SOC LEVEL 1 ESSENTIALS – PART F: CYBERSECURITY FOUNDATIONS (POSTS 46–50)

Essential Cryptography, Security Concepts, and Analyst Skills for SOC Foundations

SEPTEMBER 12, 2025

INAAM KABBARA
SECURITY ANALYST | CYBERSECURITY CONTENT CREATOR | EPITA MSC GRADUATE

Table of Contents

1- Hashing vs Encryption – Know the Difference

Both protect data but serve different purposes
Understanding their roles helps you detect misconfigurations
Have you ever spotted weak hashes or missing encryption in your logs?

What's the difference?
Encryption = Reversible protection of data
→ Used for confidentiality (e.g., TLS, PGP, disk encryption)
→ Requires a key to decrypt
→ Two types: Symmetric (same key) & Asymmetric (public/private)
Hashing = Irreversible data fingerprint
→ Used for integrity (e.g., password storage, file verification)
→ One-way only – can't decrypt a hash
→ Example algorithms: SHA256, bcrypt

Why it matters in SOC
✓ Spot plaintext credentials or weak hashes (e.g., MD5)
✓ Validate encrypted vs unencrypted traffic in packet captures
✓ Monitor hash types in SIEM alerts
✓ Check file hashes to verify integrity

Quick Examples
Encryption Use Cases
TLS in HTTPS traffic
PGP for secure emails
VPN or encrypted backups
Hashing Use Cases
Password storage with SHA256 + salt
File integrity check during malware analysis
Log tampering detection

Pro Tip
If you see passwords stored in plaintext or MD5 without salt — escalate it. It's a vulnerability.

Have you validated hashes or analyzed encrypted traffic during investigations?

Hachage vs cryptage : connaître la différence

🔐 Quelle est la différence ?

Chiffrement = Protection réversible des données

➞ Utilisé pour la confidentialité (ex : TLS, PGP, sauvegardes)

➞ Fonctionne avec une clé

➞ Deux types : symétrique et asymétrique

Hachage = Empreinte irréversible d'une donnée

➞ Utilisé pour l'intégrité (ex : mot de passe, vérification de fichier)

➞ Impossible de retrouver la donnée d'origine

➞ Exemples : SHA256, bcrypt

🔐 Pourquoi c'est utile en SOC

✓ Détecter les mots de passe en clair

✓ Identifier les algorithmes faibles (ex : MD5)

✓ Vérifier si le trafic est chiffré ou non

✓ Contrôler l'intégrité de fichiers suspects

📊 Exemples concrets

🟩 Cas d'usage du chiffrement

TLS dans le trafic HTTPS

PGP pour les emails sensibles

VPN ou sauvegardes chiffrées

🟩 Cas d'usage du hachage

Stockage des mots de passe avec SHA256 + salt

Vérification d'intégrité des fichiers (ex : analyse de malwares)

Détection de falsification des logs

🤓 Astuce

Un hash MD5 sans salt ou un mot de passe visible ? → Alerte immédiate 🚨

💬 Avez-vous déjà validé un hash ou analysé un flux chiffré ?

HASHING VS ENCRYPTION

HASHING

- Irreversible data fingerprint
- Used for integrity (e.g., password storage, file verification)
- One-way only – can't decrypt a hash

ENCRYPTION

- Reversible protection of data
- Used for confidentiality (e.g., TLS, PGP, disk encryption)
- Requires a key to decrypt

INAAM

2- Symmetric vs Asymmetric Cryptography – Key Differences

Understand encryption methods and how keys work in each case
This helps you assess data confidentiality and secure communications
Have you ever analyzed encrypted traffic or key exchange mechanisms?

What's the difference?
Symmetric Cryptography
➞ Uses one key to encrypt and decrypt
➞ Fast and efficient
➞ Shared secret must be securely exchanged
➞ Examples: AES, DES, ChaCha20

Asymmetric Cryptography
➞ Uses a key pair: public key (encrypt) + private key (decrypt)
➞ Enables secure key exchange over insecure channels
➞ Slower but essential for digital certificates, TLS
➞ Examples: RSA, ECC

Why it matters in SOC
✓ Understand protocols using symmetric vs asymmetric
✓ Spot weak key exchange methods
✓ Analyze TLS handshakes
✓ Alert if encryption is missing or misconfigured
✓ Recognize phishing attempts using spoofed certificates

Pro Tip
In many cases, asymmetric encryption is used only to exchange the symmetric session key — then symmetric encryption takes over for performance.

Have you analyzed key exchange patterns in PCAPs or logs?

Chiffrement symétrique vs asymétrique – Les différences clés

Quelle est la différence ?
Chiffrement symétrique
➞ Une seule clé pour chiffrer et déchiffrer

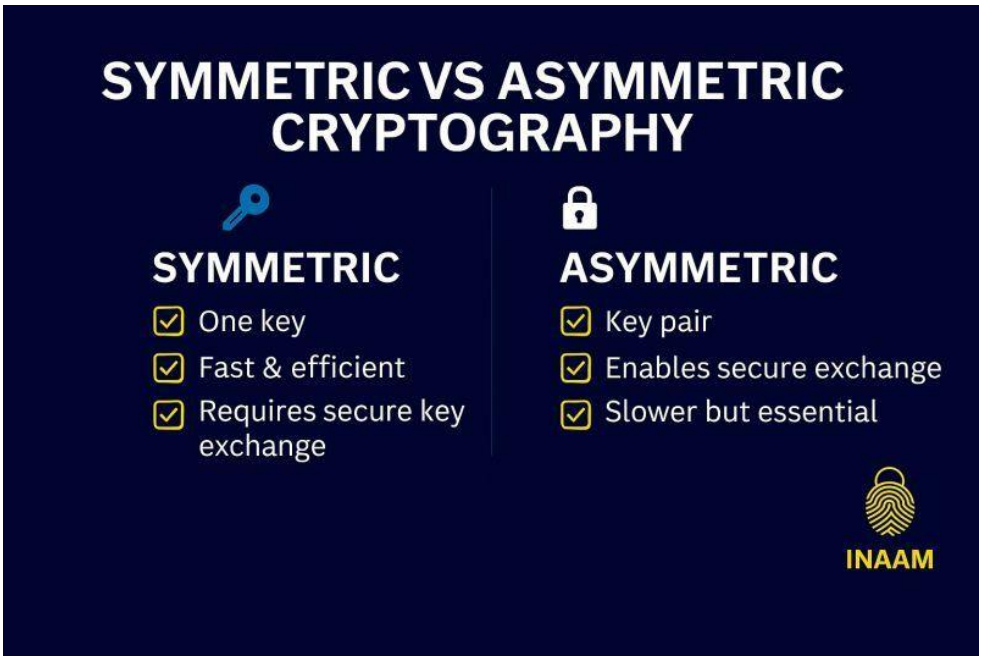
➞ Rapide et efficace
➞ La clé doit être échangée de façon sécurisée
➞ Exemples : AES, DES, ChaCha20

Chiffrement asymétrique
➞ Utilise une paire de clés : publique (chiffrer), privée (déchiffrer)
➞ Permet un échange sécurisé sur un canal non sûr
➞ Plus lent mais indispensable (certificats, TLS)
➞ Exemples : RSA, ECC

🔍 Pourquoi c'est utile en SOC
✓ Identifier les protocoles utilisés (symétrique ou asymétrique)
✓ Détecter les échanges de clés faibles
✓ Analyser les handshakes TLS
✓ Alerter en cas d'absence de chiffrement
✓ Identifier les certificats frauduleux

💡 Astuce
Souvent, l'asymétrique sert uniquement à échanger la clé symétrique, utilisée ensuite pour chiffrer les données efficacement.

❓ Avez-vous déjà analysé un échange de clés dans une capture réseau ?



3- What Are Honeypots and Why Do SOCs Use Them?

🎣 Honeypots are security mechanisms designed to deceive attackers
🕵️ They provide visibility into adversary tactics and help SOC teams learn from real intrusions
📌 Have you ever analyzed alerts from a honeypot system?

📍 What's a Honeypot?
A honeypot is a decoy system or service designed to attract attackers.
Instead of protecting production assets directly, it serves as a trap to monitor malicious activity.

👮 SOC Relevance
Even at L1, understanding honeypots helps you:
✓ Differentiate between real assets and traps
✓ Recognize how attackers probe and exploit systems
✓ Generate high-fidelity alerts with almost zero false positives
✓ Gain threat intelligence from observed attacks

🧠 Types of Honeypots
🟩 Low-interaction – Simulates limited services (e.g., SSH login page)
🟩 High-interaction – Full systems, allowing attackers to deploy malware for study
🟩 Honeytokens – Fake credentials, API keys, or files that trigger alerts when used

💡 Pro Tip
Honeypots don't replace prevention — they complement monitoring and detection.
They're most effective when integrated with SIEM/SOC pipelines for enriched threat intel.

👇 Have you worked with honeypots in your training or lab projects?

Qu'est-ce qu'un honeypot et pourquoi les SOC les utilisent-ils ?

📍 Qu'est-ce qu'un honeypot ?
Un honeypot est un système ou service factice destiné à attirer les attaquants.
Plutôt que de protéger directement, il sert de piège pour observer les activités malveillantes.

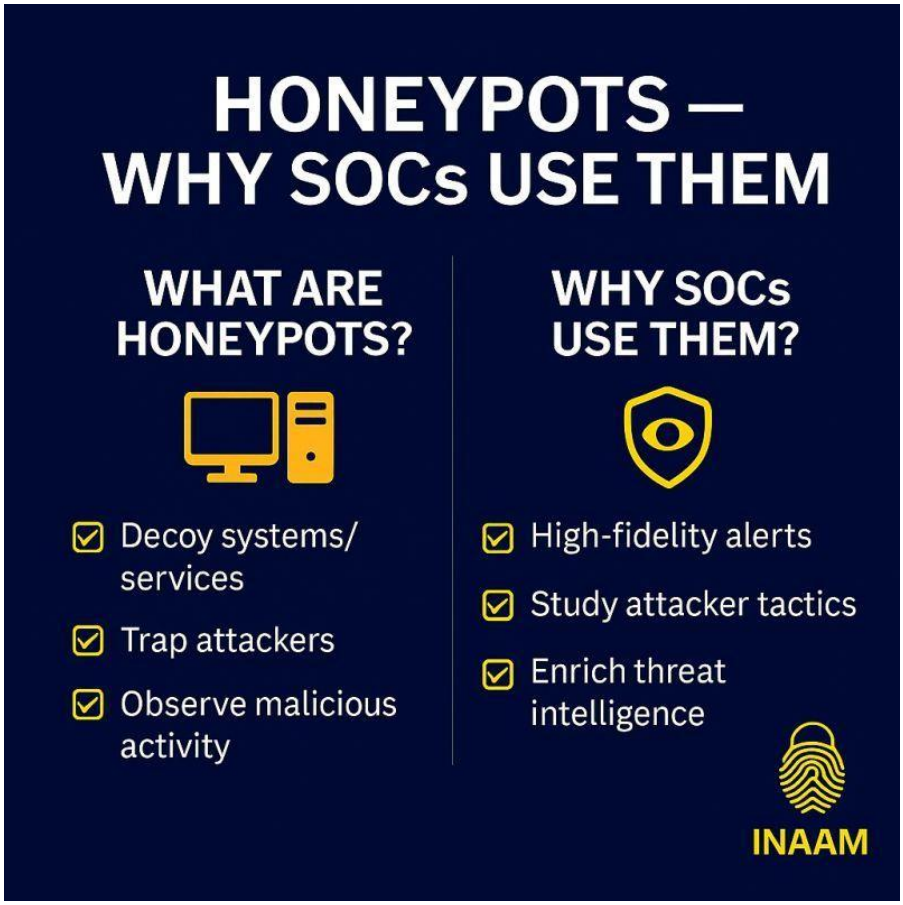
👮 Utilité en SOC
Même au niveau L1, comprendre les honeypots vous aide à :
✓ Distinguer les vrais actifs des leurres
✓ Comprendre comment les attaquants explorent et exploitent

✓ Générer des alertes fiables avec très peu de faux positifs
✓ Collecter du renseignement sur les menaces

🔍 Types de honeypots
🟩 Low-interaction – Simule des services limités (ex : SSH factice)
🟩 High-interaction – Systèmes complets pour observer les attaques
🟩 Honeytokens – Identifiants, clés API ou fichiers leurres déclenchant une alerte

💡 Astuce
Les honeypots ne remplacent pas la prévention — ils la complètent.
Ils sont particulièrement utiles intégrés à un SIEM/SOC pour améliorer la détection.

🎯 Avez-vous déjà testé un honeypot dans un labo ou une mission ?



4- Red Team vs Blue Team – Core Differences

In cybersecurity, Red and Blue teams represent attack vs defense roles
Understanding both helps SOC analysts anticipate attacker tactics and strengthen defenses
Have you ever participated in a Red/Blue exercise?

Red Team (Attackers)
Offensive security professionals
Simulate real-world attacks
Goal: test resilience of systems, people, and processes
Tools: exploitation frameworks, social engineering, malware simulation

Blue Team (Defenders)
Defensive security professionals
Monitor, detect, and respond to threats
Goal: protect and defend the organization
Tools: SIEM, IDS/IPS, EDR, threat intel

SOC Relevance
✓ Blue Teams form the core of SOC operations
✓ Red Team simulations provide valuable training for Blue Teams
✓ Together, they enable continuous improvement of security posture

Pro Tip
Think of it like a sparring match — Red Team sharpens the Blue Team, and the Blue Team hardens defenses against real-world threats.

Have you seen how Red Team tests improved Blue Team detection in your environment?

Red Team vs Blue Team – Différences clés

En cybersécurité, les équipes Red et Blue représentent les rôles attaque vs défense
Comprendre les deux aide les analystes SOC à anticiper et renforcer la protection
Avez-vous déjà participé à un exercice Red/Blue ?

Red Team (Attaquants)
Experts en sécurité offensive
Simulent des attaques réelles
Objectif : tester la résilience des systèmes, des utilisateurs et des processus

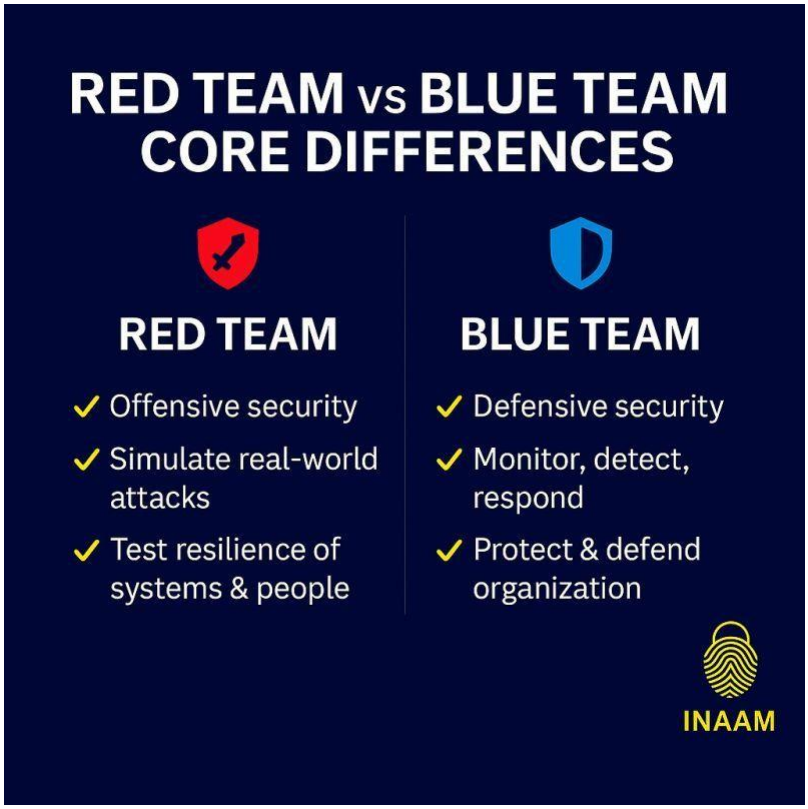
Outils : frameworks d’exploitation, ingénierie sociale, simulation de malwares

🔵 Blue Team (Défenseurs)
Experts en sécurité défensive
Surveillent, détectent et répondent aux menaces
Objectif : protéger et défendre l’organisation
Outils : SIEM, IDS/IPS, EDR, renseignement sur les menaces

🚨 Utilité en SOC
✓ Les Blue Teams sont le cœur du SOC
✓ Les simulations Red Team sont un entraînement précieux
✓ Ensemble, elles assurent une amélioration continue de la sécurité

💡 Astuce
Comme un entraînement de boxe : la Red Team pousse la Blue Team à progresser, et la Blue Team renforce ses défenses contre les menaces réelles.

🔥 Avez-vous déjà vu une simulation Red Team améliorer la détection SOC ?



5- Soft Skills That Make a Great SOC Analyst

🎯 Technical expertise is essential, but in real SOC environments, soft skills often make the difference
💡 They improve teamwork, communication, and decision-making during incidents
❓ Which soft skill do you think matters most in cybersecurity?

🧠 Core Soft Skills
✓ Communication – Explain technical issues clearly to both technical and non-technical staff
✓ Teamwork – Collaborate with SOC peers, IR teams, IT, and management
✓ Critical Thinking – Analyze alerts logically, avoid assumptions
✓ Problem-Solving – Find effective solutions under pressure
✓ Adaptability – Stay calm in fast-changing threat landscapes
✓ Attention to Detail – Spot anomalies others might miss

🕵️ SOC Relevance
SOC work isn't just about tools and logs — it's about people, processes, and collaboration.
A strong SOC analyst balances technical expertise with soft skills to handle incidents effectively.

🤓 Pro Tip
During interviews, don't just highlight your technical stack — show how your soft skills helped you during investigations, teamwork, or high-pressure incidents.

👇 What's the #1 soft skill that helped you most in SOC work or training?

Les soft skills qui font un bon analyste SOC

🎯 Les compétences techniques sont essentielles, mais ce sont souvent les compétences humaines qui font la différence dans un SOC
💡 Elles améliorent la collaboration, la communication et la prise de décision en situation de crise
❓ Selon vous, quelle compétence humaine est la plus importante en cybersécurité ?

🧠 Soft Skills clés
✓ Communication – Expliquer clairement aux profils techniques et non techniques
✓ Travail en équipe – Collaborer avec les analystes, l'IR, l'IT et la direction
✓ Esprit critique – Analyser les alertes sans conclusions hâtives
✓ Résolution de problèmes – Trouver des solutions efficaces sous pression

✓ Adaptabilité – Garder son calme face à des menaces changeantes
✓ Sens du détail – Repérer des anomalies invisibles aux autres

🔭 Utilité en SOC
Le travail en SOC ne se limite pas aux outils et aux logs — il repose sur les personnes et la collaboration.
Un bon analyste combine compétences techniques et soft skills pour gérer les incidents efficacement.

🍔 Astuce
En entretien, ne parlez pas seulement de vos outils — illustrez comment vos soft skills vous ont aidé à résoudre un incident ou à gérer le stress.

🤔 Quelle est la compétence la plus précieuse pour vous en SOC ?