

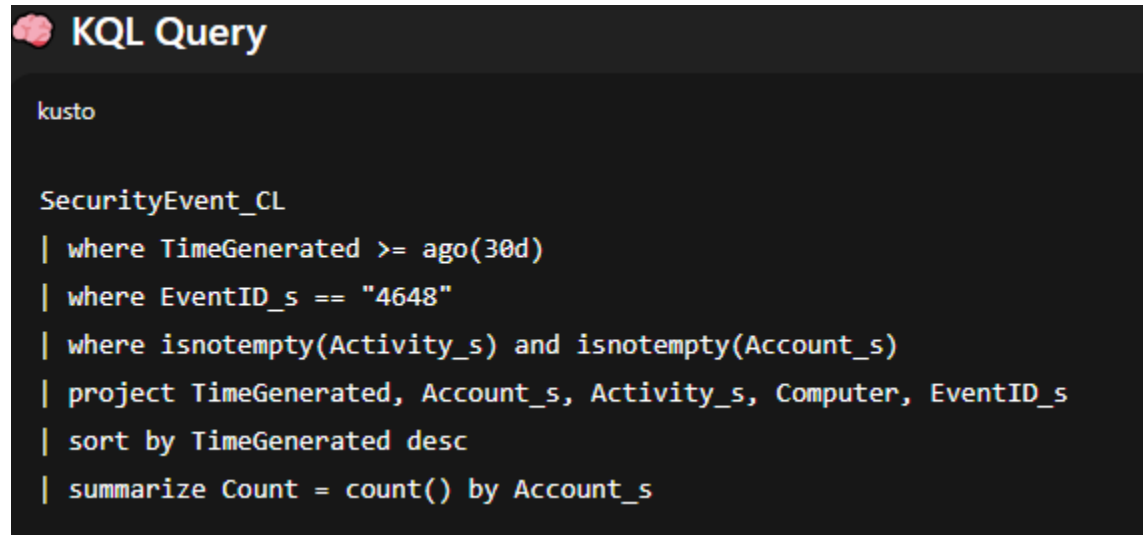
Adding panels to your Sentinel dashboard

KQL Threat Hunting Example: Investigating Explicit Credential Logons (Event ID 4648)

As part of my Microsoft Sentinel detective work, I use KQL to hunt for suspicious authentication activity—especially events tied to credential misuse and lateral movement.

The query below focuses on **Event ID 4648**, which indicates that a process attempted to log on using **explicit credentials** (often associated with attacker techniques such as pass-the-hash or privilege escalation).

KQL Query



```
kusto

SecurityEvent_CL
| where TimeGenerated >= ago(30d)
| where EventID_s == "4648"
| where isnotempty(Activity_s) and isnotempty(Account_s)
| project TimeGenerated, Account_s, Activity_s, Computer, EventID_s
| sort by TimeGenerated desc
| summarize Count = count() by Account_s
```

✅ KQL Query Breakdown (Simplified Bullet Points)

- **Filters Security Logs**
Queries the SecurityEvent_CL table where Windows Security Events are stored.
- **Last 30 Days Only**
| where TimeGenerated >= ago(30d)
Focuses the investigation on recent activity.
- **Looks for Event ID 4648**
| where EventID_s == "4648"
This event shows when a process uses **explicit credentials** — a common sign of lateral movement, credential theft, or privilege escalation.
- **Removes Empty/Noisy Logs**
| where isnotempty(Activity_s) and isnotempty(Account_s)
Ensures only clean, useful records are analyzed.
- **Shows Only Important Fields**
| project TimeGenerated, Account_s, Activity_s, Computer, EventID_s
Displays the key details for investigation:

- Time
- Account used
- Activity performed
- Computer
- Event ID
- **Sorts by Newest Activity**
 - | sort by TimeGenerated desc
 - Makes it easier to spot suspicious events in order.
- **Counts Events per Account**
 - | summarize Count = count() by Account_s
 - Helps identify:
 - Accounts authenticating more than usual
 - Abnormal service account behavior
 - Credential testing / brute-force attempts
 - Unexpected movement across systems

```
SecurityEvent_CL
| where TimeGenerated >= ago(30d)
| where EventID_s == "4648"
| where isnotempty(Activity_s) and isnotempty(Account_s)
| project TimeGenerated, Account_s, Activity_s, Computer, EventID_s
| sort by TimeGenerated desc
| summarize Count = count() by Account_s
```

