Task 2: Security Alert Monitoring & Incident Response Simulation

Tasks

- 1. Set up and explore a free or demo SIEM tool (Security Information and Event Management) like Elastic Stack (ELK) or Splunk Free Trial
- 2. Analyze incoming security alerts and logs (simulated data provided)
- 3. Identify suspicious activities such as failed logins, unusual IP addresses, or malware alerts
- 4. Categorize and prioritize alerts based on severity
- 5. Draft an incident response report outlining the threat, impact, and suggested next steps (**This report itself is task 5)**
- 6. Simulate communication with stakeholders about the incident
- 7. Learn how SOC teams track and manage threats using dashboards and playbooks

Key Features to Include

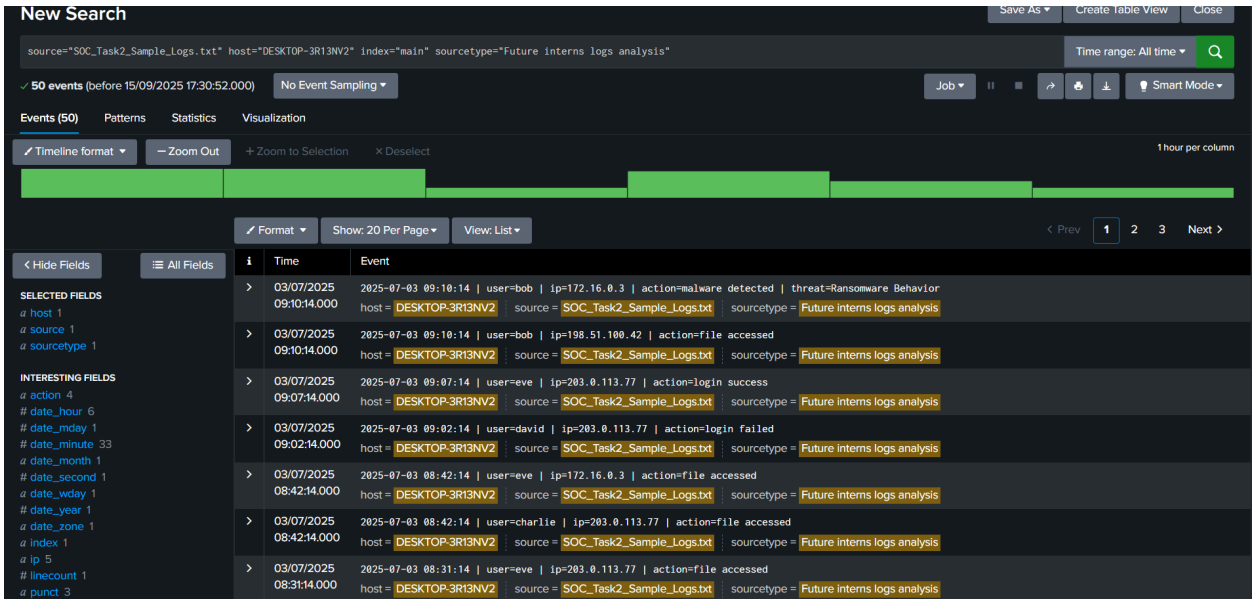
- Ability to identify 3–5 suspicious alerts from logs
- Incident classification by priority (High, Medium, Low)
- Detailed incident response report with timeline, impact, and remediation suggestions
- A summary dashboard screenshot from the SIEM tool
- (Optional) A communication email template reporting the incident to management

Task 1: Set up and explore a free or demo SIEM tool (Security Information and Event Management) like Elastic Stack (ELK) or Splunk Free Trial

Set up

- Installed Splunk Enterprise 10.0.0 on windows
- Gathered on the “add data” section on the splunk dashboard
- This now taken me towards the “Select Source” page where I will be uploading the sample logs provided by future interns

- Now I am on the Set Source Type, I will just be choosing the default section to make things much simple
- After checking the input Settings and reviewing everything, I am now ready to use splunk and start searching
- I was able to use SQL commands in the new search text box where I was able to grab certain parts of the log sample and record it into a table (e.g index="main" sourcetype="future interns log analysis" **failed (only returns failed login logs only)** This made life easier as I wouldn't have to keep scrolling through 50 events just to find all the specific security alert (lets say I want to find only the alerts that detected malware but instead of using SQL commands I would have to scroll through the 50 events which will take forever) which will take up most of my time..



Task 2 Log analysis (covers both task 2 ,3 and 4)

Spreadsheet/excel

I've used microsoft edge to organise raw data that I have collected through the use of splunk enterprise into separate, simple, defined tables. Each table that is shown below is identified through the specific type of security alert (malware alert, failed login etc).

By separating these logs using this method, I have managed to:

- Quickly identify the type of security event and its associated details

- Spotting patterns that can help me understand what type of threat is being conducted and quickly find ways to prevent that specific threat.
- Able to trace IP addresses across different events, like seeing the same IP address across different tables.

Table 1 failed login

Table 1 shows the failed login action

time	host	source	sourcetype	user and date	IP address	Action
2025-07-03T09:02:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 09:02:14 | user=david	| ip=203.0.113.77	login failed
2025-07-03T07:02:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 07:02:14 | user=alice	| ip=203.0.113.77	login failed
2025-07-03T04:47:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:47:14 | user=bob	| ip=10.0.0.5	login failed
2025-07-03T04:23:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:23:14 | user=bob	| ip=172.16.0.3	login failed
2025-07-03T04:23:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:23:14 | user=charlie	| ip=198.51.100.42	login failed

As you can see, there are two accounts that tried to sign into the system with the exact same IP address, with the user Alice that tried to login into the system but failed then 2 minutes later another user “david” with the same ip address tried to log into the system but failed. As a result multiple failed logins were observed for users like david, alice, bob and charlie. This is a brute-force attack, no mistake.

Threat(low): You can see that multiple attempts to get into the system were observed. Especially from IP address 203.0.113.77 that tried to log into multiple users accounts but failed .

Impact: Accounts might eventually get stolen if they're not taken care well security wise, allowing attackers to get into their accounts allowing authorised access

Next steps:

- Use a firewall to block suspicious IP address like 203.0.113.77
- Encourage users to use strong passwords
- To fully prevent a brute-force attack make sure to lock the account after 3 attempts are made

Table 2 success login table

Table 2 shows the login success table

time	host	source	sourcetype	user and date	IP address	Action
2025-07-03T09:07:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 09:02:14 | user=david	| ip=203.0.113.77	login success
2025-07-03T08:30:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 07:02:14 | user=alice	| ip=172.16.0.3 |	login success
2025-07-03T08:00:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:47:14 | user=bob	| ip=198.51.100.42	login success
2025-07-03T07:46:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:23:14 | user=bob	| ip=10.0.0.5	login success
2025-07-03T06:21:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:23:14 | user=charlie	| ip=203.0.113.77	login success
2025-07-03T05:18:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 05:18:14 | user=charlie	| ip=172.16.0.3	login success
2025-07-03T05:12:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 05:12:14 | user=alice	| ip=198.51.100.42	login success
2025-07-03T05:04:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 05:04:14 | user=bob	| ip=192.168.1.101	login success
2025-07-03T04:53:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:53:14 | user=david	| ip=203.0.113.77	login success
2025-07-03T04:46:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:46:14 | user=david	| ip=203.0.113.77	login success
2025-07-03T04:18:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:18:14 | user=bob	| ip=198.51.100.42	login success

This is the table that consists of successful logins; this means the attacker has managed to gain authorised access after facing a lot of failed attempts (you can view those failed attempts in Table 1). You can see the same suspicious IP address 203.0.113.77 occurring a lot of times during the brute - force attack. You can also see

another IP address like “198.51.100.42” appearing a lot of times. Overall this means that the attacker has managed to finally get in after a lot of failed attempts using a suspicious ip address, this also means that the system can not handle an attack such as a brute-force attack.

Threat(high): This shows that the attacker may of gained authorized access to the system after facing multiple of failed attempts via brute force attack
Impact: This may result in serious lawsuits against the company holding the accounts due to lack of security and allowing the attackers to touch sensitive data in which they could encrypt the data and hold it for ransomware.
Possible next steps:

- Add an authentication system. This means even if the attacker manages to get in the system, they will have to crack the authentication code to see if it's the correct person that logged in.
- Introduce a captcha style puzzle system where the user has to solve the human puzzle to prove it's not an automated hacking tool that logs in the user accounts.

Table 3 malware alert table

Table 3 shows the malware alert table

time	host	source	sourcetype	user and date	IP address	Action and threat
2025-07-03T09:10:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 09:10:14 | user=bob	| ip=172.16.0.3	action=malware detected | threat=Ransomware Behavior
2025-07-03T07:51:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 07:51:14 | user=eve	| ip=10.0.0.5	action=malware detected | threat=Rootkit Signature
2025-07-03T07:45:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 07:45:14 | user=charlie	| ip=172.16.0.3	action=malware detected | threat=Trojan Detected
2025-07-03T05:48:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 05:48:14 | user=bob	| ip=10.0.0.5	action=malware detected | threat=Trojan Detected
2025-07-03T05:45:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 05:45:14 | user=david	| ip=172.16.0.3	action=malware detected | threat=Trojan Detected
2025-07-03T05:42:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 05:42:14 | user=eve	| ip=203.0.113.77	action=malware detected | threat=Trojan Detected
2025-07-03T05:30:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 05:30:14 | user=eve	| ip=192.168.1.101	action=malware detected | threat=Trojan Detected
2025-07-03T05:06:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 05:06:14 | user=bob	| ip=203.0.113.77	action=malware detected | threat=Worm Infection Attempt
2025-07-03T04:41:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:41:14 | user=alice	| ip=172.16.0.3	action=malware detected | threat=Spyware Alert
2025-07-03T04:29:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:29:14 | user=alice	| ip=192.168.1.101	action=malware detected | threat=Trojan Detected
2025-07-03T04:19:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:19:14 | user=alice	| ip=198.51.100.42	action=malware detected | threat=Rootkit Signature

This table records multiple malware detections affecting many users and heavily damaging the system. This table shows that both the system and the users were affected by malware like trojan, worms, spyware , etc the list goes on. One key feature of this table that I noticed is that the IP address “172.16.0.3” showed that it faced multiple malware threats, suggesting it is a heavily compromised endpoint.

Threat(high): This shows that the system detected multiple malware, especially harming certain users like the user using the ip address “172.16.0.3” > showing lack of cybersecurity awareness.
Impact: If not handed well, the malware will conduct a malicious intent such as deleting certain users files, encrypt user data, leak the data, etc.
Possible next steps:

- Cybersecurity awareness > train users to understand basic cybersecurity concepts such as identifying a potential trojan threat (popular virus people fell for in table 3)

- Installing anti-virus applications that deals with malware alerts for you and protects you
- Understand the key vulnerabilities and learn how to patch it

Table 4 - Files that has been accessed

Table 4 will show the files that has been accessed

time	host	source	sourcetype	user and date	IP address	Action
2025-07-03T09:10:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 09:10:14 | user=bob	| ip=198.51.100.42	action=file accessed
2025-07-03T08:42:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 08:42:14 | user=eve	| ip=172.16.0.3	action=file accessed
2025-07-03T08:42:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 08:42:14 | user=charlie	| ip=203.0.113.77	action=file accessed
2025-07-03T08:31:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 08:31:14 | user=eve	| ip=203.0.113.77	action=file accessed
2025-07-03T07:57:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 07:57:14 | user=david	| ip=10.0.0.5	action=file accessed
2025-07-03T07:18:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 07:18:14 | user=bob	| ip=203.0.113.77	action=file accessed
2025-07-03T06:10:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 06:10:14 | user=david	| ip=192.168.1.101	action=file accessed
2025-07-03T06:01:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 06:01:14 | user=bob	| ip=172.16.0.3	action=file accessed
2025-07-03T05:44:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 05:44:14 | user=bob	| ip=198.51.100.42	action=file accessed
2025-07-03T05:33:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 05:33:14 | user=david	| ip=198.51.100.42	action=file accessed
2025-07-03T04:53:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:53:14 | user=alice	| ip=203.0.113.77	action=file accessed

This table shows that a user has able to access a file but however using our knowledge from the earlier table, the malicious ip address we identified appeared multiple of times again in this table and managed to gain control over a file (IP 203.0.113.77) This shows that those files could potentially be used in a malicious attempt (ransomware, file deletion,) .

Threat(high): A file has been accessed by a malicious ip address meaning if this is not taken care well those files that has been accessed by the malicious ip address could be used in a wrong intent that will cause harm to the system.
Impact: Risk of data thefts and sensitive data being viewed by an unauthorized person.
Possible next steps:

- Firewall to block any malicious IP address and restrict it to necessary users
- Monitor if any data has been exposed and close the account to prevent any future harm

Table 5 - Connection Attempt

Table 5 shows if a connection attempt has been made

time	host	source	sourcetype	user and date	IP address	Action
2025-07-03T08:21:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 08:21:14 | user=david	| ip=172.16.0.3	action=connection attempt
2025-07-03T08:20:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 08:20:14 | user=charlie	| ip=192.168.1.101	action=connection attempt
2025-07-03T07:44:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 07:44:14 | user=bob	| ip=192.168.1.101	action=connection attempt
2025-07-03T07:44:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 07:44:14 | user=bob	| ip=203.0.113.77	action=connection attempt
2025-07-03T07:38:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 07:38:14 | user=charlie	| ip=172.16.0.3	action=connection attempt
2025-07-03T07:36:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 07:36:14 | user=david	| ip=10.0.0.5	action=connection attempt
2025-07-03T07:22:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 07:22:14 | user=charlie	| ip=192.168.1.10	action=connection attempt
2025-07-03T06:13:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 06:13:14 | user=charlie	| ip=10.0.0.5	action=connection attempt
2025-07-03T05:49:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 05:49:14 | user=charlie	| ip=192.168.1.101	action=connection attempt
2025-07-03T05:27:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 05:27:14 | user=david	| ip=203.0.113.77	action=connection attempt
2025-07-03T04:27:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:27:14 | user=david	| ip=172.16.0.3	action=connection attempt
2025-07-03T04:19:14.000+01:00	DESKTOP-3R13NV2	SOC_Task2_Sample_Logs.txt	Future interns logs analysis	2025-07-03 04:19:14 | user=david	| ip=10.0.0.5	action=connection attempt

Threat (med): This shows a connection attempt that was made by the internal and external IP address and the fact that the same IP addresses appear again from the previous tables shows lateral movements attempted within the network.
Impact: Attackers will spread throughout the system allowing more attackers to attack the system if not taken care well
Next steps:

- Block external malicious IPs.
- Segment the network to reduce lateral movement.
- Monitor internal connections for unusual traffic.

Task 6: Simulate communication with stakeholders about the incident

Subject: Security Alert! Action needed!

Dear, team

Our monitoring has identified many failed Logins, malicious IP address gaining authorized access towards users accounts, multiple malware attempts and suspicious file access from an external IP address. This could ending up suggesting that most accounts were stolen and broken in.

We recommend blocking the malicious IPs, resetting user credentials, and scanning affected machines immediately.

Please take action as fast as possible before it’s too late.

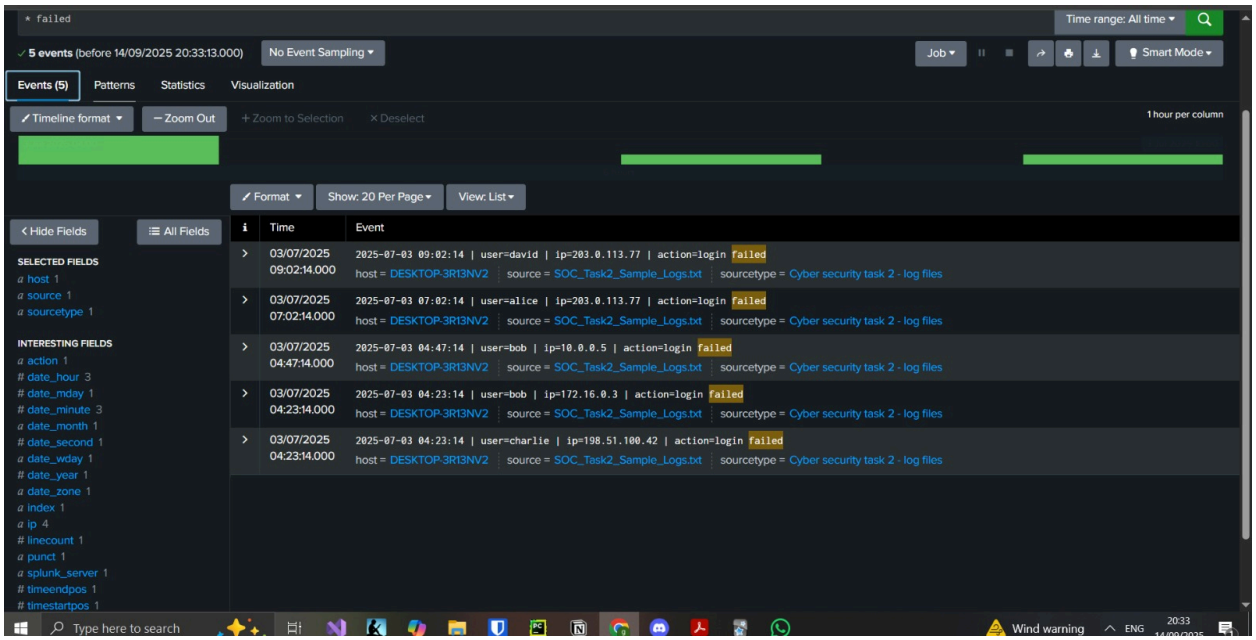
Thank you for reading this,

Yours sincerely, the SOC analyst team.

Task 7: Learn how SOC teams track and manage threats using dashboards and playbooks

I've used the splunk dashboard to visualise and filter security alert events. For example, the screenshot I have provided below shows the failed login attempts that splunk had turned the data into a table for better readability, this table covered the user name, the suspicious IP address, the time, etc. Dashboards made it very easy to cover and detect suspicious events without having to scroll down forever through raw, unorganised data.

SOC teams also use playbooks, which are step by step guides that explain how to respond to different types of incidents. (brute-force attack, trojans, spyware etc). Playbooks ensure that analyst follows a consistent process, reduce mistake and respond to a threat at a fast rate when it occurs.


* failed
Time range: All time
5 events (before 14/09/2025 20:33:13.000)
No Event Sampling
Job
Smart Mode
Events (5)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 1
date_hour 3
date_mday 1
date_minute 3
a date_month 1
date_second 1
a date_wday 1
date_year 1
a date_zone 1
a index 1
a ip 4
linecount 1
a punct 1
a splunk_server 1
timeendpos 1
timestartpos 1
Time
Event
03/07/2025 09:02:14.000
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
host = DESKTOP-3R13NV2 source = SOC_Task2_Sample_Logs.txt sourcetype = Cyber security task 2 - log files
03/07/2025 07:02:14.000
2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
host = DESKTOP-3R13NV2 source = SOC_Task2_Sample_Logs.txt sourcetype = Cyber security task 2 - log files
03/07/2025 04:47:14.000
2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed
host = DESKTOP-3R13NV2 source = SOC_Task2_Sample_Logs.txt sourcetype = Cyber security task 2 - log files
03/07/2025 04:23:14.000
2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login failed
host = DESKTOP-3R13NV2 source = SOC_Task2_Sample_Logs.txt sourcetype = Cyber security task 2 - log files
03/07/2025 04:23:14.000
2025-07-03 04:23:14 | user=charlie | ip=198.51.100.42 | action=login failed
host = DESKTOP-3R13NV2 source = SOC_Task2_Sample_Logs.txt sourcetype = Cyber security task 2 - log files
Type here to search
Wind warning
ENG
20:33