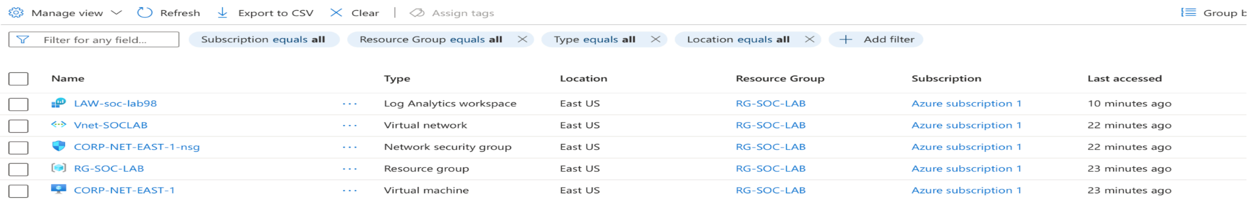
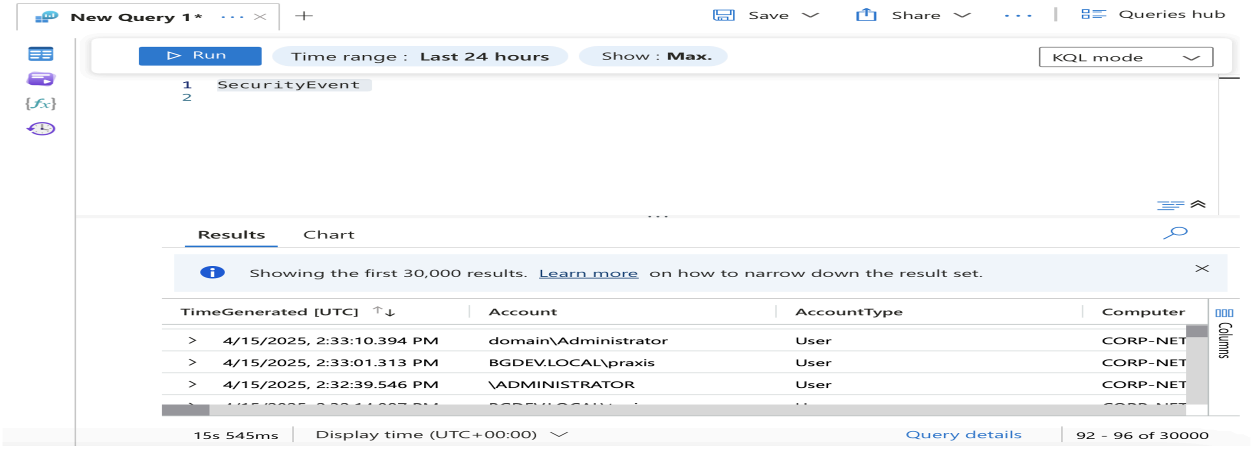
Honey pot home soc lab on Azure



Name	Type	Location	Resource Group	Subscription	Last accessed
LAW-soc-lab98	Log Analytics workspace	East US	RG-SOC-LAB	Azure subscription 1	10 minutes ago
Vnet-SOCLAB	Virtual network	East US	RG-SOC-LAB	Azure subscription 1	22 minutes ago
CORP-NET-EAST-1-nsg	Network security group	East US	RG-SOC-LAB	Azure subscription 1	22 minutes ago
RG-SOC-LAB	Resource group	East US	RG-SOC-LAB	Azure subscription 1	23 minutes ago
CORP-NET-EAST-1	Virtual machine	East US	RG-SOC-LAB	Azure subscription 1	23 minutes ago

Created a resource group and added a VM with a VN configured it in log analytics workspace.



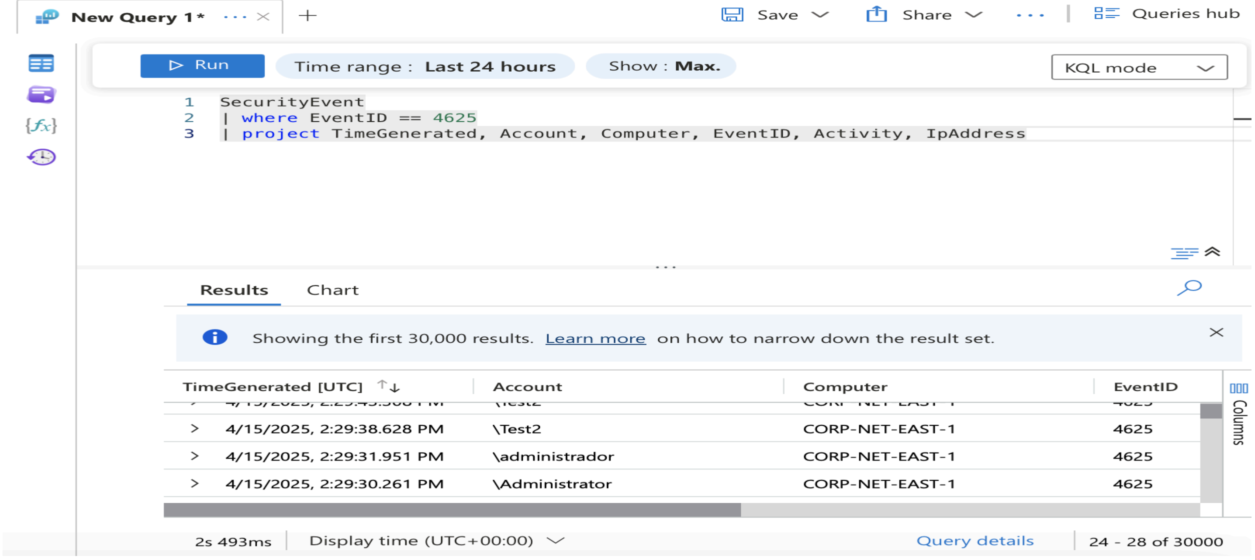
```
SecurityEvent
```

Showing the first 30,000 results. Learn more on how to narrow down the result set.

TimeGenerated [UTC]	Account	AccountType	Computer
4/15/2025, 2:33:10.394 PM	domain\Administrator	User	CORP-NET
4/15/2025, 2:33:01.313 PM	BGDEV.LOCAL\praxis	User	CORP-NET
4/15/2025, 2:32:39.546 PM	\ADMINISTRATOR	User	CORP-NET

15s 545ms | Display time (UTC+00:00) | Query details | 92 - 96 of 30000

Log analytics



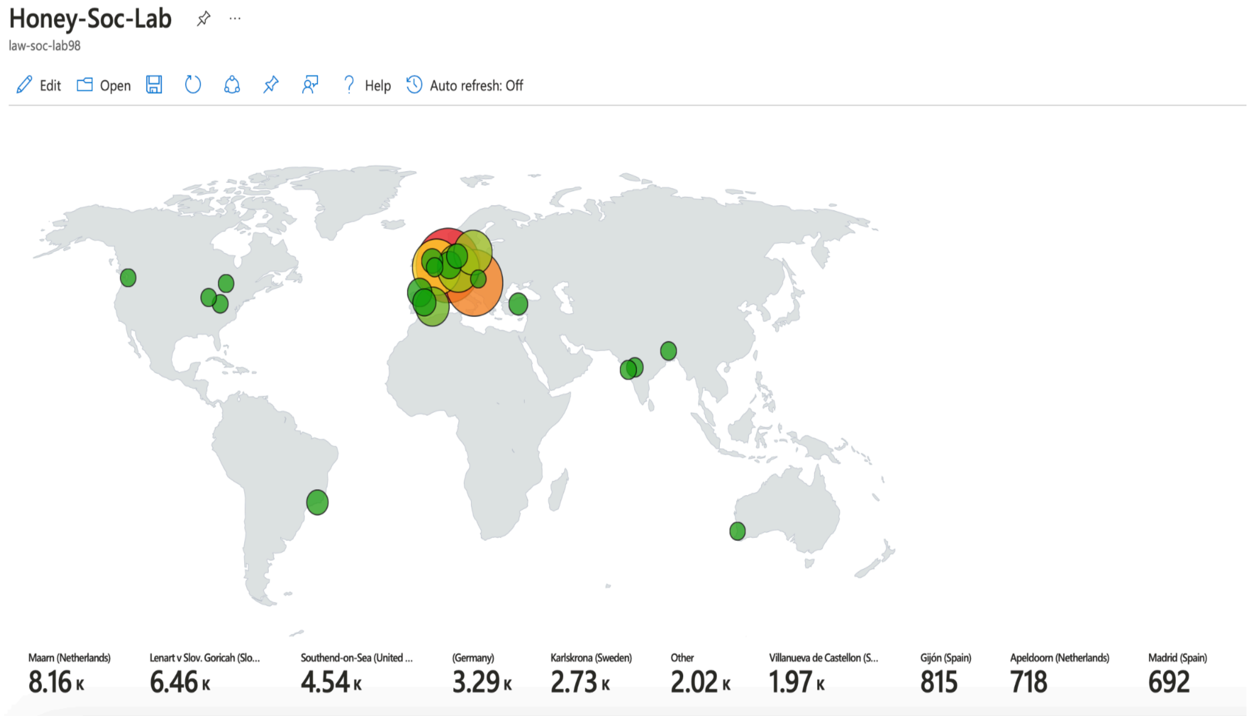
```
SecurityEvent
| where EventID == 4625
| project TimeGenerated, Account, Computer, EventID, Activity, IpAddress
```

Showing the first 30,000 results. Learn more on how to narrow down the result set.

TimeGenerated [UTC]	Account	Computer	EventID
4/15/2025, 2:29:38.628 PM	\Test2	CORP-NET-EAST-1	4625
4/15/2025, 2:29:31.951 PM	\administrador	CORP-NET-EAST-1	4625
4/15/2025, 2:29:30.261 PM	\Administrator	CORP-NET-EAST-1	4625

2s 493ms | Display time (UTC+00:00) | Query details | 24 - 28 of 30000

Failed login attempts



Honey-Soc-Lab

law-soc-lab98

Maarn (Netherlands)	Lenart v Slov. Goricah (Slo...	Southend-on-Sea (United ...	(Germany)	Karlskrona (Sweden)	Other	Villanueva de Castellon (S...	Gijón (Spain)	Apeldoorn (Netherlands)	Madrid (Spain)
8.16 K	6.46 K	4.54 K	3.29 K	2.73 K	2.02 K	1.97 K	815	718	692

Live map of real failed login attempts on sentinel with Ip Addresses and locations