# SOC LEVEL 1 ESSENTIALS – PART E: REAL-WORLD USE CASES & SCENARIOS (POSTS 38 – 45)

From Brute-Force to Beaconing: Practical Detection Scenarios Every SOC Analyst Should Know

AUGUST 29, 2025

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

# Table of Contents

# 1- SSH Brute-Force Detection – Practical Steps

🧠 Learn how to spot repeated login attempts in logs
💡 Use SIEM logic or scripts to catch brute-force behavior
❓ Have you implemented SSH brute-force rules in your SOC?

What Is SSH Brute-Force?
A brute-force attack targets the SSH (Secure Shell) service by trying many username/password combinations until access is gained.
It's a common attack against public-facing Linux servers — often automated and persistent.

🔎 How to Detect SSH Brute-Force Attempts
✓ Review auth logs (/var/log/auth.log, EDR, or SIEM)
• Look for repeated Failed password or Invalid user entries
• Check for generic usernames like admin, root, test

✓ Detection logic
• More than X failed logins from one IP in Y minutes
• Login attempts on port 22
• Username enumeration patterns

✓ Tools you can use
• SIEM queries (e.g., in Kibana, Splunk)
• Fail2Ban to block attackers
• Custom Python/Bash scripts to scan logs and trigger alerts

💡 Pro Tip
Correlate IPs with CTI sources like AbuseIPDB or OTX — many are already flagged.

❓ How do you detect or block SSH brute-force in your environment?

---

## Qu’est-ce qu’une attaque brute-force SSH ?

C’est une attaque ciblant le service SSH (Secure Shell), qui tente de multiples identifiants jusqu’à trouver le bon.
Elle vise souvent les serveurs Linux exposés, avec des scripts automatisés.

🔎 Comment la détecter efficacement ?
✓ Consultez les logs d’authentification (/var/log/auth.log, EDR, ou SIEM)

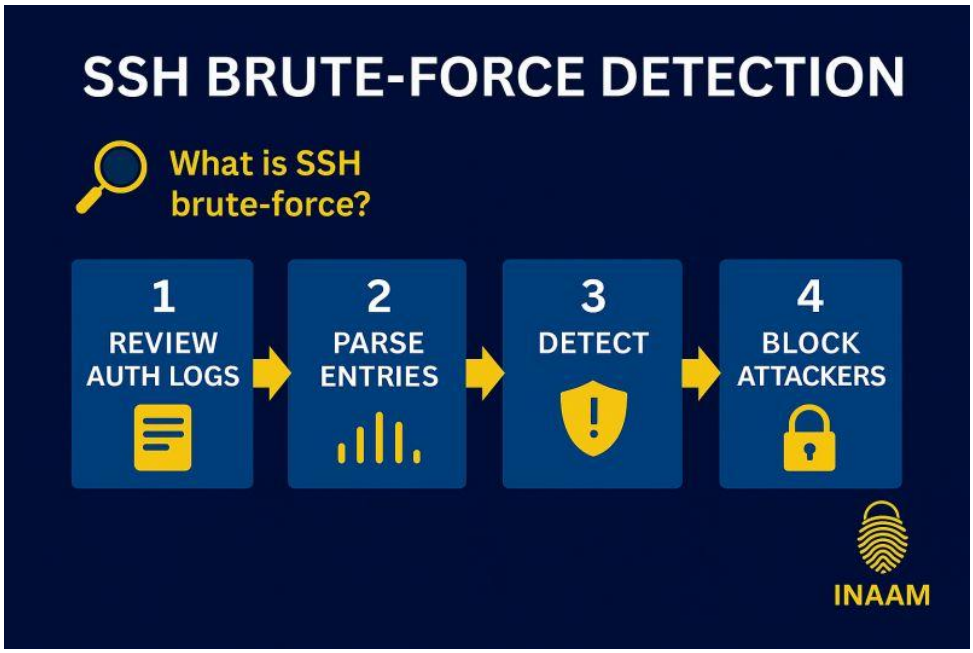
• Recherchez des entrées Failed password, Invalid user répétées
• Noms d’utilisateurs suspects : admin, root, test…

✓ Logique de détection
• X échecs en Y minutes depuis la même IP
• Tentatives sur le port 22
• Multiples essais avec des identifiants différents

✓ Outils disponibles
• Requêtes SIEM (Kibana, Splunk…)
• Fail2Ban pour bloquer automatiquement
• Scripts Python/Bash pour automatiser les détections

💡 Astuce
Enrichissez vos résultats avec AbuseIPDB ou OTX pour vérifier les IPs malveillantes connues.

❓ Et vous, comment gérez-vous ces tentatives dans votre SOC ?



# 2- How to Analyze a Phishing Email Alert

🧠 Master the key steps of email threat analysis in the SOC
💡 Learn which headers, links, and behaviors to examine
❓ Have you ever dissected a real phishing email? What stood out?

Why Analyze Phishing Emails?
Phishing is still one of the most common attack vectors. SOC analysts must be able to quickly analyze alerts, validate threats, understand attacker intent, and escalate properly.

🕹️ Step-by-Step Analysis Workflow
1️⃣ Review Email Headers
• Check sender, return path, and Received: lines
• Spot spoofing, forged domains, mismatched IPs

2️⃣ Inspect URLs & Attachments
• Hover and extract links safely
• Use VirusTotal, URLScan, Hybrid Analysis
• Sandbox attachments (e.g., Joe Sandbox, **Any.Run**)

3️⃣ Evaluate Content & Language
• Signs: urgency, errors, impersonation (CEO, IT)
• Social engineering: fake logins, password resets

4️⃣ Check External Threat Intel
• Cross-check IOCs via MISP, OTX, AbuseIPDB
• Spot campaign patterns or phishing kits

5️⃣ Document & Tag in SIEM
• Add notes and tags (e.g., phishing, malicious_link)
• Share with CTI team if needed

💡 Pro Tip: Always use a virtual machine or isolated lab to extract indicators safely.

❓ What's the most convincing phishing email you've seen?

---

## Pourquoi analyser les emails de phishing ?

Le phishing reste l'un des vecteurs les plus fréquents. Les analystes SOC doivent valider les alertes rapidement, comprendre l'intention de l'attaquant, et escalader efficacement.

🎣 Étapes de l'analyse
1- En-têtes d'email
• Adresse expéditeur, retour, lignes Received
• Spoofing, domaines usurpés, IP incohérentes

2- Liens et pièces jointes
• Survol et extraction des URLs
• VirusTotal, URLScan, Hybrid Analysis
• Sandbox : Joe Sandbox, **Any.Run**

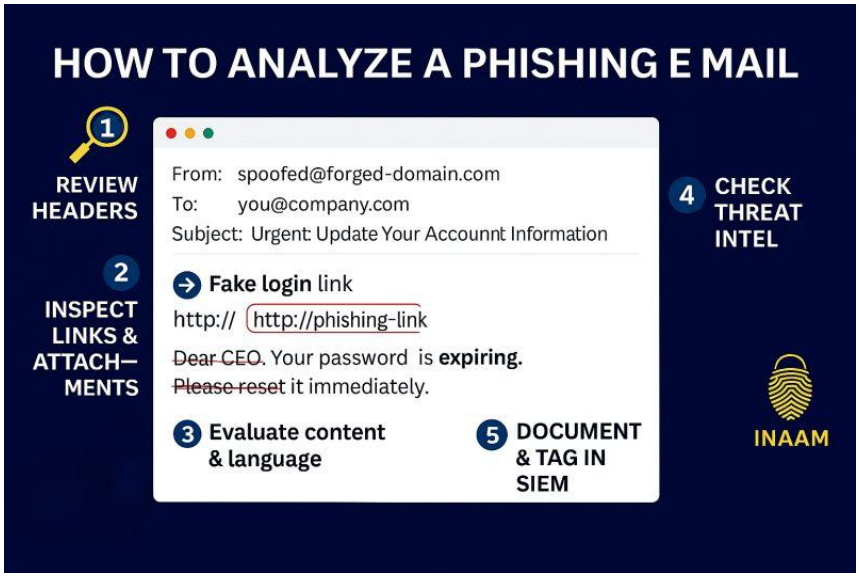
3- Contenu et langage
• Urgence, fautes, usurpation (PDG, IT)
• Ingénierie sociale : fausse connexion, reset mot de passe

4- Vérification Threat Intel
• Vérifiez les IOCs (MISP, OTX, AbuseIPDB)
• Campagnes et kits de phishing connus

5- Documentation dans le SIEM
• Notes, tags (phishing, malicious_link)
• Partage avec l'équipe CTI si nécessaire

💡 Astuce : Utilisez une VM ou un lab isolé pour analyser les indicateurs sans risque.

❓ Quel phishing vous a le plus surpris ?



# 3- RDP Misuse – Detection and Logging Tips

🧠 Understand how attackers abuse RDP in real environments
💡 Learn what to log and how to spot anomalies
❓ Have you reviewed your RDP logs this week?

What is RDP Misuse?
Remote Desktop Protocol (RDP) is widely used for remote administration. But when exposed or misconfigured, it's a prime target for brute-force attacks, lateral movement, and data exfiltration.

Common misuse includes:
Unauthorized access to servers
Use of default or weak credentials
RDP connections outside business hours
Suspicious lateral movement via RDP

🔐 SOC Relevance
As a junior SOC analyst, you can contribute by:
✓ Monitoring RDP access in logs (event ID 4624, 4625, 4778, 4779, etc.)
✓ Alerting on unusual login times or geolocations
✓ Detecting brute-force attempts and multiple failed logins
✓ Investigating RDP use from/to unexpected hosts

🔧 Logging Tips
Enable full RDP logging (successful + failed logins)
Correlate Windows Event Logs with firewall/VPN logs
Add threat intelligence context (IP reputation, geoIP)
Look for anomalies: logins from service accounts or at odd hours

💡 Pro Tip
RDP should be restricted via firewall, VPN, and MFA.
But even in secure setups, log review is critical.
Start by asking: "Who used RDP today? Is it normal?"

❓ Have you ever detected RDP abuse during log review?

---

## C'est quoi l'abus de RDP ?

Le protocole RDP est souvent utilisé pour l'administration à distance. S'il est exposé ou mal configuré, c'est une cible facile pour les attaques :
Connexions non autorisées

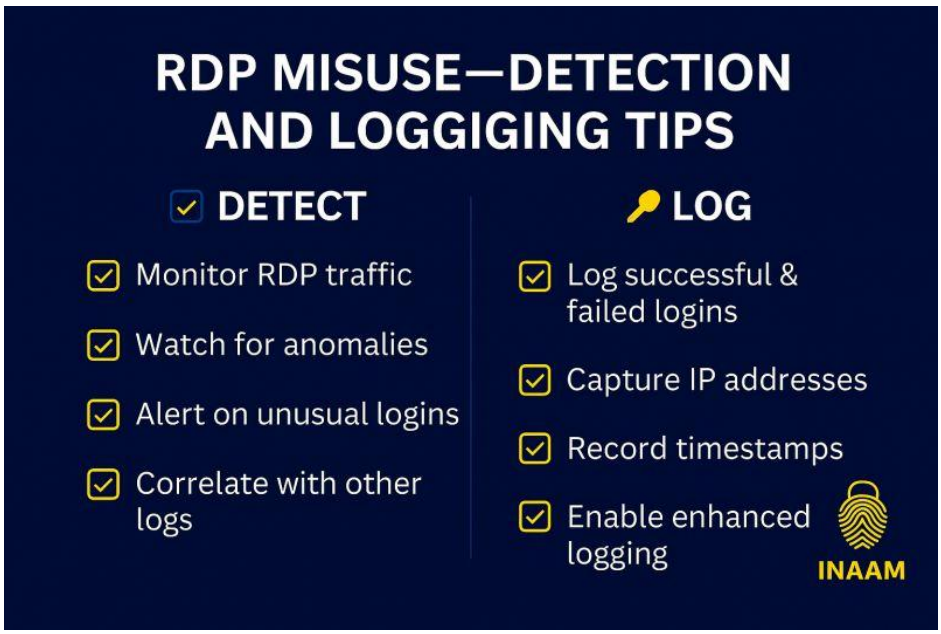
Utilisation de mots de passe faibles
Connexions en dehors des horaires
Mouvements latéraux suspects via RDP

🔐 Utilité en SOC
Même en tant qu'analyste junior, vous pouvez :
✓ Surveiller les accès RDP dans les logs (ID 4624, 4625, 4778...)
✓ Alerter sur les horaires/lieux inhabituels
✓ Détecter les tentatives de force brute
✓ Analyser les connexions entre hôtes inattendus

🔧 Conseils de journalisation
Activez les logs complets RDP (succès + échecs)
Corrélez avec les logs VPN/firewall
Ajoutez le contexte CTI (réputation IP, géoIP)
Recherchez les anomalies : comptes système, horaires bizarres

💡 Astuce
Même avec un VPN et MFA, la revue des logs RDP reste essentielle.
Demandez-vous : "Qui s'est connecté en RDP aujourd'hui ? Est-ce normal ?"

❓ Avez-vous déjà détecté un abus de RDP ?



# 4- Lateral Movement in Networks – What to Watch For

🧠 Understand how attackers pivot between systems
💡 Learn how to detect and disrupt their path
❓ Do you know what “normal movement” looks like on your network?

What is Lateral Movement?
Once inside a network, attackers often don’t stay where they landed.
They move laterally to reach higher-value systems (like AD, databases, backups).
This is a key stage in most targeted attacks (APT, ransomware).

🛠 Common techniques:
RDP or SMB access to other hosts
Pass-the-Hash / Pass-the-Ticket
Remote execution via WMI, PsExec, WinRM
Credential dumping to impersonate users

🔐 SOC Relevance
As a junior SOC analyst, you should:
✓ Watch for unusual internal connections (new host-to-host patterns)
✓ Investigate privilege escalation signs
✓ Correlate logs (auth, firewall, EDR)
✓ Tag abnormal behavior early to avoid full compromise

🔧 Detection Tips
Set baselines for internal communication
Alert on lateral tool usage (WMI, PsExec, etc.)
Monitor access to domain controllers and admin shares
Flag changes in user behavior (login times, destinations)

💡 Pro Tip
Normal movement in a network has patterns.
Lateral movement breaks them.
Know your baselines and question the exceptions.

❓ Have you ever traced lateral movement from logs?

---

## C’est quoi un mouvement latéral ?

Une fois dans le réseau, un attaquant ne reste pas sur la machine d’entrée.
Il se déplace latéralement pour atteindre les systèmes critiques (AD, bases de données, sauvegardes).

C’est une étape clé des attaques ciblées (APT, ransomware).

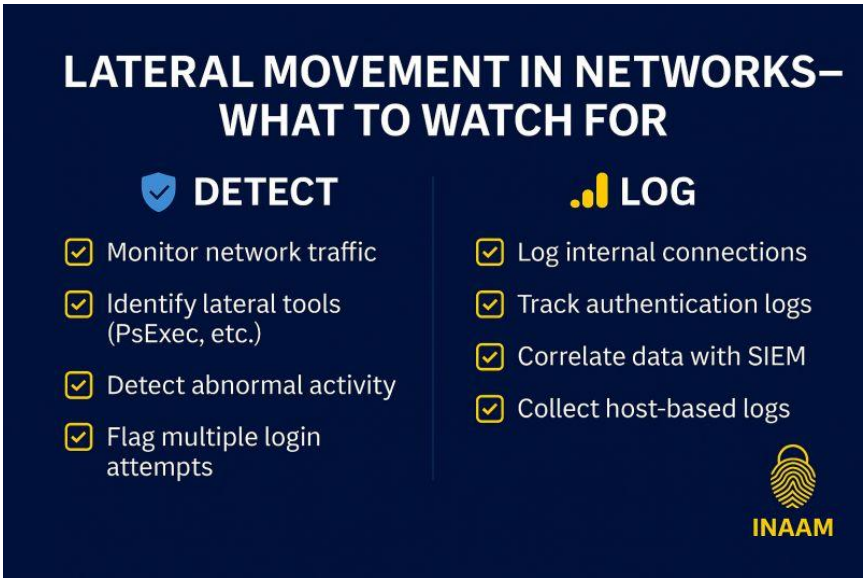
🛠 Techniques courantes :
Accès à distance via RDP, SMB
Pass-the-Hash / Pass-the-Ticket
Exécution distante avec WMI, PsExec, WinRM
Vol de credentials pour usurpation

🔐 Utilité en SOC
Même en tant que junior, vous pouvez :
✓ Surveiller les connexions internes inhabituelles
✓ Rechercher les signes d’élévation de privilèges
✓ Corréler les logs (authentification, firewall, EDR)
✓ Étiqueter les comportements anormaux dès le début

🔧 Conseils de détection
Définir un “normal” des flux internes
Alerter sur l’usage d’outils suspects (WMI, PsExec...)
Surveiller l’accès aux DC et partages admin
Repérer les changements de comportement utilisateur

💡 Astuce
Les mouvements normaux ont des schémas.
Le mouvement latéral les casse.
Connaissez vos baselines, et interrogez les anomalies.

❓ Avez-vous déjà repéré un mouvement latéral dans les logs ?



# 5- Malware Alert – What to Do First

🧠 Learn the immediate steps to take when malware is detected
💡 Don't panic — act with process and precision
❓ What's your first reflex when a malware alert hits?

What Is a Malware Alert?
It's a notification that a file, process, or behavior matches known malicious indicators — based on antivirus, EDR, SIEM correlation, or sandbox results.

🛑 But not all alerts mean full infection.
You must validate, contain, and investigate before escalating.

🔐 SOC Relevance
As a junior SOC analyst, your first reaction can shape the entire response:
✓ Acknowledge the alert and gather context (host, user, source)
✓ Verify with other tools (EDR, sandbox, hashes)
✓ Tag the asset as suspicious
✓ Communicate early with the incident lead or senior analyst

🔧 First Steps to Take
1️⃣ Isolate the host if required (via EDR or network)
2️⃣ Capture volatile data (processes, network connections)
3️⃣ Check for spread: lateral movement, similar alerts
4️⃣ Save evidence: file hash, alert metadata, logs
5️⃣ Document every action from the first click

💡 Pro Tip
Use a checklist or playbook for malware alerts.
It avoids confusion and ensures consistent response — especially during pressure.

❓ Have you created a malware triage checklist for your team?

---

C'est quoi une alerte malware ?
C'est une détection indiquant qu'un fichier, processus ou comportement correspond à une menace connue — via antivirus, EDR, SIEM ou sandbox.

🛑 Mais toutes les alertes ne sont pas des infections confirmées.
Il faut valider, contenir et enquêter avant d'escalader.

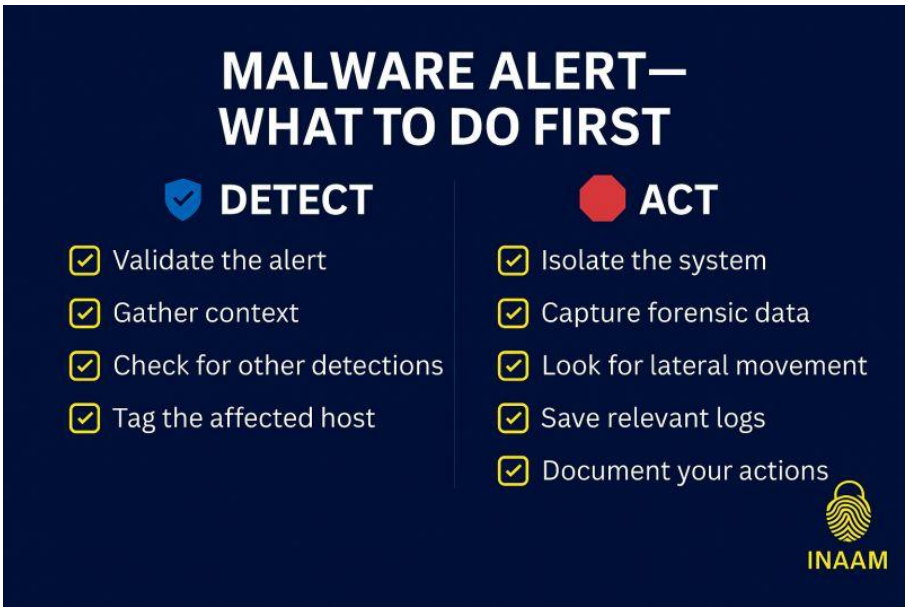
🔐 Utilité en SOC

En tant qu’analyste SOC junior, votre réaction immédiate est cruciale :
✓ Accuser réception de l’alerte, récupérer le contexte (machine, utilisateur, source)
✓ Vérifier via d'autres outils (EDR, hash, sandbox)
✓ Taguer l’élément comme suspect
✓ Informer rapidement l’équipe de réponse ou un analyste senior

🔧 Étapes prioritaires
1- Isoler la machine si nécessaire (EDR, pare-feu)
2- Capturer les données volatiles (processus, connexions réseau)
3- Vérifier la propagation (alertes similaires, mouvements latéraux)
4- Sauvegarder les preuves (hash, logs, fichiers suspects)
5- Documenter chaque action, dès la première

💡 Astuce
Utilisez une checklist ou playbook pour les alertes malware.
Cela évite les erreurs et garantit une réponse cohérente, même sous pression.

❓ Avez-vous mis en place une checklist de triage malware ?



# 6- Unusual Outbound Traffic – Analysis Techniques

🧠 Outbound flows can reveal compromise — if you know where to look
💡 Learn how to spot data exfiltration and beaconing
❓ Have you checked your outbound logs this week?

What is Unusual Outbound Traffic?
It refers to unexpected or unauthorized data leaving the internal network.
This traffic often signals threats like:
Malware communicating with C2 servers
Data exfiltration via FTP, HTTP, or DNS
Beaconing patterns from implants or RATs
Unapproved cloud uploads or external shares

🔐 SOC Relevance
Even as a junior SOC analyst, you can:
✓ Monitor outbound flows by destination IP, port, and protocol
✓ Identify traffic to rare geolocations or suspicious ASN
✓ Correlate flows with host, user, and alert context
✓ Detect repetitive low-volume traffic (beaconing)

🔧 Analysis Techniques
Use firewall/proxy/DNS logs to track outbound flows
Filter traffic by protocol and destination reputation
Visualize volume and frequency over time (heatmaps/timelines)
Compare against a whitelist of approved services/domains

💡 Pro Tip
Outbound traffic is often overlooked — but it's one of the best signals for early detection of compromise.
Normalize baselines and alert on deviation.

❓ What's your go-to method for detecting malicious outbound activity?

---

## C'est quoi un trafic sortant inhabituel ?

C'est un flux de données sortant du réseau interne de manière inattendue.
Cela peut signaler :
Une communication avec un serveur de commande (C2)
De l'exfiltration de données via FTP, HTTP ou DNS

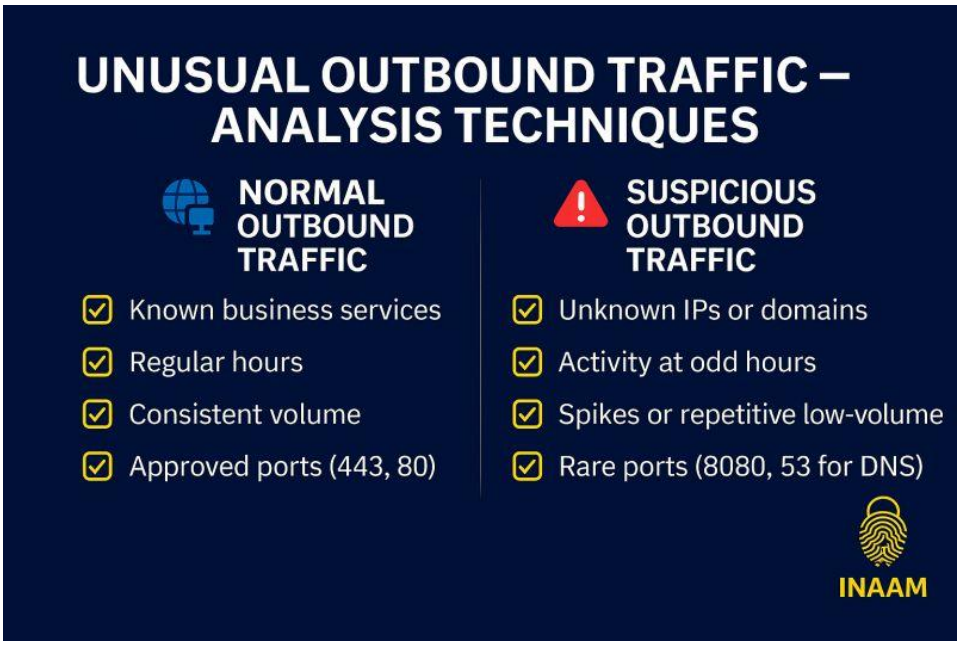
Des patterns de beaconing depuis un implant ou un RAT
Des envois vers le cloud non autorisés

🔐 Utilité en SOC
Même en tant que junior, vous pouvez :
✓ Surveiller les flux sortants (IP, port, protocole)
✓ Identifier les destinations rares ou suspectes
✓ Corréler les flux avec les journaux et les alertes
✓ Détecter les patterns répétitifs à faible volume (beaconing)

🔧 Techniques d'analyse
Exploiter les logs firewall, proxy ou DNS
Filtrer selon le protocole et la réputation des destinations
Visualiser les volumes et fréquences (graphes, heatmaps)
Comparer avec une liste blanche de services autorisés

💡 Astuce
Le trafic sortant est souvent sous-estimé, mais c'est l'un des meilleurs indicateurs de compromission.
Basez-vous sur des normes internes, puis alertez sur les écarts.

❓ Quelle est votre méthode préférée pour détecter un trafic sortant malveillant ?



# 7- DNS Tunneling – How to Spot It

🧠 Understand how attackers hide data exfiltration in DNS traffic
💡 Learn key signs of abuse even without deep packet inspection
❓ Have you ever reviewed DNS logs for suspicious patterns?

🧨 What is DNS Tunneling?
DNS tunneling is a covert technique where attackers encode data in DNS queries/responses to bypass security. It's often used for data exfiltration or to maintain command-and-control—even in restricted environments.
It exploits the fact that DNS is usually allowed by firewalls and rarely inspected.

🔐 SOC Relevance
Even as a junior SOC analyst, you can:
✓ Review DNS logs for abnormal patterns
✓ Alert on queries to rare/unknown domains
✓ Flag excessive TXT-type DNS records
✓ Note high-frequency or large-sized DNS requests

🔎 Detection Techniques
✅ Long or encoded subdomains (base64-like)
✅ Excessive DNS queries from one host
✅ Frequent TXT or NULL record types
✅ Dynamic DNS domains or uncommon TLDs
✅ Regular beaconing patterns (every X secs/mins)

Helpful tools: Wireshark, Zeek, Suricata, Sigma rules, pDNS services

💡 Pro Tip
DNS tunneling is subtle—but not invisible.
Start with a DNS baseline: what's normal?

Then ask:
🔎 "Who uses DNS too much?"
🔎 "Why does this host query a domain every 30 seconds?"
❓ Ever detected covert DNS usage?

---

## C'est quoi le DNS Tunneling ?

Technique de canal caché : des données sont encodées dans les requêtes DNS pour échapper

aux contrôles.
Utilisé pour voler des données ou garder un accès distant, même en environnement restreint.
Le DNS est souvent autorisé et peu inspecté.

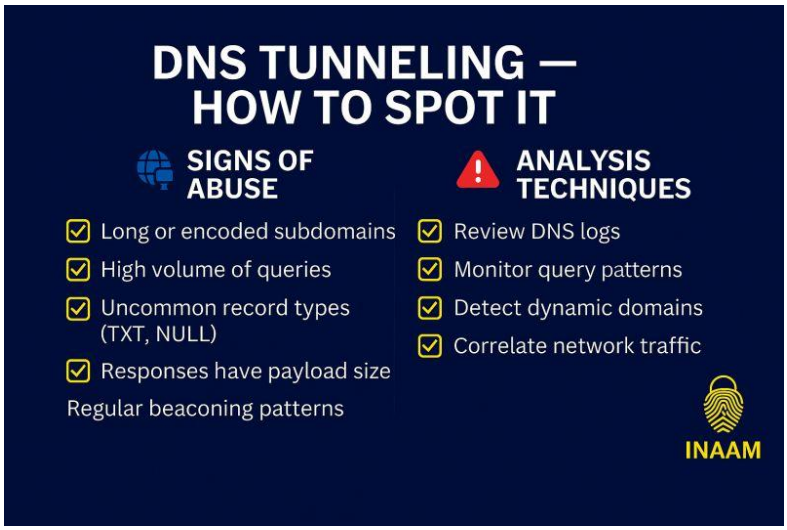
🔐 Utilité en SOC
Même en tant que junior :
✓ Surveillez les logs DNS pour les anomalies
✓ Alertez sur les domaines rares/inconnus
✓ Détectez les enregistrements TXT/NUL suspects
✓ Repérez les requêtes fréquentes ou volumineuses

🔎 Techniques de détection
✅ Sous-domaines longs ou encodés (ex: base64)
✅ Requêtes DNS excessives d'un seul hôte
✅ Enregistrements TXT/NUL fréquents
✅ Domaines dynamiques ou TLDs rares
✅ Schémas réguliers toutes les 30s/5min…

Outils utiles : Wireshark, Zeek, Suricata, règles Sigma, DNS passif

💡 Astuce
Le tunneling DNS est discret mais détectable.
Commencez par connaître le trafic DNS normal.

Posez-vous ensuite :
🔎 "Qui interroge le DNS trop souvent ?"
🔎 "Ce domaine rare est-il légitime ?"
👇 Avez-vous déjà détecté du DNS tunneling ?



# 8- Indicators of Credential Stuffing Attacks

🧠 Learn how attackers abuse reused passwords at scale
💡 Spot key patterns in logs to alert early
❓ Have you ever reviewed failed logins for stuffing signs?

🛑 What is Credential Stuffing?
It's a brute-force attack using leaked usernames & passwords (from past breaches) on various platforms to hijack accounts.

Common targets: webmail, cloud portals, VPNs.

🔐 SOC Relevance
As a SOC analyst, you should:
✓ Detect login bursts from the same IP
✓ Track failed logins across many accounts
✓ Identify logins to rarely used accounts
✓ Monitor logins from unusual locations/devices

🔎 Detection Techniques
✅ Failed logins from one IP to many users
✅ Multiple logins using old credentials
✅ High login rate to dormant accounts
✅ Access from IPs flagged by CTI tools
✅ Logins outside user/business-hour patterns

🧰 Helpful Tools
SIEM (ELK, Splunk, Sentinel)
AbuseIPDB, OTX
GeoIP-based alerting
User behavior baselining
MFA enforcement checks

💡 Pro Tip
Set alerts for:
• 10+ failed logins from 1 IP in <5 min
• Logins to >5 accounts in <10 min
• Access from multiple countries in <1h

💬 Ask yourself:
🔎 "Who is failing logins across many users?"
🔎 "Do we see abnormal login geography?"

---

## C’est quoi le Credential Stuffing ?

Une attaque de type brute-force utilisant des identifiants divulgués (fuites) pour accéder à des services en ligne.
Cibles : webmails, portails cloud, VPNs.

🔐 Utilité en SOC
En tant qu’analyste SOC :
✓ Repérez les IPs avec connexions échouées
✓ Surveillez les tentatives sur plusieurs comptes
✓ Détectez les connexions vers comptes dormants
✓ Analysez les connexions inhabituelles

🔎 Techniques de détection
✅ Échecs multiples depuis une même IP
✅ Succès avec identifiants anciens
✅ Tentatives vers comptes rarement utilisés
✅ IPs signalées dans la CTI
✅ Connexions à des heures ou lieux anormaux

🧰 Outils utiles
SIEM, AbuseIPDB, OTX
Alertes GeoIP
Analyse comportementale
Vérification MFA

💡 Astuce
Déclenchez des alertes pour :
• 10 échecs depuis une IP en <5 min
• Connexions à 5+ comptes en <10 min
• Plusieurs pays en <1h

💬 Posez-vous ensuite :
🔎 « Qui échoue les connexions sur plusieurs utilisateurs ? »
🔎 « Voit-on une géolocalisation étrange ? »

# INDICATORS OF CREDENTIAL STUFFING ATTACKS

**COMMON INDICATORS**

- Failed logins from the same source
- High volume of login attempts
- Logins to rarely used accounts
- Access attempts from flagged IPs

INAAM