Investigation Report

KQL created to answer the questions for Day-7 - 30-Day MyDFIR Microsoft Challenge

```
SecurityEvent_CL
| where EventID_s == "4625"  // 4625 failed logon event
| where TimeGenerated >= ago(30d)
| summarize FailedLogons = count(), FirstSeen = min(TimeGenerated), LastSeen = max(TimeGenerated) by Account = Account_s, Computer
| where FailedLogons >= 1000
| sort by FailedLogons desc
| project Account, FailedLogons, Computer, FirstSeen, LastSeen
```

Account	FailedLogons	Computer	FirstSeen	LastSeen
\ADMINISTRATOR	9997	SOC-FW-RDP	Nov 1, 2025 7:23:41 PM	Nov 1, 2025 7:23:42 PM
\admin	1988	SHIR-Hive	Nov 1, 2025 7:23:41 PM	Nov 1, 2025 7:23:42 PM
\administrator	1740	SHIR-Hive	Nov 1, 2025 7:23:41 PM	Nov 1, 2025 7:23:42 PM

Findings

First Failed Logon Seen: Nov 1, 2025 7:23:41 PM

Last Failed Logon Seen: Nov 1, 2025 7:23:42 PM

Period: 30 days

Accounts are experiencing the most failed logons: ADMINISTRATOR, admin, administrator

Computers used by accounts with the most failed logons: SOC-FW-RDP, SHIR-Hive

Investigation

On Nov 1, 2025 7:23:41 UTC, three accounts with “administrator” privileges were trying to accessing the network through two computers. Since the alert showed a high rate of failed logon in only one minute, it is an indicator that all of them were attempts of a brute force attack. To verify if some of those attempts were successful logins for those accounts, the next KQL was executed.
It showed none of those accounts got a successful logon as we can see in the screenshot below.

```
SecurityEvent_CL
| where EventID_s == "4624"  // successful logon event
| where TimeGenerated >= ago(30d)
| summarize SuccessLogons = count(), FirstSeen = min(TimeGenerated), LastSeen = max(TimeGenerated) by Account = Account_s, Computer
| project Account, SuccessLogons, Computer, FirstSeen, LastSeen
```

Account	SuccessLogons	Computer	FirstSeen	LastSeen
CONTOSO.AZURE\AATPService	4	VictimPc.Contoso.Azure	Nov 1, 2025 7:23:41 PM	Nov 1, 2025 7:23:41 PM
CONTOSO.AZURE\AATPService	4	AdminPc.Contoso.Azure	Nov 1, 2025 7:23:42 PM	Nov 1, 2025 7:23:42 PM
CONTOSO.AZURE\ADMINPC2$	1	AdminPc2.Contoso.Azure	Nov 1, 2025 7:23:42 PM	Nov 1, 2025 7:23:42 PM
CONTOSO\RonHD	6	VictimPc.Contoso.Azure	Nov 1, 2025 7:23:41 PM	Nov 1, 2025 7:23:42 PM
CONTOSO\SamiraA	12	AdminPc.Contoso.Azure	Nov 1, 2025 7:23:41 PM	Nov 1, 2025 7:23:42 PM
NT AUTHORITY\SYSTEM	14	VictimPc.Contoso.Azure	Nov 1, 2025 7:23:41 PM	Nov 1, 2025 7:23:42 PM
NT AUTHORITY\SYSTEM	19	VictimPC2	Nov 1, 2025 7:23:41 PM	Nov 1, 2025 7:23:42 PM
NT AUTHORITY\SYSTEM	3	TrustedVMDemo	Nov 1, 2025 7:23:41 PM	Nov 1, 2025 7:23:42 PM
NT AUTHORITY\SYSTEM	10	SOC-FW-RDP	Nov 1, 2025 7:23:41 PM	Nov 1, 2025 7:23:42 PM
NT AUTHORITY\SYSTEM	6	SHIR-SAP	Nov 1, 2025 7:23:41 PM	Nov 1, 2025 7:23:42 PM
NT AUTHORITY\SYSTEM	4	SHIR-Hive	Nov 1, 2025 7:23:42 PM	Nov 1, 2025 7:23:42 PM
NT AUTHORITY\SYSTEM	2	AdminPc2.Contoso.Azure	Nov 1, 2025 7:23:42 PM	Nov 1, 2025 7:23:42 PM
NT AUTHORITY\SYSTEM	8	AdminPc.Contoso.Azure	Nov 1, 2025 7:23:41 PM	Nov 1, 2025 7:23:42 PM

Who	**ADMINISTRATOR, admin, administrator**
What	Over 1000 failed logon attempts in one minute using three elevated accounts.
When	From Nov 1, 2025 7:23:41 PM UTC to Nov 1, 2025 7:23:42 PM UTC No more records were found of similar attempts before, or after the time range reported.
Where	Two computers: SOC-FW-RDP, SHIR-Hive
Why	We do not know what was the intent of these attempts.
How	It was a Credential Access (tactic); T1110 (technique) used by the attacker.

Recommendations

Enable MFA for All Administrator Accounts.

Identify the source IPs of the failed logons from the logs.

Reset passwords for all accounts involved in the failed logon attempts, especially those with administrator privileges to ensure no credentials were compromised.