AI & Data Enthusiast | Where Vision Lead Me.

Daniel Aqil

WWW.LINKEDIN.COM/IN/DANIELAQIL/

Where Vision Lead Me.

ABOUT ME

Muhammad Daniel Aqil Bin Mohd Rashidi

43000, Kajang

24 Years Old @ 2025

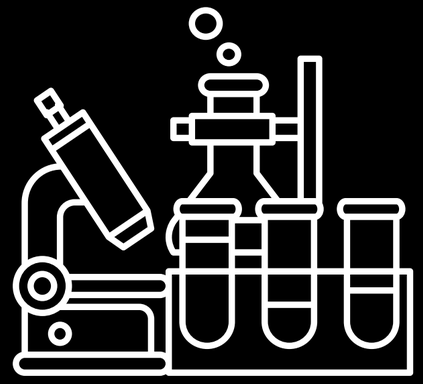
To enhance problem-solving capabilities and provide strategic solutions that drive business growth.

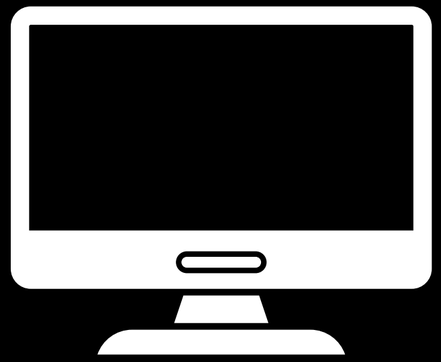
Company Introduction & Background

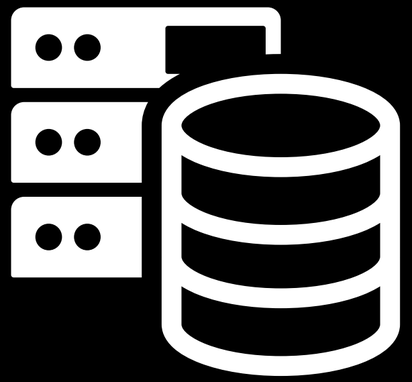
Zecon Medicare Sdn Bhd

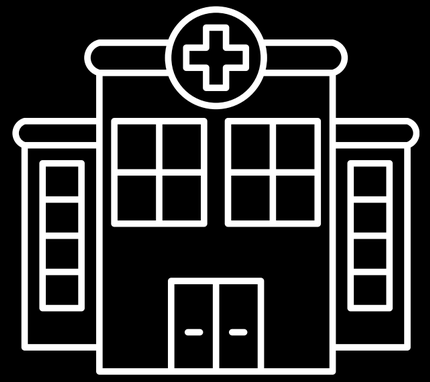
📍 Located at Hospital Pakar Kanak-Kanak Universiti Kebangsaan Malaysia (HPKK-UKM), Cheras

Zecon Medicare Sdn Bhd is a leading healthcare facility management company specializing in hospital support services, medical infrastructure maintenance, and IT solutions for the healthcare industry. Located at Hospital Pakar Kanak-Kanak UKM (HPKK-UKM), Cheras, we are dedicated to ensuring seamless hospital operations through innovative technology, efficient facility management, and cutting-edge IT solutions.



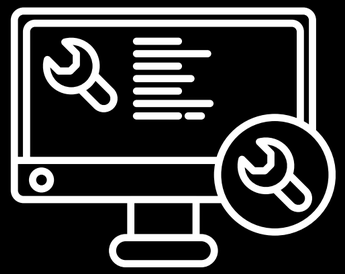






Where Vision Lead Me.

Internship Mini Project



EDR Auto-Tracking & Threat Analysis Dashboard Web-App

Real-time Insights for Enhanced Cybersecurity Monitoring

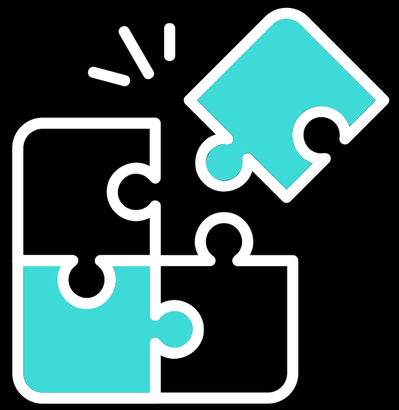
Created by Daniel Aqil

4221003382

Where Vision Lead Me.

Problem Statement

In today's cybersecurity landscape, organizations rely on Endpoint Detection and Response (EDR) systems to monitor and mitigate threats. However, existing EDR solutions face several limitations that hinder efficient threat analysis and decision-making



Where Vision Lead Me.

Problem Statement

1) Lack of Department Identification

The current EDR system is unable to determine which department an IP address belongs to, making it difficult for security teams to pinpoint the source of potential threats. Without this mapping, organizations struggle to assess which departments are most vulnerable and require immediate attention.

2) Limited Visualization & Reporting

The existing system primarily generates PDF reports for threat analysis instead of providing an interactive, real-time dashboard. This limitation prevents security teams from dynamically exploring data, identifying trends, and detecting anomalies efficiently, leading to slower decision-making and delayed threat responses.

3) No Filtering Capabilities

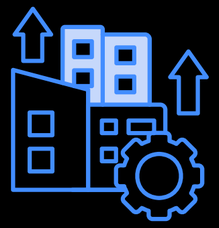
The current EDR system lacks a filtering function, making it challenging to analyze threats based on specific criteria such as date, department, threat type, status, or antivirus engine. Without filtering options, security teams must manually sift through large datasets, resulting in inefficiencies and a time-consuming analysis process.

Where Vision Lead Me.

OBJECTIVES

Where Vision Lead Me.

Objective



Enhance Departmental Mapping for Threat Analysis

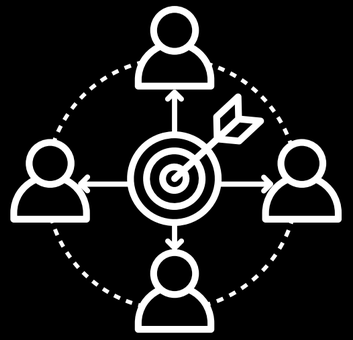
Develop an improved EDR system that can accurately associate IP addresses with specific departments. This enhancement will help security teams quickly identify which departments are most affected by threats, allowing for more targeted incident response and risk mitigation.

Implement an Interactive Dashboard for Real-Time Visualization

Replace static PDF reports with a dynamic, real-time dashboard that provides comprehensive visual insights into threats. This dashboard will enable security teams to explore data interactively, identify patterns more efficiently, and make quicker, data-driven decisions.

Integrate Advanced Filtering Capabilities for Efficient Threat Analysis

Incorporate a filtering function that allows users to refine threat data based on key attributes such as department, time, threat type, status, and antivirus engine. This will improve data accessibility, streamline analysis, and enhance the ability to extract actionable insights with minimal effort.



Where Vision Lead Me.

TECHNOLOGY STACK

Where Vision Lead Me.

TECHNOLOGY STACK

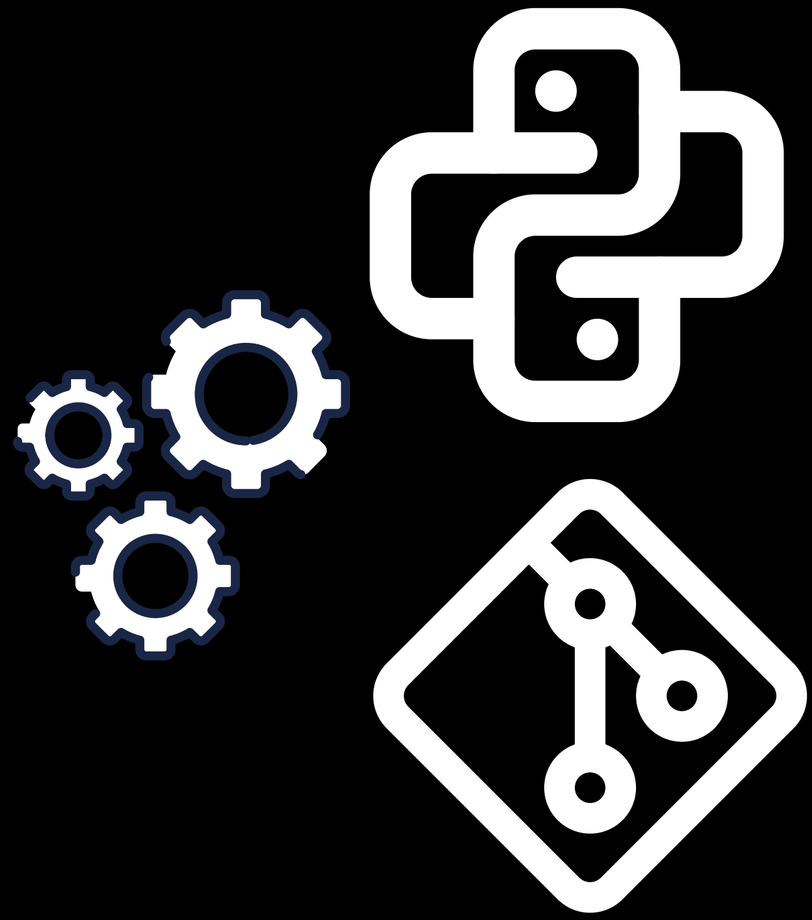
📌 Programming Language: Python 🐍

📌 Framework: Streamlit ⚡

📌 Data Processing: Pandas 📊

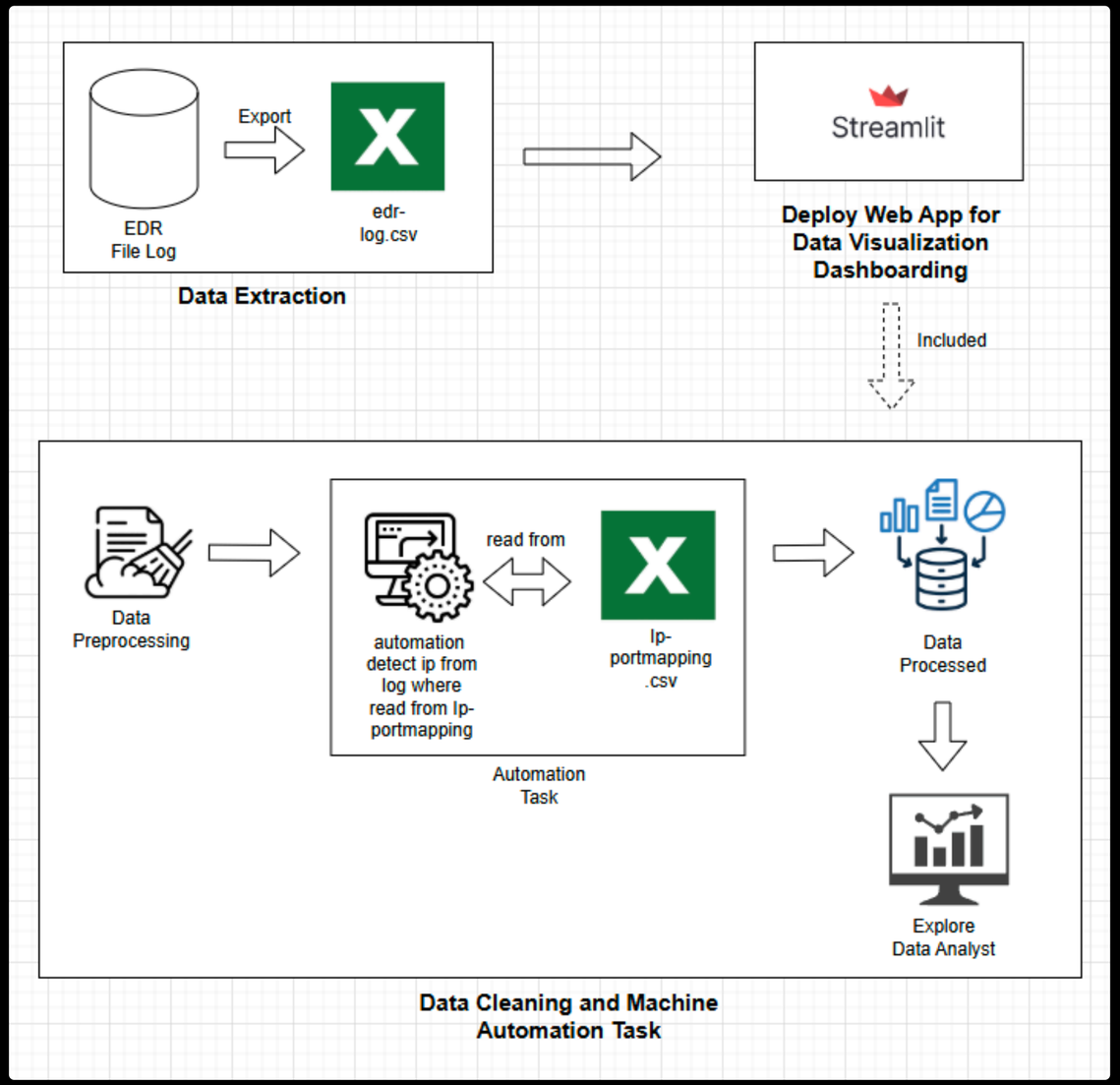
📌 Visualization: Plotly 📈

📌 Deployment: Local / Cloud Hosting ☁️



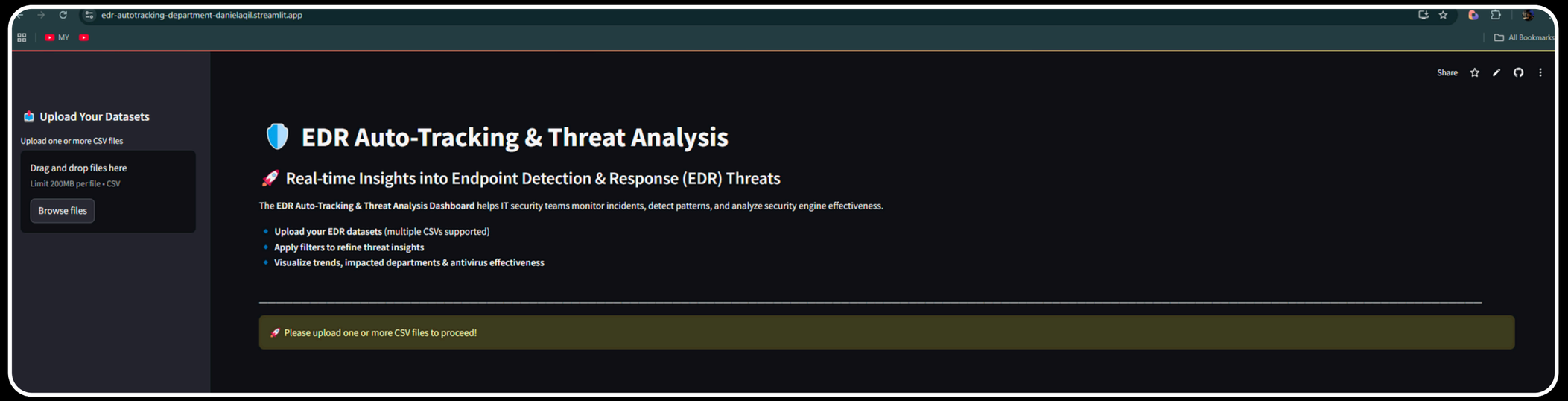
Where Vision Lead Me.

System Architecture



Where
Vision
Lead Me.

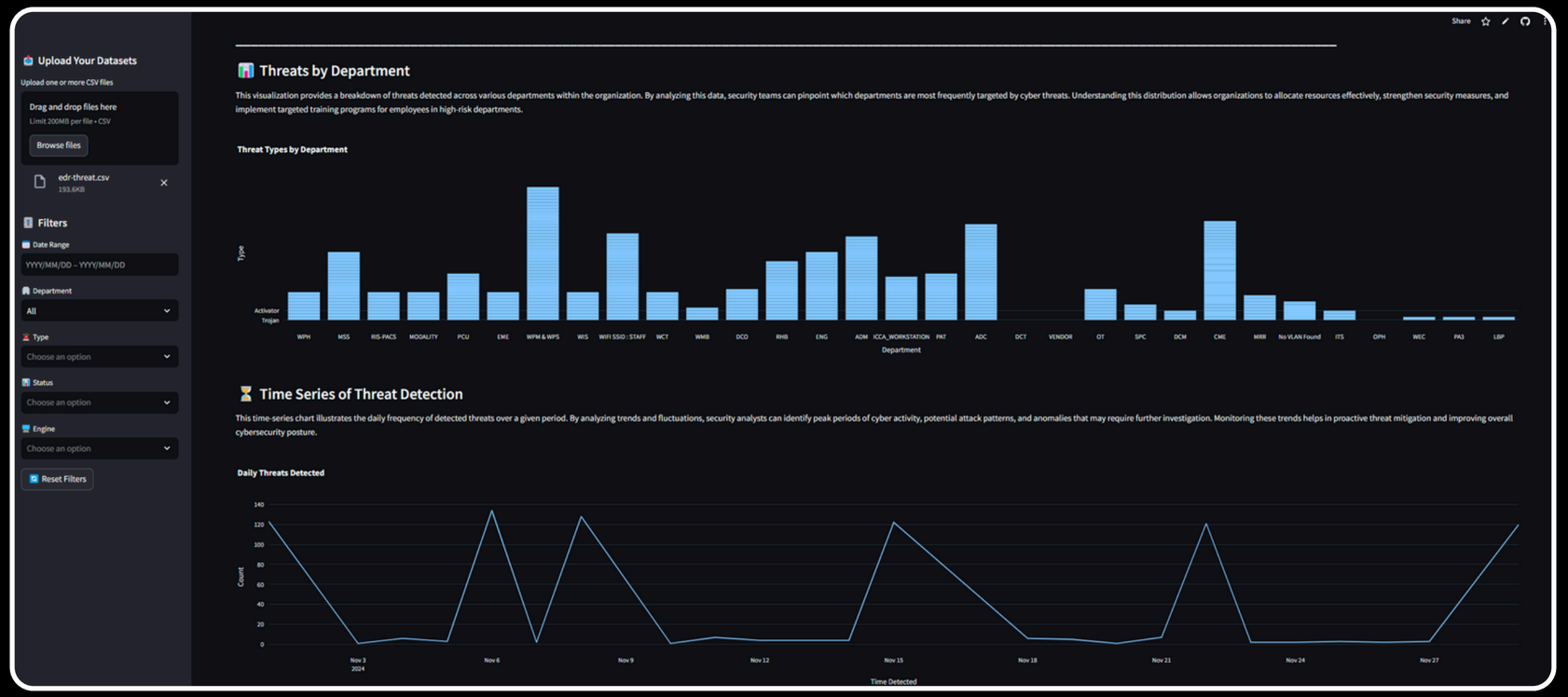
User Interface



User Interface before uploading file

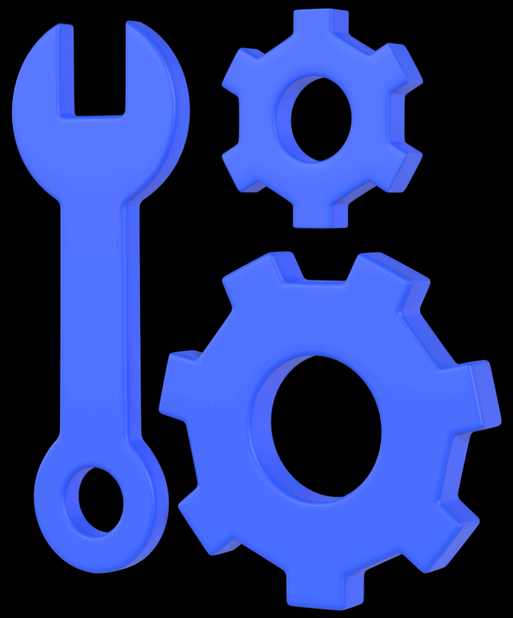
Where Vision Lead Me.

User Interface



User Interface after uploading file

Where Vision Lead Me.



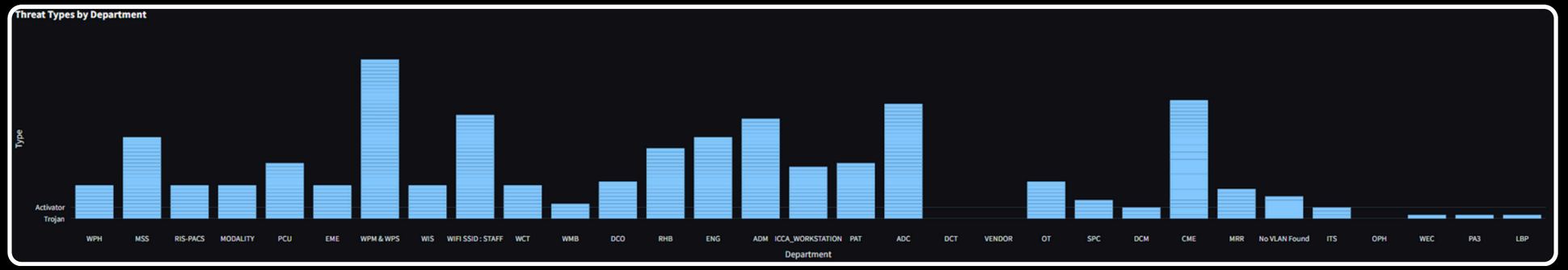
EDA Modules Inside

Where Vision Lead Me.

EDA Modules Inside

Threats by Department

This visualization provides a breakdown of threats detected across various departments within the organization. By analyzing this data, security teams can pinpoint which departments are most frequently targeted by cyber threats. Understanding this distribution allows organizations to allocate resources effectively, strengthen security measures, and implement targeted training programs for employees in high-risk departments.

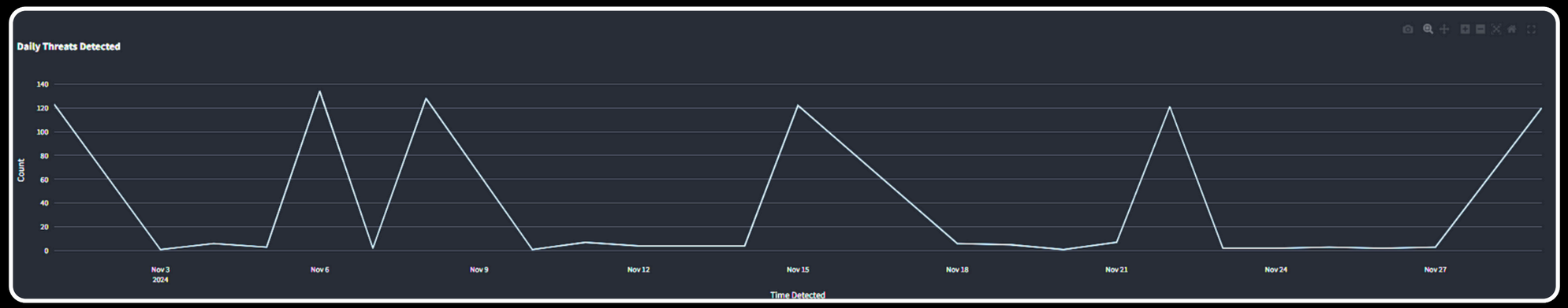


Where Vision Lead Me.

EDA Modules Inside

Time Series of Threat Detection

This time-series chart illustrates the daily frequency of detected threats over a given period. By analyzing trends and fluctuations, security analysts can identify peak periods of cyber activity, potential attack patterns, and anomalies that may require further investigation. Monitoring these trends helps in proactive threat mitigation and improving overall cybersecurity posture.

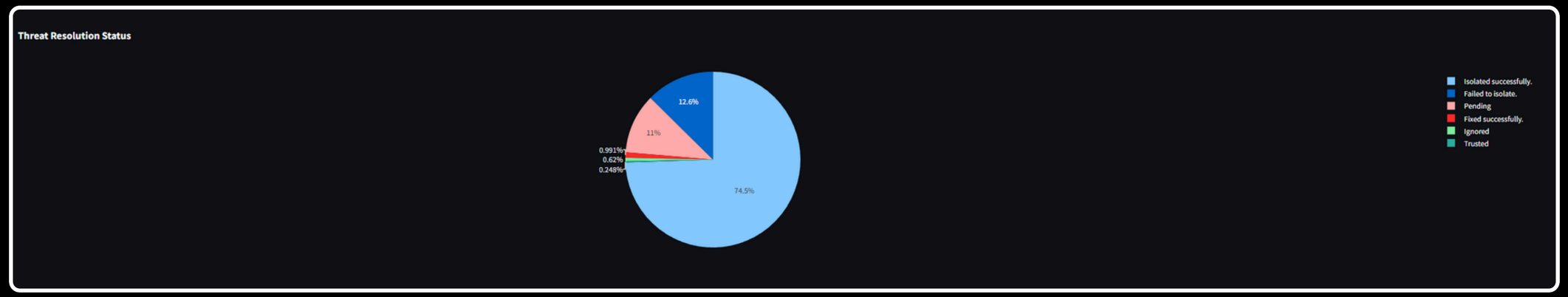


Where Vision Lead Me.

EDA Modules Inside

Status of Threat Resolutions

This pie chart provides an overview of the resolution status of detected threats within the system. It categorizes threats based on whether they have been successfully resolved, are currently in progress, or remain unresolved. Understanding the distribution of threat resolutions helps assess the efficiency of the security response team, identify potential backlog issues, and ensure timely remediation of critical threats.

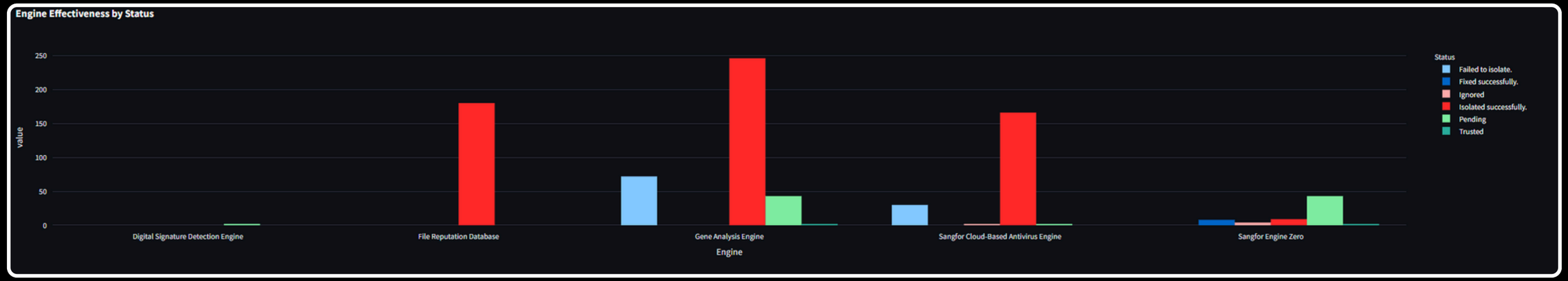


Where Vision Lead Me.

EDA Modules Inside

Antivirus Engine Effectiveness

This bar chart compares the effectiveness of different antivirus engines in detecting and resolving threats. Each security engine's performance is evaluated based on the number of detected threats and their resolution status. By analyzing this data, security teams can determine which antivirus solutions are the most reliable, identify potential gaps in protection, and make informed decisions about upgrading or fine-tuning security tools.



Where Vision Lead Me.

Tables After Processed Modules Inside

Data Table After Processed

The processed data table is a cleaned and structured version of the uploaded dataset. It has undergone data cleaning, including removing errors, handling missing values, and assigning departments to IP addresses.

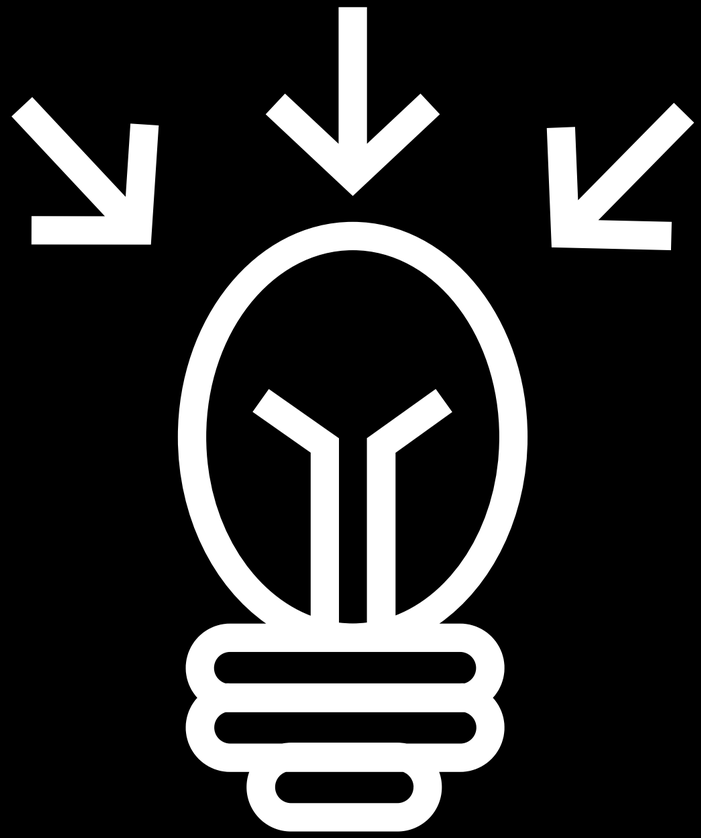
Filtered Data Table

	No.	Time Detected	Endpoint	IP Address	Type	Threat	Infected File	Time Created	File MD5	Status	Time Fixed	Engine	Antivirus database version	Department
0	1	2024-11-29 15:38:00	2F-PC-205	172.22.58.194	Trojan	Trojan.Win64.Agent.A7eg	c:\programdata\mhnjdtuyeaqo\bkyzejjgqxyc.exe	10/02/2024 8:41	C112A7B5E5320C16AC6D5BF2D3B63D53	Isolated successfully.	29/11/2024 15:39	Sangfor Cloud-Based Antivirus Engine	20241100000000	WPH
1	2	2024-11-29 15:03:00	1F-PC-207	172.22.54.233	Others	Gen:Variant.Barys.320900	c:\programdata\mhnjdtuyeaqo\bkyzejjgqxyc.exe	10/02/2024 8:40	C112A7B5E5320C16AC6D5BF2D3B63D53	Isolated successfully.	04/12/2024 16:27	Gene Analysis Engine	20241100000000	MSS
2	3	2024-11-29 13:36:00	hpkkplazadb	172.22.36.13	Trojan	Trojan.Win32.Save.a	c:\windows\temp\onedrive.exe	01/09/2023 1:31	08B5889AF26C2C16AC90F99F5B36481C	Pending	29/11/2024 13:36	Sangfor Engine Zero	20241100000000	RIS-PACS
3	4	2024-11-29 13:36:00	hpkkplazadb	172.22.36.13	Trojan	Trojan.Win32.Save.a	c:\program files\google\chrome\updater.exe	30/08/2023 3:38	65E7F6E26F792FA94E8AF5371FD6331A	Pending	29/11/2024 13:36	Sangfor Engine Zero	20241100000000	RIS-PACS
4	5	2024-11-29 13:36:00	hpkkplazadb	172.22.36.13	Others	Gen:Variant.Barys.320900	c:\programdata\mhnjdtuyeaqo\bkyzejjgqxyc.exe	14/02/2024 6:18	C112A7B5E5320C16AC6D5BF2D3B63D53	Isolated successfully.	04/12/2024 16:27	Gene Analysis Engine	20241100000000	RIS-PACS
5	6	2024-11-29 13:30:00	5F-PC-054	172.22.68.92	Others	Gen:Variant.Barys.320900	c:\programdata\mhnjdtuyeaqo\bkyzejjgqxyc.exe	10/02/2024 8:41	C112A7B5E5320C16AC6D5BF2D3B63D53	Isolated successfully.	04/12/2024 16:27	Gene Analysis Engine	20241100000000	MODALITY
6	7	2024-11-29 13:25:00	2F-PC-071	172.22.57.146	Trojan	Trojan.Win64.Agent.A7eg	c:\programdata\mhnjdtuyeaqo\bkyzejjgqxyc.exe	10/02/2024 8:41	C112A7B5E5320C16AC6D5BF2D3B63D53	Isolated successfully.	04/12/2024 16:27	Sangfor Cloud-Based Antivirus Engine	20241100000000	PCU
7	8	2024-11-29 13:21:00	GF-PC-080	172.22.59.145	Trojan	Trojan.Win32.Save.a	c:\program files (x86)\common files\adobe\arm\1.0\armsvc.exe	31/07/2024 10:15	B2DD77DA74376DEF8B79BB72807E8E01	Fixed successfully.	29/11/2024 13:21	Sangfor Engine Zero	20180800000000	EME
8	9	2024-11-29 13:21:00	GF-PC-080	172.22.59.145	Others	Suspicious.Win32.Save.a	c:\program files (x86)\medweb\plugin\mwipcserver.exe	17/11/2017 14:14	B02E5059D3FB9B9980554625BE3EB04D	Fixed successfully.	29/11/2024 13:21	Sangfor Engine Zero	20180800000000	EME
9	10	2024-11-29 13:20:00	4F-PC-027	172.22.61.195	Others	Gen:Variant.Barys.320900	c:\programdata\mhnjdtuyeaqo\bkyzejjgqxyc.exe	10/02/2024 8:41	C112A7B5E5320C16AC6D5BF2D3B63D53	Isolated successfully.	04/12/2024 16:27	Gene Analysis Engine	20241100000000	WPM & WPS

Where Vision Lead Me.

Conclusion

The EDR Auto-Tracking & Threat Analysis Dashboard provides a comprehensive and interactive way to monitor security threats in real time. By integrating automated department assignment, dynamic filtering, and interactive visualizations, it significantly improves threat analysis efficiency compared to traditional PDF reports. The dashboard enables faster decision-making, better incident response, and enhanced cybersecurity monitoring.



Future Enhancement

Integration with Threat Intelligence Feeds
Enhance detection capabilities by cross-referencing threats with external databases.

Automated Anomaly Detection
Implement machine learning to identify unusual patterns and potential cyberattacks.

Real-time Alerting System
Notify security teams instantly when critical threats are detected.

User Access Control & Role-Based Views
Restrict data access based on user roles to improve security.

Cloud Deployment & API Integration
Enable seamless access and integration with existing security infrastructures.

Where Vision Lead Me.