

Team Ambition

Azure Sentinel (SIEM) map with cyber attacks

About Team:

— — —

Kristiann-loves pizza, has a dog, huge Star Wars fan, loves Disney, aspiring magic key holder one day!

Lauren-enjoys a good bagel, coded first website at 12 and enjoys books on the beach

Giuliana-enjoys the theatre, musical theater to be exact and navigating network security.

Frankie-enjoys all things Star Trek, building virtual machines and building pillow forts.

Goal: Connect a live virtual machine built on Azure & illustrate live Brute Force Attacks

Technical Background

Researched:

- Azure and the implementation of a VM
- Creating logs
- Visual Demonstration of data

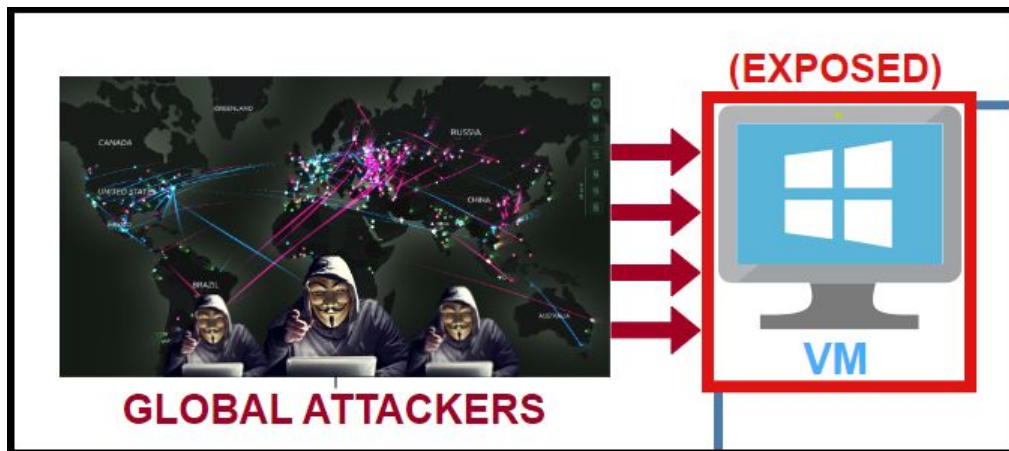
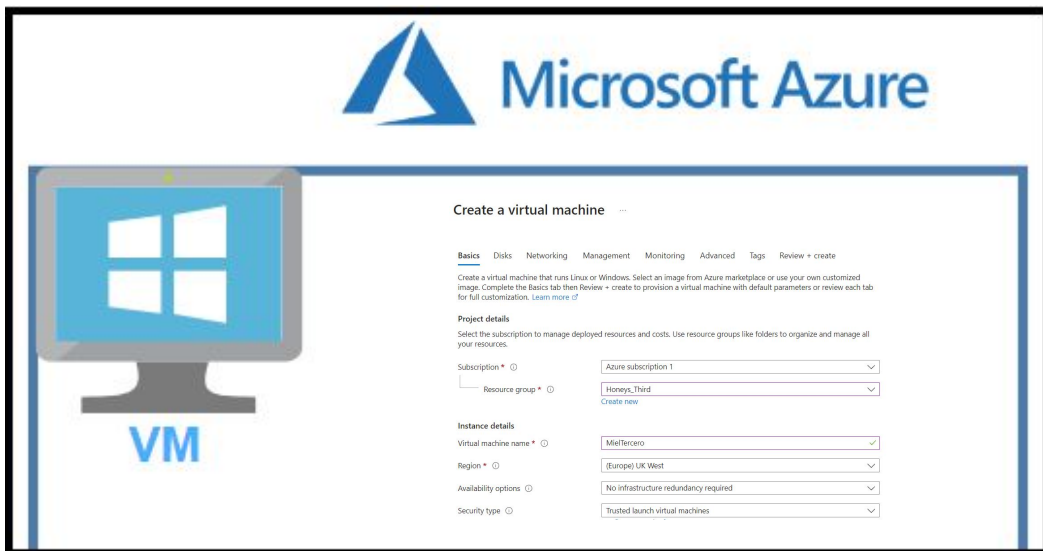
The reason we selected the topic was to demonstrate how vulnerable a machine or network is without a
FIREWALL

Concepts Applied:

Networking
Azure
SIEM
OSI
Data Recovery
Vulnerability Management

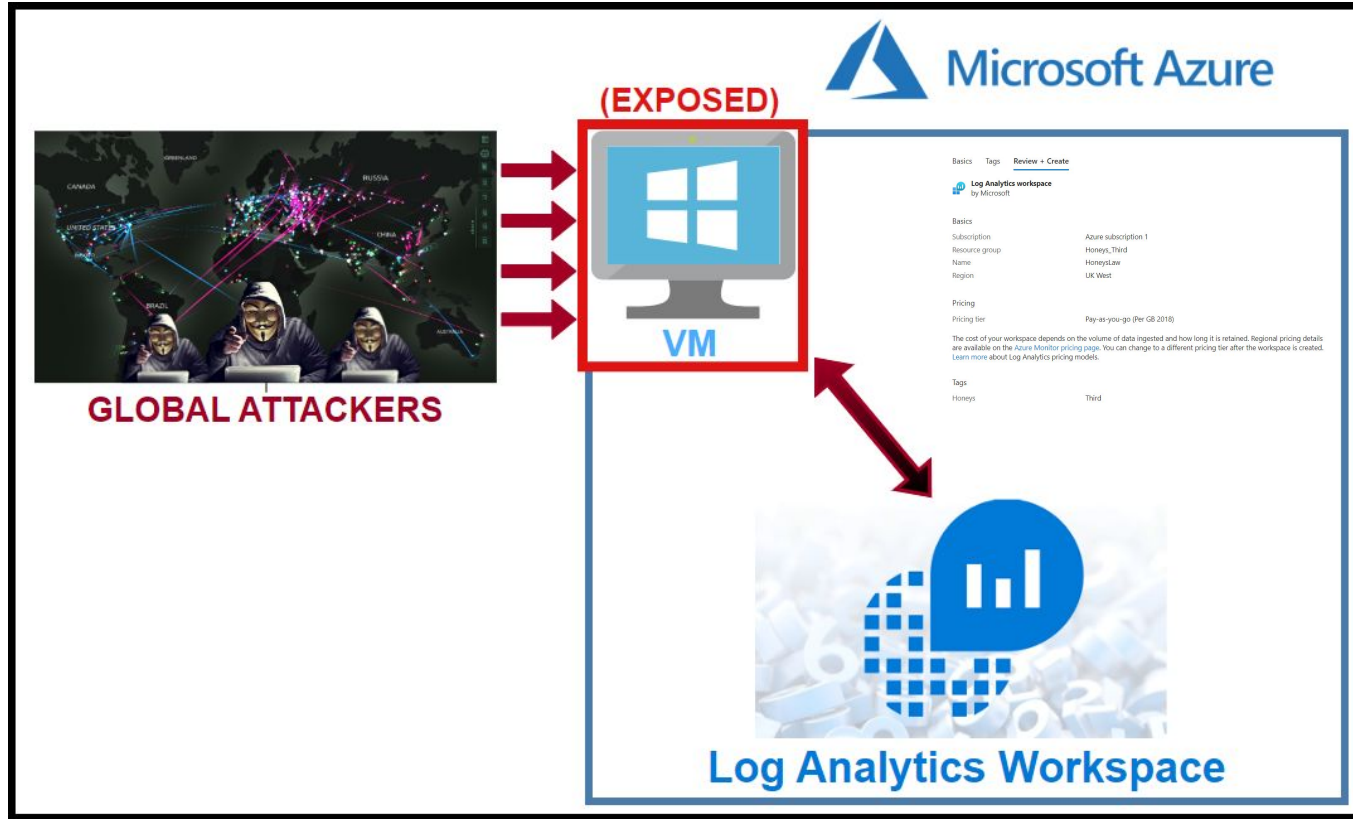
Demonstration Preview

The first step is to create a Microsoft Azure subscription. We then created a virtual machine in our Azure account.

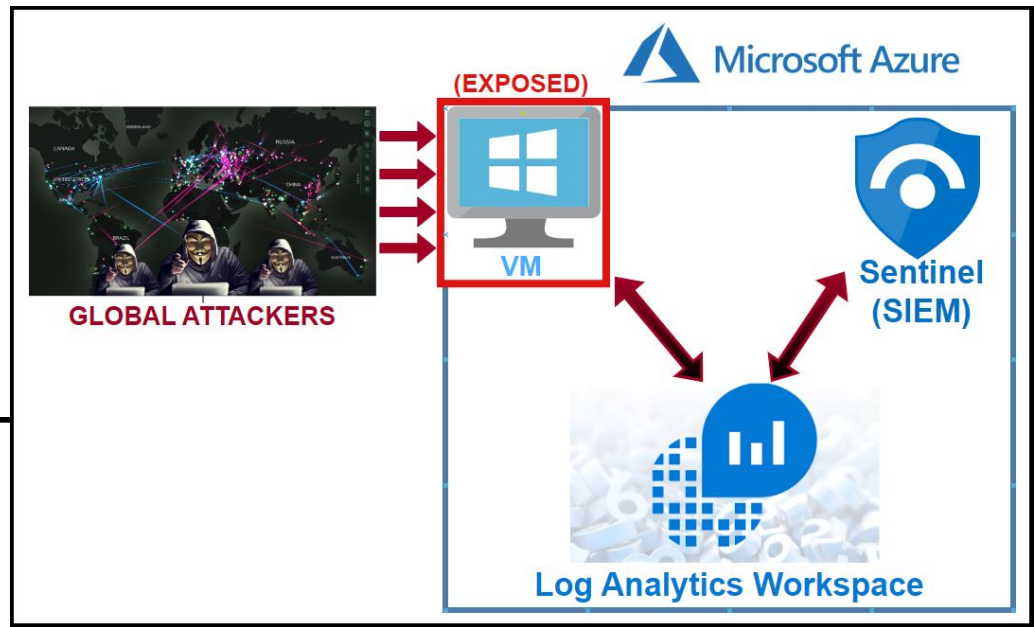


Next we turned off the external firewall as well as the Windows firewall so that our machine was extremely exposed to the internet and could be pinged by anyone in the country.

Next we created a log repository in Azure called a Log Analytics Workspace which will be used to ingest out logs from the virtual machine



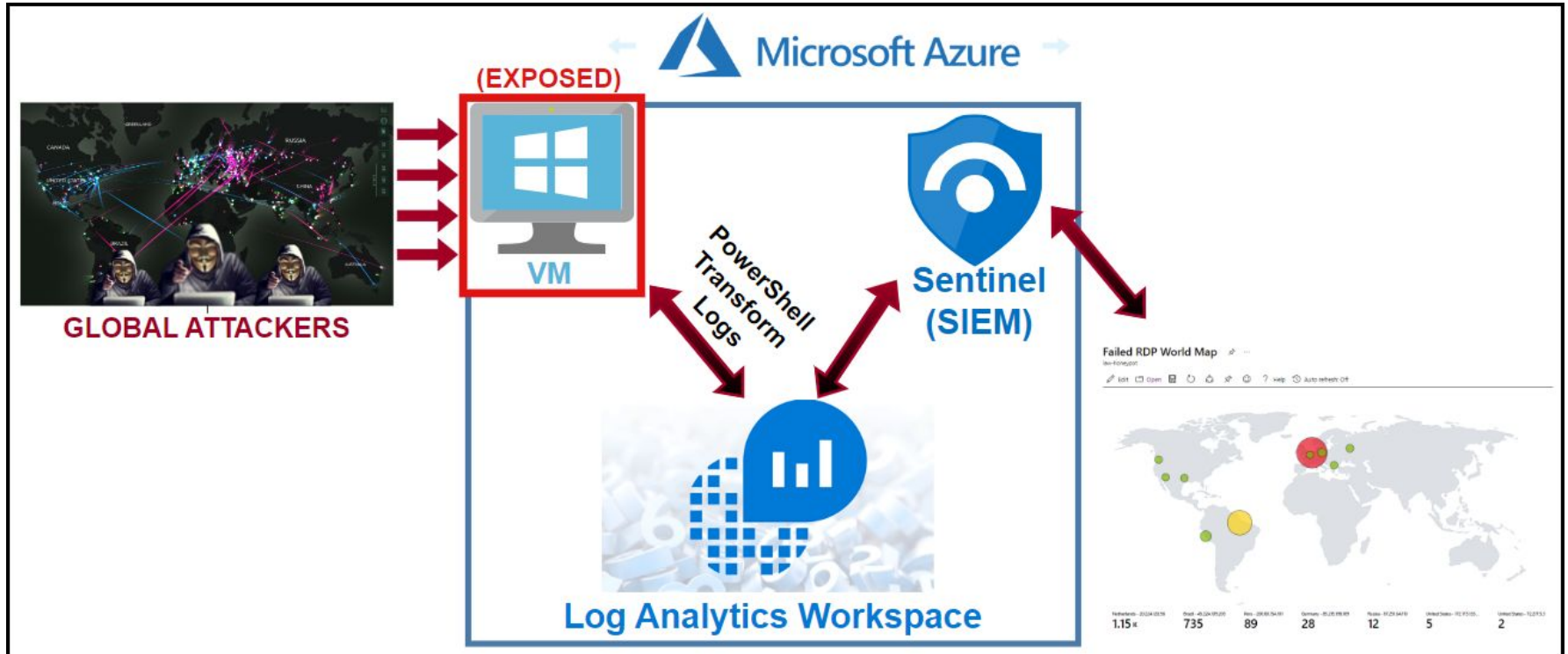
We then set up Microsoft Sentinel, which is Microsoft's cloud native SIEM.



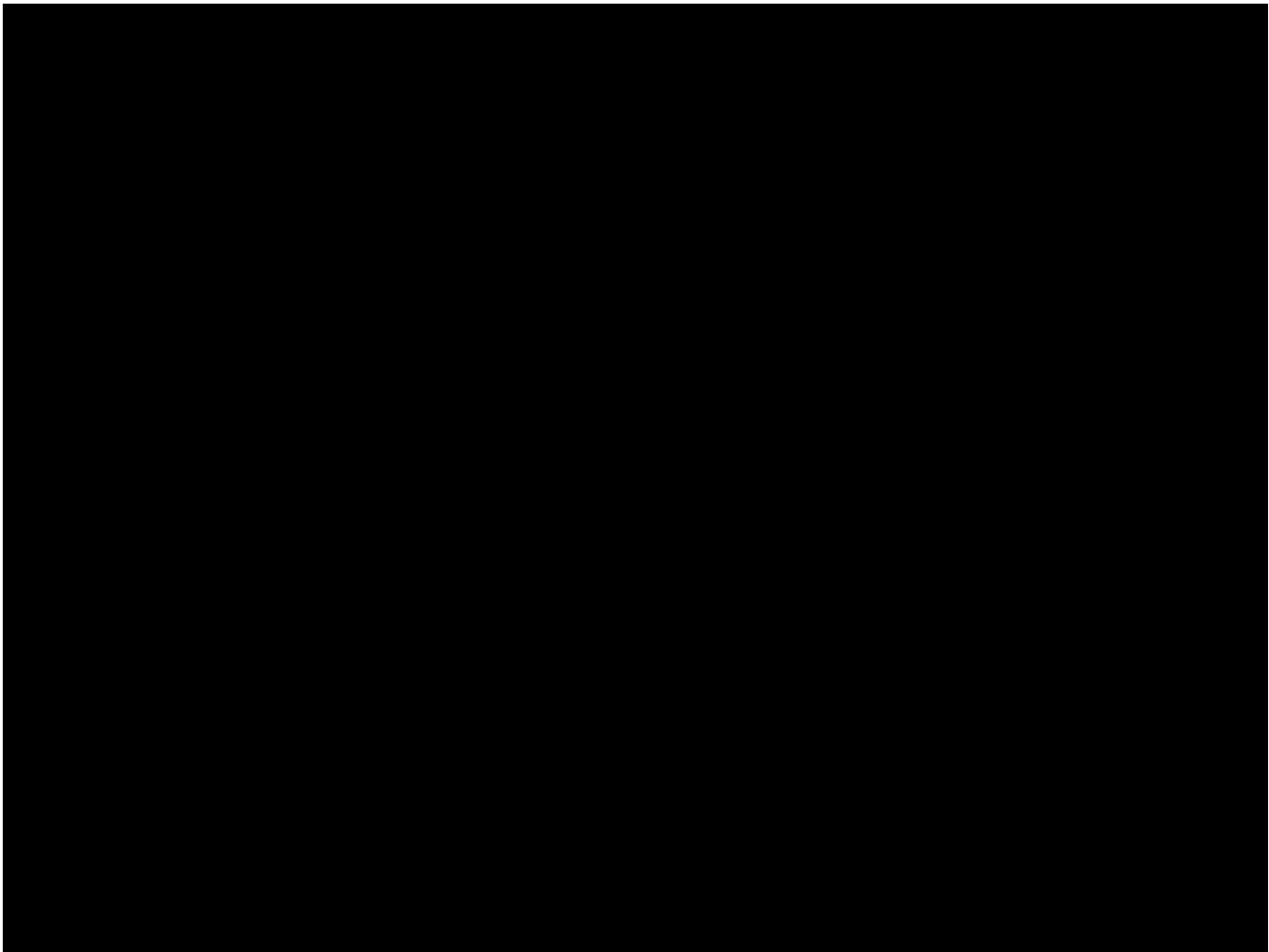
We used Sentinel to create a map to visually show all of the different attacker data to see what country they're coming from.

We used a PowerShell script** to extract the IP address from a windows log, to send it to a third party API, the API would then derive the latitude, longitude, state, and province information to send it back to our virtual machine which was used to create a custom log to include the pertinent geographic data included

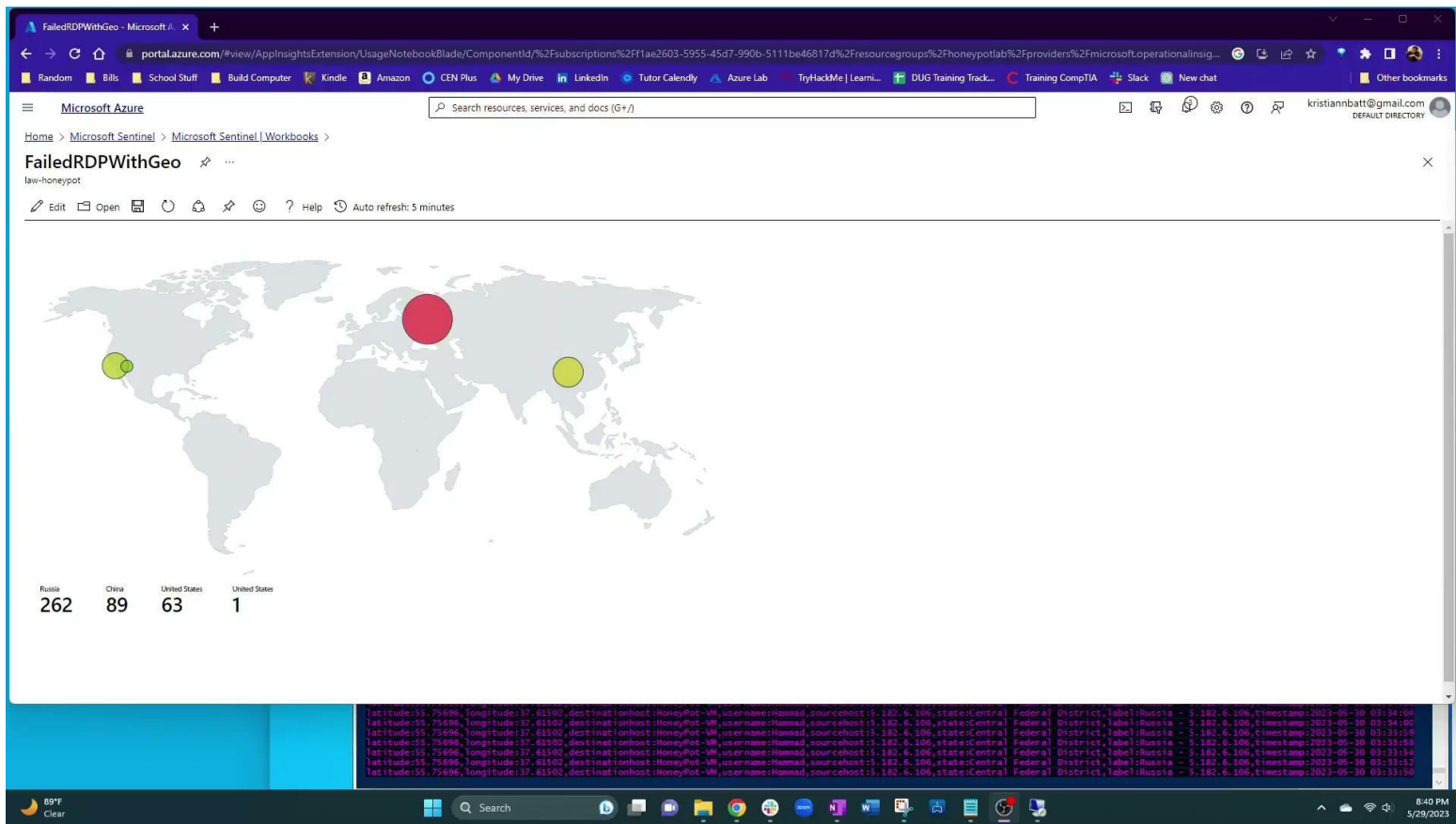
**Credit: Josh Madakor https://github.com/joshmadakor1/Sentinel-Lab/blob/main/Custom_Security_Log_Exporter.ps1



Demonstration

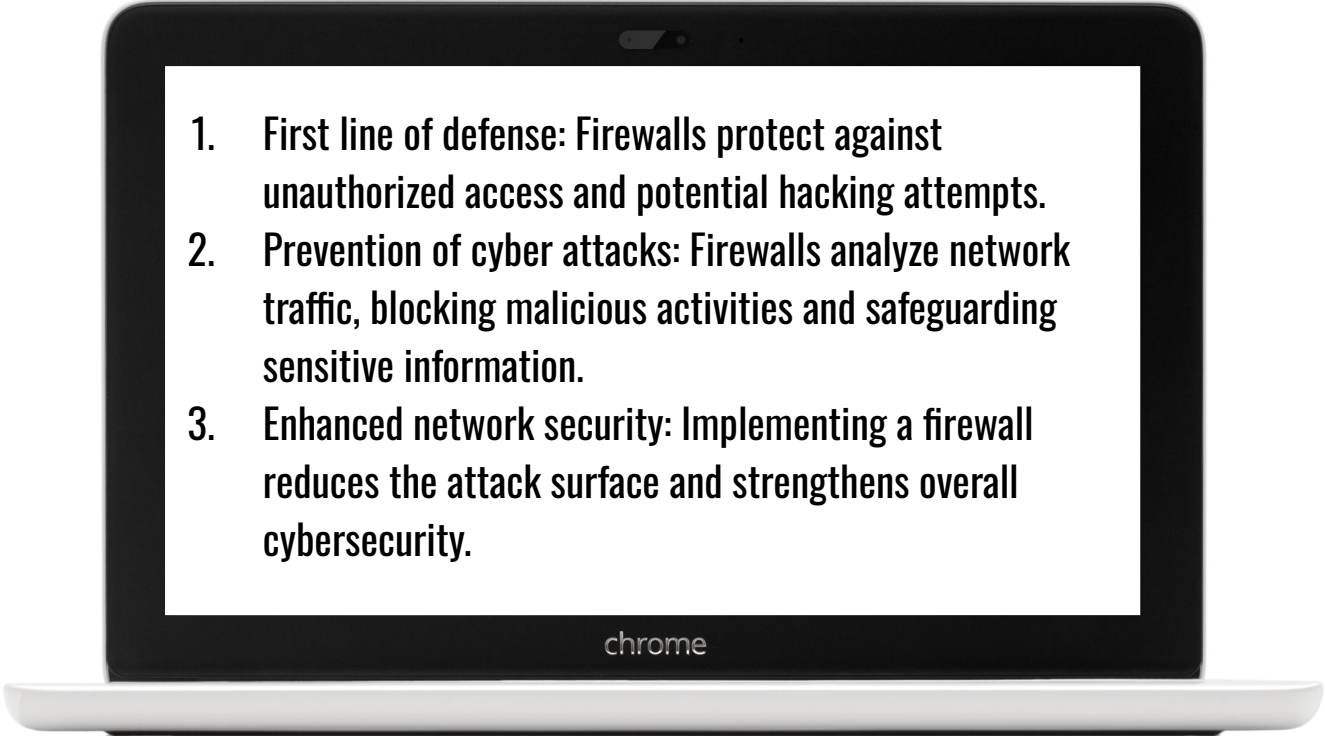


Time Lapse of Map Showing Attacks



Demonstration Summary

Summary: Without a firewall, you are not fully protected and at high risk of being hacked.

- 
- — —
1. First line of defense: Firewalls protect against unauthorized access and potential hacking attempts.
 2. Prevention of cyber attacks: Firewalls analyze network traffic, blocking malicious activities and safeguarding sensitive information.
 3. Enhanced network security: Implementing a firewall reduces the attack surface and strengthens overall cybersecurity.

chrome

Mitigation

Firewalls-they help prevent malware, block malicious traffic to your site and increase security of your computer or network.

Weekly Backups-this helps in case you are infected, you are able to recover data.

Strong Passwords-Set up policies including 12-character minimum with a mix of upper & lower case letter.

Conduct Patches-keeping software up-to-date with security patches helps protect devices from known vulnerabilities.

— — —

Contact

— — —

Lauren Barer

[linkedin.com/in/lauren-barer](https://www.linkedin.com/in/lauren-barer)

Kristann Batt

[linkedin.com/in/kristiann-batt-53b9a7259](https://www.linkedin.com/in/kristiann-batt-53b9a7259)

H Frankie Palacios

[linkedin.com/in/h-frankie-darling-palacios-b2717b267](https://www.linkedin.com/in/h-frankie-darling-palacios-b2717b267)

Giuliana Zanutta

[linkedin.com/in/gzanutta](https://www.linkedin.com/in/gzanutta)

