



CHALLENGE SISE X OPSIE

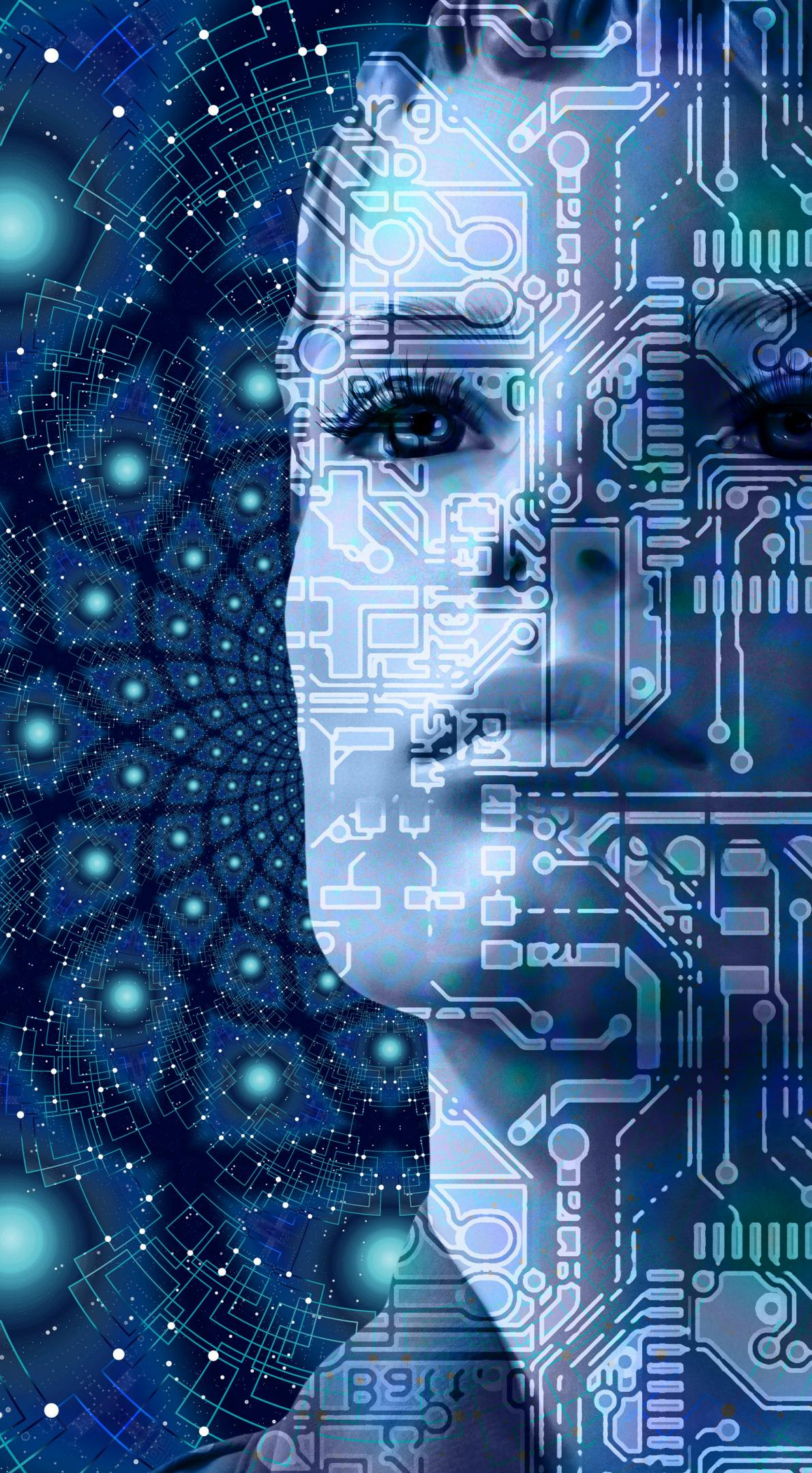
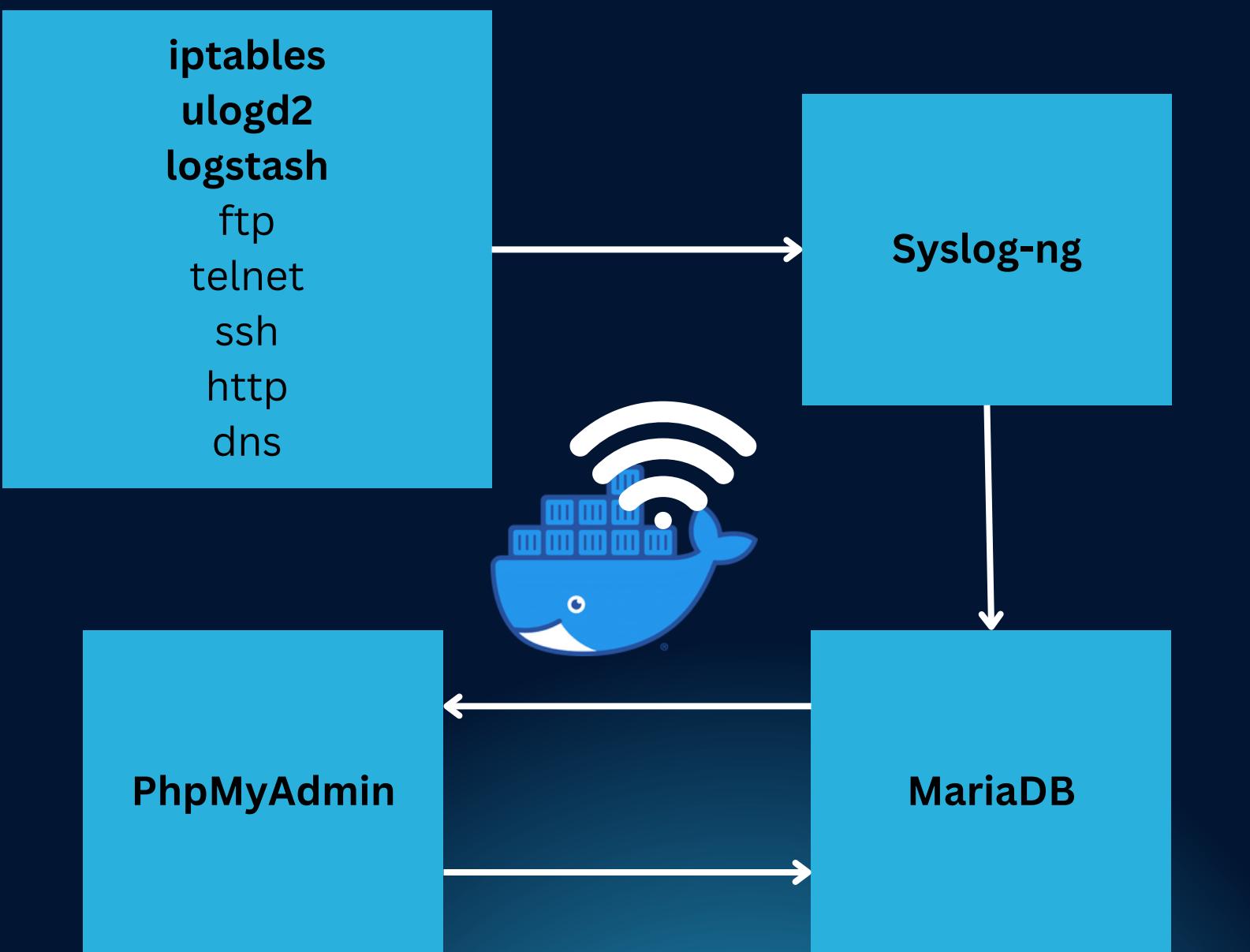
Falonne KPAMEGAN
POGNANTE Jules
Awa KARAMOKO
BELIN Thomas
Hugo COLLIN

Jeudi 27 février 2025



CHALLENGE SISE X OPSIE

- Génération de logs
- Parsing des logs et envoi sur une base de données
- Architecture :





Configuration des gestionnaires de logs

Logstash

```
input {
  file {
    path => "/var/log/iptables.log"
    start_position => "beginning"
    sincedb_path => "/dev/null"
  }
}

filter {
  grok {
    match => {
      "message" => "%{SYSLOGTIMESTAMP:timestamp}\s+ %{HOSTNAME:host}\s+ ACTION=%{DATA:action}\s+ RULE=%{DATA:rule}\s+ IN=%{DATA:intin}(?: OUT=%{DATA:intout})?\s+ MAC=%{DATA:mac}\s+ SRC=%{IP:ipsrc}\s+ DST=%{IP:ipdst}\s+ LE
N=%{NUMBER:len}\s+ TOS=%{NUMBER:tos}\s+ PREC=%{DATA:prec}\s+ TTL=%{NUMBER:ttl}\s+ ID=%{NUMBER:id}\s+ (%{WORD:df})?\s+ PROTO=%{WORD:proto}\s+ SPT=%{NUMBER:portsrc}\s+ DPT=%{NUMBER:portdst}\s+ SEQ=%{NUMBER:seq}\s+ ACK=%{NUMBER:ack}\s+ WINDOW=%{NUMBER>window}\s+ (%{WORD:flags}|\s+ (%{WORD:flags2}))?\s+ URGP=%{NUMBER:urgp}\s+ (%{NUMBER:uid})?\s+ GID=%{NUMBER:gid})?\s+ MARK=%{DATA:mark}"
    }
  }
  mutate {
    remove_field => ["timestamp", "host", "intin", "intout", "mac", "len", "tos", "prec", "ttl", "id", "df", "seq", "ack", "window", "flags", "flags2", "urgp", "uid", "gid", "mark", "log", "event"]
  }
}

output {
  syslog {
    host => "172.43.0.7"
    port => 514
    protocol => "tcp"
    codec => "json"
  }
}
```



CHALLENGE SISE X OPSIE

Syslog-ng

```
parser p_firewall {
    json-parser(
        prefix(".json.")
    );
};

filter f_ignore_syslogloop {
    not (
        "${.json.ipsrc}" eq "172.43.0.7" and
        "${.json.portsrc}" eq "514"
    );
};

destination d_mariadb {
    sql(
        type(mysql)
        host("172.43.0.12")
        username("root")
        password("mypass123")
        database("Logs_fw")
        table("FW")
        columns(
            "date",
            "ipsrc",
            "ipdst",
            "proto",
            "portsrc",
            "portdst",
            "rule",
            "action"
        )
        values(
            "$YEAR-$MONTH-$DAY $HOUR:$MIN:$SEC",
            "${.json.ipsrc}",
            "${.json.ipdst}",
            "${.json.proto}",
            "${.json.portsrc}",
            "${.json.portdst}",
            "${.json.rule}",
            "${.json.action}"
        )
    );
};
```



Scripts/Outils pour la génération de logs

- nmap



- gobuster



- nikto



- hping3



```
# 8. Balayage avec un spoof-mac d'une adresse active
echo "8. Balayage avec un spoof-mac d'une adresse active..."
timeout 30s nmap -p- -T5 -sV -Pn --spoof-mac "$MAC_ADDRESS" "$TARGET"

# 9. Attaque par brute force sur le service FTP
echo "9. Attaque par brute force sur le service FTP..."
timeout 30s nmap -p 21 -T5 --script ftp-brute --script-args userdb=users.txt,passdb=passwords.txt "$TARGET"

# 10. Recherche de répertoires avec Gobuster
echo "10. Recherche de répertoires avec Gobuster..."
timeout 30s gobuster dir -u "http://$TARGET" -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt

# 11. Attaque web via Nikto
echo "11. Attaque web via Nikto..."
timeout 30s nikto -h "http://$TARGET"

# 12. Balayage des 100 ports les plus utilisés avec un délai d'une seconde
echo "12. Balayage des 100 ports les plus utilisés..."
timeout 30s nmap --top-ports 100 -T5 -sV -Pn --max-rate 1 "$TARGET"

# 13. Test de scripts Nmap orientés « http », « ftp » et « ssh »
echo "13. Test de scripts Nmap orientés http..."
timeout 30s nmap -p 80 -T5 -sV -Pn --script http-* "$TARGET"

echo "13. Test de scripts Nmap orientés ftp..."
timeout 30s nmap -p 21 -T5 -sV -Pn --script ftp-* "$TARGET"

echo "13. Test de scripts Nmap orientés ssh..."
timeout 30s nmap -p 22 -T5 -sV -Pn ssh-* "$TARGET"

# 14. Relâcher un DDOS via un SYN Flood (avec hping3)
echo "14. Relâcher un DDOS via un SYN Flood..."
timeout 30s hping3 --faster -S -p 80 --flood "$TARGET"
```



CHALLENGE SISE X OPSIE

Détection des Anomalies dans le Trafic Réseau

Objectif : Identifier des comportements anormaux dans le trafic réseau (comme des scans de ports ou des attaques par force brute).

Méthodes :

Clustering (K-Means, DBSCAN) pour regrouper les flux similaires et détecter les anomalies.

Analyse des statistiques de trafic (p. ex. fréquence des connexions, ports fréquemment utilisés, types d'actions).

Détection de pics de trafic inhabituels (par exemple, de nombreuses connexions dans un court laps de temps).



Classification des Adresses IP en Fonction de Leur Comportement

Objectif : Classifier les adresses IP en "sources légitimes" et "sources suspectes" en fonction de leur comportement dans le réseau.

Méthodes : Apprentissage supervisé LightGBM pour classifier les IPs en fonction de leur activité dans les logs.

si une adresse IP a envoyé trop de connexions en peu de temps, elle est classée comme suspecte.





CHALLENGE SISE X OPSIE

