Design and Implementation of Mini SIEM/SOAR For Comprehensive Monitoring in Azure

Department of Computer Science, Stephen F. Austin State University

[1]Taofeek O. Agboola, Faculty Mentor. [2*]Dr. Pushkar Ogale, [3]Dr. Jianjun Zheng, [4]Dr. Gina Harden
[1]Email: agboolato@jacks.sfasu.edu , [2*]Email: ogalep@sfasu.edu

ABSTRACT

This project investigates how cybersecurity capabilities can be improved by creating and deploying a scaled-down version of Security Orchestration, Automation, and Response (SOAR) within Security Information and Event Management (SIEM) systems in Azure environments that can monitor various aspects including Network Security Group "firewall," endpoints, networks, and cloud resources. Acknowledging the mounting challenges faced by traditional security operation centers (SOC), they are overwhelmed with the ever-increasing volumes of data/alerts, while cyberattacks grow more sophisticated, often eluding conventional detection methods. Leveraging SOAR technology, SOC teams previously overwhelmed with repetitive and time-consuming tasks can now enhance their incident resolution efficiency, leading to cost reduction, coverage gap mitigation, and increased productivity.

In response, this project will be developing an incidence auto-response to automate concurrent incidents by automating repetitive tasks and orchestrating workflows with Logic App which enable SOC analysts to focus on more strategic and complex security issues.

INTRODUCTION

In today's digital world, cyberattacks are a constant threat, targeting everyone from individuals to large corporations as the persistent threat of cyberattacks poses a significant challenge to organizations worldwide. Sensitive data, often stored on computer systems, is increasingly vulnerable. As hackers employ more sophisticated tactics, organizations need to react swiftly to security breaches before attackers gain a foothold or access to critical systems.

Security professionals are drowned in a sea of security alerts generated by traditional, reactive security solutions. This overwhelming volume leads to a delay in detecting and responding to cyberattacks. On average, companies take approximately 20.9 hours to respond to cyberattacks, which equates to over two "working" days (VentureBeat, October 13, 2021). On average, a SOC receives over 4000 alerts daily and it takes a minimum of 10 minutes to investigate and incident/alert with nearly 50%

INTRODUCTION CONTD.

false positive (Critical Start). This slow response time and significantly increases the risk of data breaches, costing organizations millions and damaging organizational reputation. The current practice in most organization is Alert Tuning. Tuning alerts involves refining the parameters and conditions that trigger alerts in Azure Monitor tuning alerts focuses on the detection phase, while Logic App Playbooks facilitate response and remediation actions.

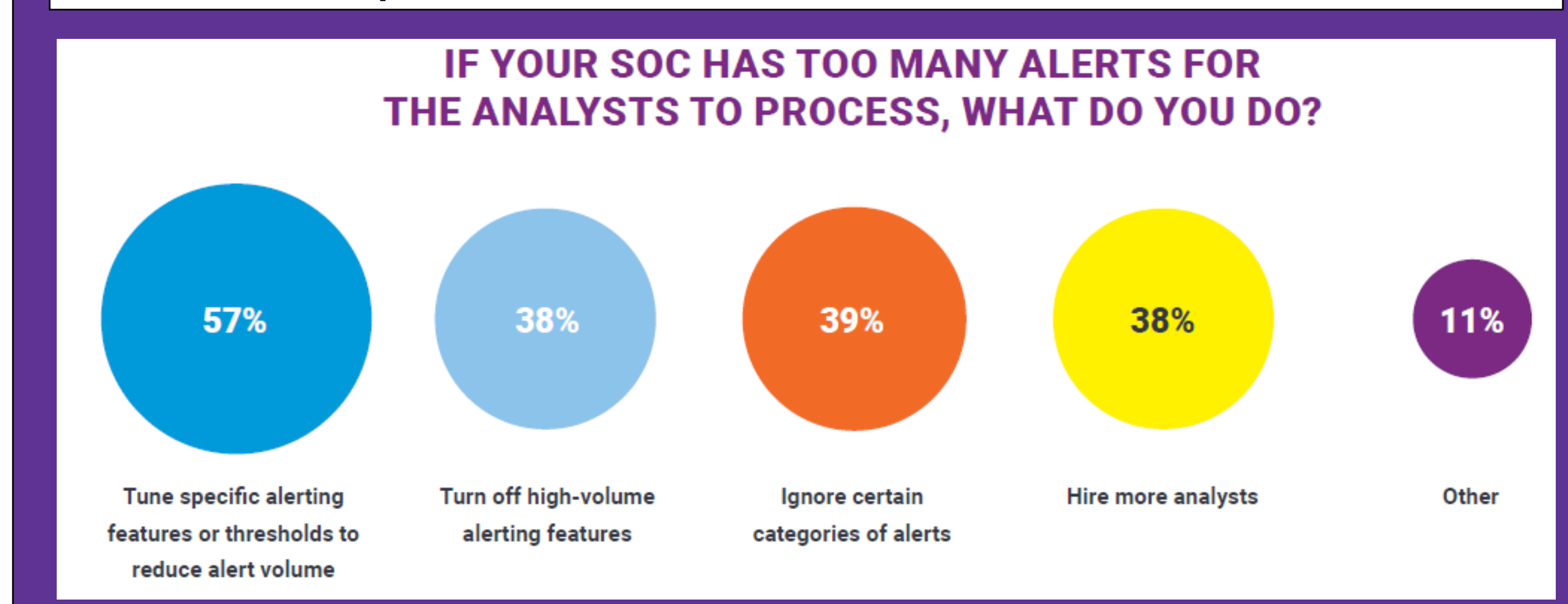


Figure 1. Survey carried out by Critical Start

SOLUTION DESCRIPTION

- Honeypot Setup: Set up two Windows and a Linux Virtual Machine; one Windows and the Linux VM positioned in the same region will act as honeypots, enticing potential attackers positioned in the same region with Microsoft SQL Server, while the other Windows VM installed in a different region will trigger alerts and test Remote Desktop Protocol and SSH connections during configuration to simulate realistic attack.
- Log Collection and Analysis: Log Analytic Workspace (LAW) functions as the central repository of logs, while Azure Sentinel serves as the Security Information and Event Management (SIEM) platform, will collect logs from network devices, endpoints, firewalls, and cloud resources for centralized analysis.
- Secure the cloud: We utilize private endpoint connections via Azure Private Link to set up the key vault and storage in a subnet, preventing them from accessing the public internet. This setup is similar to how an intranet restricts connections to users outside its network.
- NIST and Playbook: We implemented NIST 800-53 to ensure high security for our system and data, resulting in a strong security score. Additionally, NIST 800-61 guides the creation of security playbooks using Azure Logic App, detailing strategic actions for handling different security issues.
- Automate Incidence Response: Establish rules to trigger automatic responses to incidents according to predefined conditions. This process will involve invoking Azure Logic App as part of the incident response workflow, executing tasks outlined in the playbook.

SOLUTION DESCRIPTION CONTD.

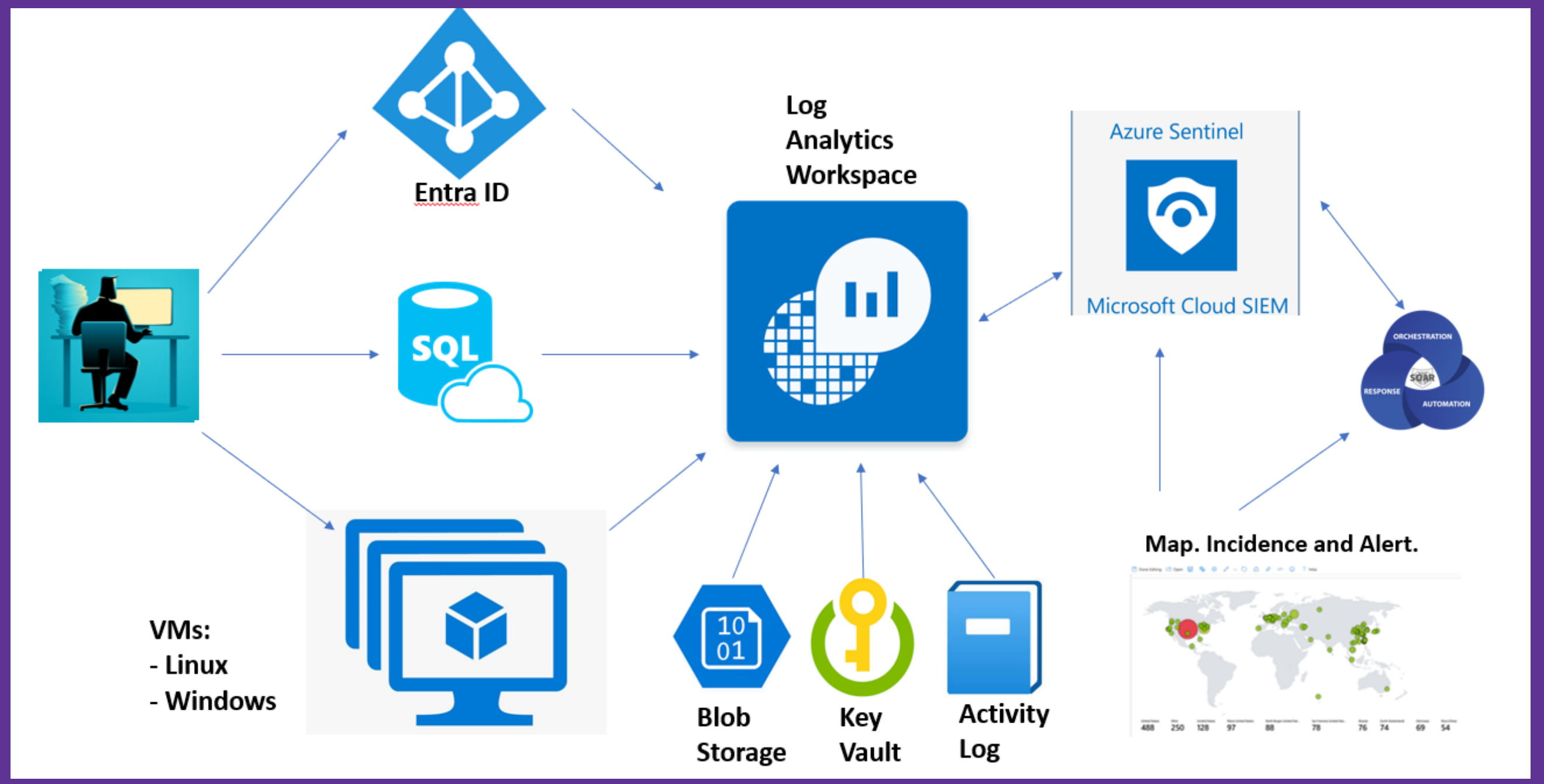


Figure 2. Solution Architecture

RESULTS

Testing involved simulating attacks to generate and analyze security logs, evaluating the effectiveness of the implemented security measures. The results demonstrated the system's capability to detect and respond to known logs effectively.

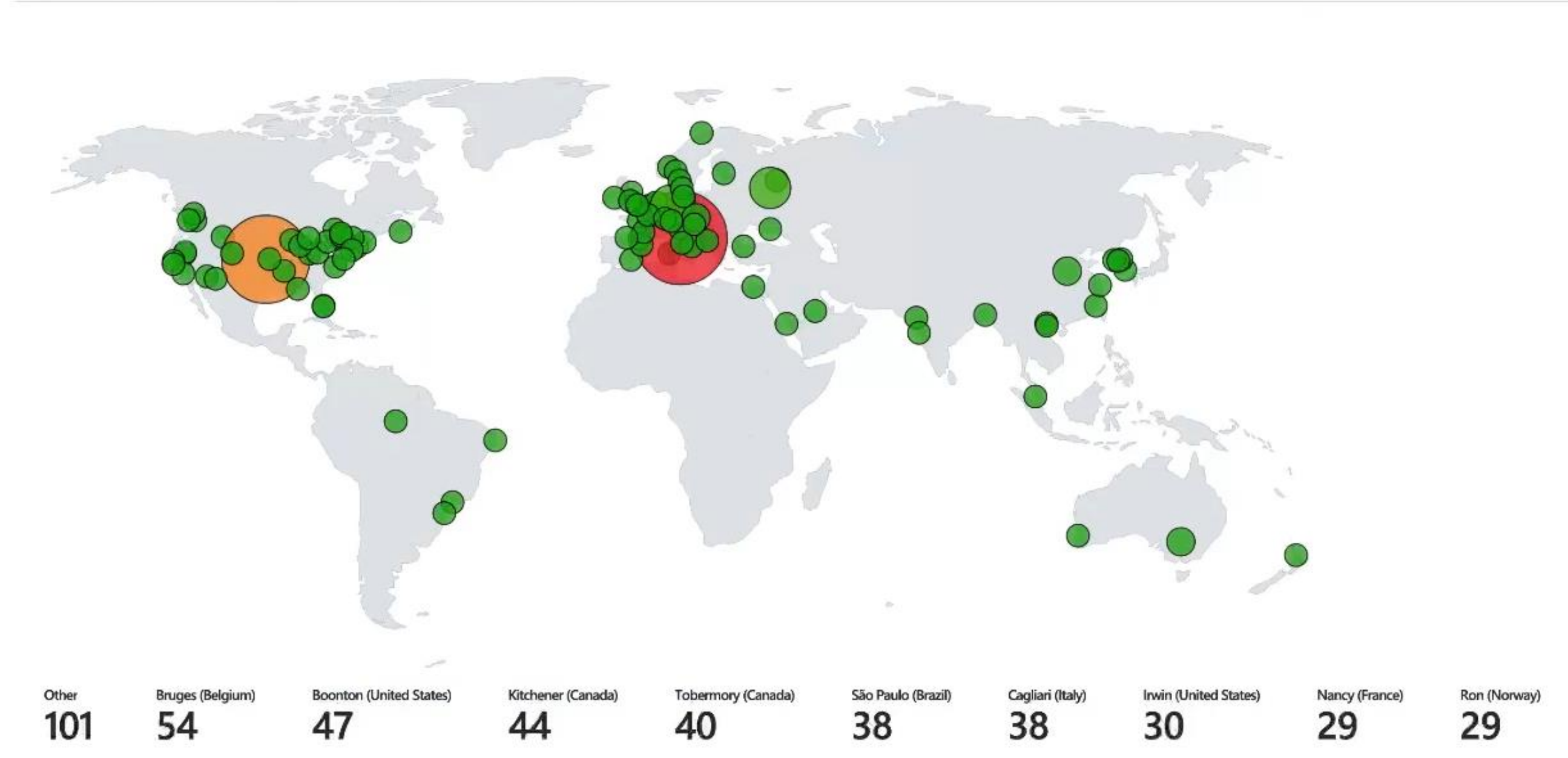
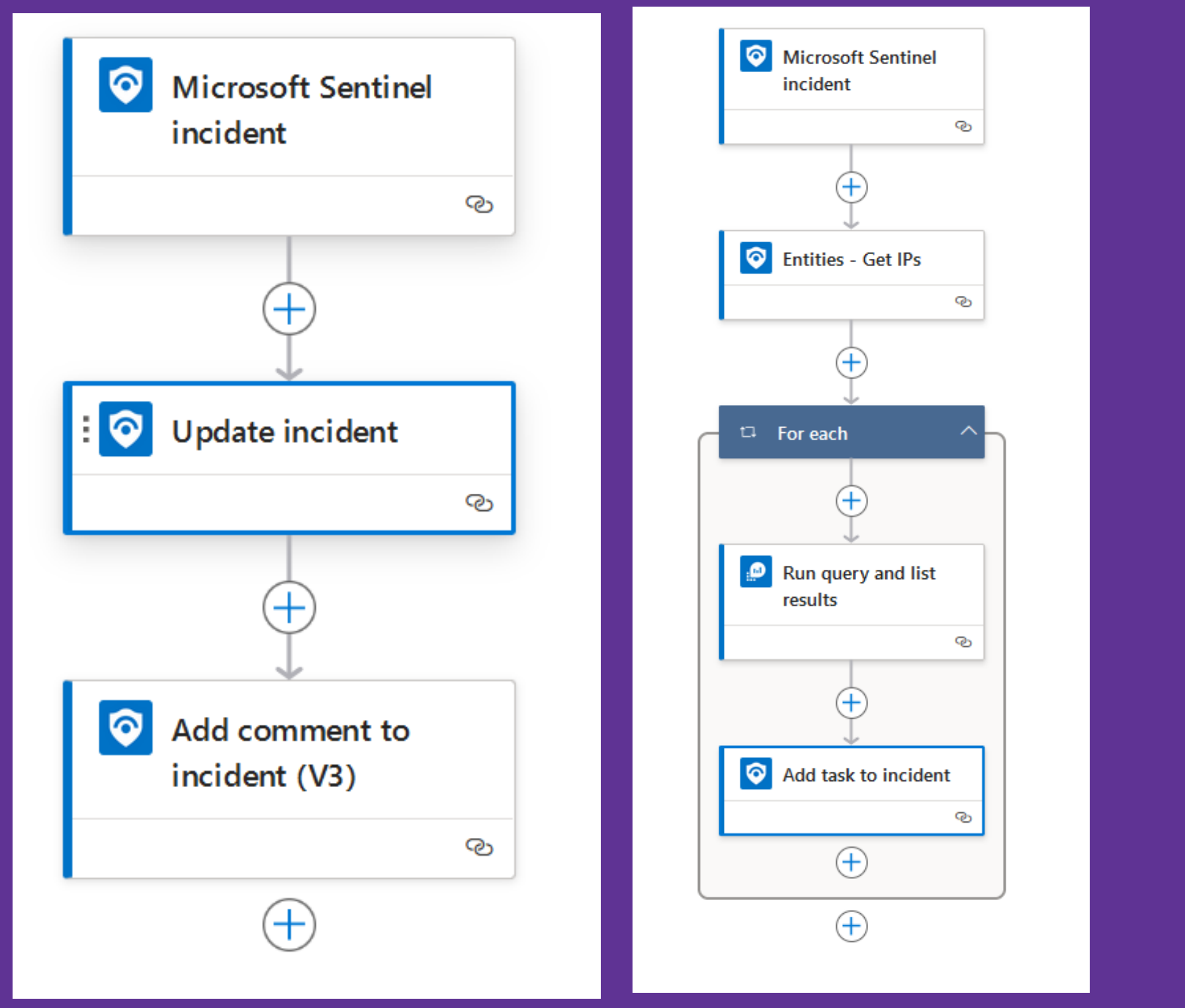


Figure 3. Attack Map

Every icon displayed on the attack map corresponds to the data of individual systems interacting with the honeypot. The green color denotes individual systems, while red indicates areas of highest density, and orange represents busy locations from which attacks originate.

Score	Before	After
Start Time	2/8/2024, 2:16:52.698 PM	2/12/2024, 9:28:19.972 PM
Stop Time	2/9/2024, 2:16:52.698 PM	2/13/2024, 9:28:19.972 PM
Security Events (Windows VMs)	8007	779
Syslog (Linux VMs)	886	5
Security Alert (Microsoft Defender for Cloud)	9	0
Security Incident (Sentinel Incidents)	94	0
NSG Inbound Malicious Flows Allowed	312	0

Table 1. Score board



Microsoft Sentinel incident

Update incident

Add comment to incident (V3)

Microsoft Sentinel incident

Entities - Get IPs

For each

Run query and list results

Add task to incident

Figure 4: Logic App

CONCLUSION

The project demonstrates the effectiveness of integrating SIEM and SOAR functionalities into Azure to enhance cybersecurity measures. The findings advocate for the adoption of cloud-based cybersecurity frameworks, emphasizing the importance of automation in cost and time savings, enabling SOC Analysts to prioritize monitoring suspicious alerts in addressing the dynamic cyber threat environment.

REFERENCES

A. Serckumecka, I. M. (2019). Low-Cost Serverless SIEM in the Cloud: 2019 38th Symposium on Reliable Distributed Systems (SRDS). (pp. 381-3811). Lyon, France: IEEE. doi:10.1109/SRDS47363.2019.00057

Davis, C. (2019). *Cloud-Native Patterns: Designing Change-Tolerant Software.* Manning Publications. Retrieved from https://www.manning.com/books/cloud-native-patterns

Gartner, Inc. (2017). *Innovation Insight for Security Orchestration, Automation and Response.* Retrieved 2024, from https://www.gartner.com/en/documents/3834578

VentureBeat. (October 13, 2021). *Cyberattack response time averages 2 days.* Retrieved 2024, from https://venturebeat.com/business/cyberattack-response-time-averages-2-days-report-finds/

Wiem Tounsi, H. R. (2018). *A survey on technical threat intelligence in the age of sophisticated cyber attacks.* Elsevier. doi:https://doi.org/10.1016/j.cose.2017.09.001

ACKNOWLEDGEMENTS

I extend my deepest gratitude to Dr. Pushkar Ogale, my practicum advisor, for his invaluable guidance and indefatigable support throughout this project. My appreciation also goes to the project committee members Dr. Jianjun Zheng and Dr. Gina Harden, whose insights and feedback were instrumental in shaping this research and to the organizers of this Luncheon and Capstone Poster Session.