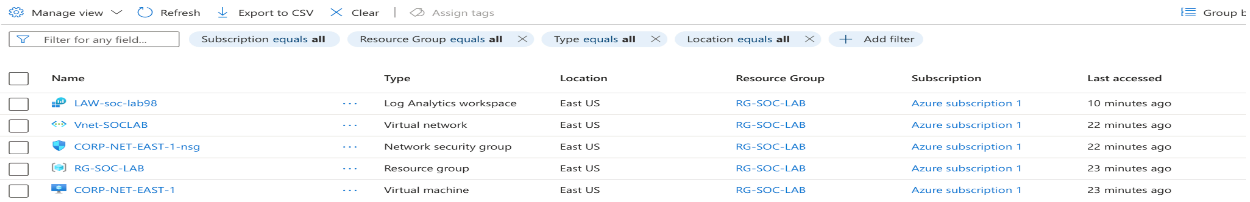
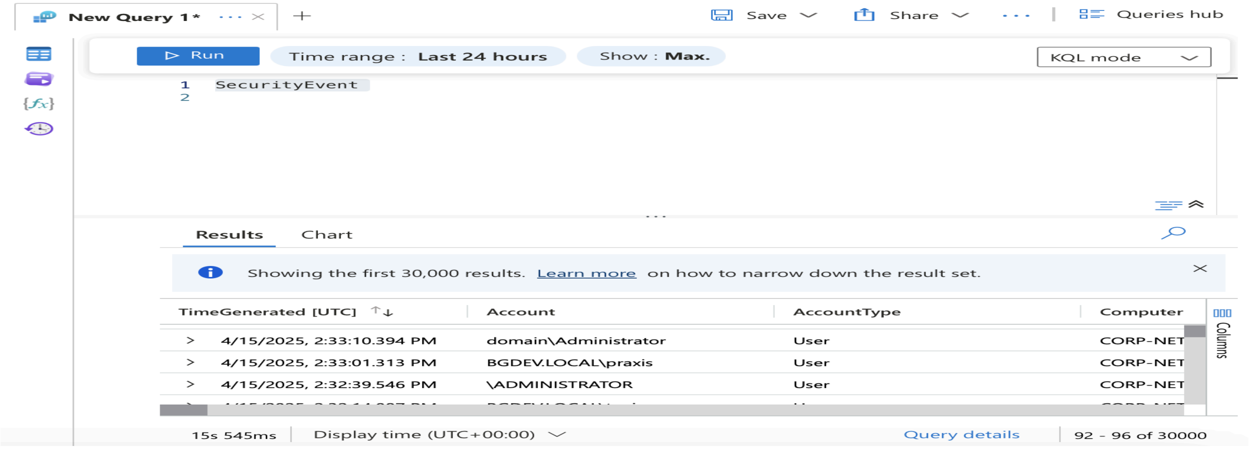
Honey pot home soc lab on Azure



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.



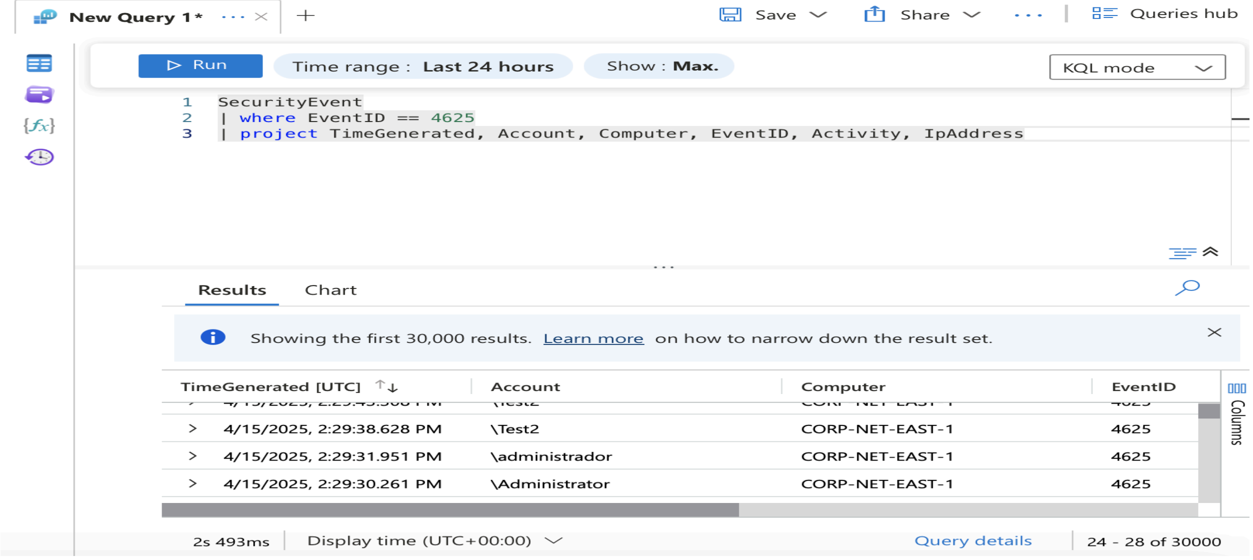
```
SecurityEvent
```

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



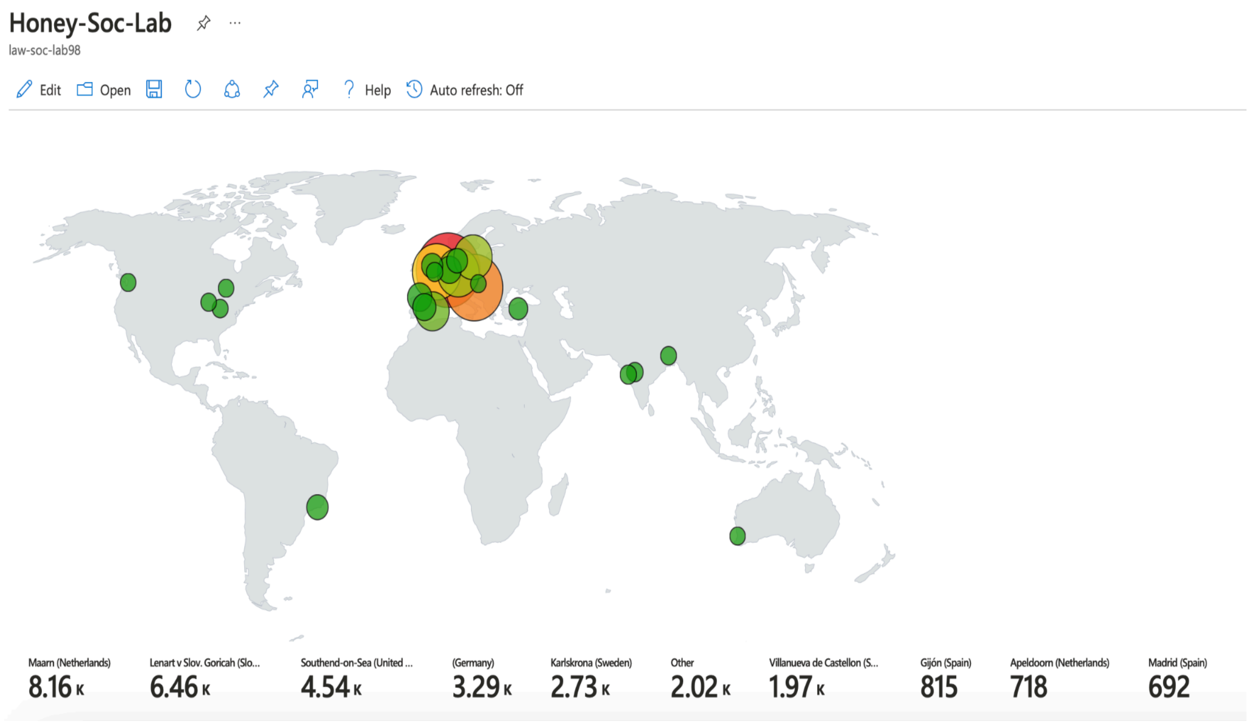
```
SecurityEvent
| where EventID == 4625
| project TimeGenerated, Account, Computer, EventID, Activity, IpAddress
```

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

Honeypot Lab – Home SOC Simulation on Azure

Author: Kevin Hamzai
Environment: Microsoft Azure, Azure Virtual Network (VNet), Log Analytics Workspace, Azure Sentinel

---

1. Objective

The purpose of this lab was to simulate a small-scale Security Operations Center (SOC) environment in a home lab using Azure resources. The lab aimed to:

- Gain practical experience in network monitoring and threat detection.
- Analyze malicious activity by capturing failed login attempts.
- Visualize attack sources and patterns using Azure Sentinel.
- Demonstrate the ability to document and report security incidents professionally.

---

2. Lab Environment Setup

Azure Resources Provisioned:

- Resource Group: Created a dedicated resource group for the lab to organize resources.
- Virtual Machine (VM): Deployed a Linux VM to serve as the honeypot target.
- Virtual Network (VNet): Configured a VNet to isolate and secure the VM while allowing monitoring traffic.
- Log Analytics Workspace: Integrated the VM with Log Analytics for data collection and monitoring.

---

3. Methodology

1. VM and Network Configuration
    - ○ Provisioned a VM with default security settings.
    - ○ Configured a VNet with appropriate subnets and routing to allow controlled external access.
    - ○ Connected the VM to Azure Log Analytics Workspace for centralized logging.

2. Data Collection
    - Configured logging to capture failed login attempts on the VM.
    - Integrated Azure Sentinel to aggregate logs and visualize potential threats in real time.
3. Monitoring and Visualization
    - Created dashboards in Sentinel to track incoming connection attempts.
    - Mapped IP addresses of failed login attempts to their geographic locations using Sentinel's built-in map visualization.
4. Analysis
    - Identified patterns of unauthorized access attempts.
    - Tracked attack frequency, source regions, and repeated IPs to simulate threat intelligence reporting.

---

4. Results

- Successfully captured multiple failed login attempts targeting the VM.
- Generated a live map of attack sources, showing geographic locations and IP addresses.
- Developed dashboards for visualizing and analyzing suspicious activity in near real-time.
- Gained insight into common attack vectors and methods used by external actors.

---

5. Lessons Learned

- Practical understanding of how to set up and manage a SOC environment in a cloud platform.
- Hands-on experience with Azure Sentinel, Log Analytics, and VM monitoring.
- Learned the importance of structured documentation to communicate findings to stakeholders.
- Reinforced skills in detecting and analyzing threats, visualizing attack patterns, and preparing actionable reports.

---

6. Conclusion

This lab successfully demonstrated the deployment and management of a honeypot environment on Azure. By monitoring failed login attempts and visualizing attack sources, the lab provided valuable experience in SOC operations, incident detection, and threat intelligence analysis.

Proper documentation of the workflow, configurations, and findings ensures that employers can quickly understand your technical competency and ability to manage security projects professionally.