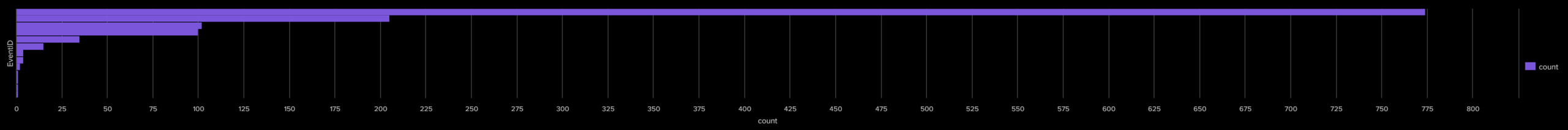
SOC Visibility Board

ti...

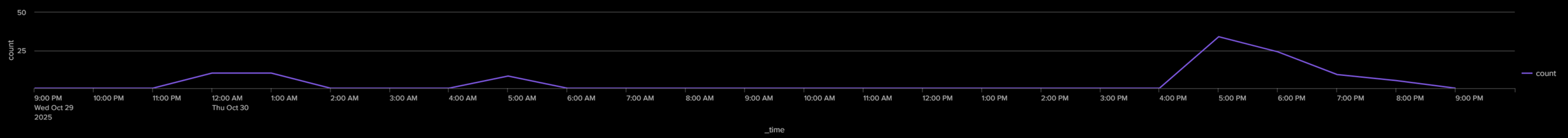
Last 24 hours

Top Windows Security Events by Frequency - Displays the most common Windows Security Event IDs extracted from XML logs to identify which activities dominate the dataset.

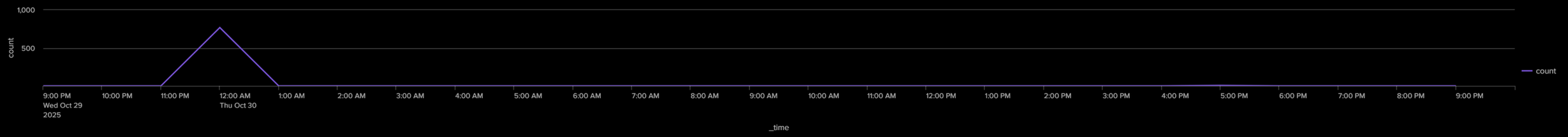


Successful User Logons (Event ID 4624) - Tracks all successful authentication events over time, helping detect login bursts or unusual access periods.

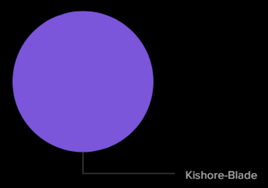
Privileged Logons – Administrator or Service Accounts (Event ID 4672) - Highlights high-privilege logons granted to administrator or service accounts, which could indicate privilege escalation.



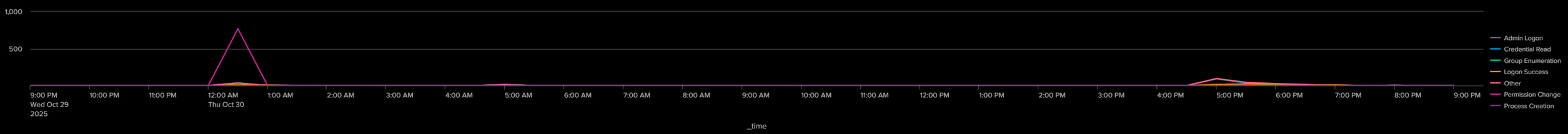
Permission and Policy Modifications (Event ID 4907) - Monitors events involving permission or security descriptor changes — key for detecting potential insider or privilege abuse.



Credential Access Activity by Host (Event ID 5379) - Shows how frequently credential read attempts occurred per host, useful for identifying possible credential harvesting or dumping activity.



Security Events Overview by Category (Sysmon + Security Logs) - Aggregates major security event types — logons, process creation, permission changes, and credential reads — into a unified timeline for visibility across all hosts.



Event Distribution: Sysmon vs Windows Security Sources - Shows the proportion of total indexed events collected from Sysmon telemetry and Windows Security logs, helping validate data source coverage in the SOC environment.