SOC EXPERTS

SOC ANALYST

INTERVIEW QUESTIONS & ANSWERS

Category - Raw Logs

What are the reasons for Login failures in Windows?

Status and Sub Status Codes	Description
0xC0000064	User name does not exist
0xC000006A	User name is correct but the password is wrong
0xC0000234	User is currently locked out
0xC0000072	Account is currently disabled
0xC000006F	User tried to logon outside his day of week or time of day restrictions
0xC0000070	Workstation restriction, or Authentication Policy Silo violation
0xC0000193	Account expiration
0xC0000071	Expired password
0xC0000133	Clocks between DC and other computer too far out of sync
0xC000015B	The user has not been granted the requested logon type (aka logon right) at this machine

What logs do you collect from a database?

Audit Logs

Difference between Flows and Events.

Event is a log of a particular action.

A flow records information like number of packets, bytes sent, bytes received and connection time.

Why do we need raw logs?

The raw logs are required for Forensics and Compliance purposes.

Difference between an Event, Alert and Incident

Event is a log of particular action on a server.

Alert is a suspicious (not confirmed) activity in the network.

An incident is a confirmed malicious activity.

SOC EXPERTS

Cybersecurity Careers for Everyone

Cybersecurity Career Launcher (CCL)
For Graduates | 3 months

Career Switch to Cybersecurity (CSC)
For Working Professionals | 2 Months

+91 773-774-8282

learn@socexperts.com

www.socexperts.com