Entretien Sopra Steria - SOC Analyst

26 fevrier 2026 a 14h00 | 6 Questions RH Insider | Maxime LAUNOY

A NE JAMAIS DIRE :

- "J'ai toujours ete passionne par la cybersecurite depuis tout petit"
- "Je gere un SIEM au quotidien" / "J'analyse des alertes tous les jours"
- "Je suis expert en..." quoi que ce soit en SOC
- "Mon poste chez Harvest c'etait nul/ennuyeux" (dire "plus statique" ou "oriente conformite")
- "C'est bien paye la cyber"
- "Mes collegues du SOC m'ont dit que..."
- Ne pas mentionner le prix des outils IA (100$/mois)

Si on te demande la pause depuis sept 2024 :

Version courte : "Apres mon alternance en septembre 2024, j'ai pris du recul pour definir mon orientation. J'ai travaille sur des projets personnels, notamment autour de la crypto et de la blockchain, et j'ai approfondi mes competences techniques en securite. Depuis la rentree 2025, je me suis focalise sur la recherche d'un poste en SOC parce que c'est le cote investigation et analyse qui m'interesse."

Si insistance : "J'ai fait du trading crypto ce qui m'a amene a faire de la tracabilite de wallets, j'ai monte un homelab pour pratiquer, et j'ai pris le temps de cibler precisement le type de poste que je voulais. Je ne voulais pas accepter n'importe quoi juste pour travailler."

Q1 Qu'avez-vous appris par vous-meme lors de vos differentes missions, sans que cela soit demande par votre management ?

De quoi je parle :

- Sondes PRTG a installer sur 100+ VM a la main → j'ai appris Ansible tout seul pour automatiser
- PowerShell + API PRTG pour deployer les sondes
- J'ai monte un env de test en local avant (serveur PRTG test + VM test) → prudence
- Solution retenue et utilisee en prod
- SIEM : j'ai demande a la SSI d'avoir acces par curiosite, ils m'ont forme
- Alertes non complexes traitees → ca m'a donne envie du SOC

Ce que j'ai le plus appris par moi-meme, c'est a prendre des initiatives quand une tache peut etre optimisee.

Exemple concret : on m'a demande d'installer manuellement des sondes PRTG sur des machines virtuelles hors couverture de monitoring. C'etait une tache repetitive sur plus de 100 VM. Plutot que de le faire a la main, j'ai pris le temps d'apprendre Ansible par moi-meme pour automatiser le deploiement. J'ai scripte en PowerShell via l'API de PRTG pour deposer les sondes, et utilise Ansible pour modifier les configurations sur chaque machine au prealable.

Et surtout, comme je debutais sur ces outils, j'ai eu le reflexe de monter un environnement de test en local : un serveur PRTG de test, des VM de test, pour valider ma solution avant de la proposer. La solution a ete retenue et utilisee en production.

L'autre chose que j'ai apprise par curiosite, c'est la prise en main du SIEM. Mon poste etait oriente securite operationnelle : hardening, conformite ISO 27001, veille, patch management. Mais on travaillait en proximite avec la SSI qui gerait le SIEM. J'ai demande a avoir acces, ils nous ont formes et laisse traiter des alertes non complexes. C'est cette curiosite pour le cote investigation qui m'a donne envie d'en faire mon metier.

Conseil : Commence par Ansible/PRTG (le plus fort). SIEM en deuxieme couche, plus court. Dis "repetitif" jamais "chiant".

Ansible + PRTG + API sur 100+ VM | Env de test en local = rigueur | Solution retenue en production | SIEM par curiosite = transition SOC

Q2 Si on vous avait donne carte blanche, quel est le premier point que vous auriez ameliore dans votre derniere mission ?

De quoi je parle :

- Veille vulne : chaque semaine, eplucher les bulletins CERT manuellement
- Pour chaque CVE : verifier si ca concerne nos outils, comparer les versions
- Creer les fiches Jira une par une, rapport hebdo au COMEX + comite secu
- J'aurais voulu : systeme qui croise auto bulletins CERT x inventaire assets/versions
- Detection auto de ce qui nous concerne, pre-generation des fiches
- Avec l'IA c'est faisable maintenant → l'analyste se concentre sur l'analyse, pas la collecte

Si j'avais eu carte blanche, j'aurais automatise le processus de veille vulnerabilites.

Chaque semaine, je devais passer plusieurs heures a eplucher manuellement les bulletins du CERT, verifier pour chaque CVE si elle concernait un outil de notre parc, comparer les versions pour savoir si on etait impacte, puis creer les fiches Jira une par une. Tout ca alimentait un rapport hebdomadaire presente au COMEX et au comite de securite.

Ce que j'aurais aime construire, c'est un systeme qui croise automatiquement les bulletins CERT avec notre inventaire d'assets et de versions. A chaque nouvelle publication, il detecte ce qui nous concerne, flag les versions impactees, et pre-genere les fiches. Le rapport serait alimente automatiquement avec les donnees complementaires comme l'etat des sauvegardes.

Aujourd'hui avec l'IA et les outils disponibles, c'est tout a fait faisable. C'est le genre de tache repetitive a forte valeur ajoutee qui merite d'etre automatisee pour que l'analyste se concentre sur l'analyse et la remediation plutot que sur la collecte.

Conseil : Dis "chronophage" jamais "relou". Insiste que tu aurais VOULU le faire mais le temps manquait = frustration constructive.

Veille CERT manuelle = pain point concret | Chaine : CERT → CVE → Jira → COMEX | Solution realiste proposee | Mindset d'optimisation

Q3 Pourquoi avez-vous choisi la cybersecurite ? Qu'est-ce qui vous motive ? (challenge sincerite + CTF)

De quoi je parle :

- Numerique + jeux video depuis petit → informatique = chemin naturel
- Declic a l'INSA pendant les cours cyber
- Ce qui motive : le cote investigation, remonter un fil, escape game / enquete
- Chez Harvest j'ai touche au SIEM par curiosite → c'est la que j'ai accroche
- Role precedent trop oriente conformite, je veux du dynamique
- IA x cyber : me fascine et m'inquiete (attaques evolvent, fuites de donnees)
- CTF : honnete, pas un acharne, j'en fais quand le theme accroche (ex: Resident Evil)
- Si challenge CTF → "je trace des wallets sur Solscan/Etherscan = OSINT blockchain"

J'ai grandi dans le numerique et les jeux video, donc l'informatique c'etait le chemin naturel. C'est a l'INSA pendant les cours de cybersecurite que le declic s'est fait.

Ce qui me motive, c'est plusieurs choses. D'abord le cote investigation. Quand j'ai pu toucher au SIEM chez Harvest par curiosite, j'ai retrouve ce que j'aime : comprendre ce qui s'est passe, remonter un fil, c'est comme un escape game ou une enquete. C'est stimulant intellectuellement. Et c'est justement ce que je ne retrouvais pas assez dans mon role precedent qui etait plus oriente conformite.

Ensuite, c'est un domaine qui ne stagne jamais. L'intersection avec l'IA par exemple me fascine autant qu'elle m'inquiete. On voit que les attaques evoluent, que les fuites de donnees deviennent regulieres, et je trouve qu'il y a un vrai sens a proteger les gens dans ce contexte.

Pour etre honnete, je ne suis pas un acharne de CTF. J'en fais quand le theme m'accroche, par exemple un CTF sur le theme Resident Evil, c'est fun. Mais ce qui me drive au quotidien c'est plus le cote defense et utilite concrete que le cote competition.

Conseil : Ne surjoue PAS la passion. L'honnetete CTF est ta meilleure arme.
Si challenge CTF : "Mon cote investigation, je le pratique autrement : en crypto je trace des wallets sur Solscan et Etherscan, c'est de l'OSINT blockchain. Et chez Harvest j'ai demande a acceder au SIEM par curiosite." = moment de glisser l'OSINT.

Jeux video → INSA → declic | Investigation = escape game | IA x cyber = fascination | CTF assume, pas acharne | Si challenge → OSINT blockchain

Q4 Question technique : lecture de logs, decrire ce qui se passe et quels pivots vous feriez

De quoi je parle :

- 1. OBSERVER 5 sec : source du log, timestamp, IP/user, action, resultat
- 2. DECRIRE en 1 phrase : "je vois X evenements de type Y depuis [source]..."
- 3. PIVOTER : "je pivoterais sur [IP/user/hash] pour chercher..."
- 5 codes : 4624=login OK, 4625=echec, 4672=admin, 7045=service, 1102=logs effaces
- Pivots : IP → reputa VT/AbuseIPDB | User → autres actions | Process → parent/LOLBins | Hash → VT
- Vocabulaire a placer : IOC, pivoter, chaine d'execution, mouvement lateral, C2, TTPs, triage
- Si je connais pas un code : "je vois dans le message que..." + "je verifierais dans la doc"
- **Cas 1 Brute Force :** 4x 4625 + 1x 4624 meme IP = brute force reussi → pivot IP, hostname, threat intel
- **Cas 2 SQL Injection :** GET avec OR 1=1 puis UNION SELECT, tailles reponses croissantes = injection qui marche → bloquer IP, contacter equipe app, WAF
- **Cas 3 Sysmon/C2 :** cmd → powershell -enc (base64) + connexion sortante IP externe = C2 → decoder base64, reputation IP, remonter parent process

METHODO EN 3 ETAPES :

1. OBSERVER (5 sec) : Source du log ? Timestamp ? Acteurs (IP, user) ? Action ? Resultat ?
2. DECRIRE : "Je vois X evenements de type Y, depuis [source] vers [dest], entre [heure] et [heure]."
3. PIVOTER : "Pour confirmer, je pivoterais sur [element] pour chercher [quoi]."

5 EVENT CODES A CONNAITRE :
4624 = Login OK | 4625 = Login ECHOUE | 4672 = Droits admin | 7045 = Service installe | 1102 = Logs effaces

PIVOTS CLASSIQUES :
IP suspecte → autres connexions, geoloc, reputation (VirusTotal, AbuseIPDB)
User compromis → autres actions, horaires inhabituels
Process suspect → chaine d'execution, parent process, LOLBins
Hash de fichier → reputation VT, autres machines avec ce hash

VOCABULAIRE A PLACER : IOC, pivoter, chaine d'execution, mouvement lateral, C2, LOLBins, TTPs, triage

========== **CAS CONCRET 1 : BRUTE FORCE** ==========

EventCode=4625 Account_Name=j.martin Src_IP=185.220.101.34 (x4)
EventCode=4624 Account_Name=j.martin Src_IP=185.220.101.34

Tu dis : "Je vois 4 evenements 4625, des echecs d'authentification, sur le compte j.martin, suivis d'un 4624, un login reussi, le tout depuis la meme IP externe en quelques secondes. C'est un brute force reussi.
Pivots : 1) IP source → a-t-elle cible d'autres comptes ? 2) Hostname cible → que s'est-il passe apres le login ? 3) Threat intel → verifier cette IP sur VirusTotal ou AbuseIPDB."

========== **CAS CONCRET 2 : SQL INJECTION** ==========

185.43.12.8 "GET /search?q=test' OR 1=1--" 200 4532
185.43.12.8 "GET /search?q=test' UNION SELECT username,password FROM users--" 200 8921

185.43.12.8 "GET /search?q=test' UNION SELECT credit_card,cvv FROM payments--" 200 12340

Tu dis : "Je vois des requetes GET depuis la meme IP avec des payloads SQL injection. OR 1=1 c'est un test classique, puis UNION SELECT pour exfiltrer users puis payments. Les tailles de reponse croissantes (4K, 8K, 12K) suggerent que l'injection fonctionne.
Pivots : verifier tous les endpoints cibles par cette IP, contacter l'equipe applicative, bloquer au WAF, verifier si data breach potentiel."

Splunk : index=web src_ip="185.43.12.8" | where like(uri_query, "%UNION%") OR like(uri_query, "%OR 1=1%")

========== **CAS CONCRET 3 : EXECUTION SUSPECTE (Sysmon/C2)** ==========

EventCode=1 ParentImage="cmd.exe" Image="powershell.exe"
CommandLine="powershell -enc aQBlAHgAIAAoAG4AZQB3AC0A..." User="CORP\j.dupont"
EventCode=3 Image="powershell.exe" DestIP=91.234.56.78 DestPort=443

Tu dis : "cmd.exe lance PowerShell avec un argument encode en base64 (-enc). C'est un indicateur classique d'execution malveillante. Juste apres, ce PowerShell etablit une connexion sortante vers une IP externe port 443 : ca ressemble a du C2.
Pivots : decoder le base64, verifier la reputation de l'IP, pivoter sur le user j.dupont (phishing ?), remonter le parent process de cmd.exe, chercher si d'autres machines contactent cette IP."

Splunk : index=windows sourcetype=sysmon EventCode=1 CommandLine="*powershell*-enc*"

> **Conseil :** Prends 5 secondes avant de parler. Le PIVOT est plus important que la lecture initiale. Propose toujours au moins 3 pivots. Si tu ne reconnais pas un code, dis "je vois dans le message qu'il s'agit de..." et montre ta methodo.

Observer → Decrire → Pivoter | Minimum 3 pivots concrets | 5 EventCodes par coeur

Pas grave si tu connais pas, montre la methodo

Q5 Quel est votre point de vue sur l'IA et l'utilisez-vous aujourd'hui ? Si oui, pourquoi ?

De quoi je parle :

- Tres favorable, utilisation quotidienne, c'est un AMPLIFICATEUR (pas un remplacement)
- Precautions : jamais de donnees confidentielles, modeles locaux si besoin
- Outils : Claude Code au quotidien + veille sur les nouveaux modeles
- Projet 1 : SaaS trouverunprof.com (auth multi-roles, calendrier, paiement CB, notifs)
- Projet 2 : outil recherche emploi en local (scraping, analyse compatibilite, CV adaptes, suivi)
- Case study dispo si ca interesse
- Lien cyber : IA x securite, attaques massifiees cote attaquant, detection patterns cote defenseur

Je suis tres favorable a l'IA et je l'utilise au quotidien. Pour moi c'est un amplificateur : gain de temps, gain de creativite, et surtout un accelerateur d'apprentissage. Evidemment avec des precautions, notamment en contexte professionnel, ne jamais y injecter de donnees confidentielles, privilegier des modeles locaux quand c'est necessaire. Le facteur humain reste central, l'IA assiste mais ne remplace pas.

Concretement, j'utilise des outils comme Claude Code au quotidien et je fais beaucoup de veille sur les nouveaux modeles et les nouvelles pratiques pour en tirer le maximum.

Exemples concrets de projets realises :

1) SaaS complet : trouverunprof.com, plateforme de mise en relation professeurs/etudiants. Authentification multi-roles, calendrier, paiement par CB avec credits, notifications. Construit de A a Z, en securisant donnees et transactions.

2) Outil d'automatisation de recherche d'emploi en local : scraping d'offres, analyse de compatibilite, generation de CV adaptes (angle d'approche, pas contenu), tableau de suivi. Case study documente disponible.

Pour le lien cyber : l'intersection IA et cyber me passionne. Cote attaquant, l'IA va permettre des attaques massifiees. Cote defenseur, il faudra utiliser l'IA pour detecter les patterns et anticiper. C'est un sujet sur lequel je compte me former activement.

Conseil : Ne cite PAS le prix (100$/mois). Dis "j'investis dans des outils professionnels". Le mot "amplificateur" = tu restes maitre. Propose le case study naturellement sans forcer.

Amplificateur, pas remplacement | Precaution donnees confidentielles = reflexe secu | SaaS trouverunprof.com = livre | Outil emploi = mindset automatisation | Vision IA x cyber

Q6 Avez-vous des hobbies ou activites personnelles qui vous servent dans votre travail ?

De quoi je parle :

- Builder : je vais voir mes proches, "quel probleme tu veux automatiser ?", et je le construis
- Exemple : trouverunprof.com pour ma fiancee (plateforme prenait trop de frais)
- Blockchain + DeFi : terrain d'entrainement secu en conditions reelles
- Attaques permanentes : drains, phishing, faux smart contracts → argent en jeu directement
- Cold wallet physique : cles privees hors ligne, separation wallets, verif chaque transaction
- Tracer des wallets sur Solscan/Etherscan, suivre flux de transactions
- Correlation comptes Twitter / adresses crypto = OSINT blockchain
- Meme etat d'esprit que SOC : vigilance, analyser, pivoter, remonter une piste
- Musculation : clarte mentale pour le travail d'analyse

Mon principal hobby c'est de construire des solutions concretes pour resoudre des problemes autour de moi. Je vais voir mes proches, je leur demande quel probleme ils aimeraient automatiser, et je le construis. C'est comme ca qu'est ne trouverunprof.com pour ma fiancee.

L'autre activite qui me sert enormement, c'est la blockchain et la DeFi. Je suis tres actif dans cet ecosysteme et honnetement, c'est un terrain d'entrainement a la securite en conditions reelles. En DeFi, les tentatives d'attaque sont permanentes : drains de wallets, phishing cible, faux smart contracts. Les gens attaquent pour acceder directement a ton argent, donc l'enjeu est immediat.

D'ailleurs je stocke mes cryptos sur des cold wallets physiques. Cles privees hors ligne, separation des wallets, verification de chaque transaction. C'est de l'hygiene de securite appliquee a mes propres finances.

Concretement ca m'amene a tracer des wallets sur Solscan et Etherscan, suivre des flux de transactions, et parfois faire de la correlation entre des comptes Twitter et des adresses crypto. C'est de l'OSINT applique a la blockchain.

L'etat d'esprit c'est exactement le meme qu'en SOC : etre vigilant en permanence, analyser ce qu'on voit, pivoter d'un element a l'autre pour remonter une piste. Sauf qu'en DeFi, c'est mon propre argent qui est en jeu.

Sinon cote physique, la musculation regulierement, ca aide a garder la clarte mentale pour un travail d'analyse.

Conseil : C'est ta reponse la plus puissante. N'oublie JAMAIS la crypto.
Si le recruteur rebondit sur l'OSINT : "En DeFi on fait de l'OSINT en permanence sans forcement le nommer. Tracer un wallet, correler une adresse avec une identite, analyser un smart contract suspect, c'est le meme reflexe que d'enrichir un IOC en SOC. Les outils sont differents mais la demarche d'investigation est identique." Laisse-le parler apres, il va partager son interet.

Builder = proactif | DeFi = securite en conditions reelles | Cold wallet = hygiene secu | Solscan/Etherscan = OSINT blockchain | Correlation Twitter/wallet = OSINT | "Mon propre argent" = sincerite

Recap : Fil rouge de toutes tes reponses

Question	Ton angle fort	Piege a eviter

Q1 Appris seul	Ansible + PRTG + env de test	Ne pas trop detailler, reste concis
Q2 Carte blanche	Automatisation veille CERT/CVE	Dis "chronophage" pas "relou"
Q3 Pourquoi cyber	Investigation = escape game + honnetete CTF	Ne surjoue pas la passion
Q4 Lecture logs	Methodo : observer, decrire, pivoter	Prends 5 sec avant de parler
Q5 IA	Projets concrets (SaaS, outil emploi)	Ne cite pas le prix, dis "outils pro"
Q6 Hobbies	Builder + crypto/OSINT blockchain + cold wallet	N'oublie pas la crypto !

Ton fil rouge : tu prends des initiatives, tu automatises, tu investigues par curiosite. C'est exactement le profil SOC.