ESATIC
ECOLE SUPERIEURE AFRICAINE DES TIC

Evaluation Module SIEM

Sujet de 2 heures · Cas CREDIVOIRE

Dr DIAKO Jérôme — ESATIC

Module RNCP39781BC02FM04 · Bloc BC02 · Année académique 2026-2027

Consignes générales

Épreuve écrite individuelle de 2 heures, notée sur 20

Documents : non autorisés, sauf l'annexe A (aide-mémoire Wazuh) fournie à la fin de la partie 5.

Calculatrice : autorisée (non communicante).

Compétences évaluées : C14 (sécurité des communications), C15 (mise en place, contrôle et Mise en situation : « CREDIVOIRE sous surveillance »

CREDIVOIRE est une institution de microfinance de 220 salariés : siège au Plateau (Abidjan) et 12 agences, dont Bouaké, Yamoussoukro, San-Pédro et Korhogo. Elle émet des cartes de paiement prépayées et propose un portail client relié à une API de mobile money ; elle est donc soumise à PCI DSS v4.0.1 et à son régulateur bancaire.

Élément du SI	Quantité
Contrôleurs de domaine Active Directory	2
Pare-feu périmétrique avec VPN (agences et nomades)	1
Serveurs Windows (fichiers, messagerie, applications)	18
Serveurs Linux (dont le core banking « CBS »)	10
Portail client web et passerelle API mobile money	2
Postes de travail Windows (Sysmon prévu)	200
Microsoft 365	1 tenant

L'équipe informatique compte cinq personnes, dont une seule dédiée à la sécurité. Le budget est limité. Une plateforme pilote **Wazuh 4.14** « tout-en-un » a été installée sur WAZUH-SRV (10.20.0.10).

Le lundi 26 octobre 2026, l'audit interne découvre qu'un fichier de 48 210 clients a été exporté du core banking pendant la nuit du samedi 24 au dimanche 25 octobre. La direction vous confie l'analyse de l'incident et la suite du projet SIEM.

Toutes les adresses IP publiques utilisées dans le sujet appartiennent à des plages réservées à la documentation (RFC 5737).

Partie 1 — QCM de cours (2 points, 10 min)

Une seule bonne réponse par question ; 0,25 point par bonne réponse, pas de point négatif.

1. Dans le critère DICP, la lettre **P** désigne : a) la performance b) la preuve (traçabilité) c) la protection d) la persistance.
2. Le niveau d'un risque se calcule par : a) vraisemblance + gravité b) vraisemblance × gravité c) gravité − mesures existantes d) impact × coût.
3. L'événement Windows **1102** signale : a) un échec d'ouverture de session b) la création d'un compte c) l'effacement du journal d'audit d) l'installation d'un service.
4. Ranger les champs extraits d'un journal dans un modèle commun (ECS, CIM, ASIM) s'appelle : a) l'enrichissement b) la normalisation c) l'indexation d) la corrélation.
5. « Une même IP teste plus de 20 comptes différents en 10 minutes » est une règle : a) unitaire b) de séquence c) de cardinalité d) d'absence.
6. Les agents Wazuh envoient leurs événements au manager sur le port : a) 443/TCP b) 514/UDP c) 1514/TCP d) 9200/TCP.
7. Selon PCI DSS v4.0.1, l'historique des journaux doit être conservé : a) 3 mois b) 6 mois dont 1 disponible c) 12 mois dont 3 immédiatement disponibles d) 5 ans.
8. Les règles personnalisées Wazuh s'écrivent : a) dans ossec.conf, ID libres b) dans local_rules.xml, ID ≥ 100000 c) dans agent.conf, ID ≥ 1000 d) dans alerts.json.

Partie 2 — Risques et cas d'usage (3 points, 20 min)

L'analyse de risques de CREDIVOIRE a retenu les quatre risques ci-dessous. Échelles de 1 à 5. Seuils : niveau ≤ 4 faible, 5 à 12 modéré, ≥ 15 critique.

Risque	Vraisemblance (V)	Gravité (G)
R1 — Fraude interne : un agent modifie le solde ou le plafond d'un client dans le core banking	3	5
R2 — Prise de contrôle d'un compte administrateur du domaine par force brute via le VPN	4	5
R3 — Indisponibilité du portail client par déni de service distribué (DDoS)	3	3
R4 — Effacement des journaux par un attaquant après une intrusion	2	4

2.1 (0,5 pt) Calculez le niveau de chaque risque, classez-le (faible, modéré, critique) et indiquez les deux risques à traiter en premier.

2.2 (1,5 pt) Pour chaque risque, formulez un cas d'usage SIEM sous la forme « Je détecte… dans les journaux de… », indiquez les sources de journaux nécessaires et une priorité (P1 dès le démarrage, P2 ensuite). Un collègue propose pour R3 le cas d'usage « mettre en place une protection anti-DDoS » : est-ce recevable ? Justifiez en une phrase.

2.3 (1 pt) Rédigez la fiche détaillée du cas d'usage associé à R2 : objectif, sources, logique de détection (événements, seuil, fenêtre de temps, entité commune), technique MITRE ATT&CK, sévérité, réponse attendue, responsable.

Partie 3 — Normalisation, chronologie et corrélation (5 points, 30 min)

Vous disposez des journaux de la nuit de l'incident, issus de trois sources. Informations complémentaires :

- Mme Aminata Koné (compte `a.kone`) est chargée de clientèle à Bouaké, en congé depuis le 20 octobre. Son compte n'a pas de MFA et appartient au groupe « Support-Agences », administrateur local de SRV-FILE01.
- Le VPN et le core banking sont synchronisés en NTP et horodatent en UTC (heure d'Abidjan).
- Un contrôle ultérieur montre que le service de temps de SRV-FILE01 était arrêté : son horloge **avançait d'une heure**.

Trace A — pare-feu/VPN (Syslog)

```
Oct 24 23:41:05 fw-vpn01 vpnd[1203]: login user=a.kone status=failure
    reason=bad_password src=203.0.113.77
[... 36 lignes identiques entre 23:41:09 et 23:44:31 ...]
Oct 24 23:44:52 fw-vpn01 vpnd[1203]: login user=a.kone status=success
    src=203.0.113.77 assigned_ip=10.20.5.14
```

Trace B — serveur de fichiers SRV-FILE01 (journal Sécurité, extrait clé=valeur)

```
2026-10-25 00:47:10 SRV-FILE01 EventID=4624 TargetUserName=a.kone
    LogonType=10 IpAddress=10.20.5.14
2026-10-25 00:49:30 SRV-FILE01 EventID=4720 SubjectUserName=a.kone
    TargetUserName=svc_backup2
2026-10-25 00:50:02 SRV-FILE01 EventID=4732 SubjectUserName=a.kone
    MemberName=svc_backup2 TargetUserName=Administrateurs
2026-10-25 01:12:44 SRV-FILE01 EventID=1102 SubjectUserName=svc_backup2
```

Trace C — application core banking CBS (JSON)

```
{"ts":"2026-10-24T23:58:13Z","app":"cbs","event":"export","user":"AKONE",
 "rows":48210,"client_ip":"10.20.5.14","result":"OK"}
```

3.1 (1,5 pt) Recopiez et complétez le tableau de normalisation pour quatre événements : le succès VPN, le 4624, le 4720 et l'export CBS. Citez ensuite deux obstacles qui empêchent un outil de rapprocher automatiquement ces traces.

Champ normalisé	VPN (succès)	4624	4720	Export CBS
Horodatage UTC corrigé				
Utilisateur				
Adresse IP source				
Action				
Résultat				
Machine source du journal				

3.2 (1,5 pt) Reconstituez la chronologie complète de l'attaque en heures UTC corrigées. Qualifiez la situation (événement, alerte ou incident) et indiquez les critères DICP atteints. Une règle « succès VPN puis ouverture de session RDP depuis l'IP attribuée en moins de 15 minutes » se serait-elle déclenchée ? Expliquez.

3.3 (1 pt) Rattachez cinq étapes de l'attaque à une tactique et une technique MITRE ATT&CK.

3.4 (1 pt) Proposez deux règles de corrélation qui auraient permis de détecter cette attaque plus tôt. Pour chacune, donnez le type (unitaire, seuil, séquence, cardinalité, absence…), l'entité commune et la fenêtre de temps, en langage naturel (« si… puis…, pour le même…, en moins de… »).

Partie 4 — Dimensionnement et choix de solution (5 points, 30 min)

A. Dimensionnement (3 points)

Hypothèses : taille moyenne d'un événement 600 octets ; 1 Go = 10^9 octets ; facteur d'indexation et de réplication 1,5 ; marge de croissance 25 %.

Source	Nombre	EPS moyen par équipement	
Contrôleurs de domaine	2	120	
Pare-feu et VPN	1	600	
Serveurs Windows	18	8	
Serveurs Linux	10	6	
Core banking CBS	1	50	
Portail web et passerelle API	2	25	
Postes de travail (Sysmon)	200	1	
Total			

4.1 (1 pt) Calculez l'EPS total, puis le volume brut par jour en Go.

4.2 (1 pt) Calculez le stockage indexé pour 90 jours consultables, marge comprise (en To). Pour satisfaire PCI DSS, calculez aussi le volume d'archives compressées sur 365 jours, avec un taux de compression de 10:1 et sans facteur d'indexation.

4.3 (1 pt) Une installation Wazuh « tout-en-un » est-elle adaptée à CREDIVOIRE ? Appuyez-vous sur le nombre d'agents et sur le choix « alertes seules » ou « tous les événements ». Proposez deux leviers pour réduire le volume sans perdre en détection.

B. Grille pondérée (2 points)

Le comité a noté deux solutions de 1 (faible) à 5 (excellent).

Critère	Poids initial	Poids révisé	Note Wazuh	Note Splunk ES
Couverture fonctionnelle	20 %	15 %	4	5
Intégration des sources	15 %	10 %	3	5
Coût total sur 3 ans (TCO)	20 %	25 %	5	1
Performance et évolutivité	10 %	10 %	3	5
Facilité d'exploitation	10 %	10 %	3	4
Conformité et rapports	10 %	10 %	4	5
Souveraineté et hébergement	5 %	15 %	5	4
Support et écosystème	10 %	5 %	3	4

4.4 (1 pt) Calculez le score pondéré de chaque solution avec les poids initiaux, puis avec les poids révisés. Que constatez-vous ?

4.5 (1 pt) Les poids révisés ont été fixés **après** la notation, à la demande du directeur informatique, favorable à Wazuh. Que pensez-vous de cette démarche ? Proposez la manière correcte de confirmer le choix, avec trois critères de réussite mesurables.

Partie 5 — Wazuh : décodeur, règles, collecte et durcissement (5 points, 25 min)

Le core banking écrit son journal d'audit dans `/var/log/cbs/audit.log` sur le serveur Linux SRV-CBS (agent du groupe `cbs`). Exemples de lignes :

```
2026-10-24 23:20:41 CBS-AUDIT action=LOGIN user=akone src=10.20.5.14 status=FAILED
2026-10-24 23:58:13 CBS-AUDIT action=EXPORT user=akone rows=48210 src=10.20.5.14 status=OK
```

5.1 (1 pt) Écrivez le décodeur (fichier `local_decoder.xml`) qui reconnaît ces lignes et extrait `action`, `user`, `rows` (lorsqu'il existe), `srcip` et `status`.

5.2 (1,5 pt) Écrivez dans `local_rules.xml` les règles suivantes, avec des ID ≥ 100000 et un rattachement MITRE quand il existe :

- une règle de base, niveau 3, pour tout événement décodé par votre décodeur ;
- un échec de connexion, niveau 5 ;
- cinq échecs de connexion en 2 minutes depuis la même IP, niveau 10 ;
- un export de 10 000 lignes ou plus, niveau 8 ;
- le même export réalisé entre 19 h et 7 h, niveau 12.

5.3 (0,5 pt) Écrivez le bloc à placer dans `/var/ossec/etc/shared/cbs/agent.conf` pour collecter ce journal. Citez l'outil qui vérifie la syntaxe de ce fichier et celui qui valide votre décodeur et vos règles sur une ligne de journal.

5.4 (2 pts) Voici un extrait de l'état de la plateforme pilote WAZUH-SRV. Relevez **quatre** faiblesses de sécurité. Pour chacune, indiquez la menace et la correction.

```
# extrait de /var/ossec/etc/ossec.conf
<auth>
  <disabled>no</disabled>
  <port>1515</port>
  <use_password>no</use_password>
</auth>
<remote>
  <connection>syslog</connection>
  <port>514</port>
  <protocol>udp</protocol>
  <allowed-ips>0.0.0.0/0</allowed-ips>
</remote>

# sudo ufw status
22/tcp                     ALLOW  Anywhere
443,1514,1515,55000/tcp    ALLOW  10.20.0.0/16
9200/tcp                   ALLOW  Anywhere

# sudo ls /root
wazuh-install.sh   wazuh-install-files.tar
# le compte admin du tableau de bord est partagé par les 5 membres de l'équipe
```

Annexe A — Aide-mémoire Wazuh (autorisé)

Élément	Syntaxe
Décodeur parent	`<decoder name="x"><prematch>texte</prematch></decoder>`
Décodeur enfant	`<decoder name="y"><parent>x</parent><regex>...</regex><order>champ1, champ2</order></decoder>` ; plusieurs enfants peuvent porter le même nom (décodeurs « frères »)

Élément	Syntaxe
Regex Wazuh	`\S+` suite de caractères non blancs, `\d+` chiffres, `( )` capture ; `type="pcre2"` pour PCRE2
Conditions de règle	`<decoded_as>`, `<if_sid>`, `<if_matched_sid>`, `<match>`, `<regex>`, `<field name="...">`, `<same_source_ip />`, `<time>7 pm - 7 am</time>`
Fréquence	attributs `frequency="N"` et `timeframe="secondes"` sur `<rule>`
MITRE	`<mitre><id>T1110</id></mitre>`
Collecte de fichier	`<localfile><log_format>syslog</log_format><location>chemin</location></localfile>`