

A
Minor Project-I Report
on
THREAT DETECTION AND RESPONSE

Submitted to



BHILAI INSTITUTE OF TECHNOLOGY, DURG

An Autonomous Institute

Affiliated to

CHHATTISGARH SWAMI VIVEKANAND TECHNICAL

UNIVERSITY

BHILAI(C.G.)

In partial fulfillment of the requirement for the award of

Bachelor of Technology

in

Computer Science and Engineering

By

Hitesh Verma, 300102221067

Pratik Dewangan, 300102221119

Saket Yadav, 300102221069

Under the Guidance of

Prof. Vibhore Jain

Assistant Professor

Session 2023-2024

DECLARATION BY THE CANDIDATES

We the undersigned solemnly declare that the report of the project work entitled *Threat Detection And Response System*, is based on my own work carried out during the course of my study under the supervision of *Prof. Vibhore Jain*.

We assert that the statements made and conclusions drawn are an outcome of the project work.

We further declare that to the best of my knowledge and belief that the report does not contain any part of any work which has been submitted for the award of any other degree/diploma/certificate in this University/ any other University of India or any other country.

(Signature of Student):

Hitesh Verma

Roll No.: 300102221067

Enrollment No.: CA6424

(Signature of Student):

Saket Yadav

Roll No.: 300102221069

Enrollment No.: CA6425

(Signature of Student):

Pratik Dewangan

Roll No.: 300102221119

Enrollment No.: CB4303

CERTIFICATE

This is to Certify that the report of the project submitted is an outcome of the project work entitled Threat Detection And Response System carried out by Hitesh Verma **bearing Roll No. 300102221067, Enrollment No. CA6424; Saket Yadav bearing Roll No. 300102221069, Enrollment No. CA6425; Pratik Dewangan bearing Roll No. 300102221119, Enrollment No. CB4303.**

Under my guidance and supervision in partial fulfillment of Bachelor of Technology in Computer Science from Bhilai Institute of Technology, Durg, an autonomous institute affiliated to Chhattisgarh Swami Vivekanand Technical University, Bhilai (C.G).

To the best of my knowledge and belief the project

- i) Embodies the work of the candidate himself / herself,
- ii) Has duly been completed,
- iii) Fulfills the requirement of the Ordinance relating to the B. Tech. degree of the University,
- iv) Is up to the desired standard for the purpose of which is submitted.

Signature of Coordinator
Dr. Sumit Kumar Sar
Associate Professor
Computer Sc. & Engg

Signature of Coordinator
Prof. Saurabh Singh
Assistant Professor
Computer Sc. & Engg.

Signature of Guide
Prof. Vibhore Jain
Assistant Professor
Computer Sc. & Engg.

The Project work as mentioned above is hereby being recommended and forwarded for examination and evaluation.

Dr. (Mrs.) Sunita Soni
Head of the Department
Computer Sc. & Engg.

CERTIFICATE BY THE EXAMINERS

This is to Certify that the project the entitled

“THREAT DETECTION AND RESPONSE SYSTEM”,

Submitted by

Hitesh Verma	Enrollment No: CA 6424	Roll No: 300102221067
Pratik Dewangan	Enrollment No: CB 4303	Roll No: 300102221119
Saket Yadav	Enrollment No: CA 6425	Roll No: 300102221069

Have been examined by the undersigned as a part of the examination for the award of Bachelor of Technology degree in Computer Science and Engineering from Bhilai Institute of Technology, Durg, an autonomous institute affiliated to Chhattisgarh Swami Vivekanand Technical University, Bhilai (C.G)

(Internal Examiner)

Name:

Date:

(External Examiner)

Name:

Date:

ACKNOWLEDGEMENT

We have great pleasure in the submission of this project report entitled **Threat Detection And Response System** in partial fulfillment the degree of Bachelor of Engineering (CSE). While submitting this Project report, We take this opportunity to thank those directly or indirectly related to project work.

We would like to thank our guide **Prof. Vibhore Jain** who has provided the opportunity and organizing project for us. Without his active co-operation and guidance, it would have become very difficult to complete task in time.

We would like to express sincere thanks and gratitude to Dr. Arun Arora, **Principal of the Institution**, Dr. (Mrs.) Sunita Soni, **Head of the Department** Computer Science & Engineering for their encouragement and cordial support.

While Submission of the project, we also like to thanks to Dr Sumit Kumar Sar and Prof Saurabh Singh **Project Coordinator**, faculties and all the staff of department of Computer Science & Engineering, **Bhilai Institute of Technology, Durg** for their continuous help and guidance throughout the course of project.

Acknowledgement is due to our parents, family members, friends and all those persons who have helped us directly or indirectly in the successful completion of the project work.

Hitesh Verma

Roll No.: 300102221067

Enrollment No.:CA6424

Saket Yadav

Roll No.: 300102221069

Enrollment No.: CA6425

Pratik Dewangan

Roll No.: 300102221119

Enrollment No.: CB4303

ABSTRACT

The "Threat Detection And Response" project is a system implemented using Azure services including Microsoft Sentinel, Log Analytics workspace, virtual machine and PowerShell script enriched with API integration from <https://ipgeolocation.io/>. The primary objective is to find the unusual login attempts via Microsoft proprietary RDP protocol running on virtual machine, showing specific information such as attacker's position and the payload used to log in to the virtual machine, serving the admin user as Threat Detection feature.

Key to the project's efficacy is its ability to extract specific information related to detected threats, such as the geographic position of the attacker. Leveraging the IP geolocation API from <https://ipgeolocation.io/> the system enriches threat data by providing precise insights into the physical location of the threat actor. This information is then visually represented on a map within Microsoft Sentinel, allowing administrators to comprehend the spatial distribution of potential threats through longitude and latitude coordinates.

Moreover, the system captures and analyzes the payload utilized during login attempts, offering critical details on the methodology and tools employed by potential attackers.

The Virtual Machine infrastructure serves as the foundation for monitoring and evaluating RDP login attempts. The combination of Azure services, PowerShell scripts, and external API data creates a holistic ecosystem that empowers administrators with actionable insights, enabling them to respond swiftly to potential security breaches. By incorporating a map feature within Microsoft Sentinel, the project provides a comprehensive visual representation of attacker positions, enhancing the administrator's situational awareness and facilitating effective decision-making in response to security incidents.

In essence, the "Threat Detection And Response" project underscores the convergence of cutting-edge Azure technologies, API integration, and visual analytics to create a dynamic security solution. This amalgamation not only bolsters the defenses of Microsoft environments against evolving cyber threats but also exemplifies the proactive and adaptive nature of contemporary cybersecurity measures.

List of Figures

S. No	Fig. No.	Fig. Name	Page No.
1	4.1	Context Diagram	17
2	4.2	Use Case Diagram	19
3	4.3	Sequence Diagram	21
4	4.4	Activity Diagram	22
5	5.1	Virtual Machine Configuration	24
6	5.2	Network Configuration	25
7	5.3	Firewall Switch Off	26
8	5.4	Powershell Script	27
9	5.5	Log File	27
10	5.6	Log Analytics Workspace	28
11	5.7	Custom Log Creation	29
12	5.8	Path Selection	29
13	5.9	Overview Setup	30
14	6.1	Windows Stratup	32
15	6.2	Windows Setup	33
16	6.3	Powershell Output	33
17	6.4	Log Data Output	33
17	6.4	RDP Login	34
18	6.5	Map Overview	35

CONTENTS

DECLARATION BY THE CANDIDATES	i
CERTIFICATE.....	ii
CERTIFICATE BY THE EXAMINERS	iii
ACKNOWLEDGEMENT.....	iv
ABSTRACT	v
LIST OF FIGURES	vi
1. INTRODUCTION	
1.1 OBJECTIVE.....	1
1.2 PROJECT DESCRIPTION	2-3
2. SYSTEM STUDY	
2.1 FEASIBILITY AND PROPOSED SYSTEM.....	4
2.2 FEASIBILITY STUDY	5
2.3 TOOLS AND TECHNOLOGIES USED.....	6-7
2.4 HARDWARE AND SOFTWARE REQUIREMENTS.....	8-9
3. SOFTWARE REQUIREMENTS SPECIFICATION	
3.1 USER ACCESS.....	10
3.2 FUNCTIONAL REQUIREMENTS.....	11-12
3.3 NON-FUNCTIONAL REQUIREMENTS.....	13-14
4. SYSTEM ANALYSIS AND DESIGN	
4.1 SYSTEM PERSPECTIVE	15-16
4.2 CONTEXT DIAGRAM.....	17-18
4.3 USE CASE DIAGRAM.....	19-20
4.4 SEQUENCE DIAGRAM.....	21
4.5 ACTIVITY DIAGRAM.....	22-23
5. IMPLEMENTATION	
5.1 SUMMARY OF IMPLEMENTATION.....	24-31
6. SOFTWARE TESTING	
6.1 TEST CASES.....	32-35
7. CONCLUSION	36
8. FUTURE ENHANCEMENTS	37
9. BIBLIOGRAPHY	38

CHAPTER-1

INTRODUCTION

1.1.OBJECTIVE

The "Threat Detection And Response" initiative aims to fortify cybersecurity in windows computers through a system built on Azure services. The primary focus is on identifying irregular login attempts using the proprietary RDP protocol on virtual machines. By integrating Azure services, PowerShell scripts, and the API from <https://ipgeolocation.io/>, the project extracts vital threat information, including the geographic position of potential attackers. This information is visually presented on a map within Microsoft Sentinel, providing administrators with a clear understanding of the spatial distribution of threats based on longitude and latitude. Additionally, the system analyzes login attempt payloads, IP address, offering crucial insights into the tactics and tools employed by potential attackers. This comprehensive approach facilitates swift responses to security breaches, showcasing the project's commitment to proactive and adaptive cybersecurity measures.

1.1.1. TECHNICAL SYNERGY

The " Threat Detection And Response " project thrives on the technological synergy of virtualbox, Sentinel, and log analytical workspace services provided by the Azure forming the backbone of the project's frontend representation. Powershell scripts and API components are strategically integrated to extract the attacker's data from the VM and create a log file out of it and the data extracted is represented through the powershell script, showing real time anonymous log in details. Including API integrations serves as a bridge, enabling the retrieval of user's location data, such as state and country, based on their IP address. This data can then be plotted in Sentinel.

The synergy between these cutting-edge technologies is absolutely crucial in delivering an unparalleled and flawlessly seamless user experience. The virtual machine, acting as the victim machine, plays a pivotal role in this process. Additionally, the log analytical workspace not only trains and refines the data but also securely stores them, ensuring their availability for future analysis. The sentinel component of this technological ecosystem provides valuable insights by revealing the location and number of attacks. Last but not least,

the powershell script plays a vital role in the extraction of failed event logs from the event viewer, guaranteeing accuracy and efficiency, and further consolidating the process by creating a comprehensive and detailed log file that can be easily analyzed.

1.1.2. User Centric Design

The "Threat Detection and Response" initiative leverages a robust technological synergy to enhance cybersecurity on Windows computers utilizing Azure services. The focus is on early detection of irregular login attempts through the proprietary RDP protocol on virtual machines. By integrating Azure services, PowerShell scripts, and the IP geolocation API, the project extracts crucial threat information, including the geographic position of potential attackers. This proactive approach allows administrators to visualize threat distributions on a map within Microsoft Sentinel, offering a spatial understanding based on longitude and latitude. The system also analyzes login attempt payloads, providing insights into potential attackers' tactics and tools.

The technological synergy of VirtualBox, Sentinel, and Azure services ensures a seamless user experience, with PowerShell scripts and API integrations playing pivotal roles in data extraction and representation. This comprehensive approach underscores the project's commitment to proactive and adaptive cybersecurity measures, facilitating swift responses to emerging threats.

1.1.3. PEDAGOGICAL INNOVATION

Pedagogical innovation is crucial in modern education, enhancing learning outcomes through new teaching methods and technologies. Incorporating virtualbox, Sentinel, and Azure's log analytical workspace revolutionizes pedagogical practices. Virtualbox simulates real-world scenarios, providing hands-on experience in a safe environment. Log analytical workspace and Sentinel offer insights into student performance, enabling personalized learning experiences and progress monitoring. Leveraging PowerShell scripts and APIs for real-time data extraction and visualization allows tailored instruction and timely feedback. Embracing pedagogical innovation and cutting-edge technologies fosters creativity, critical thinking, and collaboration, preparing students for the digital age.

1.2. PROJECT DESCRIPTION

1.2.1. Project Description

The "Threat Detection And Response" project is a comprehensive cybersecurity system designed to fortify Windows computers against evolving threats. Leveraging Azure services,

PowerShell scripts, and API integration, this initiative focuses on identifying and mitigating irregular login attempts using the proprietary RDP protocol on virtual machines.

The core objective of the project is to provide administrators with actionable insights into potential security breaches. By extracting vital threat information, including the geographic position of attackers, the system enhances the understanding of threat distributions based on longitude and latitude. This information is visually represented on a map within Microsoft Sentinel, facilitating effective decision-making and response to security incidents.

The project's technological synergy relies on the integration of virtualbox, Sentinel, and Azure's log analytical workspace. Virtualbox creates a simulated environment for real-world scenarios, enabling hands-on experience in a safe setting. The log analytical workspace refines and securely stores data, ensuring its availability for future analysis. Additionally, the powershell script plays a crucial role in extracting failed event logs and creating comprehensive log files for analysis, guaranteeing accuracy and efficiency.

Furthermore, the project incorporates the IP geolocation API from <https://ipgeolocation.io/> to enrich threat data with precise insights into the physical location of potential attackers. This integration enhances situational awareness and aids in the identification of emerging threats.

The "Threat Detection And Response" project exemplifies proactive and adaptive cybersecurity measures, empowering administrators to respond swiftly to evolving threats. By embracing cutting-edge technologies and pedagogical innovation, the project fosters creativity, critical thinking, and collaboration, preparing students for the digital age.

In summary, the project offers a dynamic security solution that bolsters the defenses of Microsoft environments, exemplifying the convergence of Azure technologies, API integration, and visual analytics.

CHAPTER-2

SYSTEM STUDY

2.1. EXISTING AND PROPOSED SYTEM

2.1.1 Existing System:

The prevailing landscape in the domain of security is characterized by antivirus, IDS, IPS and firewall resources that predominantly rely on textual descriptions to convey attacker's information. Users relying on existing platforms encounter challenges related to attacker's data and their location, especially those who wants to find hackers and make analysis out of it based on the area. The lack of visual aids, dynamic content, and interactive elements hinders the effectiveness of conveying attacker's information and may result in a less robustness to the security.

In the current scenario, users often find themselves navigating through log files, relying on fragmented information scattered across various log files. The absence of a centralized analysis and comprehensive representation for attackers leaves industries, particularly bigger organizations, with an incomplete understanding of intrusions happening on their organization which leads to security vulnerability.

2.1.2 Proposed System:

Addressing the inadequacies of conventional IDS and IPS systems, the "Threat Detection And Response" project introduces an innovative solution to redefine how users interact with attacker information. Unlike the existing security landscape that relies heavily on textual descriptions, the proposed system envisions a dynamic and centralized platform. Leveraging the power of security events, Microsoft Sentinel, log analytical workspace, and APIs, this project aims to provide a comprehensive visual representation and analytical experience for understanding potential threats. The integration of virtual machine, PowerShell scripts, and the IP geolocation API further elevates the system, enriching the data with real-time insights into attackers' tactics and precise geographic positions.

In the proposed system, users move beyond navigating through scattered log files and enter a realm of dynamic content and interactive elements. This transformation empowers administrators to visualize threat distributions on a map, facilitating a spatial understanding

of attacks based on longitude and latitude. The centralized analysis ensures that industries, especially larger organizations, gain a holistic understanding of intrusions, reducing security vulnerabilities. By fostering a more proactive and adaptive cybersecurity approach, the "Threat Detection And Response" project exemplifies a paradigm shift in security, providing actionable insights and robust defense mechanisms against evolving threats.

2.2 Feasibility Study

2.2.1 Technical Feasibility:

The "Threat Detection And Response" project demonstrates robust technical feasibility by seamlessly integrating cutting-edge technologies to fortify Windows computers against evolving cyber threats. Leveraging the secure and scalable infrastructure of Microsoft Azure provides a foundation that ensures reliable performance and efficient threat management. Virtualbox plays a pivotal role in creating a simulated environment for practical, hands-on experiences, allowing administrators to enhance their skills and responses to real-world scenarios.

The project's technical innovation shines through the strategic use of PowerShell scripts, automating the extraction of threat-related information from virtual machines. This not only streamlines the process but also ensures the accuracy and efficiency of handling vast amounts of data in real-time, enabling administrators to respond swiftly to security breaches.

The integration of the IP geolocation API enhances the system by providing precise geographic insights into potential attackers, thereby enhancing overall situational awareness. The seamless collaboration between Azure Sentinel and log analytical workspace ensures the secure storage, analysis, and visualization of threat data, offering a comprehensive and user-friendly experience.

2.2.2 Economic Feasibility:

The project demonstrates economic feasibility by leveraging Microsoft Azure's first-month free subscription, allowing users to explore threat detection and response capabilities at no initial cost. This cost-effective approach aligns with budgetary considerations, offering an opportunity for organizations to evaluate the benefits of services like Azure Sentinel, VirtualBox, and Log Analytical Workspace without immediate financial commitment. As the project scales, users can make informed decisions on continued investment based on the value derived from these services, ensuring a financially prudent and sustainable threat management solution.

2.2.3 Operational Feasibility:

Operational Feasibility:

The "Threat Detection And Response" project stands out in terms of operational feasibility, harmonizing its advanced cybersecurity measures with practical considerations for seamless integration into operational frameworks. The project strategically utilizes Microsoft Azure services, VirtualBox, and PowerShell scripts to ensure an operational landscape that enhances the efficiency of threat detection and response operations.

By leveraging Microsoft Azure's first-month free subscription, the project minimizes initial financial barriers, allowing organizations to explore and evaluate its operational benefits without immediate financial commitments. This approach aligns with practical considerations, enabling a gradual adoption of the system based on its demonstrated value and performance.

The incorporation of VirtualBox contributes to operational feasibility by providing a controlled environment for hands-on training and simulations. This ensures that administrators can seamlessly incorporate the project into their daily operations, fostering familiarity and expertise in handling real-world cybersecurity scenarios.

The integration of PowerShell scripts further streamlines operational processes, automating complex tasks and reducing manual intervention. This not only enhances the overall efficiency of threat management but also ensures a user-friendly experience, contributing to the project's operational feasibility.

2.3 Tools and Technologies Used

2.3.1 Virtual Machine

A virtual machine (VM) is a fundamental component at the core of the "Threat Detection And Response" project, providing a dynamic and secure environment for practical cybersecurity scenarios. Operating within a virtualization platform, VMs enable administrators to create, manage, and replicate diverse operating systems, establishing a simulated setting for immersive hands-on training. This technology offers a controlled space where administrators can precisely mimic real-world cybersecurity situations, honing their skills in threat detection and response.

As an essential feature of the project's infrastructure, virtual machines support the deployment of various operating systems in isolated instances, ensuring a secure testing

environment without compromising the integrity of the host system. VMs also leverage features like snapshotting, allowing instantaneous captures of machine states. This functionality facilitates efficient testing, analysis, and recovery processes, enhancing the project's overall cybersecurity capabilities.

states. This functionality facilitates efficient testing, analysis, and recovery processes, enhancing the project's overall cybersecurity capabilities.

2.3.2 Sentinel:

Microsoft Sentinel is a key component, offering a centralized platform for security event management. It facilitates the visualization of threat data on maps, enhancing spatial understanding for administrators. Sentinel provides valuable insights into the location and number of attacks, contributing to proactive cybersecurity measures scalability.

2.3.3 Log Analytical Workspace

Azure's Log Analytical Workspace is a crucial element in the architecture of the "Threat Detection And Response" project, serving as a sophisticated data refinement and storage solution. This tool efficiently processes and refines data extracted from virtual machines, preparing it for in-depth analysis. The Log Analytical Workspace securely stores this information, guaranteeing its availability for future investigations and comprehensive threat analyses. By providing a centralized and secure repository, this workspace enhances the project's capacity to manage and analyze vast datasets, contributing to the overall effectiveness of threat detection and response efforts within the dynamic landscape of cybersecurity.

2.3.4 Responsive Design:

A critical aspect of the technological toolkit employed in the "Fitness Companion" project is responsive design principles. Responsive design ensures that the user interface adapts seamlessly to various devices and screen sizes, providing an optimal viewing and interaction experience. This approach is particularly important in the context of fitness education, where users may access the platform from diverse devices such as desktops, laptops, tablets, or smartphones. The integration of responsive design principles contributes to the project's accessibility and usability, enhancing the overall user experience across a spectrum of devices.

2.4 Hardware and Software Requirements

2.4.1 Hardware Requirements:

The "Threat Detection And Response" project is meticulously designed with minimal hardware requirements, prioritizing accessibility for a broad user base. The platform is crafted to operate seamlessly on standard computing devices, encompassing desktops, laptops, tablets, and smartphones. These widely available devices serve as the primary interfaces, ensuring users can engage effortlessly with the Sentinel platform.

A fundamental hardware prerequisite is reliable internet connectivity. The system relies on login data from across the globe, making a stable internet connection indispensable. This connectivity ensures users have access to the latest and most pertinent information, enhancing the system's overall utility. Whether users are on desktops in office settings, laptops on the go, or tablets and smartphones for remote monitoring, the project's adaptability to diverse devices and its dependency on a stable internet connection underscore its commitment to user convenience and real-time threat responsiveness.

2.4.2 Software Requirements:

The software requirements for the "Threat Detection And Response" are RDP protocol and a standard browser. Whole system works on the basis of azure website and RDP protocol if the system ensures that it has a standard browser that can run azure website and RDP protocol smoothly then it's compatible to run the project.

The following software components contribute to the smooth functioning of the platform:

Web Browsers: The system can run on modern web browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, and others. Ensuring compatibility with a range of browsers enhances the accessibility of the platform, allowing users to choose their preferred browser for engagement.

Microsoft Azure Support: Since the project is built on Microsoft Azure, the software requirements include browsers that support Azure. This ensures that users can fully experience the interactive and visually engaging elements integrated into the system.

Windows environment: As the whole system is based on the windows 10 virtual machine so we need windows iso file. However the whole system can be implemented on other operating

systems too, we only have to change the powershell script with bash script and change the file location, then it will be ready to use.

Powershell : Since the log analytical workspace takes the data from virtual machine using log file and location details through sending IP address to the ipgeolocation api all this work is done using the powershell script which is continuously running on the VM's background ensuring continuous data flow.

In conclusion, the hardware and software requirements for the "Threat Detection And Response" project are intentionally designed to be inclusive and user-friendly. By adhering to these minimal requirements.

CHAPTER-3

SOFTWARE REQUIREMENTS SPECIFICATION

3.1 User Access

3.1.1 Access Model:

The "Threat Detection And Response" platform embraces an accessible and open access model, welcoming users to explore its robust cybersecurity resources without the requirement for user profiles or authentication. This inclusive approach ensures that security professionals, enthusiasts, and individuals of varying expertise levels can freely access the platform's comprehensive content. Users can seamlessly navigate the system, gaining insights into threat detection and response strategies without encountering barriers related to authentication. This user-friendly design promotes a collaborative and open environment for cybersecurity education, accommodating both novices and experts. By removing access restrictions, the project encourages widespread engagement and knowledge-sharing within the cybersecurity community, contributing to a collective and informed response to evolving threats.

3.1.2 User Characteristics:

Users engaging with the "Threat Detection And Response" project may employ a range of devices, encompassing desktop computers, laptops, tablets, or smartphones. The project's design philosophy is attuned to diverse user characteristics, catering to individuals with varying levels of technological expertise and learning preferences within the realm of cybersecurity. Whether users are seasoned security professionals seeking advanced threat detection insights or beginners in search of foundational information, the project guarantees a user-friendly experience for all. The platform is thoughtfully crafted to ensure accessibility and inclusivity, recognizing the diverse needs of users and promoting a seamless engagement with cybersecurity education, regardless of their background or proficiency level.

3.1.3 User Goals:

The open access model in the "Threat Detection And Response" project aims to empower users to achieve their cybersecurity objectives without constraints. Users,

irrespective of their expertise levels, can freely delve into a wealth of cybersecurity insights, gain a profound understanding of threat detection techniques, and access valuable information to enhance their grasp of cybersecurity principles.

This user-centric approach aligns with the platform's commitment to providing an inclusive and accessible resource for individuals seeking to embark on or advance their cybersecurity journeys. The absence of mandatory user profiles ensures that users can seamlessly and freely navigate the platform's offerings, promoting a culture of open learning and exploration in the cybersecurity domain.

3.2 Functional Requirements

3.2.1 Resource Group:

The Resource Group page serves as the central gateway to the "Threat detection and response" system, to offer an engaging and informative view. It includes:

- Service details: Resource group contains all the services that are under that resource group whether running or not, user has the ability to access each service they want to use or turn on or off, providing users complete control over the system features.
- Service setting : Resource group allows to manage all the services present to make the system more stretchable, if user wants to add new virtual machine that can be done from here.

3.2.2 log analytical workspace Section:

The log analytical workspace Section forms the heart of the platform, offering a comprehensive database of details that target machine can get from the external world. This section includes:

- Log Analytics Workspace can collect and ingest data from various sources, including Azure resources, on-premises servers, virtual machines, and custom logs. This enables centralized data storage for comprehensive analysis.
- Query Language (Kusto Query Language - KQL): Kusto Query Language (KQL) is a powerful query language used in Log Analytics Workspace. It allows users to query and analyze large datasets effectively. Users can perform complex queries to extract meaningful insights from log data.

- **Alerting and Monitoring:** Users can set up alerts based on specific conditions in Log Analytics Workspace. This feature enables proactive monitoring, alerting administrators when predefined thresholds are met or exceeded.

3.2.3 Sentinel section:

- Azure Sentinel is a cloud-native security information and event management (SIEM) service provided by Microsoft Azure. It offers a range of features to help organizations collect, analyze, and respond to security threats. Here are key features of Azure Sentinel:
- **Customizable Dashboards:** Provides customizable dashboards and workbooks to visualize security data. Users can create and tailor dashboards to display key metrics and insights relevant to their specific security needs.
- **Security Information and Event Management (SIEM) Capabilities:** Functions as a SIEM solution, providing centralized visibility into security events and alerts. Security analysts can use the SIEM capabilities to investigate incidents and monitor security posture.

3.2.4 Attacker's Details:

Each attacker's detail is first stored in log events by the windows default setting, then by using our custom powershell script user's details such as username, password and ip address used to log in are extracted out, ip address is sent to through ipgeolocation api where it extracts out the location of attacker based on their ip address and send it back to the powershell, powershell collects all the data and creates simple log file at C:\ProgramData\failer_log.log, then this log file is connected to the log analytical workspace so that it can extract out the details in every span of time and store them.

3.2.5 Graphical overview:

The integration of Azure Sentinel's map graphical representation further enhances the view of attacks and threat detection. This involves:

- **Logs Fetching:** The platform fetches attacker's logs through KQL query seamlessly integrating logs into the map representation page.
- **Map view and setting:** Users can access map visual view, watching the denseness of attacks according to the location, number of attacks. Providing various functionalities

based on what user want to see the map they can set such as country, longitude and latitude, state etc.

3.2.7 KQL Functionality:

Kusto Query Language, is a powerful query language used in Azure Sentinel and Azure Monitor, enabling users to efficiently analyze and retrieve insights from large datasets through a simple and expressive syntax. Key functionalities include:

- **Data Querying and Analysis:** KQL allows users to query and analyze large datasets efficiently, enabling the extraction of meaningful insights from log and telemetry data.
- **Filtering and Aggregation:** Users can filter and aggregate data using KQL, facilitating the identification of specific patterns, trends, or anomalies within the dataset.

3.3 Non-Functional Requirements

3.3.1 Performance:

Ensuring optimal performance is critical to providing users with a seamless and responsive experience. The platform must:

- **Response Time:** Respond promptly to user interactions, with an emphasis on minimizing load times for key features such as map view and powershell output.

3.3.2 Reliability:

Reliability is paramount for user trust and satisfaction. The system must:

- **Downtime:** Maintain minimal downtime for maintenance activities, ensuring uninterrupted access to the platform for users.
- **Data Integrity:** Implement robust measures to protect user information and maintain data integrity, preventing loss or corruption of essential data.

3.3.3 Scalability:

The platform's design should allow for seamless scalability to adapt to changing needs. It must:

- **User Base Growth:** Accommodate potential growth in the user base without compromising performance, ensuring a consistent user experience as the platform expands.

3.3.4 Usability:

The user interface must be intuitive, accessible, and visually appealing to cater to users with diverse preferences and technological proficiency levels. This includes:

- **User-Centric Design:** Prioritize user experience through intuitive navigation, clear layouts, and user-friendly interactions, fostering ease of use for individuals at varying levels of digital literacy.
- **Cross-Device Compatibility:** Ensure that the platform is compatible with a range of devices, including desktops, laptops, tablets, and smartphones, providing a consistent and accessible experience across platforms.

3.3.5 Security:

Security measures must be implemented to safeguard user interactions and information. This involves:

- **User Authentication:** If introduced in the future, ensure secure user authentication and authorization mechanisms to protect against unauthorized access.
- **Data Encryption:** Implement encryption protocols to secure data transmission, preventing interception and ensuring the confidentiality of user information.

3.3.6 Compatibility:

Compatibility across devices and browsers is crucial for accessibility. The platform must:

- **Browser Compatibility:** Be designed to work seamlessly on various web browsers, including but not limited to Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari.
- **Responsive Design:** Incorporate responsive design principles to adapt the user interface to different screen sizes and resolutions, enhancing accessibility across a diverse range of devices.

CHAPTER-4

SYSTEM ANALYSIS AND DESIGN

4.1.SYSTEM PERSPECTIVE

The System Perspective, often depicted through a Context Diagram which is Fig:1, provides a high-level overview of the "Threat Detection And Response" system, illustrating its interactions with external entities. This diagram serves as a foundational representation, outlining the boundaries of the system and showcasing key components. In the context of the "Threat Detection And Response" project, the System Perspective diagram encompasses the following elements:

4.1.1. Microsoft Azure System:

At the core of the diagram is the "Threat Detection And Response" system, developed using Microsoft Azure Services. This system is the focal point that facilitates the user experience and manages the retrieval of threat-related information.

4.1.2. Sentinel:

The User Interface component is a critical aspect of the system, responsible for presenting the graphical user interface to users. It includes various functionalities such as browsing threats, getting alerts, viewing details, and user interactions. This component is the primary interface through which users engage with the platform.

4.1.3. External API:

Representing an external service, the External API plays a crucial role in enhancing the system's content. It is responsible for the retrieval of additional location data, including information, map illustrations, and country region. This external interaction enriches the platform's offerings and provides users with a more comprehensive experience.

4.1.4. log analytical workspace:

The log data serves as the centralized repository for storing and managing attack' information. This includes login credential details and location details. The log analytical workspace is a fundamental component that facilitates data retrieval and ensures that the system has access to a wide range of log content.

4.1.5.Interactions:

The User Interface of the "Threat Detection And Response" project interacts seamlessly with both the External API and the Log Analytical Workspace to retrieve and present essential threat-related data. This dynamic interaction is crucial for delivering users real-time and comprehensive information about potential security threats. The External API collaborates seamlessly with the Log Analytical Workspace, fetching additional threat intelligence to augment the existing data within the system.

4.1.6.Significance:

The System Perspective diagram offers a foundational understanding of the external interactions and relationships between key components in the "Threat Detection And Response" system. This visual representation communicates the major entities and their roles, providing a starting point for in-depth analysis and design decisions.

4.1.7.Usefulness:

Stakeholders, including developers, security analysts, and project managers, can leverage the System Perspective diagram to quickly grasp the system's architecture and external connections. It facilitates alignment among project team members and stakeholders on the high-level structure and functionalities of the "Threat Detection And Response" system. In essence, the System Perspective diagram serves as a visual guide, illustrating the external interactions and highlighting integral components that contribute to proactive cybersecurity measures and swift threat response.

4.2. CONTEXT DIAGRAM (DFD)

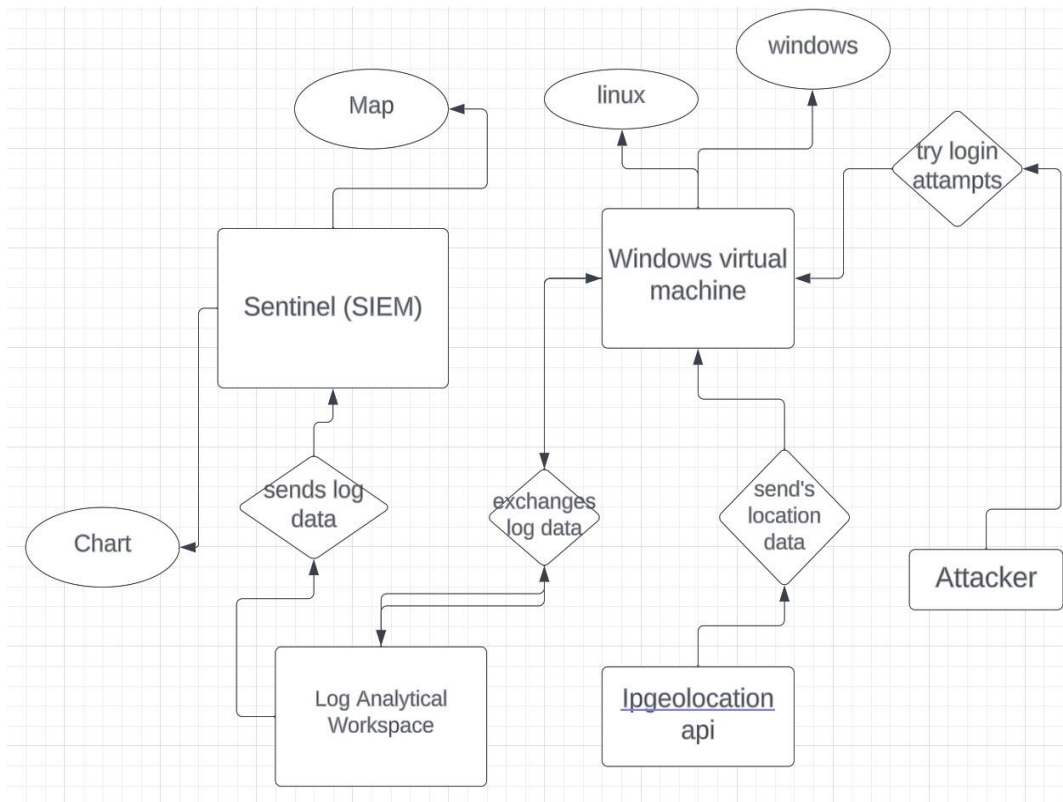


Fig-4.1: Context Diagram

Let's provide a detailed explanation of the components and interactions in the given diagram:

4.2.1. User Interface:

The User Interface component is a critical aspect of the system, responsible for presenting the graphical user interface to users. It includes various functionalities such as browsing threats, getting alerts, viewing details, and user interactions. This component is the primary interface through which users engage with the platform.

4.2.2. External API:

Representing an external service, the External API plays a crucial role in enhancing the system's content. It is responsible for the retrieval of additional location data, including

information, map illustrations, and country region. This external interaction enriches the platform's offerings and provides users with a more comprehensive experience.

4.2.3. log analytical workspace:

The log data serves as the centralized repository for storing and managing attack information. This includes login credential details and location details. The log analytical workspace is a fundamental component that facilitates data retrieval and ensures that the system has access to a wide range of log content.

4.2.4 Virtual Machine:

A virtual machine (VM) is a fundamental component at the core of the "Threat Detection And Response" project, providing a dynamic and secure environment for practical cybersecurity scenarios. Operating within a virtualization platform, VMs enable administrators to create, manage, and replicate diverse operating systems, establishing a simulated setting for immersive hands-on training. This technology offers a controlled space where administrators can precisely mimic real-world cybersecurity situations, honing their skills in threat detection and response.

4.2.5.Interactions:

The User Interface of the "Threat Detection And Response" project interacts seamlessly with both the External API and the Log Analytical Workspace to retrieve and present essential threat-related data. This dynamic interaction is crucial for delivering users real-time and comprehensive information about potential security threats. The External API collaborates seamlessly with the Log Analytical Workspace, fetching additional threat intelligence to augment the existing data within the system.

4.3. USE CASE DIAGRAM

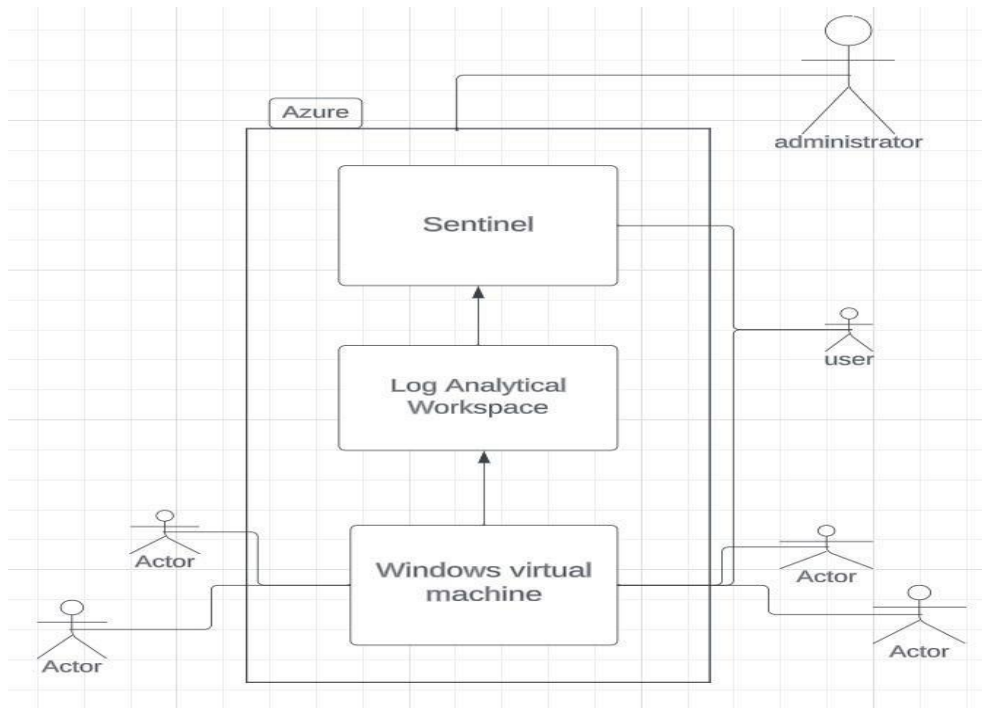


Fig-4.2 : Use Case Diagram

4.3.1. User/Administrator:

- The primary actor interacting with the system. Users or administrators who access the system for threat monitoring, analysis, and response.

4.3.2. Use Cases:

- Description: Represents the user interface developed using HTML, CSS, JavaScript, and MUI.
- Use Cases:

Allows users/administrators to view threat data retrieved from the Log Analytical Workspace and External API.

Query and Analyze Threats:

- Enables users/administrators to perform queries and analyses on threat data using Kusto Query Language (KQL) or other analytical tools.

Receive Alerts and Notifications:

- Notifies users/administrators about potential security threats through alerts and notifications.

Integrate External Threat Intelligence:

- Facilitates the integration of additional threat intelligence from the External API to enrich the existing threat data.

Generate Reports:

- Permits users/administrators to generate reports summarizing threat trends, patterns, and system activities.

4.3.3. Log Analytical Workspace:

- Represents the Azure Log Analytics Workspace, which is a critical component for storing, refining, and analyzing log data related to security events.

4.4. SEQUENCE DIAGRAMS

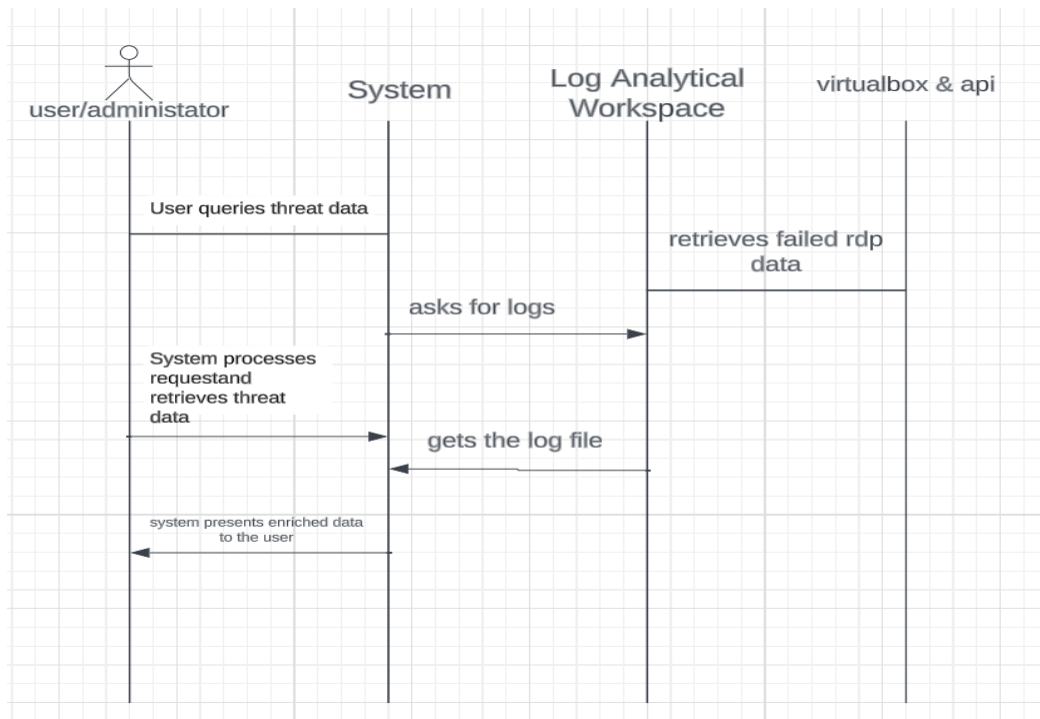


Fig-4.3 : Sequence Diagram

Creating a sequence diagram involves illustrating the interactions between various components or objects in a system over time. We'll focus on the sequence of interactions during the scenario of a user viewing detailed information about a specific exercise.

4.4.1. Azure:

The User Interface is the starting point, representing the user's interaction with the platform. In this scenario, the user clicks on a specific exercise to view detailed information.

4.4.2. External API:

The User Interface sends a request for log details to the External API.

4.4.3. Request log Details (GET):

The User Interface triggers a GET request to the External API, requesting detailed information about the selected log.

4.4.4. Retrieve log Details (Query):

The External API interacts with the log data to retrieve detailed information about the attackers.

4.4.5. Display log Details:

The User Interface receives the information from the log analytical workspace and displays comprehensive details about the attackers.

This sequence diagram illustrates the flow of interactions between the administrator, system, and log analytical workspace, when a user initiates the process of viewing detailed information about a specific attack. It emphasizes the sequence of steps involved in retrieving and presenting log details to the user.

4.5. ACTIVITY DIAGRAM

An activity diagram visually represents the flow of activities within a system. Here's a representation of a activity diagram for a "Threat Detection And Response" project:

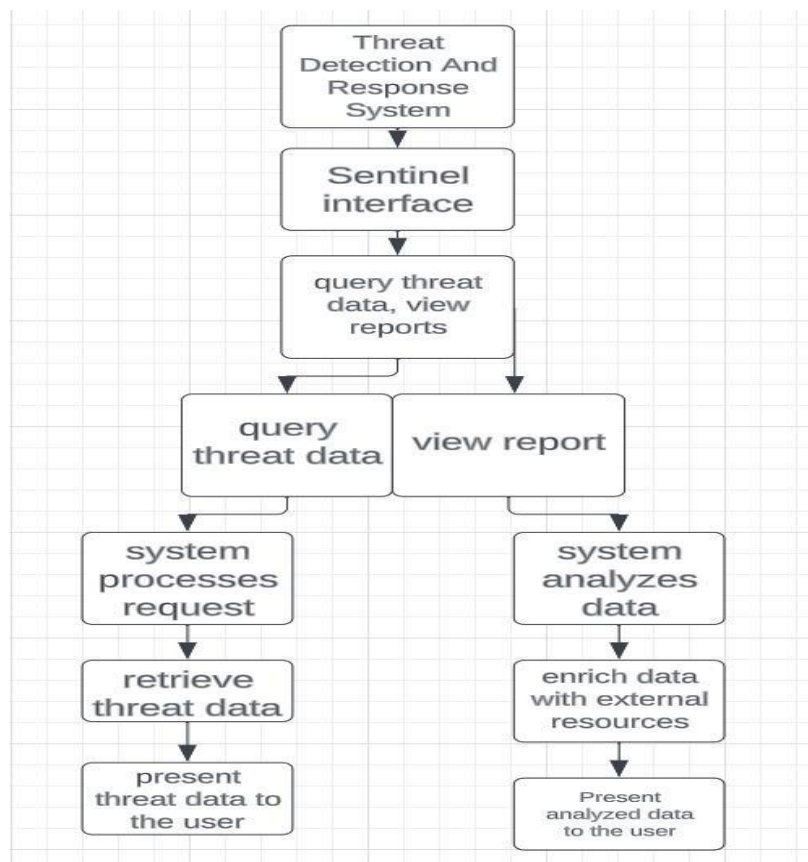


Fig-4.4 : Activity Diagram

In this diagram:

- The process begins with the "User Interface" where the user/administrator chooses an action.
- Depending on the action chosen, the system either queries threat data, analyzes data, or views reports.
- The system processes the user's request, retrieving threat data or analyzing data as needed.
- If required, the system may enrich the data with external sources.
- Finally, the system presents the results to the user, completing the interaction.

CHAPTER-5

IMPLEMENTATION

5.1 Summary of Implementation

Based on the steps for the development of this project, the following is a summary of the implementation process:

1. Virtual Machine Creation:

- First of all, we need an a vulnerable open to the world machine which can be used to test attacks.
- So we create a virtual machine in azure using the service virtual machines, we provide the windows version and architecture, resource group, security standard we need, assign username and password and click on next.

The screenshot shows the 'Create a virtual machine' wizard in the Azure portal. The 'Project details' section includes a dropdown for 'Subscription' (Azure subscription 1) and 'Resource group' ((New) honeypot1). The 'Instance details' section includes fields for 'Virtual machine name' (honeypot), 'Region' ((US) West US 3), 'Availability options' (Availability zone), 'Availability zone' (Zones 1), 'Security type' (Standard), and 'Image' (Windows 10 Pro, version 22H2 - x64 Gen1). At the bottom, there is a 'VM architecture' section with 'Arm64' selected. Navigation buttons at the bottom include 'Review + create', '< Previous', and 'Next: Disks >'. A 'Give feedback' link is also present.

Fig-5.1 : Virtua machine configuration

- Again clicking on next, we get network security group setup, where we have to delete the existing group and create a custom vulnerable security group whose security is very low, we open all the ports of the machine, set priority to 100, allow any action then after giving the name we add the security group.

The screenshot displays the Microsoft Azure portal interface. On the left, the 'Create network security group' page is visible, showing a form with 'Name' set to 'honeypot-nsg'. The 'Inbound rules' and 'Outbound rules' sections both show 'No results.' and have links to '+ Add an inbound rule' and '+ Add an outbound rule' respectively. An 'OK' button is at the bottom left.

On the right, the 'Add inbound security rule' configuration pane is open for the 'honeypot-nsg' group. The configuration details are as follows:

- Source:** Any
- Source port ranges:** *
- Destination:** Any
- Service:** Custom
- Destination port ranges:** *
- Protocol:** Any (selected), TCP, UDP, ICMP
- Action:** Allow (selected), Deny
- Priority:** 100
- Name:** Danger
- Description:** (empty field)

At the bottom of the configuration pane, there are 'Add' and 'Cancel' buttons, and a 'Give feedback' link.

Fig-5.2 : Network configuration

- Click on next & create then our virtual machine will be created.
 - To turn on the virtual machine we have to copy the ip address and launch it using RDP(Remote Desktop Protocol).
2. Turning off the windows defender firewall
- Click on search, type wf.msc and enter to open windows defender firewall.
 - Click on windows defender firewall properties
 - Turn off the firewall state of domain profile, private profile and public profile and then apply and exit.

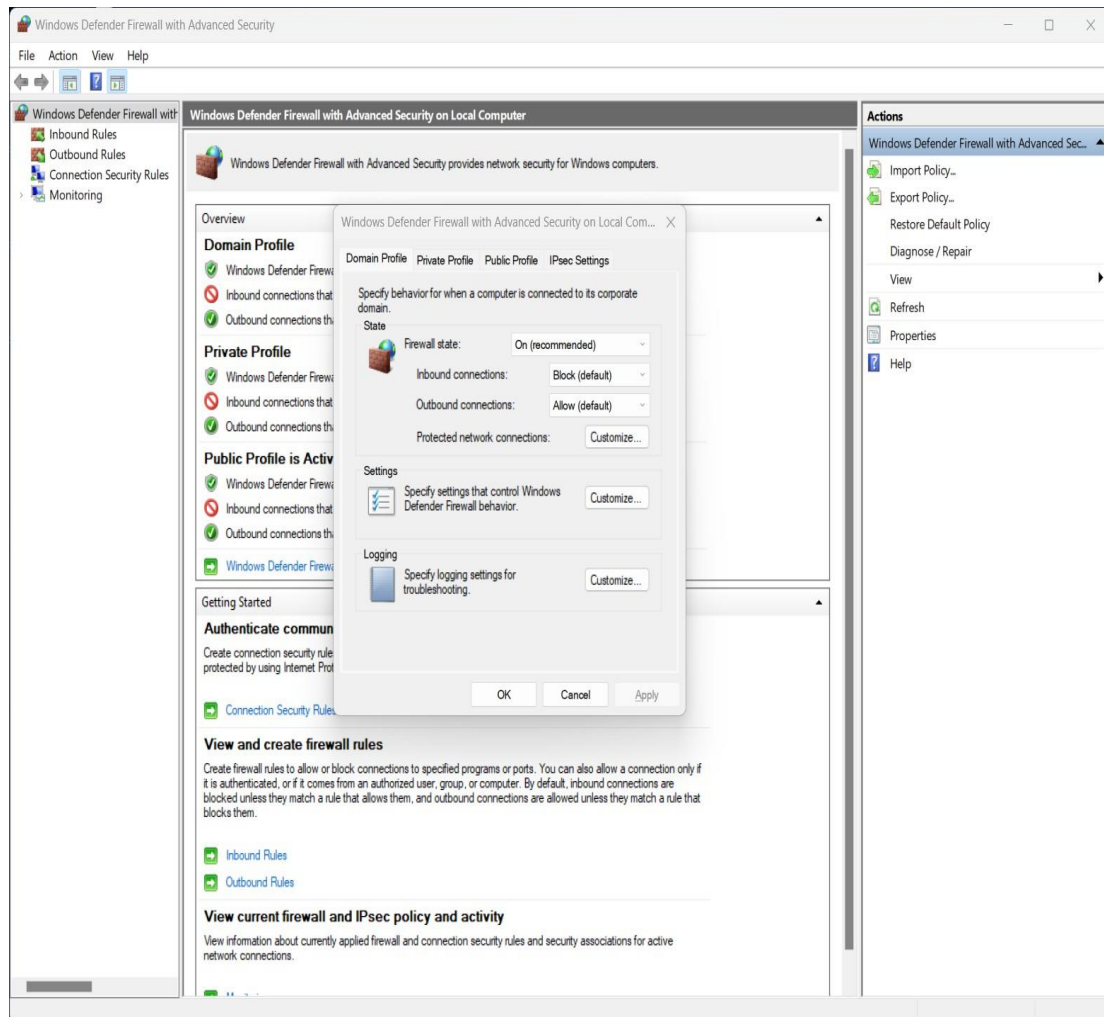


Fig-5.3 : Firewall switch off

3. API powershell script:

- Create a powershell script to extract out the failed log details.
- Send it to the ipgeolocation web app to get the location details through ip address of failed trials.
- Save a file with name log.ps1
- Run the powershell script to see the details in the console and at the same time failed_rdp.log file will be created at c:\ProgramData\

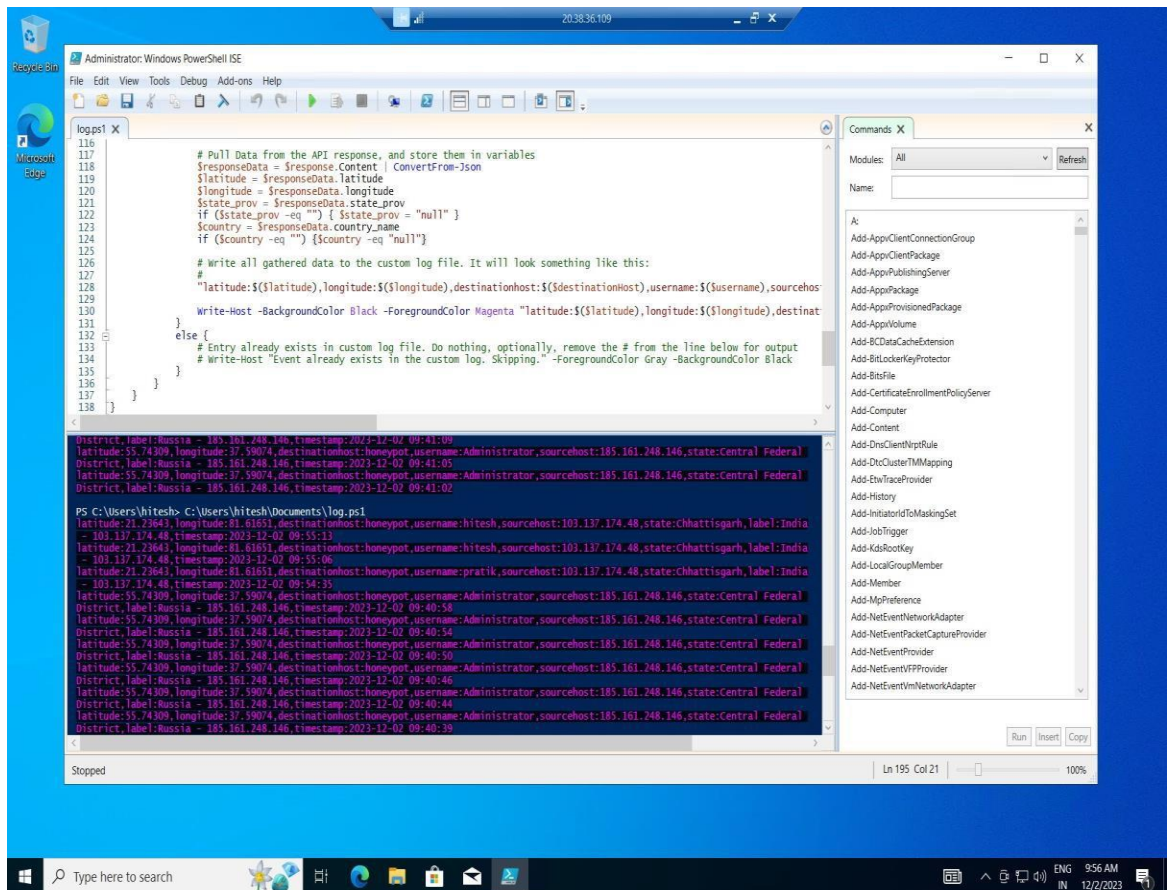


Fig-5.4 : powershell script

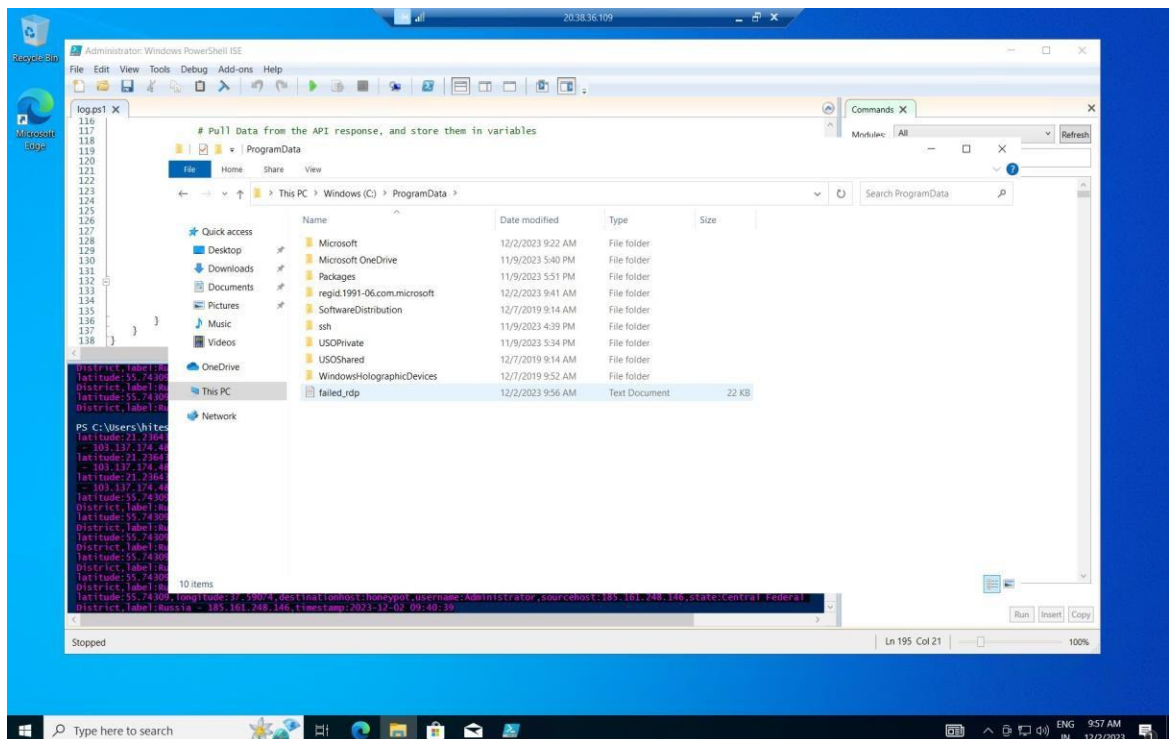


Fig-5.5 : log file

4. Log Analytical Workspace Setup:

- Select the virtual machine and resource group with which we have to connect the workspace.
- Click on create.

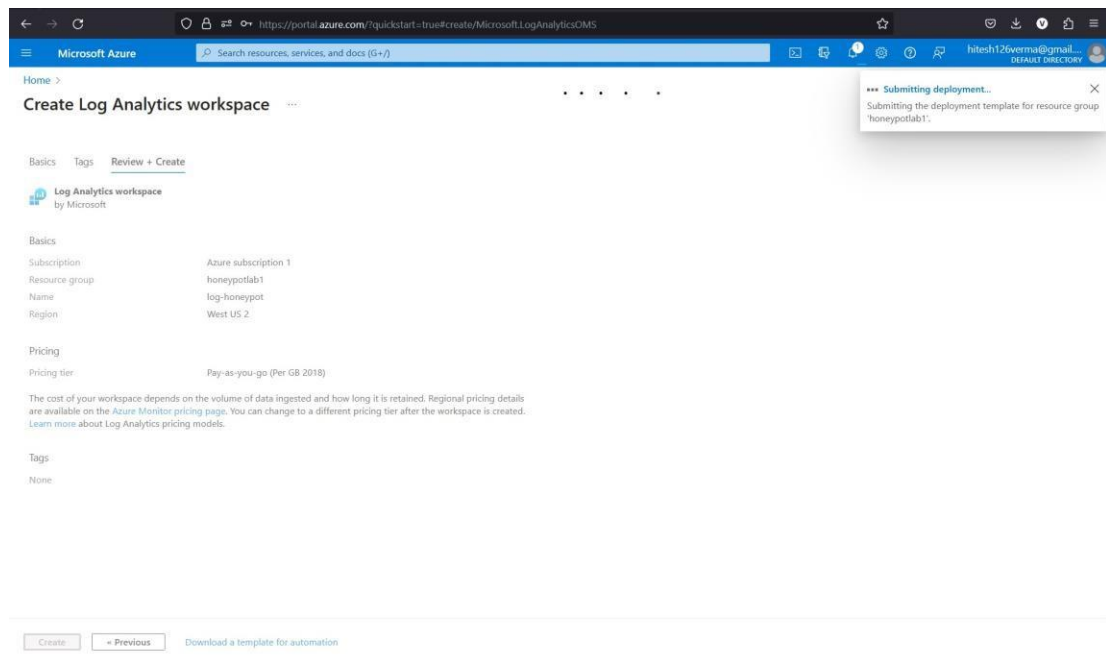


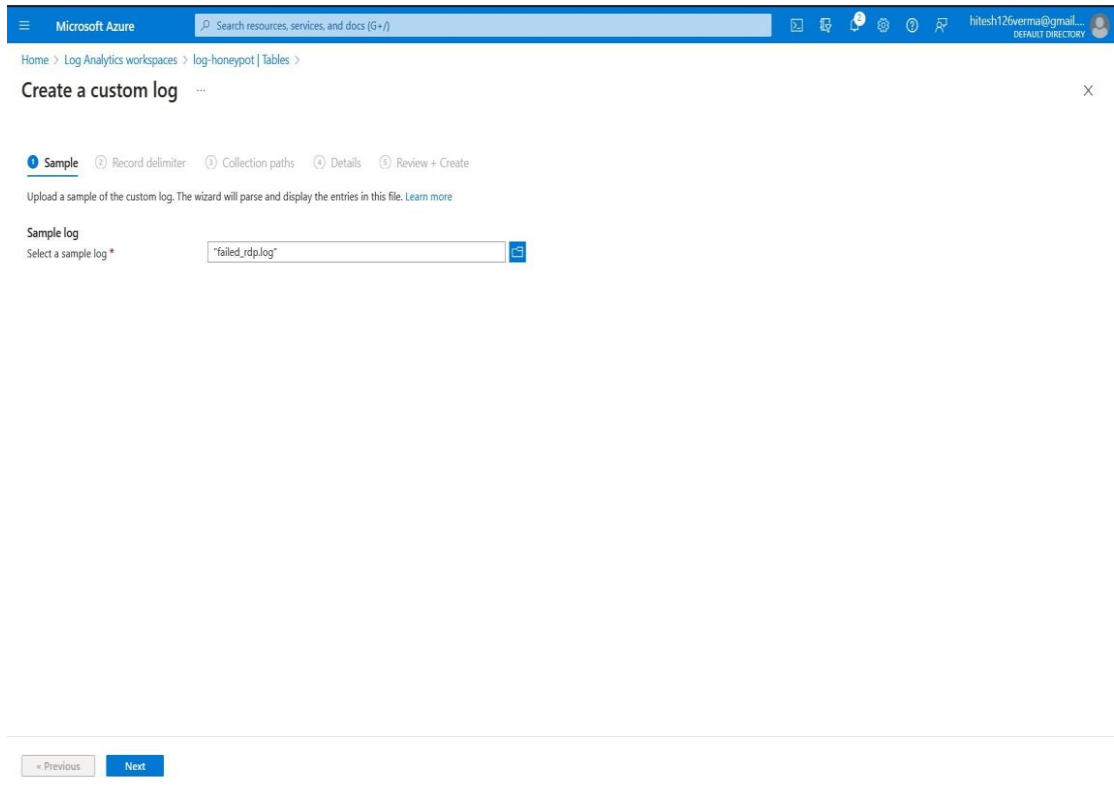
Fig-5.6 : Log Analytical Workspace

5. Create a custom log:

- Go to tables and select create a custom log.
- Select failed_rdp.log as a sample log, this will train the algorithm to understand the data.
- In collection paths, select the path of file where failed_log.log is present at our virtual machine, click next and click review + create.
- Use the KQL to extract out the data's such as longitude, latitude.

```
FAILED_RDP_WITH_GEO_CL | extend username = extract(@"username:([^\,]+)", 1, RawData), timestamp = extract(@"timestamp:([^\,]+)", 1, RawData), latitude = extract(@"latitude:([^\,]+)", 1, RawData), longitude = extract(@"longitude:([^\,]+)", 1, RawData), sourcehost = extract(@"sourcehost:([^\,]+)", 1, RawData), state = extract(@"state:([^\,]+)", 1, RawData), label = extract(@"label:([^\,]+)", 1, RawData), destination = extract(@"destinationhost:([^\,]+)", 1, RawData), country =
```

`extract(@"country:([^\,]+)", 1, RawData) | where destination != "samplehost" | where sourcehost != "" | summarize event_count=count() by latitude, longitude, sourcehost, label, destination, country`



Microsoft Azure

Search resources, services, and docs (G+/I)

Home > Log Analytics workspaces > log-honeypot | Tables >

Create a custom log

1 Sample 2 Record delimiter 3 Collection paths 4 Details 5 Review + Create

Upload a sample of the custom log. The wizard will parse and display the entries in this file. [Learn more](#)

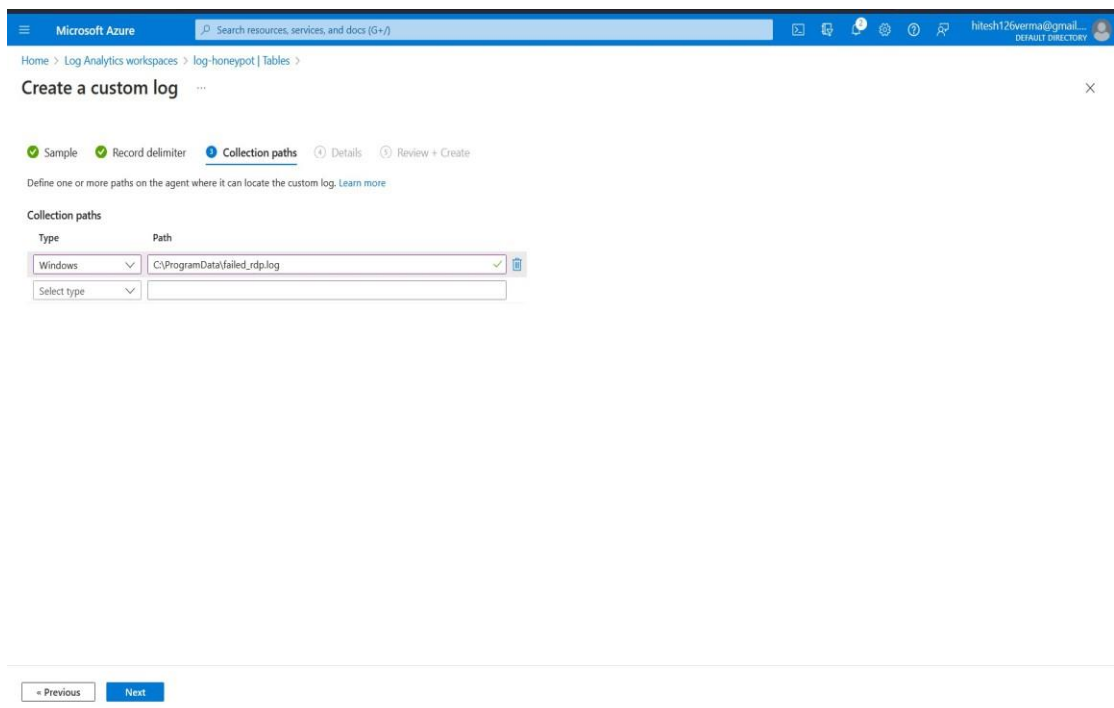
Sample log

Select a sample log *

failed_rdp.log

< Previous Next

Fig-5.7 : Custom Log creation



Microsoft Azure

Search resources, services, and docs (G+/I)

Home > Log Analytics workspaces > log-honeypot | Tables >

Create a custom log

✓ Sample ✓ Record delimiter 1 Collection paths 4 Details 5 Review + Create

Define one or more paths on the agent where it can locate the custom log. [Learn more](#)

Collection paths

Type	Path
Windows	C:\ProgramData\failed_rdp.log
Select type	

< Previous Next

Fig-5.8 : Path Selection

6. Azure Setup:

- Turn on the Sentinel service. Connect Log Analytical Workspace with Sentinel.
- Go to workbooks, click on edit and add the map there.
- Use the KQL to extract files:

```
FAILED_RDP_WITH_GEO_CL | extend username = extract(@"username:([^\,]+)", 1, RawData), timestamp = extract(@"timestamp:([^\,]+)", 1, RawData), latitude = extract(@"latitude:([^\,]+)", 1, RawData), longitude = extract(@"longitude:([^\,]+)", 1, RawData), sourcehost = extract(@"sourcehost:([^\,]+)", 1, RawData), state = extract(@"state:([^\,]+)", 1, RawData), label = extract(@"label:([^\,]+)", 1, RawData), destination = extract(@"destinationhost:([^\,]+)", 1, RawData), country = extract(@"country:([^\,]+)", 1, RawData) | where destination != "samplehost" | where sourcehost != "" | summarize event_count=count() by latitude, longitude, sourcehost, label, destination, country
```

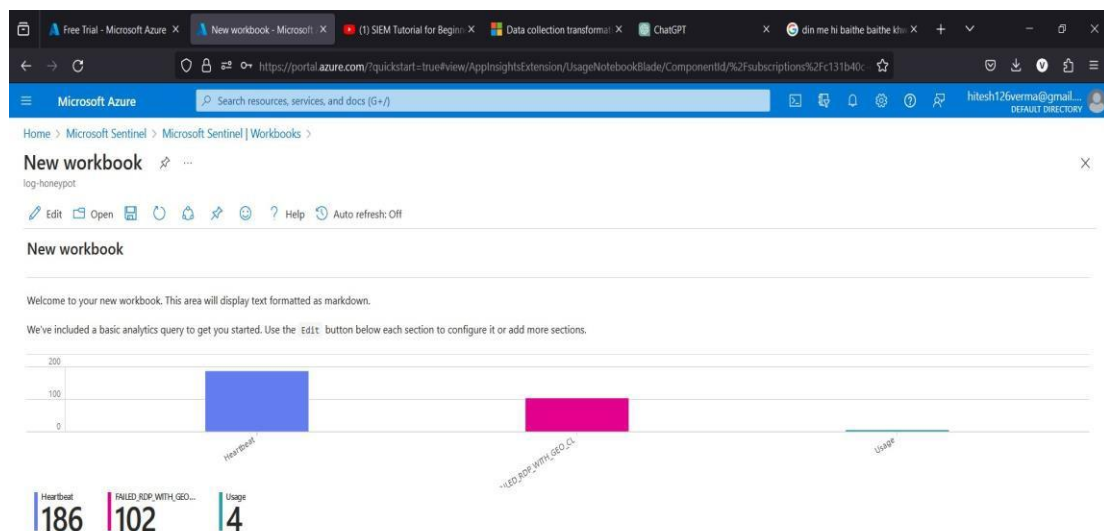


Fig-5.9 : Overview setup

CHAPTER-6

Software Testing

6.1 Test Cases

1. Run virtual machine:

- Copying ip address from azure and try to logging in with valid credentials through RDP protocol.

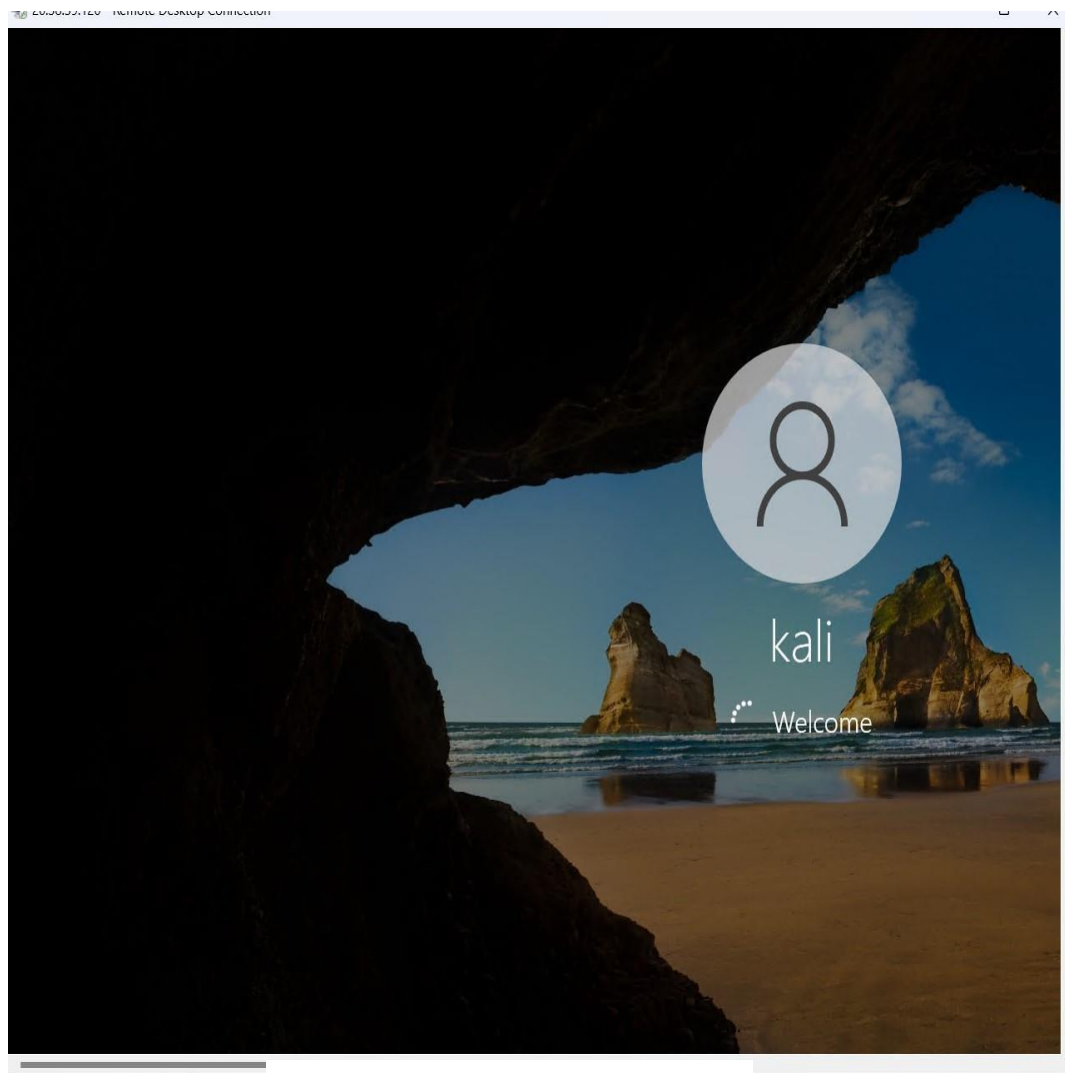


Fig-6.1 : Windows

2. Try running powershell script.

- Open the powershell ISE
- Run the script using ./log.ps1

```
District, label: Russia - 185.161.248.146, timestamp: 2023-12-02 09:41:09
Latitude: 55.74309, Longitude: 37.59074, destinationhost: honeypot, username: Administrator, sourcehost: 185.161.248.146, state: Central Federal
District, label: Russia - 185.161.248.146, timestamp: 2023-12-02 09:41:05
Latitude: 55.74309, Longitude: 37.59074, destinationhost: honeypot, username: Administrator, sourcehost: 185.161.248.146, state: Central Federal
District, label: Russia - 185.161.248.146, timestamp: 2023-12-02 09:41:02

PS C:\Users\hitesh> C:\Users\hitesh\Documents\log.ps1
Latitude: 21.23643, Longitude: 81.61651, destinationhost: honeypot, username: hitesh, sourcehost: 103.137.174.48, state: Chhattisgarh, label: India
- 103.137.174.48, timestamp: 2023-12-02 09:55:13
Latitude: 21.23643, Longitude: 81.61651, destinationhost: honeypot, username: hitesh, sourcehost: 103.137.174.48, state: Chhattisgarh, label: India
- 103.137.174.48, timestamp: 2023-12-02 09:55:06
Latitude: 21.23643, Longitude: 81.61651, destinationhost: honeypot, username: pratik, sourcehost: 103.137.174.48, state: Chhattisgarh, label: India
- 103.137.174.48, timestamp: 2023-12-02 09:54:35
Latitude: 55.74309, Longitude: 37.59074, destinationhost: honeypot, username: Administrator, sourcehost: 185.161.248.146, state: Central Federal
District, label: Russia - 185.161.248.146, timestamp: 2023-12-02 09:40:58
Latitude: 55.74309, Longitude: 37.59074, destinationhost: honeypot, username: Administrator, sourcehost: 185.161.248.146, state: Central Federal
District, label: Russia - 185.161.248.146, timestamp: 2023-12-02 09:40:54
Latitude: 55.74309, Longitude: 37.59074, destinationhost: honeypot, username: Administrator, sourcehost: 185.161.248.146, state: Central Federal
District, label: Russia - 185.161.248.146, timestamp: 2023-12-02 09:40:50
Latitude: 55.74309, Longitude: 37.59074, destinationhost: honeypot, username: Administrator, sourcehost: 185.161.248.146, state: Central Federal
District, label: Russia - 185.161.248.146, timestamp: 2023-12-02 09:40:46
Latitude: 55.74309, Longitude: 37.59074, destinationhost: honeypot, username: Administrator, sourcehost: 185.161.248.146, state: Central Federal
District, label: Russia - 185.161.248.146, timestamp: 2023-12-02 09:40:44
Latitude: 55.74309, Longitude: 37.59074, destinationhost: honeypot, username: Administrator, sourcehost: 185.161.248.146, state: Central Federal
District, label: Russia - 185.161.248.146, timestamp: 2023-12-02 09:40:39
```

Fig-6.2 : Powershell output

3. Log Analytical Workspace query

- Use query to get the desired output characterization.

The screenshot shows the Microsoft Azure portal interface for a Log Analytics workspace named 'log-honeypot'. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Logs. The main area displays a query titled 'New Query 1*' with a time range of 'Last 24 hours'. The query results are shown in a table with columns: TimeGenerated [UTC], Computer, RawData, and Type. The results list multiple failed RDP connections from various source hosts to the honeypot computer.

TimeGenerated [UTC]	Computer	RawData	Type
12/2/2023, 10:27:56.040 AM	honeypot	latitude:33.99762,longitude:6.84737,destinationhost:sampl...	FAILED_RDP_WITH_GEO_CL
12/2/2023, 10:27:56.040 AM	honeypot	latitude:5.32558,longitude:100.28595,destinationhost:sampl...	FAILED_RDP_WITH_GEO_CL
12/2/2023, 10:27:56.040 AM	honeypot	latitude:41.05722,longitude:28.84926,destinationhost:sampl...	FAILED_RDP_WITH_GEO_CL
12/2/2023, 10:27:56.040 AM	honeypot	latitude:55.87925,longitude:37.54691,destinationhost:sampl...	FAILED_RDP_WITH_GEO_CL
12/2/2023, 10:27:56.040 AM	honeypot	latitude:52.37018,longitude:4.87324,destinationhost:sampl...	FAILED_RDP_WITH_GEO_CL
12/2/2023, 10:27:56.040 AM	honeypot	latitude:17.49163,longitude:88.18704,destinationhost:sampl...	FAILED_RDP_WITH_GEO_CL
12/2/2023, 10:27:56.040 AM	honeypot	latitude:55.88802,longitude:37.65136,destinationhost:sampl...	FAILED_RDP_WITH_GEO_CL
12/2/2023, 10:27:56.040 AM	honeypot	latitude:55.74309,longitude:37.59074,destinationhost:honey...	FAILED_RDP_WITH_GEO_CL
12/2/2023, 10:27:56.040 AM	honeypot	latitude:55.74309,longitude:37.59074,destinationhost:honey...	FAILED_RDP_WITH_GEO_CL
12/2/2023, 10:27:56.040 AM	honeypot	latitude:55.74309,longitude:37.59074,destinationhost:honey...	FAILED_RDP_WITH_GEO_CL
12/2/2023, 10:27:56.040 AM	honeypot	latitude:55.74309,longitude:37.59074,destinationhost:honey...	FAILED_RDP_WITH_GEO_CL
12/2/2023, 10:27:56.040 AM	honeypot	latitude:55.74309,longitude:37.59074,destinationhost:honey...	FAILED_RDP_WITH_GEO_CL
12/2/2023, 10:27:56.040 AM	honeypot	latitude:55.74309,longitude:37.59074,destinationhost:honey...	FAILED_RDP_WITH_GEO_CL

Fig-6.3 : Log data output

4. Sentinel graphical view

- Try logging in with false credentials using RDP credentials.
- Output should be shown through Sentinel overview.

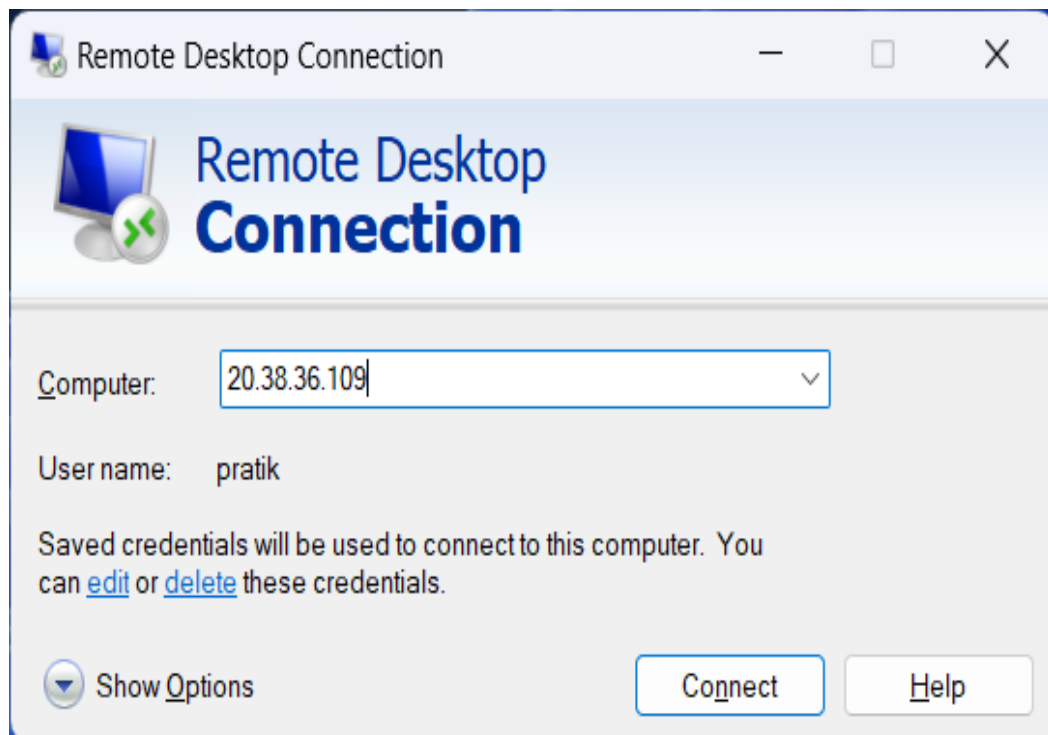


Fig-6.4 : RDP login

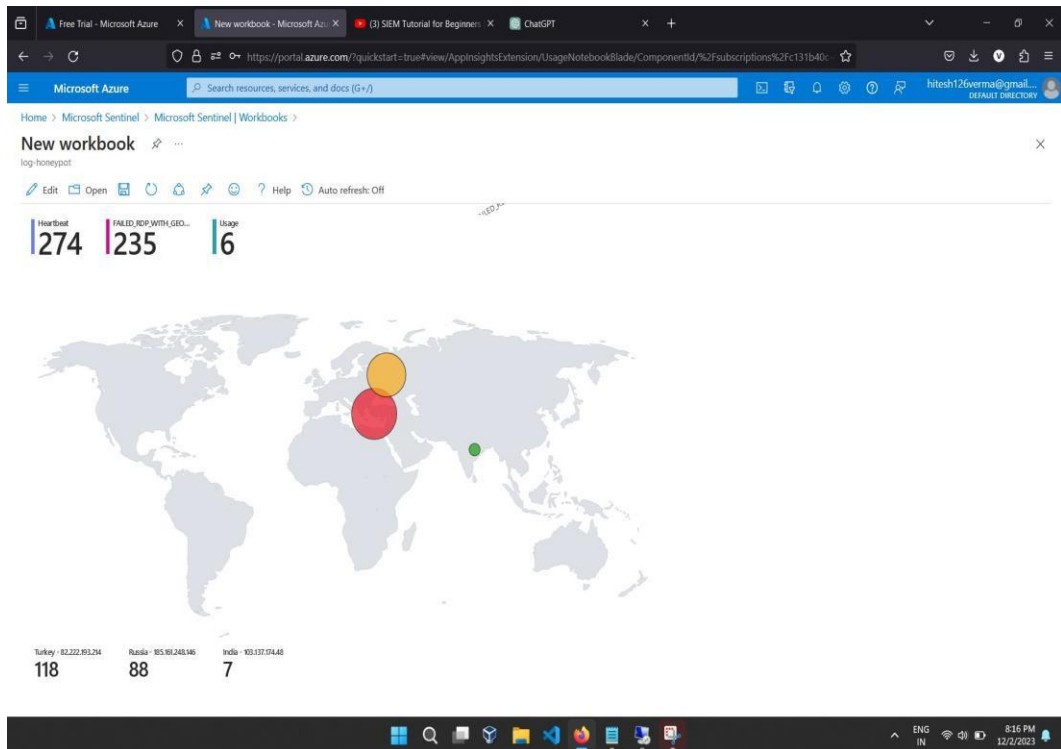


Fig-6.5 : Map Overview

Chapter 7

Conclusion

The "Threat Detection And Response" project stands as a testament to the fusion of cutting-edge technologies and proactive cybersecurity measures. By leveraging Microsoft Azure services, PowerShell scripts, and strategic API integrations, the project creates a robust system aimed at fortifying Windows computers against evolving security threats.

The technological synergy of VirtualBox, Sentinel, and Azure's Log Analytical Workspace forms the backbone of the project, ensuring a seamless user experience. This comprehensive approach allows administrators to detect irregular login attempts, analyze threat data, and respond swiftly to potential security breaches. The integration of the IP geolocation API enhances situational awareness, providing insights into the geographic position of potential attackers.

Pedagogical innovation takes center stage, revolutionizing education by incorporating real-world simulations through VirtualBox. This not only enhances hands-on experience but also fosters creativity and critical thinking among students, preparing them for the digital age.

The project's economic feasibility is underscored by leveraging Microsoft Azure's first-month free subscription, allowing organizations to explore threat detection capabilities without immediate financial commitments. This cost-effective approach aligns with budgetary considerations, ensuring a sustainable and financially prudent solution.

In conclusion, the "Threat Detection And Response" project exemplifies a paradigm shift in cybersecurity. It not only empowers administrators with actionable insights but also contributes to the education landscape by embracing innovative technologies. As the digital landscape continues to evolve, this project serves as a beacon for adaptive and proactive cybersecurity measures, ensuring the resilience of Windows environments against emerging threats.

Chapter 8

Future Enhancements

The "Threat Detection And Response" project lays a solid foundation for cybersecurity, and future enhancements can further elevate its capabilities. Here are some potential avenues for improvement:

1. Real-time Alerts and Notifications:

- Implement a robust alerting system that instantly notifies administrators when a security threat is detected. Alerts can be sent through various channels, such as email, SMS, or integrated messaging platforms, ensuring immediate awareness and response.

2. Multi-Protocol Support:

- Extend the project's capabilities to cover a broader spectrum of protocols beyond the proprietary RDP protocol. By incorporating support for various protocols, the system becomes more versatile and adept at identifying diverse cyber threats across different network layers.

3. Behavioral Analysis and Anomaly Detection:

- Integrate advanced behavioral analysis and anomaly detection algorithms. By studying user behavior patterns and identifying deviations, the system can proactively detect sophisticated threats that may not be apparent through traditional signature-based methods.

4. Automated Response Mechanisms:

- Explore the implementation of automated response mechanisms. Develop predefined actions that the system can take in response to specific types of threats, streamlining the incident response process and minimizing manual intervention.

CHAPTER 9

BIBLIOGRAPHY

[1] Josh Madakor, "Azure Sentinel Tutorial: setup Azure Sentinel and connect to live machine acting as a honey pot. (1/06/2021)

Link: <https://www.youtube.com/@JoshMadakor>

[2] @tonynoe1286. "A comprehensive comment about new changes in Azure services and KQL queries." (3/05/2023)

Link: <https://www.youtube.com/channel/UCyog0Y1CjHTuvHkReegGNLw>

[3] Microsoft.com, "Blog about how log analytics workspace works" (5/01/2022)

Link: <https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview>