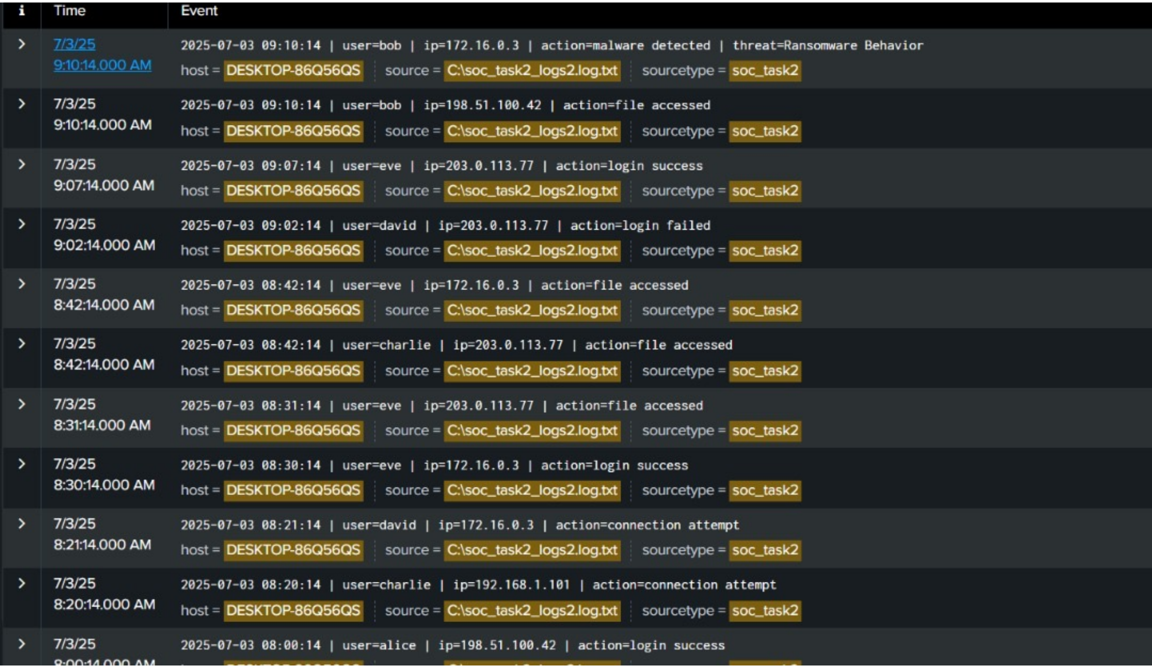
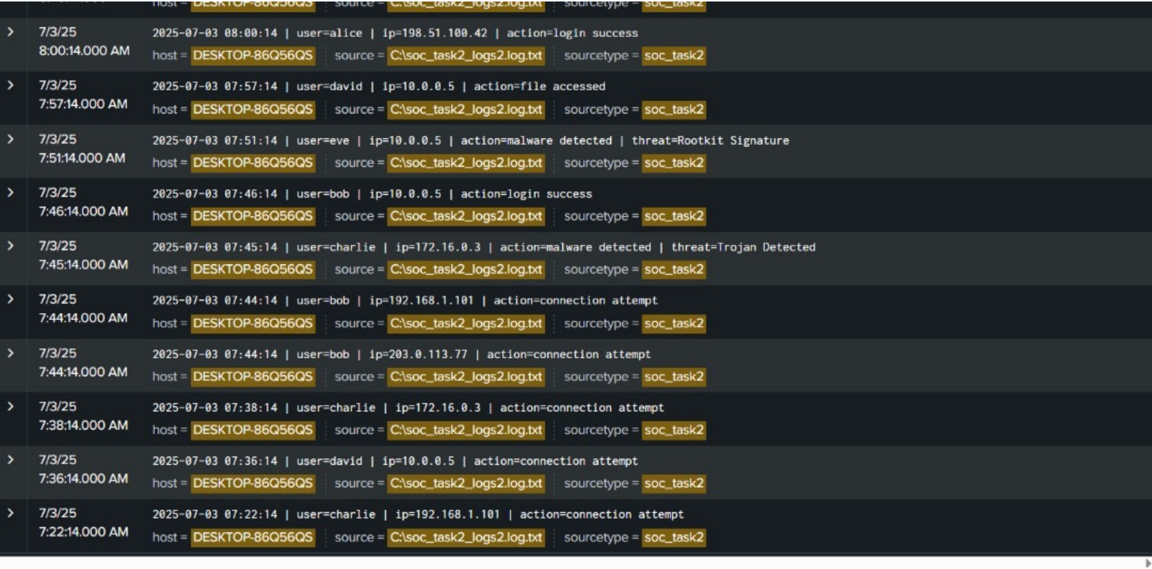
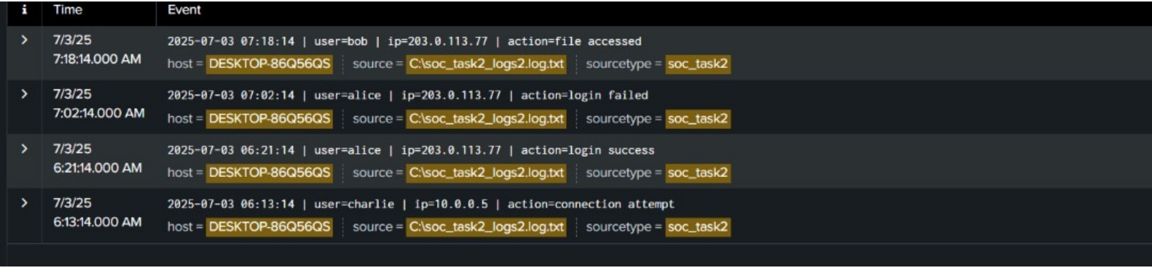


```
i   Time                Event
>   7/3/25              2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
    9:10:14.000 AM      host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25              2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
    9:10:14.000 AM      host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25              2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
    9:07:14.000 AM      host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25              2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
    9:02:14.000 AM      host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25              2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
    8:42:14.000 AM      host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25              2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
    8:42:14.000 AM      host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25              2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
    8:31:14.000 AM      host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25              2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
    8:30:14.000 AM      host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25              2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
    8:21:14.000 AM      host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25              2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
    8:20:14.000 AM      host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25              2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
    8:00:14.000 AM
```



```
      host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>  7/3/25           2025-07-03 08:00:14 | user=alice | ip=198.51.100.42 | action=login success
   8:00:14.000 AM   host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>  7/3/25           2025-07-03 07:57:14 | user=david | ip=10.0.0.5 | action=file accessed
   7:57:14.000 AM   host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>  7/3/25           2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
   7:51:14.000 AM   host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>  7/3/25           2025-07-03 07:46:14 | user=bob | ip=10.0.0.5 | action=login success
   7:46:14.000 AM   host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>  7/3/25           2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
   7:45:14.000 AM   host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>  7/3/25           2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection attempt
   7:44:14.000 AM   host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>  7/3/25           2025-07-03 07:44:14 | user=bob | ip=203.0.113.77 | action=connection attempt
   7:44:14.000 AM   host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>  7/3/25           2025-07-03 07:38:14 | user=charlie | ip=172.16.0.3 | action=connection attempt
   7:38:14.000 AM   host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>  7/3/25           2025-07-03 07:36:14 | user=david | ip=10.0.0.5 | action=connection attempt
   7:36:14.000 AM   host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>  7/3/25           2025-07-03 07:22:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
   7:22:14.000 AM   host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
```



```
i   Time                  Event
>   7/3/25                2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accessed
    7:18:14.000 AM        host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25                2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed
    7:02:14.000 AM        host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25                2025-07-03 06:21:14 | user=alice | ip=203.0.113.77 | action=login success
    6:21:14.000 AM        host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
>   7/3/25                2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
    6:13:14.000 AM        host = DESKTOP-86Q56QS   source = C:\soc_task2_logs2.log.txt   sourcetype = soc_task2
```