GRC / Risk : analyse de risques, gap ISO 27001/NIS2, PSSI, plan de remédiation.
- Blue Team : use cases SIEM, corrélations, chasse, durcissement endpoints, phishing interne.
- Red/Pentest : scoping, tests d'intrusion (autorisés !), rapports exploitables.
- AppSec/DevSecOps : SAST/DAST/SCA, revue de code, modèles de menaces, secrets.
- CloudSec : posture (CSPM), IAM, chiffrement, réseau, landing zone.
- IR/DFIR : investigation, containment, éradication, leçons tirées

Source : niceideas.ch

Une journée Type

9h : stand-up client, priorisation des risques.
10h : atelier cartographie + registre de risques.
14h : construction use cases SIEM + tableau de bord.
16h : sensibilisation / phishing simulation / débrief.
17h : reporting au sponsor (KRI/KPI) + prochaines actions.

Exemple de missions (Audit/Pentest)

Objectif : mesurer l'exposition & prioriser les remédiations

Audit (organisationnel & technique)

- Cadrage & périmètre (contexte, obligations NIS2/ISO, ROE)
- Cartographie des actifs & exposition externe (EASM)
- Revue de configuration : cloud/IAM/réseau/endpoints
- Évaluation de maturité : NIST CSF / ISO 27001 (gap analysis)
- Priorisation des risques (probabilité × impact) & plan 90 jours

Pentest (boîte noire/grise/blanche)

- Scoping, autorisations & règles d'engagement (ROE)
- Reconnaissance & énumération (OWASP/AD, services exposés)
- Exploitation contrôlée : injections, auth, élévation, latéralisation
- Post-exploitation & preuves (PoC), gestion de l'impact en test
- Rapport exploitable : risques, remédiations, quick wins, re-test

Livrables

- Executive summary (1 page)
- Rapport technique détaillé + PoC/évidences
- Plan de remédiation priorisé (90 jours)
- Restitution au management & équipes tech

KPIs / Résultats

- Vulnérabilités critiques trouvées (#)
- Temps de correction (MTTR vulnérabilité)
- Couverture du périmètre audité (%)
- Score de maturité / risque résiduel

Exemple de missions (Crises / Remédiation)

Objectif : contenir, éradiquer, reconstruire & capitaliser

Gestion de crise / DFIR

- Activation cellule de crise & rôles (RACI), journal d'événements
- Containment : isolement endpoints, blocage IOC, segmentation
- Forensics : acquisition, timeline, IOC/TTP (MITRE ATT&CK)
- Communication : juridique/DPO/assureur/autorités (CERT-FR/ANSSI)
- Retour à la normale planifié & suivi de risque résiduel

Remédiation & durcissement

- Correctifs & réinstallation immaculée (golden images, clés propres)
- Rotation secrets/identités, MFA, durcissement AD/Azure AD
- Sauvegardes : 3-2-1, immutables, tests PRA réguliers
- Use cases SIEM, règles EDR, blocage latéral, détection exfiltration
- Leçons tirées & plan 30-60-90 jours (priorisé, budgété)

Livrables

- Timeline d'incident & rapport d'investigation (IR/DFIR)
- Liste IOC (hash/URL/IP), règles détection (Sigma/EDR)
- Playbooks de réponse mis à jour
- Plan de remédiation & supervision renforcée

KPIs / Résultats

- MTTR incident, dwell time (temps de présence)
- % parc remédié / re-imaged
- Taux de succès des restaurations testées
- Couverture use cases SIEM/EDR

Compétences Coeur

- Tech : Linux/Windows, réseau, IAM, logs/EDR/XDR/SIEM, SAST/DAST/SCA, cloud (AWS/GCP/Azure), scripting (Bash/Python), crypto appliquée (PKI, TLS, chiffrement).

- Méthodo & soft skills : analyse de risques, cadrage, pédagogie, vulgarisation, éthique, rédaction et présentation de synthèse, conduite du changement.

Outillage Type

- Défense : EDR/XDR, SIEM, SOAR, IDS/WAF, vuln manager.
- AppSec : SAST/DAST/SCA, secrets scan, SBOM.
- CloudSec : CSPM/CWPP/IAM analyzer, Key Vault, KMS.
- GRC : risk register, politiques, audits.
- IR : sandbox, forensic suite, timelines.

Eviter la « tool » fatigue >> Partir d'objectifs et de cas d'usage

CYBER SCAPE 2020

Network & Infrastructure Security

Advanced Threat Protection

ICS + OT

NAC

SDN

DDoS Protection

DNS Security

Network Firewall

Deception

Network Analysis & Forensics

Web Security

Endpoint Security

Endpoint Prevention

Endpoint Detection & Response

Application Security

WAF & Application Security

Application Security Testing

MSSP

Traditional MSSP

Advanced MSS & MDR

Data Security

Encryption

DLP

Data Privacy

Data Centric Security

Mobile Security

Risk & Compliance

Risk Assessment & Visibility

Security Ratings

Pen Testing & Breach Simulation

GRC

Security Awareness & Training

Security Operations & Incident Response

SIEM

Security Incident Response

Security Analytics

Momentum Cyber

Threat Intelligence

IoT

IoT Devices

Automotive

Connected Home

Messaging Security

Identity & Access Management

Authentication

IDaaS

Privileged Management

Identity Governance

Consumer Identity

Digital Risk Management

Security Consulting & Services

Blockchain

Fraud & Transaction Security

Cloud Security

Infrastructure

Container

CASB

IA ↔ CYBER

IA au service de la cyber

détection d'anomalies, triage d'alertes, génération de runbooks, aide à la corrélation.

Cyber au service de l'IA

protection des données/propriété intellectuelle, gouvernance des modèles, sécurité des pipelines ML (accès, secrets, registres), surveillance du drift et de la fraude

Garde-fous : ne jamais coller de secret dans un outil IA; test en environnements isoles, revue humaine toujours obligatoire

Portfolio Etudiant

Blue : écrire 3 use cases SIEM + un petit **runbook** d'alerte.
Red : lab maison + **rapport** de pentest pédagogique (autorisations !).
AppSec : pipeline CI avec SAST/SCA + **fix** documenté.
GRC : mini **registre de risques** + **PSSI** d'1 page + plan 90 jours.
CloudSec : *landing zone* minimal + **CSPM report** avant/après.
Références d'entraînement : labs/CTF, TryHackMe/HackTheBox (tracks débutant → intermédiaire), BlueTeam labs.

Ethique & légal

Tests uniquement en lab ou sous contrat écrit.

Respecter données perso, propriété intellectuelle, secret pro.

Transparence, blameless post-mortem orienté amélioration

Erreurs Fréquentes

Confondre conformité et sécurité (checklist ≠ protection).

Empiler des outils sans use cases ni métriques.

Oublier inventaire / journalisation / sauvegardes testées.

Rapports trop techniques, pas de synthèse pour décideurs.

Qu'apporte le métier?

Au business

- Réduit la probabilité/impact d'incidents
- Accélère les projets
- Optimise les coûts : priorisation risque, moins de « tool fatigue »

Gouvernance & conformité

- Alignement NIS2 / ISO 27001 / RGPD avec preuves d'audit
- Maîtrise des données (PII, secrets) & des tiers (clauses sécu)

À l'IT / Produit

- Durcissement (IAM, segmentation, patching), CI/CD sécurisé, observabilité utile
- Moins de bruit d'alertes, MTTR ↓, sauvegardes & PRA testés

À la culture

- Sensibilisation qui réduit le risque humain
- Runbooks, exercices de crise, post-mortems blameless → réflexes & partage

Quelles sont les perspectives d'évolution du métier

IC/praticien

Pentester/Red → Red Lead
Blue/DFIR → Threat Hunter/IR Lead
AppSec → Product Security
CloudSec → Security Engineer/Architect
GRC → Senior Risk/ISO 27001 Lead.

Leadership / produit

SecOps/Red/Blue Manager
Head of Security/Platform
RSSI/CISO
Conseil indépendant.

Évoluer = augmenter l'**impact** (périmètre, fiabilité, acculturation), pas collectionner des badges.

- **Cadres** : NIST CSF, ISO 27001/27005, guides ANSSI, OWASP Top 10/ASVS.
- **Pratique** : Purple Teaming, Sigma rules, MITRE ATT&CK, Atomic Red Team.
- **Veille** : CERT-FR, blogs éditeurs, podcasts Sécu, newsletters (SANS, TL;DR Sec).

Questions/Réponses