

Sample prompt - Demo #1

Analyze the following log file data. Act as a senior system administrator and identify the most concerning issue. A 'concerning issue' is defined as one that indicates a high probability of system failure, security breach, severe performance degradation, or frequent, unhandled errors.

Log files – Demo #1

```
172.16.0.100 10.1.16.1 TCP 42382 -> dns (53) [SYN] Seq=0 Win=4128 Len=0 MSS=1460
10.1.16.1 172.16.0.100 TCP dns (53) -> 42382 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0
172.16.0.100 10.1.16.1 TCP 42382 -> dns (53) [ACK] Seq=1 Ack=1 Win=4128 Len=0
10.1.16.1 172.16.0.100 SSH Server: Protocol (SSH-2.0-Cisco-1.25)
172.16.0.100 10.1.16.1 SSH Client: Protocol (SSH-1.99-Cisco-1.25)
10.1.16.1 172.16.0.100 SSHv2 Server: Key Exchange Init
103.34.243.12 10.1.16.2 TCP 35014 -> ftp (21) [SYN] Seq=0 Win=65535 Len=0
10.1.16.2 103.34.243.12 TCP ftp (21) -> 35014 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
103.34.243.12 10.1.16.2 TCP 35014 -> ftp (21) [ACK] Seq=1 Ack=1 Win=65535 Len=0
10.1.16.2 103.34.243.12 FTP Response: 220 ProFTPD 1.3.0a Server
103.34.243.12 10.1.16.2 FTP Request: User FTP
10.1.16.2 103.34.243.12 FTP Response: 331 Anonymous login ok, send your complete email address
as your password.
103.34.243.12 10.1.16.2 FTP Request: Pass ftp 10.1.16.1 103.34.243.12 FTP Response: 230
Anonymous access granted, restrictions apply.
172.16.0.201 10.1.16.1 TCP 29752 -> 8080[SYN] Seq=0 Win=5840 Len=0 MSS=1460
SACK_PERM=1 TSval= 2216538 TSecr=0 WS=128
10.1.16.1 172.16.0.201 TCP 8080 -> 29752[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460
SACK PERM=1 TSval=833172636 TSecr=2916238 WS=64
172.16.0.201 10.1.16.1 TCP 29752 -> 8080 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=2217543
TSecr=833172636
172.16.0.201 10.1.16.1 HTTP GET /images/layout/logo.png HTTP/1.0
172.16.0.201 10.1.16.1 TCP 29752 -> 8080 [ACK] Seq=135 Ack=2897 Win=11648 Len=0
TSva1=2217548 TSecr=835172048
```

Sample prompt - Demo #2

As an experienced Network Administrator, your task is to analyze the following firewall log data. Scan the logs for patterns indicative of malicious activity (e.g., port scanning, excessive failed authentication attempts, or requests targeting sensitive endpoints) or severe network performance issues (e.g., unusually high request volume leading to resource exhaustion). Based on this analysis, identify the single most concerning source IP address that warrants urgent isolation and further forensics, and provide a clear, technical explanation detailing the specific suspicious activity or error pattern associated with that IP address.

Log files – Demo #2

5-4-2023 12:34:56 FROM 10.1.24.101:2762 TO 220.181.38.251:53 PERMIT UDP 247 BYTES

5-4-2023 12:34:57 FROM 10.1.16.2:31765 TO 10.1.16.1:80 PERMIT TCP 10K BYTES

5-4-2023 12:34:59 FROM 10.1.16.1:1536 TO 5.255.255.88:23 DENY TCP 1 BYTES

5-4-2023 12:35:01 FROM 10.1.24.101:2762 TO 220.181.38.251:53 PERMIT UDP 1029M BYTES

5-4-2023 12:35:13 FROM 10.1.16.11:1846 TO 1.1.1.1:53 PERMIT UDP 178 BYTES

5-4-2023 12:35:45 FROM 10.1.16.2:9648 TO 4.2.2.1:21 DENY TCP 1 BYTES

5-4-2023 12:36:25 FROM 10.1.24.13:51348 TO 204.79.197.200:80 PERMIT TCP 34K BYTES

5-4-2023 12:36:31 FROM 10.1.24.101:7777 TO 212.82.100.150:7777 DENY TCP 1 BYTES

5-4-2023 12:36:55 FROM 10.1.16.1:4918 TO 104.18.16.29:587 PERMIT 789 BYTES

Sample Prompt - Demo #3

As a Security Operations Center (SOC) Analyst, analyze the following Task Manager process table to identify the single most concerning process. A 'concerning process' is defined as one showing extreme resource usage, an unusual or obfuscated name, or a process running under an unexpected user account (e.g., system service running as a standard user). Identify the process name and the user account it is running under, and state the primary technical reason why it warrants immediate investigation.

Log files – Demo #3

Process	PID	Mem usage	CPU time	User
cmd.exe	506	27998	01:53:47	renee
explorer.exe	798	59624	01:01:37	n/a
nc.exe	135	16048	03:44:11	jaime
winlogon	664	3078	03:59:24	n/a
notepad.exe	1051	5088	01:25:41	renee
cmd.exe	113	24713	03:41:54	jaime

