FUTURE INTERN
Date: 07/16/2025

SOC

Alert Monitoring

and

Incident Simulation

-Task 2-
Incident Report

OVERVIEW:

This report summarizes the suspicious events detected from simulated log data using the Elastic Stack (Filebeat Elasticsearch Kibana) on a configured SOC monitoring VM. The logs were parsed and filtered using Kibana's Discover and Logs interfaces, with custom search queries applied to isolate malicious patterns

Environment Setup

Platform: Azure Ubuntu VM

Ingestion Tool: Filebeat

Backend: Elasticsearch (local node)

Frontend: Kibana (port 5601 exposed via NSG rule)

Custom Logs: SOC_Task2_Sample_Logs.txt manually ingested

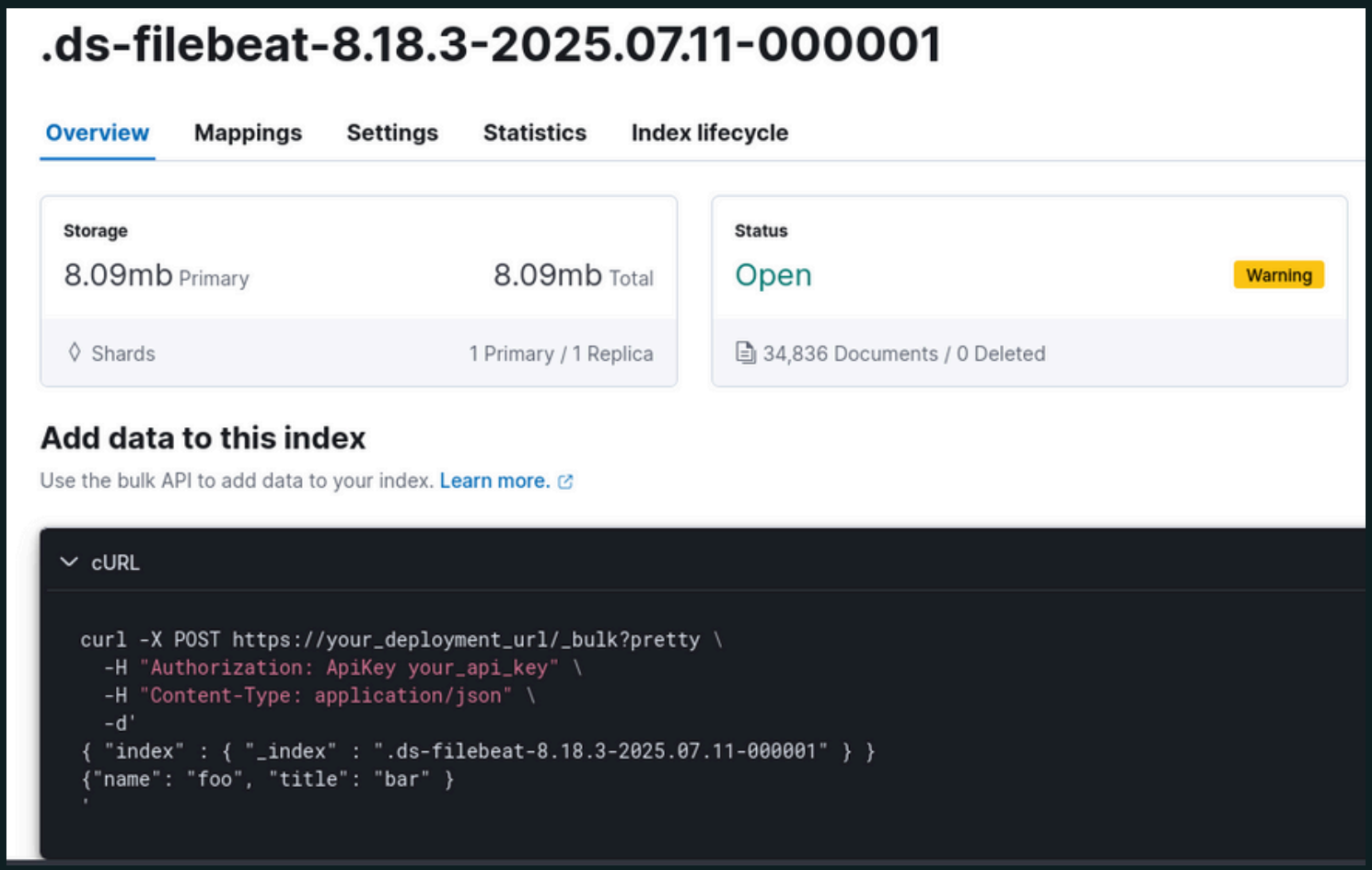
Modules Enabled:

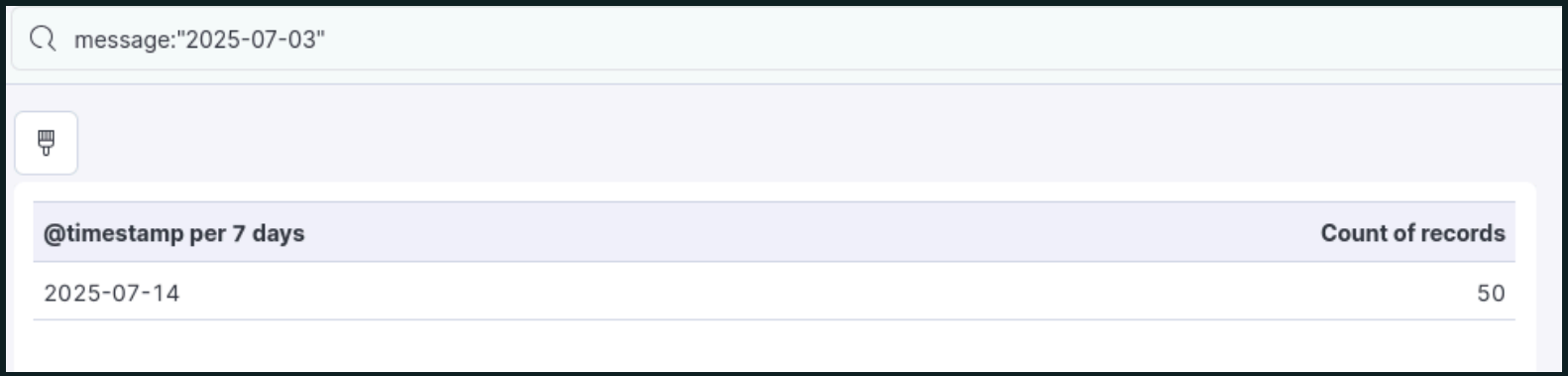
`system` (Filebeat)

Index Pattern Used: `.ds-filebeat-*`

Search Fields Used: `message`, `user`, `ip`, `action`, `threat`, `timestamp`

INCIDENT FINDINGS





1. Ransomware Behavior Detected

Timestamp: 2025-07-03 09:10:14

User: `bob`
- IP: 172.16.0.3
- Action: `malware detected`
-Threat: `Ransomware Behavior`
-Severity: High
-Description: Filebeat detected a malware alert with a ransomware behavior signature associated with user bob. The internal ip suggests this originated from within the network. Ransomware typically encrypts data and demands ransom payments, potentially halting business operations and threatening data integrity.

- Suggested Response:
- Immediately isolate Bobs host from the network.
- Block inbound/outbound traffic from the source IP.
- Run forensic scans and anti-malware tools on the host.
- Investigate lateral movement and prevent data exfiltration.

Table JSON

Copy to clipboard


```
{
  "_index": ".ds-filebeat-8.18.3-2025.07.11-000001",
  "_id": "cn2fD5gB7O4SsJF8uZmy",
  "_version": 1,
  "_source": {
    "@timestamp": "2025-07-15T19:45:29.196Z",
    "message": "2025-07-03 09:10:14 | user=bob | ip=172.16.
      0.3 | action=malware detected | threat=Ransomware
      Behavior",
    "input": {
      "type": "log"
    },
    "ecs": {
      "version": "8.0.0"
    },
    "host": {
      "name": "socmachine",
      "architecture": "x86_64",
      "os": {
```


Close

2. Suspicious File Access via Shared IP

- Timestamp: 2025-07-03 04:53:14
- User `alice`
- IP: 203.0.113.77
- Action: `file accessed`
- Severity: High
-Description: An external ip address accessed files through user alice. Repeated entries in the logs show this ip performing similar file access actions across multiple user accounts, indicating potential lateral movement by an attacker leveraging stolen credentials.

- Suggested Response:
- Investigate IP 203.0.113.77 appears to be reused across multiple user sessions.
- Filter and block repeated suspicious IPs.
- Enforce MFA and adaptive authentication for user logins.
- Implement IP reputation-based filtering.

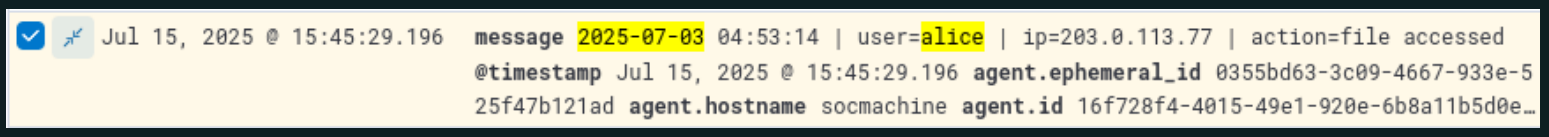
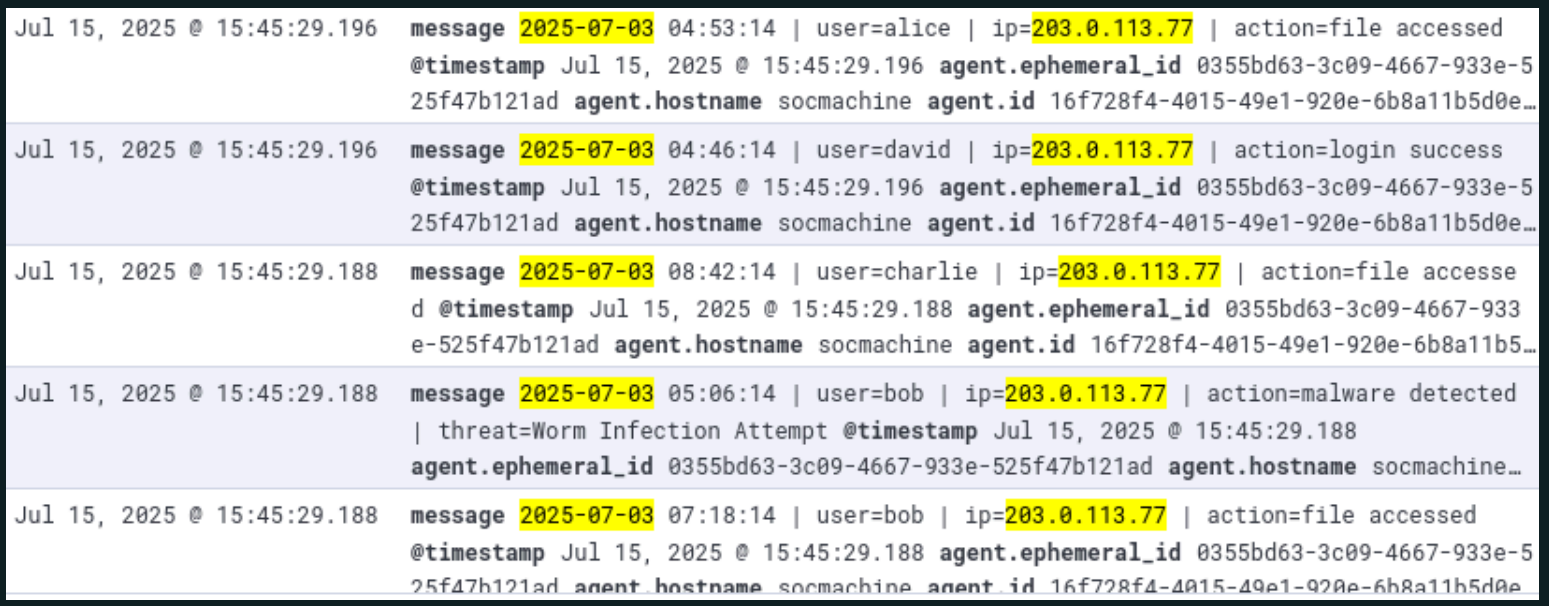


Table JSON

Copy to clipboard


```
    },
    "log": {
      "offset": 3762,
      "file": {
        "path": "/var/log/SOC_Task2_Sample_Logs.txt"
      }
    },
    "message": "2025-07-03 04:53:14 | user=alice | ip=203.0.
      113.77 | action=file accessed"
  },
  "fields": {
    "host.os.name.text": [
      "Ubuntu"
    ],
    "host.hostname": [
      "socmachine"
    ],
    "host.mac": [
      "00-0D-3A-12-41-2B"
    ],
```

3. Repeated Unauthorized Access Attempts

- Timestamp: 2025-07-03 07:22:14
- User: `charlie`
- IP: 192.168.1.101
- Action: `connection attempt`
- Severity: Medium
-Description: Multiple connection attempts were observed from internal ip under user charlie. This activity, especially repeated over different time intervals and ips, indicate an ongoing brute-force attempt aimed at password guessing.

- Suggested Response:
- Enforce account lockout policy after several failed attempts.
- Enable brute-force detection alerting.
- Require CAPTCHA or MFA during repeated logins

Jul 15, 2025 @ 15:45:29.196 **message** 2025-07-03 07:22:14 | user=charlie | ip=192.168.1.101 | action=connection attempt **@timestamp** Jul 15, 2025 @ 15:45:29.196 **agent.ephemeral_id** 0355bd63-3c09-4667-933e-525f47b121ad **agent.hostname** socmachine **agent.id** 16f728f4-4015-49e1-920e-6b8…

Jul 15, 2025 @ 15:45:29.188 **message** 2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection attempt **@timestamp** Jul 15, 2025 @ 15:45:29.188 **agent.ephemeral_id** 0355bd63-3c09-4667-933e-525f47b121ad **agent.hostname** socmachine **agent.id** 16f728f4-4015-49e1-920e-6b8…

Table JSON

Copy to clipboard


```
      "type": "Standard_B1ms"
    },
    "provider": "azure",
    "service": {
      "name": "Virtual Machines"
    }
  },
  "log": {
    "offset": 3680,
    "file": {
      "path": "/var/log/SOC_Task2_Sample_Logs.txt"
    }
  },
  "message": "2025-07-03 07:22:14 | user=charlie | ip=192.
    168.1.101 | action=connection attempt",
  "input": {
    "type": "log"
  }
},
```

4. Access Without Authorization / Least Privilege Violation

- Timestamp: 2025-07-03 06:01:14
- User: `bob`
- IP: 172.16.0.3
- Action: `file accessed`
- Severity: Medium

-Description: user bob, the same account involved in the ransomware detection, accessed a file prior to the malware alert. This suggest a potential attack chain, where the attacker gains access, performs reconnaissance, and then deploys malware.

- Suggested Response:
- Enforce least privilege on file access.
- Reclassify sensitive files and restrict user upload capabilities.
- Audit Bobs permission level vs role-based access controls.

Jul 15, 2025 @ 15:45:29.150 **message** 2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed **@timestamp** Jul 15, 2025 @ 15:45:29.150 **agent.ephemeral_id** 0355bd63-3c09-4667-933e-525f47b121ad **agent.hostname** socmachine **agent.id** 16f728f4-4015-49e1-920e-6b8a11b5d0e…

Table JSON

Copy to clipboard


```
    },
    "log": {
      "offset": 232,
      "file": {
        "path": "/var/log/SOC_Task2_Sample_Logs.txt"
      }
    },
    "message": "2025-07-03 06:01:14 | user=bob | ip=172.16.
      0.3 | action=file accessed"
  },
  "fields": {
    "host.os.name.text": [
      "Ubuntu"
    ],
    "host.hostname": [
      "socmachine"
    ],
    "host.mac": [
      "00-0D-3A-12-41-2B"
    ],
```

5. Rootkit Signature Detected

- Timestamp: 2025-07-03 07:51:14
- User: `eve`
- IP: 10.0.0.5
- Action: `malware (rootkit signature) detected`
- Severity: High
-Description: high-risk malware alert was triggered for the user on internal ip, with signature indicating a rootkit. Rootkits are designed to hide malicious activity, grant authorized persistent access, and can often evade detection by traditional security tools.

- Suggested Response:
- Immediately isolate the host from the network.
- Perform memory analysis and boot-level scans using trusted offline media.
- Conduct a forensic investigation to determine rootkit origin and entry point.
-Implement least privilege policies, endpoint protection, and kernel-level monitoring to prevent future rootkit installations.

Jul 15, 2025 @ 15:45:29.187 **message** 2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature **@timestamp** Jul 15, 2025 @ 15:45:29.187 **agent.ephemeral_id** 0355bd63-3c09-4667-933e-525f47b121ad **agent.hostname** socmachine **agent.id** 16f728f4-401…

Table JSON

Copy to clipboard


```
    "provider": "azure",
    "service": {
      "name": "Virtual Machines"
    }
  },
  "log": {
    "offset": 2088,
    "file": {
      "path": "/var/log/SOC_Task2_Sample_Logs.txt"
    }
  },
  "message": "2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature"
},
"fields": {
  "host.os.name.text": [
    "Ubuntu"
  ],
```

Conclusion

The analysis of ingested log data revealed multiple indicators of compromise within the monitored environment, including evidence of malware deployment (ransomware and rootkit), brute-force connection attempts, and unauthorized file access from external sources. These events suggest an adversary was able to exploit insufficient access controls and weak authentication mechanisms to perform lateral movement and deploy malicious code.

Immediate containment steps should focus on isolating compromised systems, performing root-cause analysis, and validating the integrity of critical data. Long-term, this incident highlights the urgent need to implement least privilege access, enhance authentication protocols, and deploy advanced endpoint protection and prevent future threats.

This investigation reinforces the importance of centralized log monitoring and correlation for early threat detection and rapid incident response across the organization.