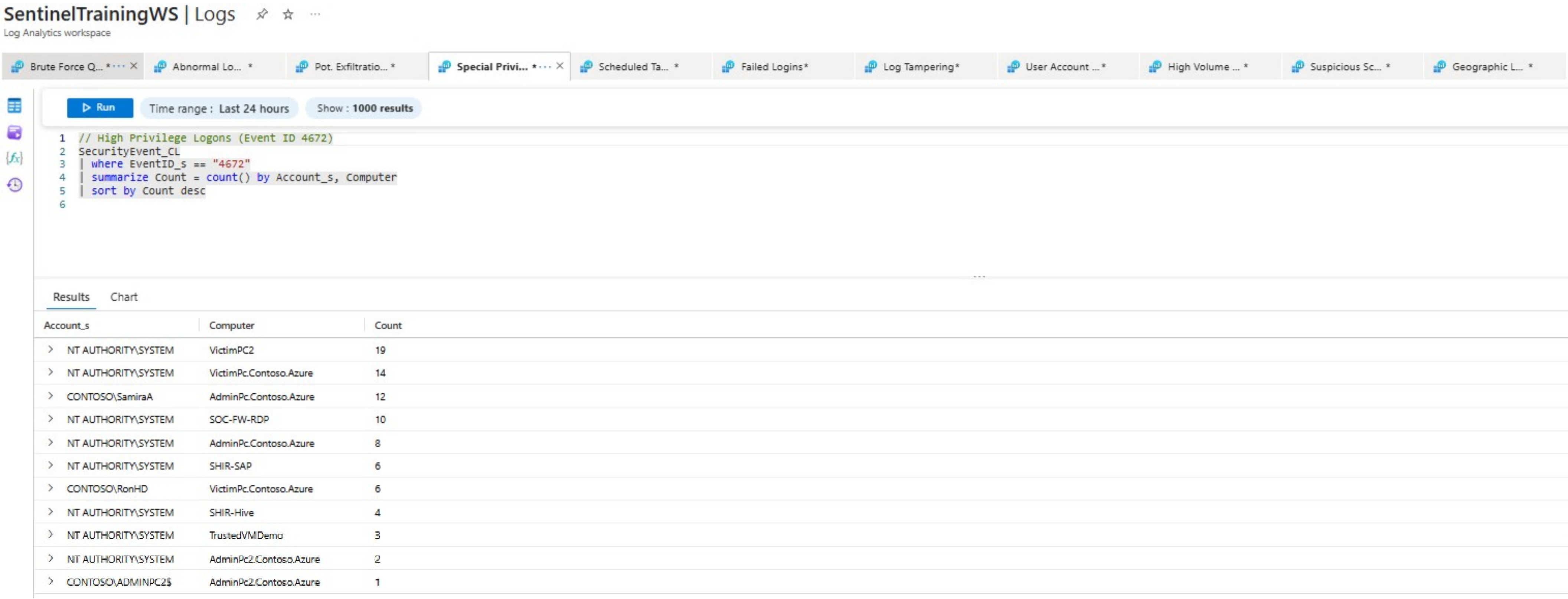
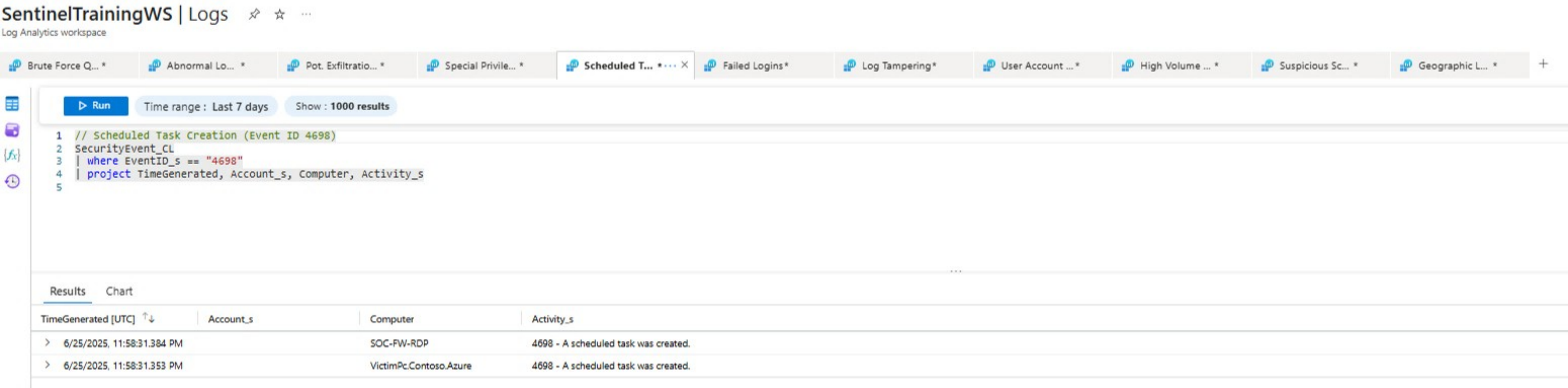


```
// High Privilege Logons (Event ID 4672)
SecurityEvent_CL
| where EventID_s == "4672"
| summarize Count = count() by Account_s, Computer
| sort by Count desc
```

Account_s	Computer	Count
NT AUTHORITY\SYSTEM	VictimPC2	19
NT AUTHORITY\SYSTEM	VictimPc.Contoso.Azure	14
CONTOSO\SamiraA	AdminPc.Contoso.Azure	12
NT AUTHORITY\SYSTEM	SOC-FW-RDP	10
NT AUTHORITY\SYSTEM	AdminPc.Contoso.Azure	8
NT AUTHORITY\SYSTEM	SHIR-SAP	6
CONTOSO\RonHD	VictimPc.Contoso.Azure	6
NT AUTHORITY\SYSTEM	SHIR-Hive	4
NT AUTHORITY\SYSTEM	TrustedVMDemo	3
NT AUTHORITY\SYSTEM	AdminPc2.Contoso.Azure	2
CONTOSO\ADMINPC2$	AdminPc2.Contoso.Azure	1



SentinelTrainingWS | Logs

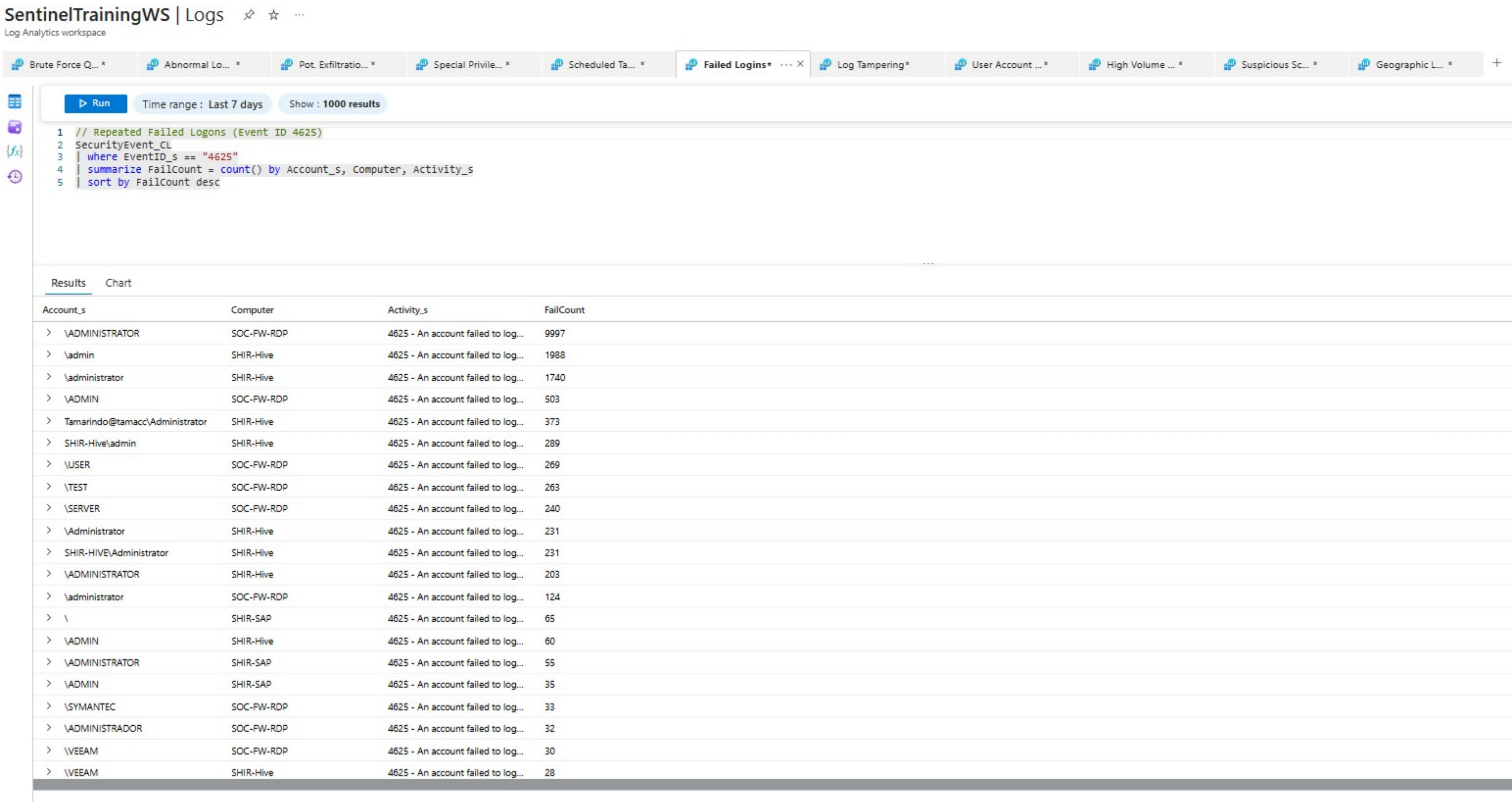
Log Analytics workspace

Time range : Last 7 days

Show : 1000 results

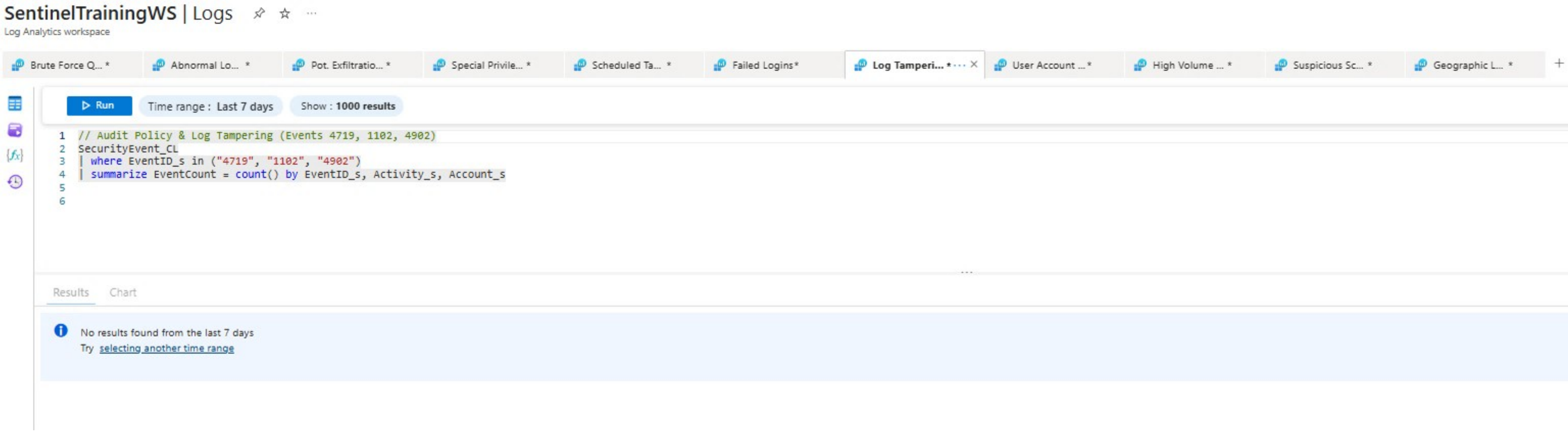
```
// Scheduled Task Creation (Event ID 4698)
SecurityEvent_CL
| where EventID_s == "4698"
| project TimeGenerated, Account_s, Computer, Activity_s
```

TimeGenerated [UTC]	Account_s	Computer	Activity_s
6/25/2025, 11:58:31.384 PM		SOC-FW-RDP	4698 - A scheduled task was created.
6/25/2025, 11:58:31.353 PM		VictimPc.Contoso.Azure	4698 - A scheduled task was created.



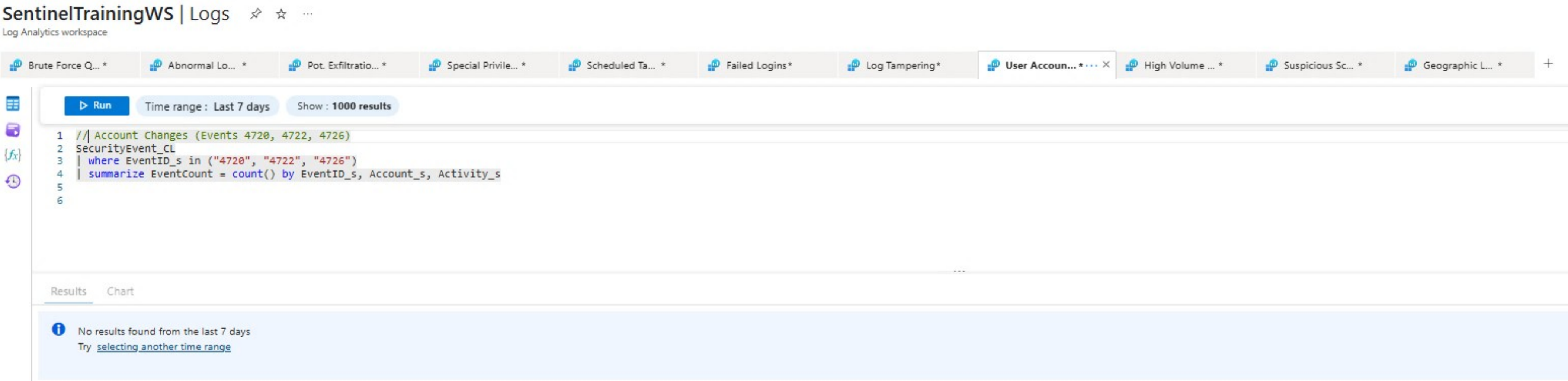
```
// Repeated Failed Logons (Event ID 4625)
SecurityEvent_CL
| where EventID_s == "4625"
| summarize FailCount = count() by Account_s, Computer, Activity_s
| sort by FailCount desc
```

Account_s	Computer	Activity_s	FailCount
\ADMINISTRATOR	SOC-FW-RDP	4625 - An account failed to log...	9997
\admin	SHIR-Hive	4625 - An account failed to log...	1988
\administrator	SHIR-Hive	4625 - An account failed to log...	1740
\ADMIN	SOC-FW-RDP	4625 - An account failed to log...	503
Tamarindo@tamacc\Administrator	SHIR-Hive	4625 - An account failed to log...	373
SHIR-Hive\admin	SHIR-Hive	4625 - An account failed to log...	289
\USER	SOC-FW-RDP	4625 - An account failed to log...	269
\TEST	SOC-FW-RDP	4625 - An account failed to log...	263
\SERVER	SOC-FW-RDP	4625 - An account failed to log...	240
\Administrator	SHIR-Hive	4625 - An account failed to log...	231
SHIR-HIVE\Administrator	SHIR-Hive	4625 - An account failed to log...	231
\ADMINISTRATOR	SHIR-Hive	4625 - An account failed to log...	203
\administrator	SOC-FW-RDP	4625 - An account failed to log...	124
\	SHIR-SAP	4625 - An account failed to log...	65
\ADMIN	SHIR-Hive	4625 - An account failed to log...	60
\ADMINISTRATOR	SHIR-SAP	4625 - An account failed to log...	55
\ADMIN	SHIR-SAP	4625 - An account failed to log...	35
\SYMANTEC	SOC-FW-RDP	4625 - An account failed to log...	33
\ADMINISTRADOR	SOC-FW-RDP	4625 - An account failed to log...	32
\VEEAM	SOC-FW-RDP	4625 - An account failed to log...	30
\VEEAM	SHIR-Hive	4625 - An account failed to log...	28



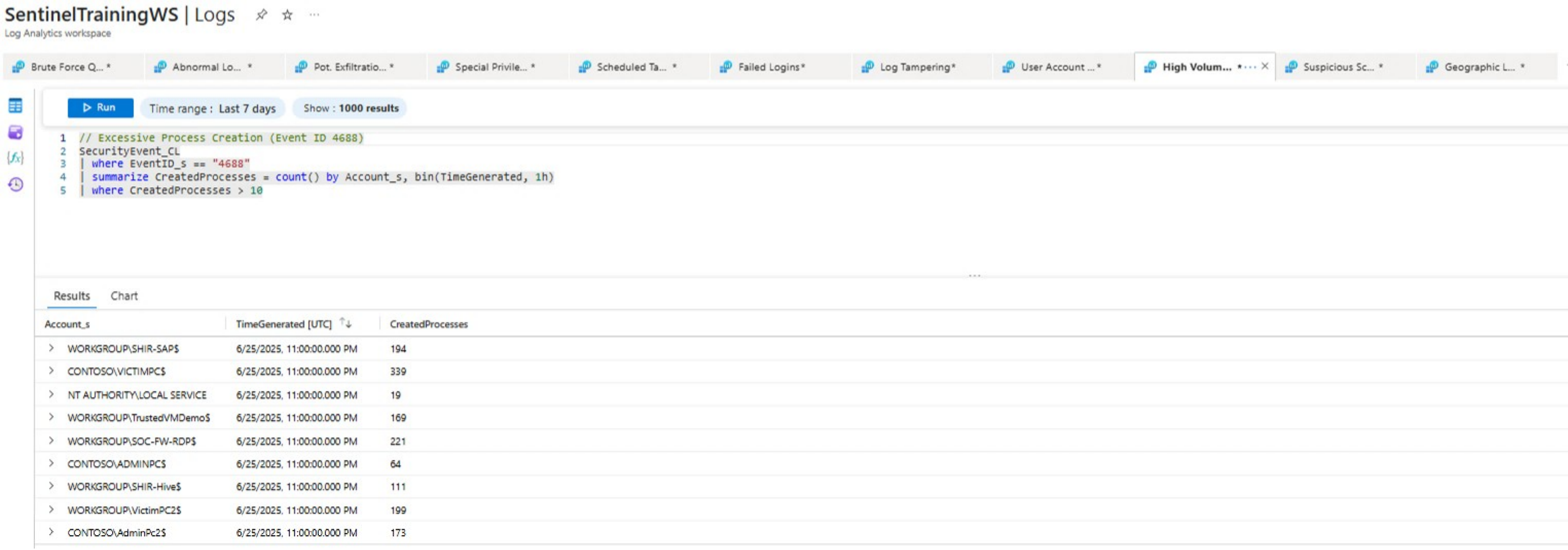
```
// Audit Policy & Log Tampering (Events 4719, 1102, 4902)
SecurityEvent_CL
| where EventID_s in ("4719", "1102", "4902")
| summarize EventCount = count() by EventID_s, Activity_s, Account_s
```

No results found from the last 7 days
Try selecting another time range



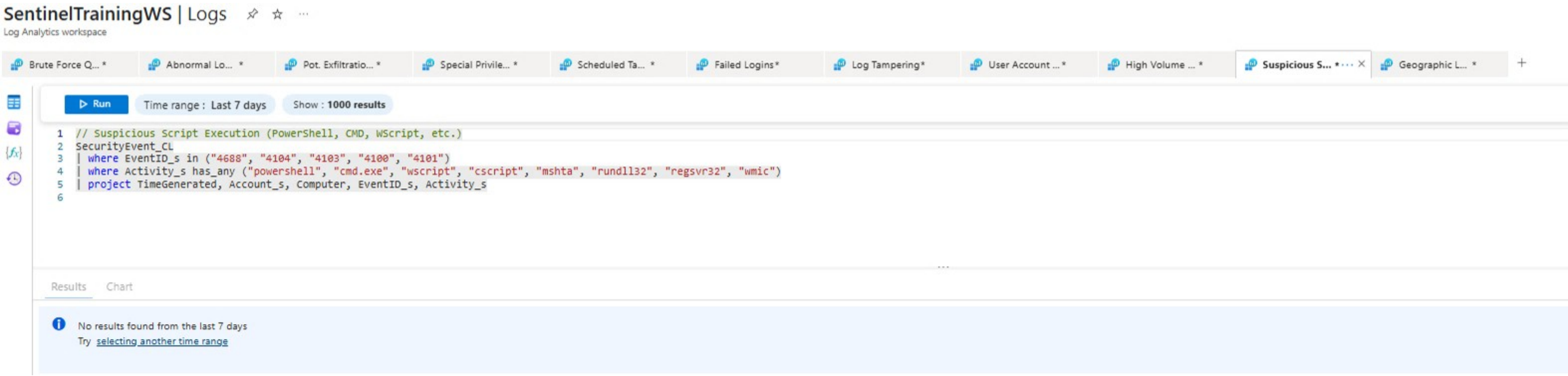
```
// Account Changes (Events 4720, 4722, 4726)
SecurityEvent_CL
| where EventID_s in ("4720", "4722", "4726")
| summarize EventCount = count() by EventID_s, Account_s, Activity_s
```

No results found from the last 7 days
Try selecting another time range



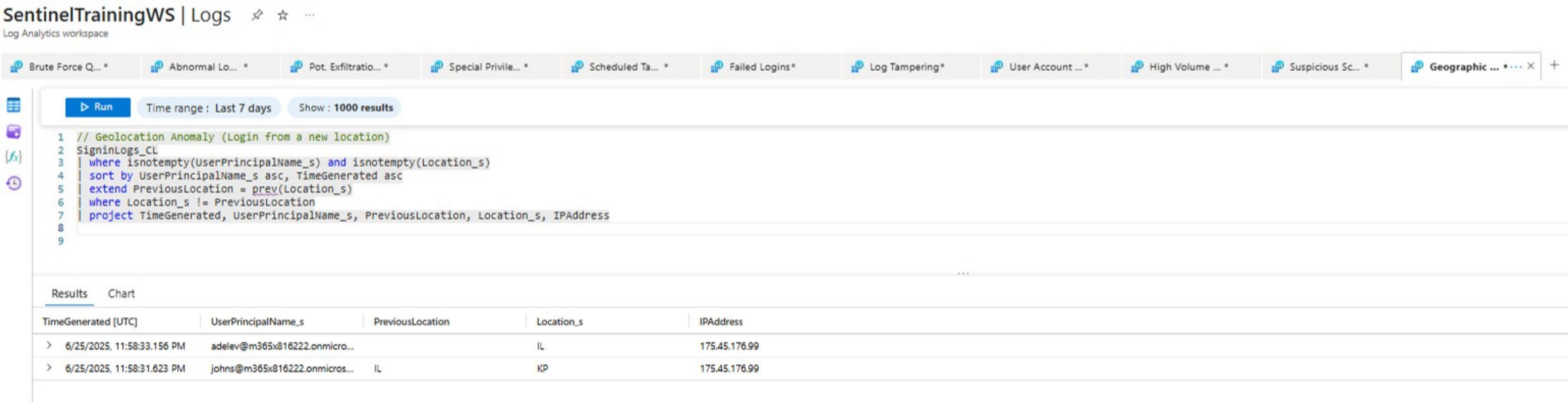
```
// Excessive Process Creation (Event ID 4688)
SecurityEvent_CL
| where EventID_s == "4688"
| summarize CreatedProcesses = count() by Account_s, bin(TimeGenerated, 1h)
| where CreatedProcesses > 10
```

Account_s	TimeGenerated [UTC]	CreatedProcesses
WORKGROUP\SHIR-SAP$	6/25/2025, 11:00:00.000 PM	194
CONTOSO\VICTIMPC$	6/25/2025, 11:00:00.000 PM	339
NT AUTHORITY\LOCAL SERVICE	6/25/2025, 11:00:00.000 PM	19
WORKGROUP\TrustedVMDemo$	6/25/2025, 11:00:00.000 PM	169
WORKGROUP\SOC-FW-RDP$	6/25/2025, 11:00:00.000 PM	221
CONTOSO\ADMINPC$	6/25/2025, 11:00:00.000 PM	64
WORKGROUP\SHIR-Hive$	6/25/2025, 11:00:00.000 PM	111
WORKGROUP\VictimPC2$	6/25/2025, 11:00:00.000 PM	199
CONTOSO\AdminPc2$	6/25/2025, 11:00:00.000 PM	173



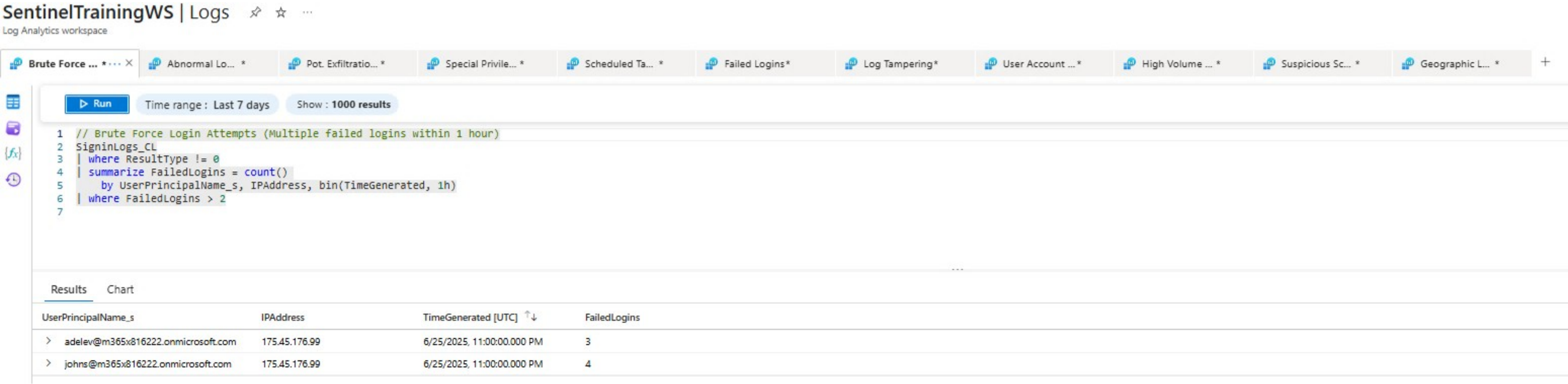
```
// Suspicious Script Execution (PowerShell, CMD, WScript, etc.)
SecurityEvent_CL
| where EventID_s in ("4688", "4104", "4103", "4100", "4101")
| where Activity_s has_any ("powershell", "cmd.exe", "wscript", "cscript", "mshta", "rundll32", "regsvr32", "wmic")
| project TimeGenerated, Account_s, Computer, EventID_s, Activity_s
```

No results found from the last 7 days
Try selecting another time range



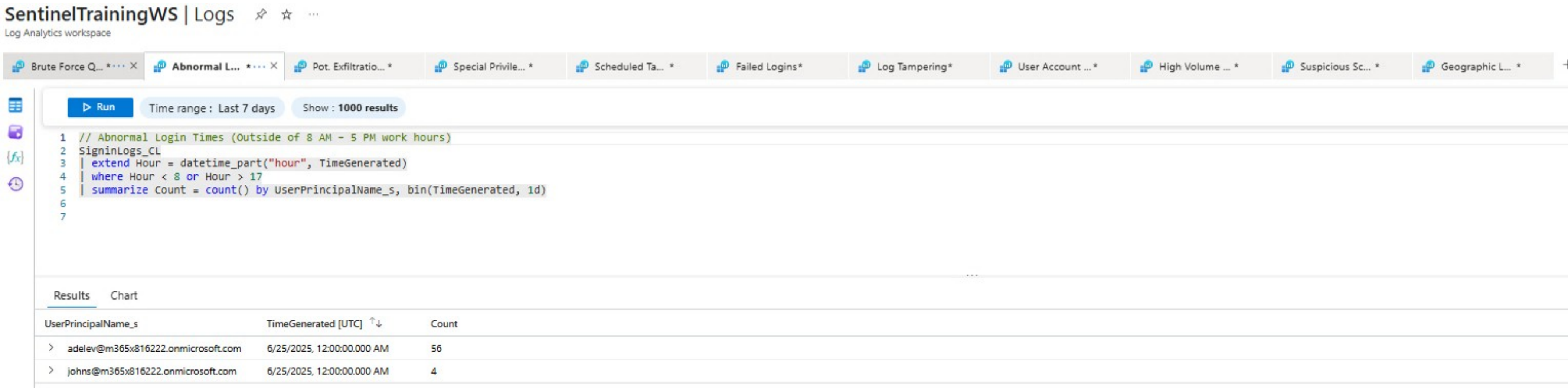
```
// Geolocation Anomaly (Login from a new location)
SigninLogs_CL
| where isnotempty(UserPrincipalName_s) and isnotempty(Location_s)
| sort by UserPrincipalName_s asc, TimeGenerated asc
| extend PreviousLocation = prev(Location_s)
| where Location_s != PreviousLocation
| project TimeGenerated, UserPrincipalName_s, PreviousLocation, Location_s, IPAddress
```

TimeGenerated [UTC]	UserPrincipalName_s	PreviousLocation	Location_s	IPAddress
> 6/25/2025, 11:58:33.156 PM	adelev@m365x816222.onmicro...		IL	175.45.176.99
> 6/25/2025, 11:58:31.623 PM	johns@m365x816222.onmicros...	IL	KP	175.45.176.99



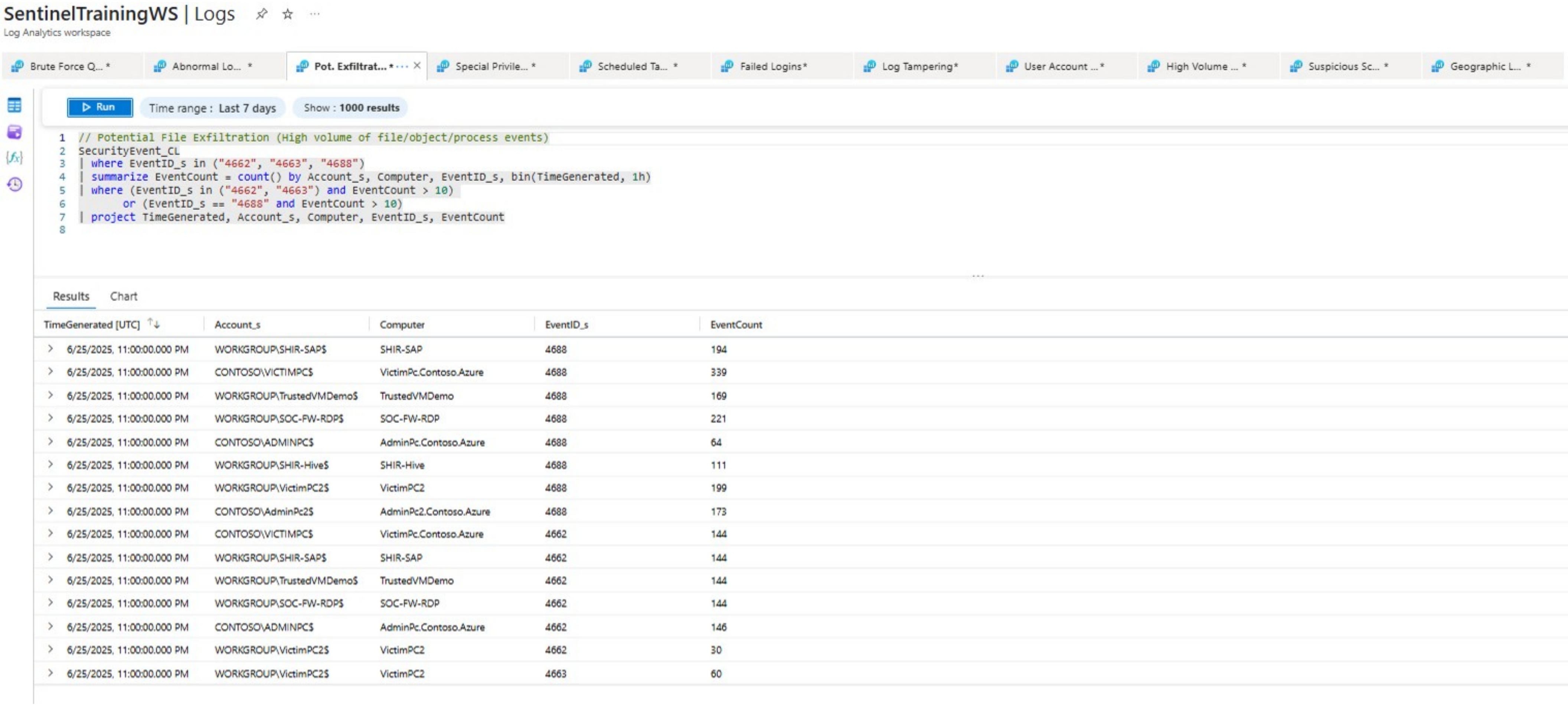
```
// Brute Force Login Attempts (Multiple failed logins within 1 hour)
SigninLogs_CL
| where ResultType != 0
| summarize FailedLogins = count()
    by UserPrincipalName_s, IPAddress, bin(TimeGenerated, 1h)
| where FailedLogins > 2
```

UserPrincipalName_s	IPAddress	TimeGenerated [UTC]	FailedLogins
adelev@m365x816222.onmicrosoft.com	175.45.176.99	6/25/2025, 11:00:00.000 PM	3
johns@m365x816222.onmicrosoft.com	175.45.176.99	6/25/2025, 11:00:00.000 PM	4



```
// Abnormal Login Times (Outside of 8 AM - 5 PM work hours)
SigninLogs_CL
| extend Hour = datetime_part("hour", TimeGenerated)
| where Hour < 8 or Hour > 17
| summarize Count = count() by UserPrincipalName_s, bin(TimeGenerated, 1d)
```

UserPrincipalName_s	TimeGenerated [UTC]	Count
adelev@m365x816222.onmicrosoft.com	6/25/2025, 12:00:00.000 AM	56
johns@m365x816222.onmicrosoft.com	6/25/2025, 12:00:00.000 AM	4



Time range : Last 7 days

Show : 1000 results

```
// Potential File Exfiltration (High volume of file/object/process events)
SecurityEvent_CL
| where EventID_s in ("4662", "4663", "4688")
| summarize EventCount = count() by Account_s, Computer, EventID_s, bin(TimeGenerated, 1h)
| where (EventID_s in ("4662", "4663") and EventCount > 10)
      or (EventID_s == "4688" and EventCount > 10)
| project TimeGenerated, Account_s, Computer, EventID_s, EventCount
```

TimeGenerated [UTC]	Account_s	Computer	EventID_s	EventCount
6/25/2025, 11:00:00.000 PM	WORKGROUP\SHIR-SAP$	SHIR-SAP	4688	194
6/25/2025, 11:00:00.000 PM	CONTOSO\VICTIMPC$	VictimPc.Contoso.Azure	4688	339
6/25/2025, 11:00:00.000 PM	WORKGROUP\TrustedVMDemo$	TrustedVMDemo	4688	169
6/25/2025, 11:00:00.000 PM	WORKGROUP\SOC-FW-RDP$	SOC-FW-RDP	4688	221
6/25/2025, 11:00:00.000 PM	CONTOSO\ADMINPC$	AdminPc.Contoso.Azure	4688	64
6/25/2025, 11:00:00.000 PM	WORKGROUP\SHIR-Hive$	SHIR-Hive	4688	111
6/25/2025, 11:00:00.000 PM	WORKGROUP\VictimPC2$	VictimPC2	4688	199
6/25/2025, 11:00:00.000 PM	CONTOSO\AdminPc2$	AdminPc2.Contoso.Azure	4688	173
6/25/2025, 11:00:00.000 PM	CONTOSO\VICTIMPC$	VictimPc.Contoso.Azure	4662	144
6/25/2025, 11:00:00.000 PM	WORKGROUP\SHIR-SAP$	SHIR-SAP	4662	144
6/25/2025, 11:00:00.000 PM	WORKGROUP\TrustedVMDemo$	TrustedVMDemo	4662	144
6/25/2025, 11:00:00.000 PM	WORKGROUP\SOC-FW-RDP$	SOC-FW-RDP	4662	144
6/25/2025, 11:00:00.000 PM	CONTOSO\ADMINPC$	AdminPc.Contoso.Azure	4662	146
6/25/2025, 11:00:00.000 PM	WORKGROUP\VictimPC2$	VictimPC2	4662	30
6/25/2025, 11:00:00.000 PM	WORKGROUP\VictimPC2$	VictimPC2	4663	60