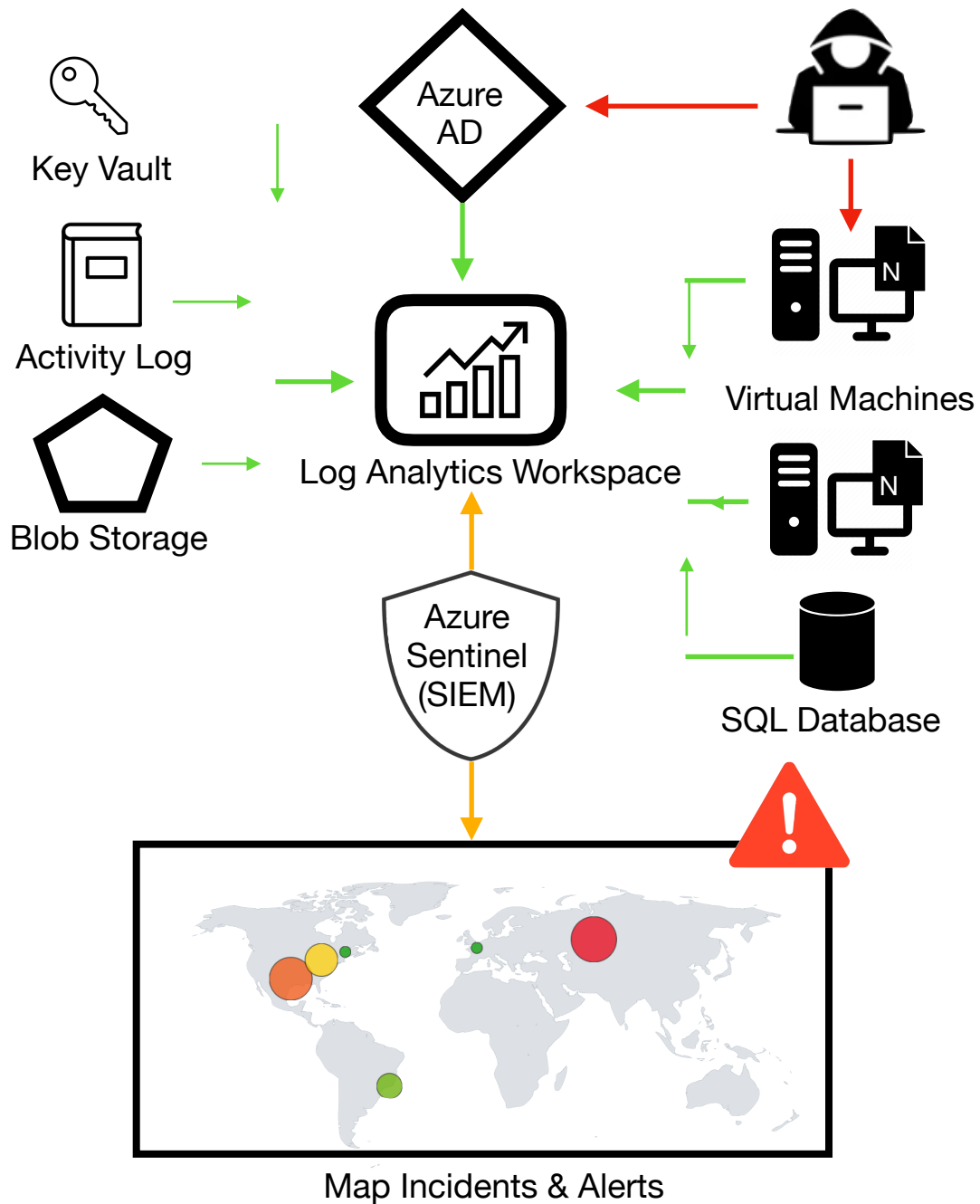


HoneyNet in Microsoft Azure and Security Operations Center



Introduction

For this project I am looking to simulate a honeynet in Microsoft Azure. I want to intentionally expose an unprotected environment to the public internet for 24 hours. This will simulate real world cyber attacks. Metrics will be collected from various log sources from the environment into the Log Analytics workspace, which is used by Microsoft Sentinel. From this, Sentinel will be able to build attack maps, create trigger alerts and incidents.

After the initial exposure, any incidents will be investigated that Sentinel generates. Security controls will be applied to address these incidents to harden the environment and improve the security posture. The environment will then be exposed again for another 24 hours and new metrics will be collected.

This project will showcase the effect of hardening the environment as well as skills in Azure, Incident Response, Security Hardening with using regularity frameworks such as NIST SP 800-53 and NIST SP 800-37.

The Architecture Components of the Lab

The list below are all the components, technologies and frameworks that will be used in a Microsoft Azure environment.

- Virtual Machines (2 Windows, 1 Linux)
- Microsoft Sentinel
- Network Security Groups
- Microsoft Defender for Cloud
- Log Analytics Workspace using Kusto Query Language
- Azure Storage Accounts
- Azure Key Vault
- Azure Virtual Network (VNet)
- NIST SP 800-53 and 800-37

Architecture Before Security Hardening

A windows and linux VM are setup and left intentionally open to the internet. Microsoft Defender for Cloud has been disabled. The Network Security Groups (NSG) and firewalls are wide open, thus allowing unrestricted access. In addition, all other resources such as storage accounts and databases were deployed with public endpoints visible to the internet.

Another windows VM has been setup but this time used as an attacker. Internally send the windows VM malicious files (these files will have a signature of a malware, but do not actually cause any harm)

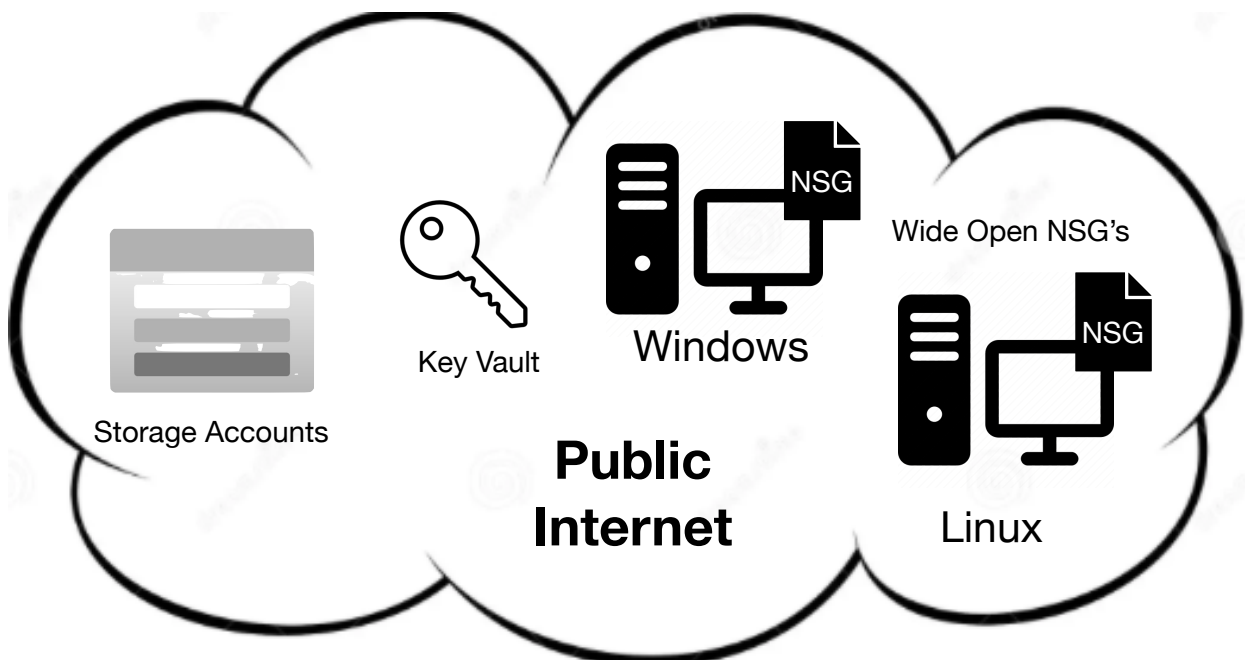


Figure 1. Visual Representation of the environment

Attack Maps Before Security Hardening

The attack map below shows Windows Authentication failures.

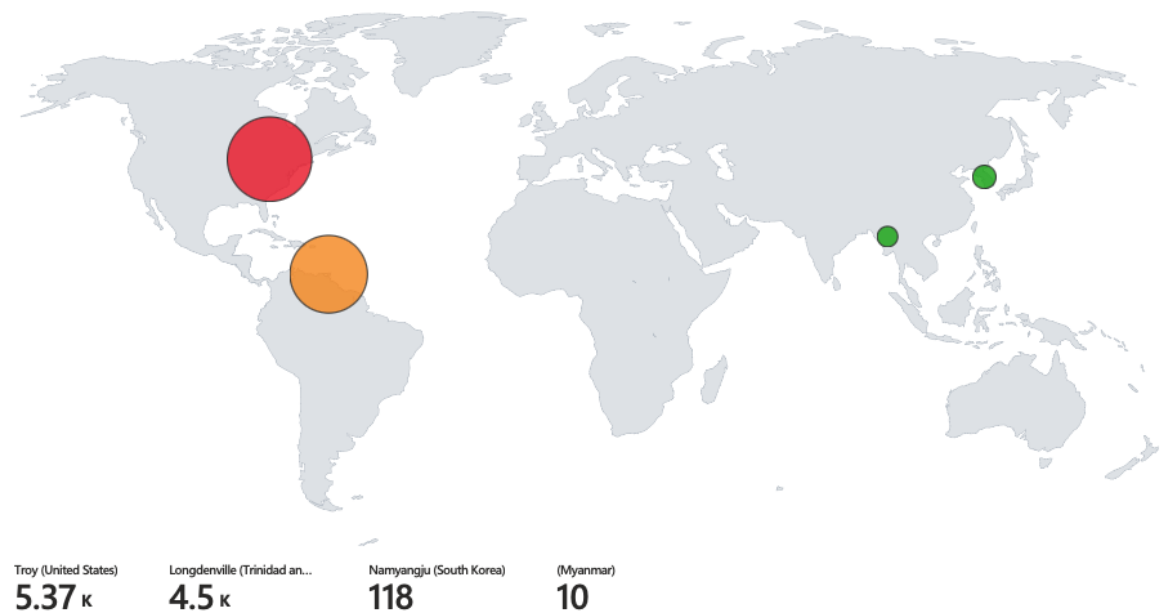


Figure 2. Windows Authentication Failures

The attack map below shows Syslog authorization failures on Linux.

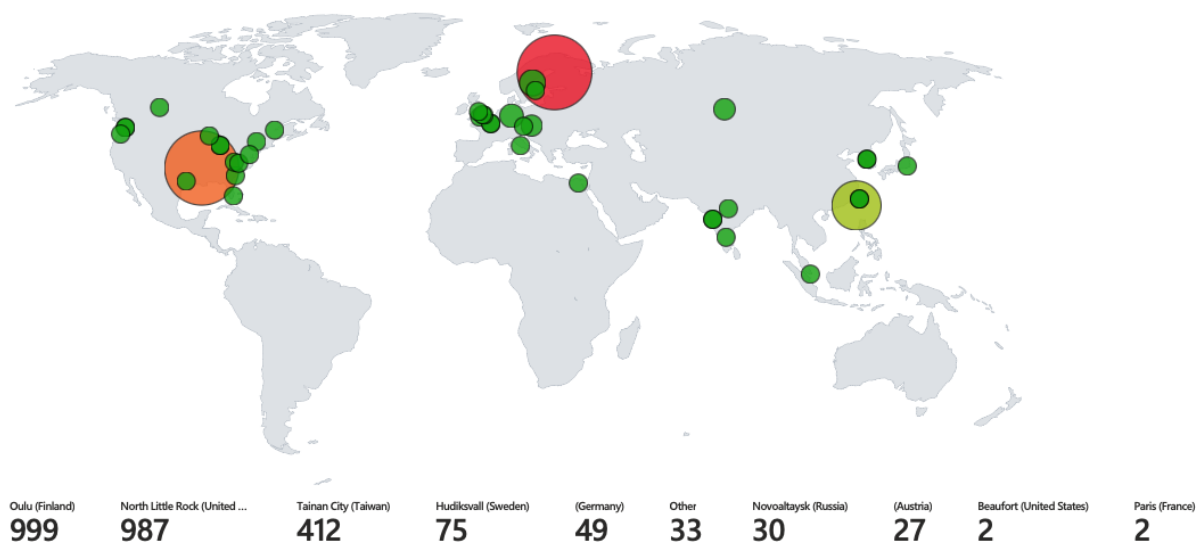


Figure 3. Syslog Authentication Failures

The attack map below shoes incidents from open Network Security Groups (NSG).

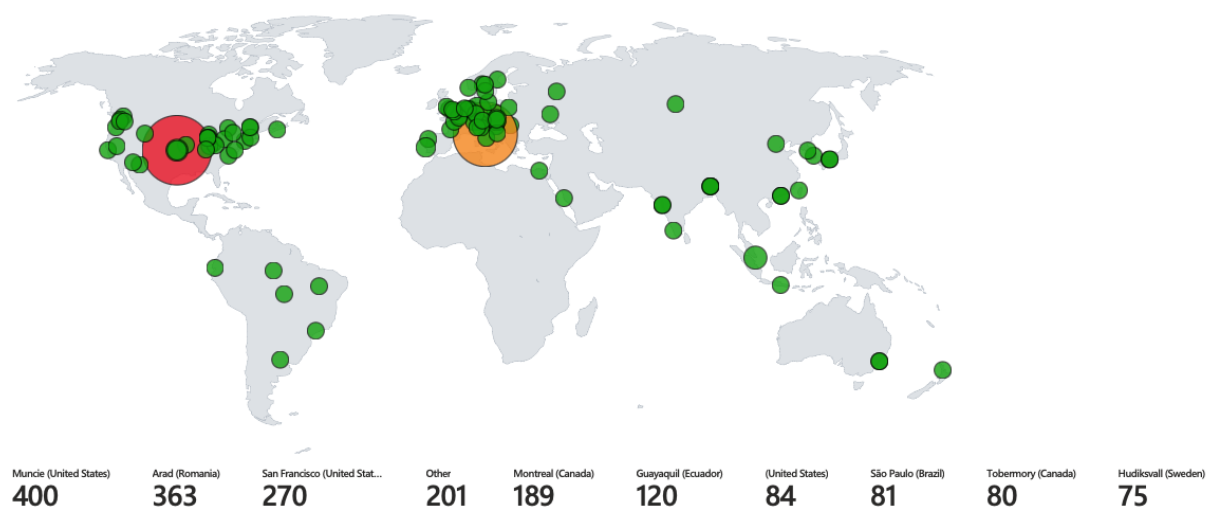


Figure 4. NSG allowing all inbound traffic

The following table shows the measurements taken in the insecure, open environment after 24 hours.

The start time was 2024-10-09 08:02:46

The stop time was 2024-10-10 08:03:02

Metric	Count
Windows VM (SecurityEvent)	10098
Linux VM (Syslog)	2616
SecurityAlert	15
SecurityIncident	765

The results from the open honeynet are unsurprisingly high. The next step is to improve the security posture and to hardened the system. Network groups were hardened by blocking all traffic but with the exception of own workstation. All public access to key vaults and resources were also blocked.

The regulatory framework of NIST 800-37 and NIST 800-53 were controls were implemented, with the expectation of reducing or eliminating the major of security incidents.

In addition Microsoft recommended security controls were also implemented.

Attack Maps After Security Hardening

The following table shows the metrics for an additional 24 hours after implementing the security controls.

The start time was 2024-10-11 08:10:35

The stop time was 2024-10-12 08:12:10

Metric	Count
Windows VM (SecurityEvent)	2938
Linux VM (Syslog)	45
SecurityAlert	0
SecurityIncident	0

After the security controls were implemented, there was a drastic reduction in the amount of events. More importantly no malicious security events were recorded following the implementation of proper controls.

Microsoft Recommended Security Controls

Microsoft Sentinel | Incidents ...
Selected workspace: 'law-cyber-lab-01'


> + Create incident (Preview) Refresh Last 24 hours Actions Delete Security efficiency workbook Columns Guides & Feedback

0 Open incidents 0 New incidents 0 Active incidents

Open incidents by severity
High (0) Medium (0) Low (0) Informational (0)

Search by ID, title, tags, owner or product Severity: All Status: 2 selected Product name: All Owner: All

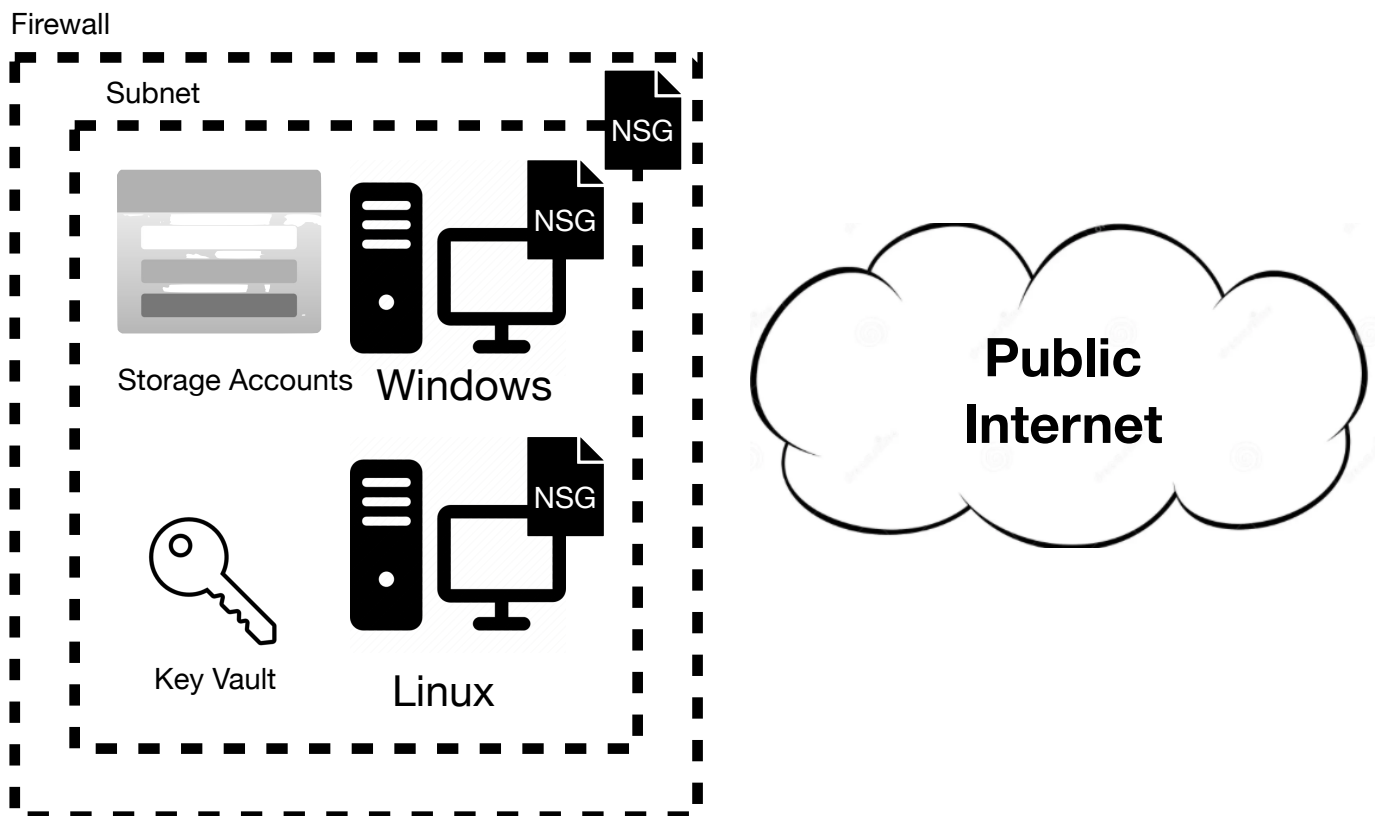
☐ Auto-refresh incidents

 **No incidents were found**

What is it?
Microsoft Sentinel incidents are containers of threats in your organization – alerts, entities and any additional related evidence. An incident is created based on alerts that you have defined in the security analytics page. The properties related to the alerts, such as severity and status are set at the incident level.

How does it work?
Incidents are automatically created as a result of alerts triggered based on detections defined in 'Security analytics'. The incidents page provide a

Architecture Before Security Hardening



Conclusion

The project involved creating a honeynet in Microsoft Azure. Microsoft Sentinel was deployed to trigger alerts and created incidents that produced logs. Metrics were measured before and after security hardening. After security measures were implemented, it drastically reduced events and incidents, which demonstrated the effectiveness of these controls. Using guidelines and control measures from NIST offered structured way to implement security controls in a standard manner.

This project was carried out in a controlled environment, it is likely that results will differ depending on situation, such as time and architecture of the honeynet.