INTERNSHIP REPORT AT FUTURE INTERNS

Task 2 : Security Alert Monitoring and Incident Response Simulation

Report Prepared By: **ISSA HASSAN YOUSSOUF**

Internship period : 17/07/2025 to 17/08/2025
Company : Future Interns

1. OVERVIEW OF THE TASK

This report aims to provide a detailed analysis of the security events detected on the day of July 3, 2025 from the logs collected by the Security Operations Center (SOC). The goal is to accurately identify security incidents, how they operate, the extent of the breach, and potential network and data risks. That is, monitor logs in Splunk, detect alerts, analyze incidents, and write a clear incident report with severity, causes, impacts, and recommendations.

2. SKILLS DEVELOPED

During this stimulation, we developed skills:

- Using a SIEM (Splunk)
- Log analysis (Authentication, network traffic, etc.)
- Alert triage and classification
- Writing an incident report.

3. TOOLS USED

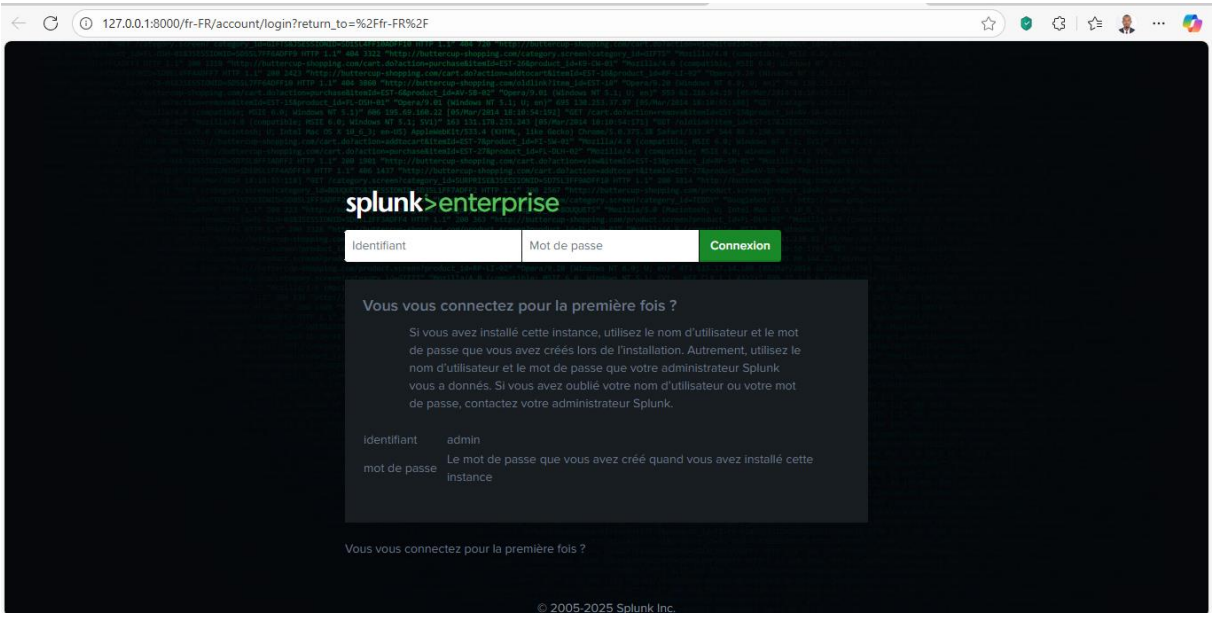
In this project, we used the following tools, namely:

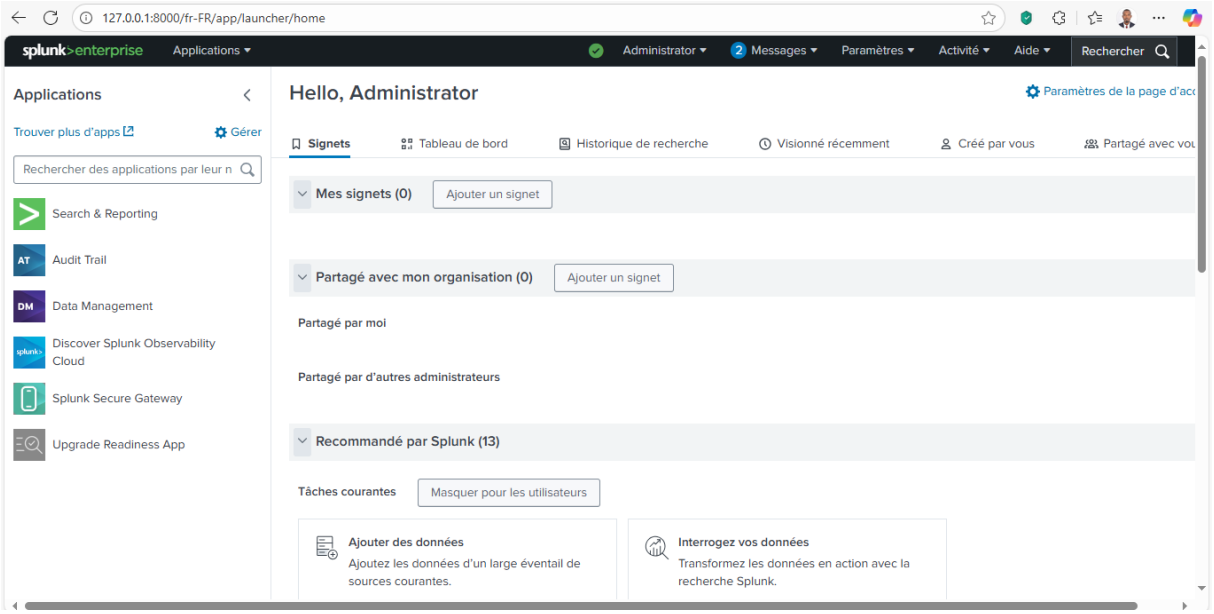
- Splunk (free version)
- Log files that were proposed by the company Future Interns
- Windows 10 operating system on-premises
- And in order to the Microsoft Edge browser.

4. INSTALLATION STEPS AND LOG ANALYSIS

Step 1: Install or access the Splunk interface

- Go to the search bar: https://www.splunk.com/en_us/download.html
- Create a Splunk account (free)
- Download **Splunk Free** (Windows version)
- Install and connect on: 127.0.0.1
- Login ID on the Splunk interface
  Login: admin
  Password during installation: Future@Inrerns2025


127.0.0.1:8000/fr-FR/account/login?return_to=%2Ffr-FR%2F
splunk>enterprise
Identifiant
Mot de passe
Connexion
Vous vous connectez pour la première fois ?
Si vous avez installé cette instance, utilisez le nom d'utilisateur et le mot de passe que vous avez créés lors de l'installation. Autrement, utilisez le nom d'utilisateur et le mot de passe que votre administrateur Splunk vous a donnés. Si vous avez oublié votre nom d'utilisateur ou votre mot de passe, contactez votre administrateur Splunk.
identifiant
admin
mot de passe
Le mot de passe que vous avez créé quand vous avez installé cette instance
Vous vous connectez pour la première fois ?
© 2005-2025 Splunk Inc.


127.0.0.1:8000/fr-FR/app/launcher/home
splunk>enterprise
Applications
Administrator
2 Messages
Paramètres
Activité
Aide
Rechercher
Applications
Trouver plus d'apps
Gérer
Rechercher des applications par leur n
Search & Reporting
Audit Trail
Data Management
Discover Splunk Observability Cloud
Splunk Secure Gateway
Upgrade Readiness App
Hello, Administrator
Paramètres de la page d'acc
Signets
Tableau de bord
Historique de recherche
Visionné récemment
Créé par vous
Partagé avec vou
Mes signets (0)
Ajouter un signet
Partagé avec mon organisation (0)
Ajouter un signet
Partagé par moi
Partagé par d'autres administrateurs
Recommandé par Splunk (13)
Tâches courantes
Masquer pour les utilisateurs
Ajouter des données
Ajoutez les données d'un large éventail de sources courantes.
Interrogez vos données
Transformez les données en action avec la recherche Splunk.

Step 2: Import the logs into Splunk

We use the logs provided by the company Future Interns to carry out our stimulation:

SOC_Task2_Sample_Logs.txt - Bloc-notes

Fichier Edition Format Affichage Aide

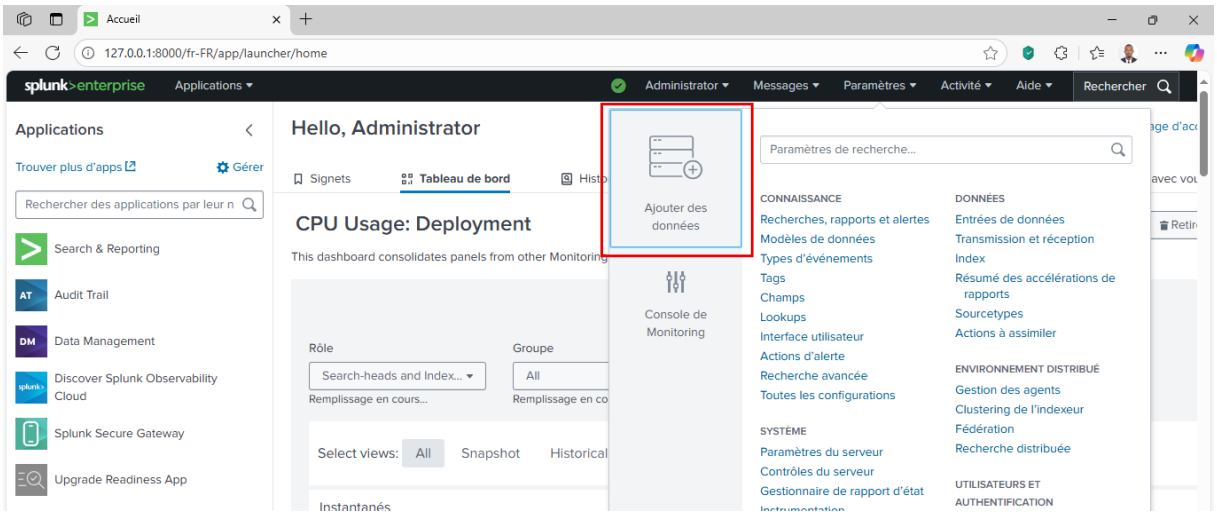
```
2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success
2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed
2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt
2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
2025-07-03 04:19:14 | user=alice | ip=198.51.100.42 | action=malware detected | threat=Rootkit Signature
2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 06:10:14 | user=david | ip=203.0.113.77 | action=file accessed
2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
2025-07-03 04:18:14 | user=bob | ip=198.51.100.42 | action=login success
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed
2025-07-03 07:38:14 | user=charlie | ip=172.16.0.3 | action=connection attempt
2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed
2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt
2025-07-03 05:33:14 | user=david | ip=198.51.100.42 | action=file accessed
2025-07-03 04:19:14 | user=david | ip=10.0.0.5 | action=connection attempt
2025-07-03 04:29:14 | user=alice | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success
2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed
2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connection attempt
2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success
2025-07-03 04:41:14 | user=alice | ip=172.16.0.3 | action=malware detected | threat=Spyware Alert
2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
2025-07-03 07:36:14 | user=david | ip=10.0.0.5 | action=connection attempt
2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
2025-07-03 06:21:14 | user=alice | ip=203.0.113.77 | action=login success
2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt
2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed
2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed
2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login success
2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login success
2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
```

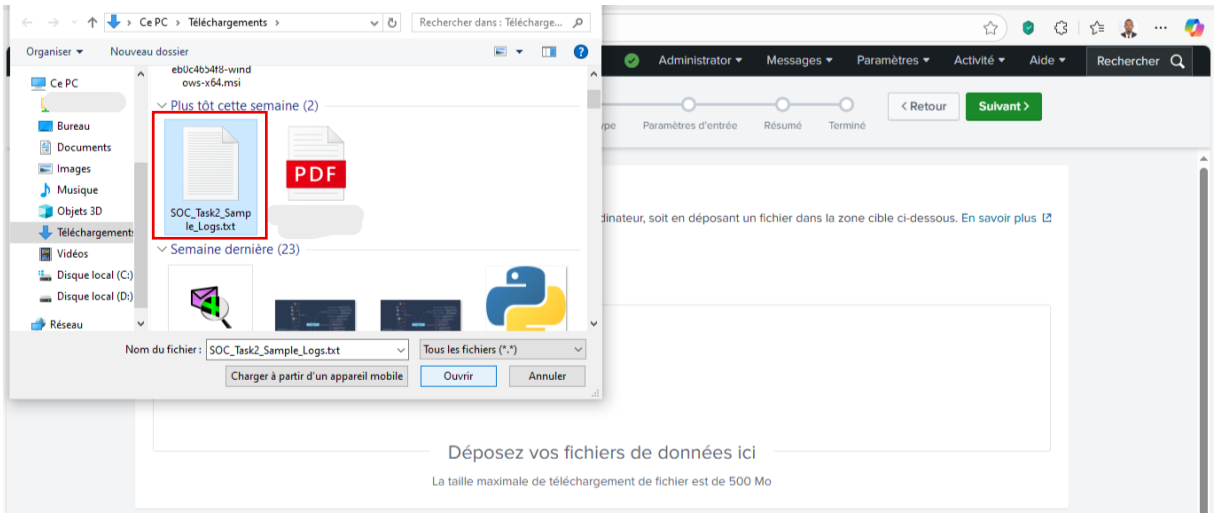
Ln 10, Col 25 | 80% | Unix (LF) | UTF-8

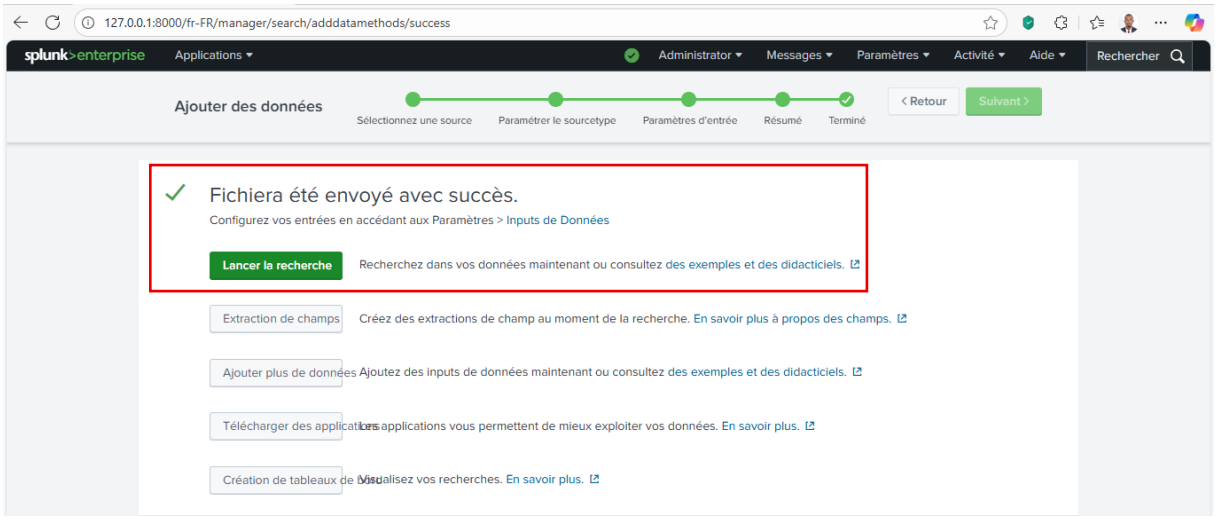
Once logged in to Splunk:

- Click on **Applications → Search & Reporting**
- At the top right, click Settings → **Add data**.
- Choose **File from my computer** and select the logs.
- Click Next, then:

  - Select the **source**
  - Give an **index name** (e.g. security_logs) so that they can be easily found.
- Click Review **& Submit** to complete the import



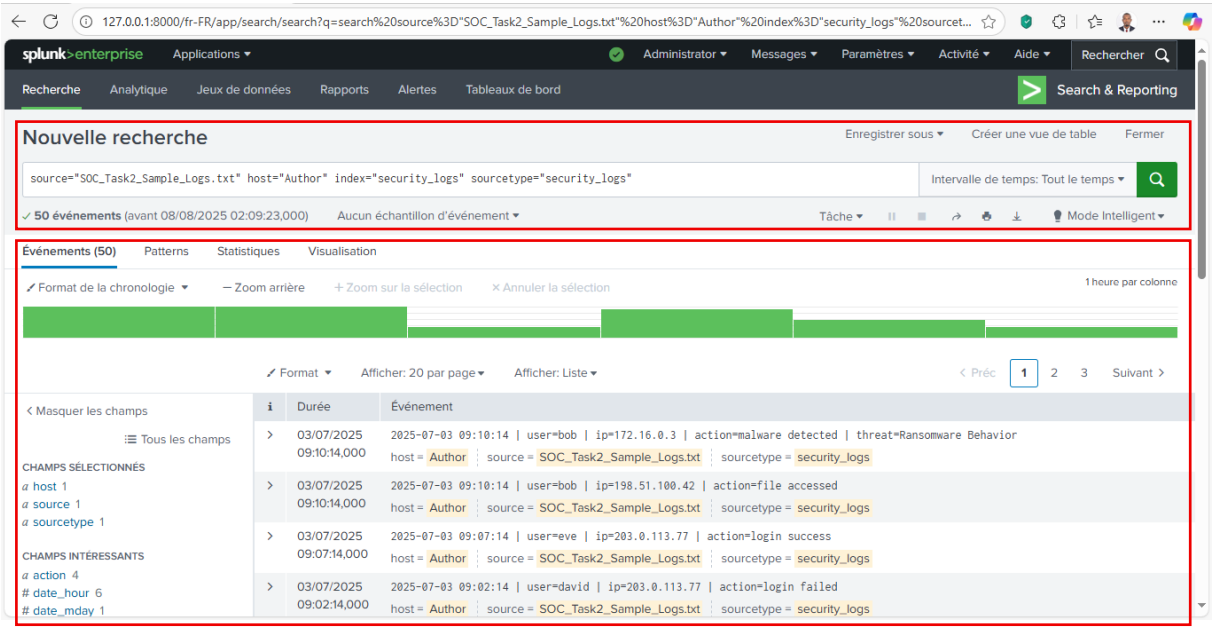




The file containing the logs has been successfully sent to the Splunk ready to perform the stimulation.

Step 3: Overall Summary of Events

- Total number of events analyzed: 50
- Types of actions identified: successful and failed connections, file access, malware detections, connection attempts, various user actions.
- Main users involved: bob, eve, david, charlie, alice
- Main types of threats detected: ransomware, trojan, rootkit, spyware, worm infection attempt



5. ANALYSIS METHODOLOGY

- Log collection and sorting by user, IP and event type.
- Classification of events according to their criticality (connection, access, malware, failure).
- Chronology of events to detect patterns, sequences and propagations.
- Behavioral analysis of suspicious users and the IPs involved.
- Technical interpretation of detected threats (ransomware, trojan, rootkit, spyware, worm).

1. **TIME-SERIES AND DETAILED ANALYSIS**
6. **1. ANALYSIS OF SUCCESSFUL AND FAILED CONNECTIONS**

SUCCESSFUL CONNECTIONS :

- Alice: 06:21, 08:00, 05:12: Alice appears to be an active user with multiple successful accesses over different time slots, likely indicating an important role or responsibilities that require continuous availability.

7/3/2025 6:21:14.000 AM
2025-07-03 06:21:14 | user=alice | ip=203.0.113.77 | action=login success

Actions d'événement

Champ	Valeur
_time	2025-07-03T06:21:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 8:00:14.000 AM
2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success

Actions d'événement

Champ	Valeur
_time	2025-07-03T08:00:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 5:12:14.000 AM
2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login success

Actions d'événement

Champ	Valeur
_time	2025-07-03T05:12:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

- Eve: 8:30 AM, 9:07 AM: Eve makes several successful connections before and after file accesses.

7/3/2025 8:30:14.000 AM
2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success

Actions d'événement

Champ	Valeur
_time	2025-07-03T08:30:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 9:07:14.000 AM

2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success

Actions d'événement

Champ	Valeur
_time	2025-07-03T09:07:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

- Bob, Charlie, David: multiple successful connections at different times, often not far apart, indicating intensive use of the system.

7/3/2025 7:46:14.000 AM

2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success

Actions d'événement

Champ	Valeur
_time	2025-07-03T07:46:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 5:18:14.000 AM

2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success

Actions d'événement

Champ	Valeur
_time	2025-07-03T05:18:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 5:04:14.000 AM

2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success

Actions d'événement

Champ	Valeur
_time	2025-07-03T05:04:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 4:53:14.000 AM

2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success

Actions d'événement

Champ	Valeur
_time	2025-07-03T04:53:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025
4:46:14.000 AM

2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login success

Actions d'événement

Champ	Valeur
_time	2025-07-03T04:46:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025
4:18:14.000 AM

2025-07-03 04:18:14 | user=bob | ip=198.51.100.42 | action=login success

Actions d'événement

Champ	Valeur
_time	2025-07-03T04:18:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

CONNECTIONS SPOTTED:

- David: Failed attempt at 09:02, which could be a forgotten password or a targeted attack.

7/3/2025
9:02:14.000 AM

2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed

Actions d'événement

Champ	Valeur
_time	2025-07-03T09:02:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

- Bob, Alice, Charlie: several failures at 04:23, 07:02, 04:47, suggesting brute force attacks or repeated mistakes.

7/3/2025
7:02:14.000 AM

2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed

Actions d'événement

Champ	Valeur
_time	2025-07-03T07:02:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 4:47:14.000 AM

2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed

Actions d'événement

Champ	Valeur
_time	2025-07-03T04:47:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 4:23:14.000 AM

2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed

Actions d'événement

Champ	Valeur
_time	2025-07-03T04:23:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 4:23:14.000 AM

2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed

Actions d'événement

Champ	Valeur
_time	2025-07-03T04:23:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

These repeated failures in a short interval are typical of brute force attempts, which may indicate an attack campaign.

6. 2. CONNECTION ATTEMPTS

Bob, Charlie, David are responsible for the majority of repeated login attempts (sometimes on several different IPs).

Example: Bob at 07:44 tries simultaneous connections on 192.168.1.101 and 203.0.113.77. This behavior could be that of a compromised account or a malicious actor scanning the network to exploit vulnerabilities.

7/3/2025 7:44:14.000 AM

2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt

7/3/2025 7:44:14.000 AM

2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt

The fact that these attempts are followed or preceded by malware events reinforces the suspicion of automated malicious activity (bots, scripts).

6. 3. FILE ACCESS

A large number of file accesses are recorded on several workstations and users:

- Bob (between 09:10, 05:44 and 06:01)

7/3/2025 9:10:14.000 AM
2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed

Actions d'événement

Champ	Valeur
_time	2025-07-03T09:10:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 6:01:14.000 AM
2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed

Actions d'événement

Champ	Valeur
_time	2025-07-03T06:01:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 5:44:14.000 AM
2025-07-03 05:44:14 | user=bob | ip=198.51.100.42 | action=file accessed

Actions d'événement

Champ	Valeur
_time	2025-07-03T05:44:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

- Eve, Charlie (between 08:31 and 08:42)

7/3/2025 8:42:14.000 AM
2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed

Actions d'événement

Champ	Valeur
_time	2025-07-03T08:42:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025
8:42:14.000 AM

2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed

Actions d'événement

Champ	Valeur
_time	2025-07-03T08:42:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025
8:31:14.000 AM

2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed

Actions d'événement

Champ	Valeur
_time	2025-07-03T08:31:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

David, Alice

7/3/2025
7:57:14.000 AM

2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed

Actions d'événement

Champ	Valeur
_time	2025-07-03T07:57:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025
6:10:14.000 AM

2025-07-03 06:10:14 | user=david | ip=203.0.113.77 | action=file accessed

Actions d'événement

Champ	Valeur
_time	2025-07-03T06:10:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025
5:33:14.000 AM

2025-07-03 05:33:14 | user=david | ip=198.51.100.42 | action=file accessed

Actions d'événement

Champ	Valeur
_time	2025-07-03T05:33:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 4:53:14.000 AM

2025-07-03 04:53:14 | user=alice | ip=203.0.113.77 | action=file accessed

Actions d'événement

Champ	Valeur
_time	2025-07-03T04:53:14.000+01:00
host	Author
index	security_logs
linecount	1
source	SOC_Task2_Sample_Logs.txt
sourcetype	security_logs
splunk_server	Author

7/3/2025 4:53:14.000 AM

2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success

These accesses are potentially legitimate but must be checked because they sometimes coincide with malware detections. For example, Bob's 9:10 AM file access corresponds to the detection of ransomware at the same time on the same IP.

Préc 1 2 3 4 5 Suivant

i	Durée	Événement
>	7/3/2025 9:10:14.000 AM	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
>	7/3/2025 9:10:14.000 AM	2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed

6. 4. MALWARE DETECTION AND ANALYSIS

Hour	User	IP	Malware Type	Technical interpretation and impact
09:10	Bob	172.16.0.3	Ransomware Behavior	Suspicious behavior detected: Encrypting or attempting to encrypt files. Ransomware can cripple machine activity.
07:51	Eve	10.0.0.5	Rootkit Signature	Rootkit: a hidden tool that allows you to have full stealth control of the machine, very difficult to detect and eliminate. Persistent access risk.
07:45	Charlie	172.16.0.3	Trojan Detected	Trojan: malware that enables a backdoor, often used for espionage or data theft.
05:48	Bob	10.0.0.5	Trojan Detected	Confirmed presence of Trojan horse on Bob's set, signal of serious compromise.
05:45	David	172.16.0.3	Trojan Detected	Trojan detected on David's machine, suggesting lateral spread of malware.
05:42	Eve	203.0.113.77	Trojan Detected	Trojan on a public IP, can indicate a compromised workstation accessible from the outside.
05:30	Eve	192.168.1.101	Trojan Detected	Trojan detected in an internal subnet, local compromise.

05:06	Bob	203.0.113.77	Worm Infection Attempt	Worm infection attempt: This type of malware spreads automatically and quickly across the network. Risk of exponential spread.
04:41	Alice	172.16.0.3	Spyware Alert	Spyware detected: data theft, user activity monitoring.
04:29	Alice	192.168.1.101	Trojan Detected	Trojan detected on Alice's internal workstation, a sign of compromise.
04:19	Alice	198.51.100.42	Rootkit Signature	Rootkit over external IP, persistent access index, and risk of remote attack.

2. INCIDENT CLASSIFICATION

Hour	User	IP	Threat Type	Gravity
09:10	Bob	172.16.0.3	Ransomware Behavior	Criticism
05:06	Bob	203.0.113.77	Worm Infection Attempt	Criticism
07:51	Eve	10.0.0.5	Rootkit Signature	Criticism
04:19	Alice	198.51.100.42	Rootkit Signature	Criticism
07:45	Charlie	172.16.0.3	Trojan Detected	High
05:48	Bob	10.0.0.5	Trojan Detected	High
05:45	David	172.16.0.3	Trojan Detected	High
05:42	Eve	203.0.113.77	Trojan Detected	High
05:30	Eve	192.168.1.101	Trojan Detected	High
04:29	Alice	192.168.1.101	Trojan Detected	High
04:41	Alice	172.16.0.3	Spyware Alert	Average
Diverse	Bob, Charlie, David	Multiple	Connection Attempt	Average
Diverse	David, Alice, Charlie	Multiple	Login Failed	Average
Diverse	Alice, Bob, Eve, David, Charlie	Multiple	File Access / Login Success	Weak

Malware Summary:

The malware detected covers a wide range of threats:

- **Ransomware** (immediate critical impact on data availability)
- **Rootkits** (allow for deep concealment and long-term control)
- **Trojan** (backdoor, espionage, exfiltration)
- **Spyware** (stealth of information)
- **Worm** (Rapid Spread)

This indicates not only a multiple and severe infection, but also a likely widespread compromise across multiple network segments and users.

3. CORRELATION ANALYSIS AND ASSUMPTIONS

- The successive appearance of malware on IPs 172.16.0.3, 10.0.0.5, 192.168.1.101 and 203.0.113.77 suggests that the threat circulates between machines, via automatic mechanisms (worm, trojan).

7/3/2025 7:45:14.000 AM	2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected

7/3/2025 5:48:14.000 AM	2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
7/3/2025 5:45:14.000 AM	2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected

7/3/2025 5:42:14.000 AM	2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
7/3/2025 5:33:14.000 AM	2025-07-03 05:33:14 | user=david | ip=198.51.100.42 | action=file accessed
7/3/2025 5:30:14.000 AM	2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
7/3/2025 5:27:14.000 AM	2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connection attempt
7/3/2025 5:18:14.000 AM	2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
7/3/2025 5:12:14.000 AM	2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login success
7/3/2025 5:06:14.000 AM	2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt

- Bob seems to be at the center of the suspicious activities (ransomware at 09:10, worm at 05:06, multiple trojans), which could mean either a primary target machine or a compromised account used for propagation.

i	Durée	Événement
>	7/3/2025 9:10:14.000 AM	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior

7/3/2025 5:06:14.000 AM	2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt

- Multiple failed and successful login attempts on the same IPs show intense activity, possibly related to the management or exploitation of compromised access.

i	Durée	Événement
>	7/3/2025 5:42:14.000 AM	2025-07-03 05:42:14 | user=eve | ip=203.0.113.77 | action=malware detected | threat=Trojan Detected
>	7/3/2025 5:33:14.000 AM	2025-07-03 05:33:14 | user=david | ip=198.51.100.42 | action=file accessed
>	7/3/2025 5:30:14.000 AM	2025-07-03 05:30:14 | user=eve | ip=192.168.1.101 | action=malware detected | threat=Trojan Detected
>	7/3/2025 5:27:14.000 AM	2025-07-03 05:27:14 | user=david | ip=203.0.113.77 | action=connection attempt
>	7/3/2025 5:18:14.000 AM	2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
>	7/3/2025 5:12:14.000 AM	2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login success
>	7/3/2025 5:06:14.000 AM	2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt
>	7/3/2025 5:04:14.000 AM	2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success
>	7/3/2025 4:53:14.000 AM	2025-07-03 04:53:14 | user=alice | ip=203.0.113.77 | action=file accessed
>	7/3/2025 4:53:14.000 AM	2025-07-03 04:53:14 | user=david | ip=203.0.113.77 | action=login success

i	Durée	Événement
>	7/3/2025 7:18:14.000 AM	2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed
>	7/3/2025 7:02:14.000 AM	2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
>	7/3/2025 6:21:14.000 AM	2025-07-03 06:21:14 | user=alice | ip=203.0.113.77 | action=login success
>	7/3/2025 6:13:14.000 AM	2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
>	7/3/2025 6:10:14.000 AM	2025-07-03 06:10:14 | user=david | ip=203.0.113.77 | action=file accessed
>	7/3/2025 6:01:14.000 AM	2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed
>	7/3/2025 5:49:14.000 AM	2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
>	7/3/2025 5:48:14.000 AM	2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
>	7/3/2025 5:45:14.000 AM	2025-07-03 05:45:14 | user=david | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
>	7/3/2025 5:44:14.000 AM	2025-07-03 05:44:14 | user=bob | ip=198.51.100.42 | action=file accessed

i	Durée	Événement
>	7/3/2025 9:10:14.000 AM	2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
>	7/3/2025 9:10:14.000 AM	2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
>	7/3/2025 9:07:14.000 AM	2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
>	7/3/2025 9:02:14.000 AM	2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
>	7/3/2025 8:42:14.000 AM	2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
>	7/3/2025 8:42:14.000 AM	2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
>	7/3/2025 8:31:14.000 AM	2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
>	7/3/2025 8:30:14.000 AM	2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
>	7/3/2025 8:21:14.000 AM	2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
>	7/3/2025 8:20:14.000 AM	2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt

- The presence of rootkits and spyware makes cleaning difficult and requires drastic measures (reinstallation, full audits).

4. TECHNICAL RECOMMENDATIONS

Immediate action

- **Complete isolation of infected machines** : especially those associated with IPs 172.16.0.3, 10.0.0.5, 192.168.1.101 and 203.0.113.77.
- **Cutting off network access** to prevent the spread of the worm and trojans.
- **Collection of evidence** (logs, memory captures, suspicious files) for forensic analysis.

Cleaning actions :

- Deployment of advanced antivirus and anti-malware tools with updates.
- Deep scan and removal of rootkits (often via secure boot or specialized tools).
- Verification of entry points (open services, ports, vulnerable applications).
- Reset affected user accounts, with mandatory password changes.
- Apply software patches and patches to all machines.

Enhanced security :

- Implementation of an intrusion detection system (IDS/IPS) and real-time alerts.
- Enhanced log monitoring with automated behavioral analysis.
- User training on best practices (phishing, passwords, downloads).
- Network segmentation to limit lateral movement of malware.

5. CONCLUSION :

The in-depth analysis of the logs reveals a major security incident with multiple network compromises. The coexistence of ransomware, trojans, rootkits, spyware and worms underlines an organized and sophisticated attack, exploiting multiple entry vectors and aiming to control the network in the long term.

Urgent intervention, combined with a comprehensive cleanup and review of security policies, is essential to restore the integrity, availability, and confidentiality of the system.