

CRATIP

CYBER RISK ASSESSMENT & THREAT INTELLIGENCE PLATFORM

"A CYBERATTACK HAPPENS
EVERY 39 SECONDS"

PROBLEM STATEMENT

Existing cyber security solutions generate large volumes of fragmented and highly technical data from scanning, vulnerability analysis, and threat intelligence tools. These outputs are difficult to correlate, prioritize, and interpret, and they largely focus on current or past threats. As a result, organizations struggle not only to understand present cyber risks but also to anticipate potential future risks, leading to reactive and delayed security decisions.



SOLUTION STATEMENT

This project proposes a multi-layered Cyber Risk Assessment and Threat Intelligence system developed in Python that integrates network scanning, threat intelligence enrichment, risk scoring, predictive analysis, AI-based summarization, and visualization into a unified platform. The system correlates data from multiple trusted sources, prioritizes risks based on real-world exploitability, predicts potential risk trends, and explains security insights in simple natural language through an interactive dashboard.

SOLUTION FLOWCHART

USER INPUT

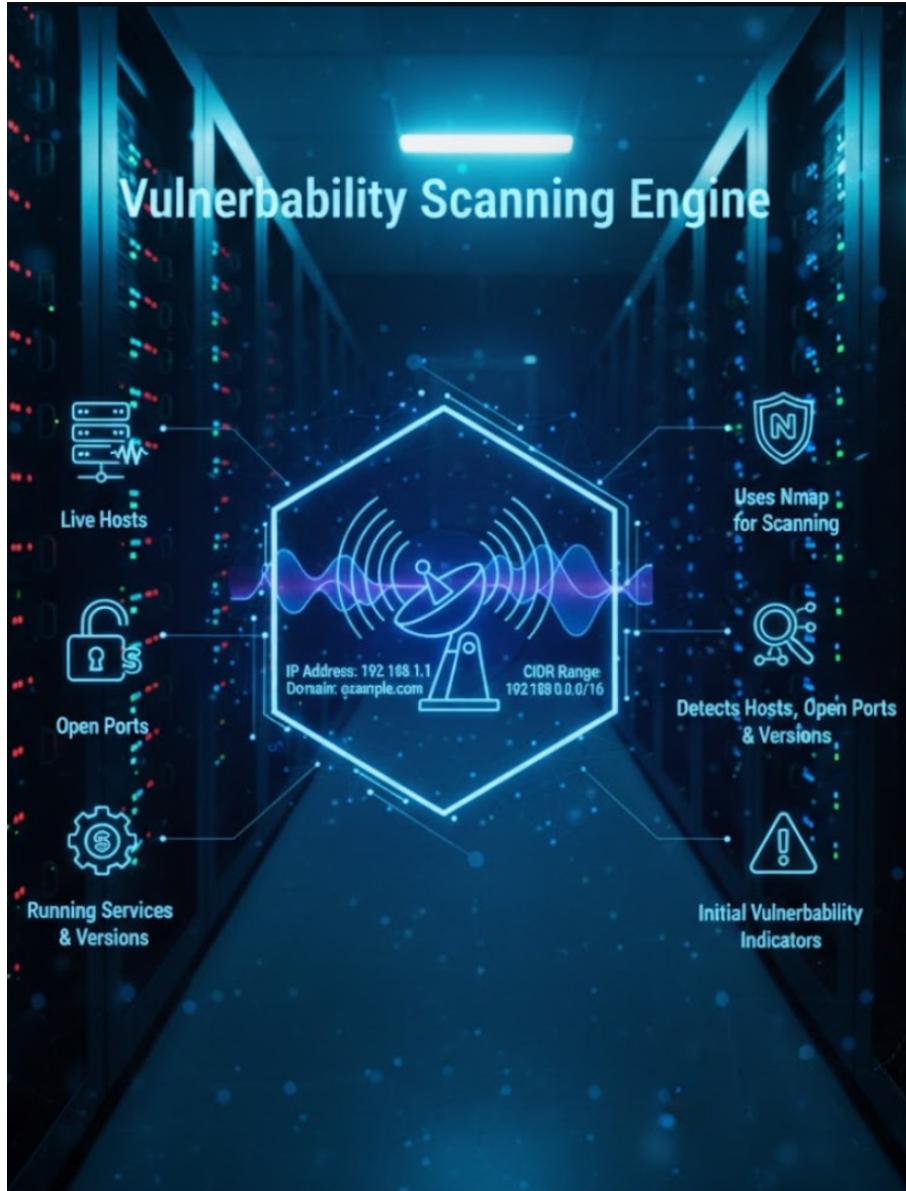
VULNERABILITY SCAN

THREAT ANALYSIS

RISK SCORING

DASHBOARD

Vulnerability Scanning Engine



VULNERABILITY SCANNING ENGINE

WHAT IS VULNERABILITY SCANNING ENGINE?

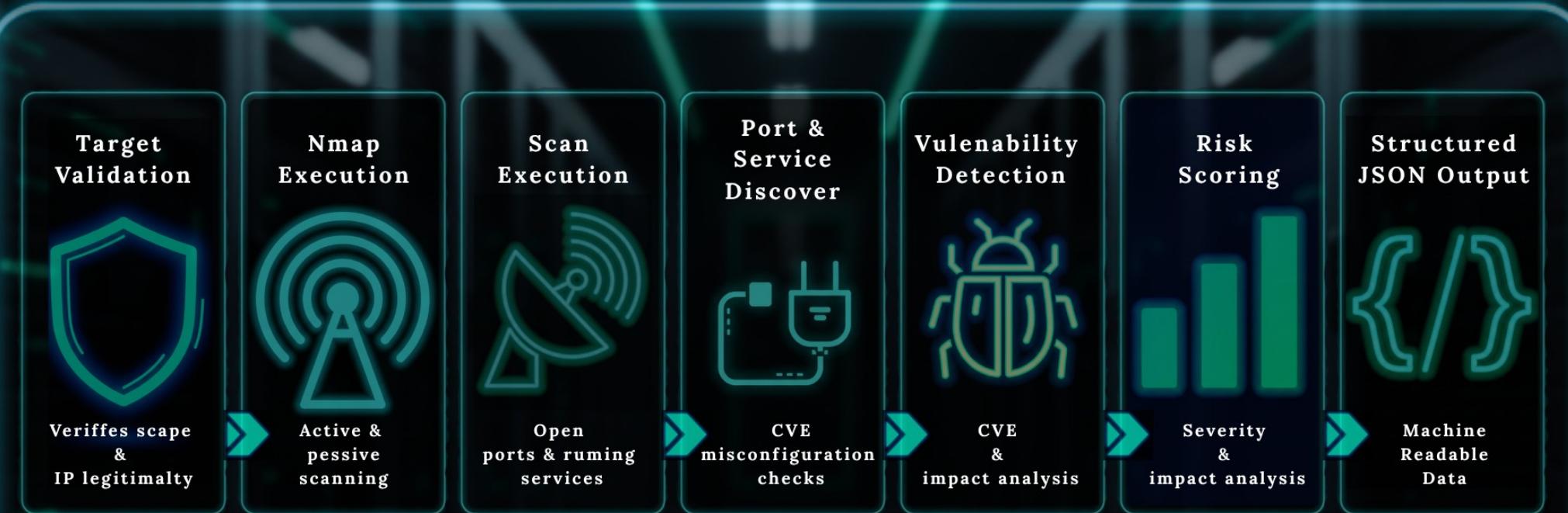
The Vulnerability Scanning Engine acts as the critical entry point of our system. Its primary role is to actively scan designated targets – whether an IP address, a domain, a range, or a CIDR block – to identify what's exposed.

WHY DO WE NEED IT?

Without a robust scanning mechanism, a vulnerability assessment cannot begin. This engine is crucial for the following:

- Discovering live hosts within a specified network segment.
- Identifying open ports, which often indicate active services.
- Pinpointing running services and their specific versions, which are key to identifying known vulnerabilities.

SCANNING ENGINE WORK FLOW

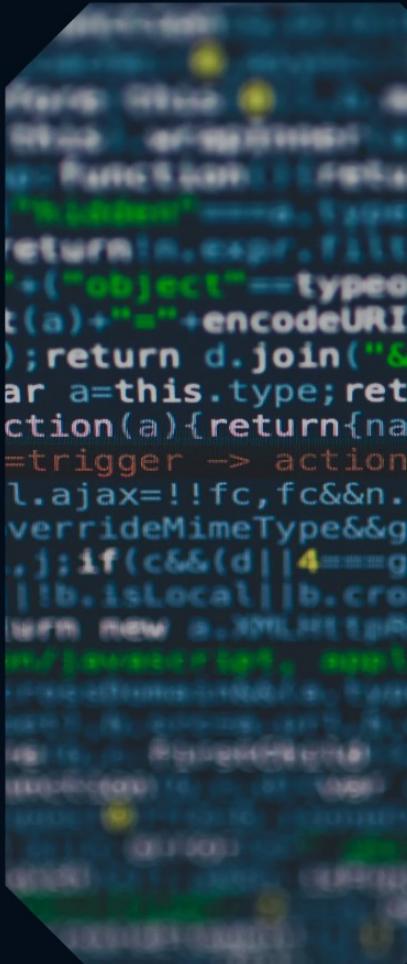


"AUTOMATES VULNERABILITY DETECTION AND RISK SCORING BY TRANSFORMING RAW SCAN DATA INTO STRUCTURED SECURITY INTELLIGENCE."

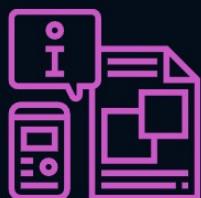
THREAT INTELLIGENCE

WHY THREAT INTELLIGENCE ?

- Converts raw scan data into actionable intelligence.
- Interprets scan results for informed decision-making.
- Bridges scanning output and risk analysis layers.
- Prevents alert overload from raw vulnerability data.



3-TIER INTEL



■

The approach is a three-tier intelligence model designed to provide 360° threat visibility.

EXPOSURE INTELLIGENCE

- Identifies internet-exposed assets using Shodan
- Highlights potential attack surfaces

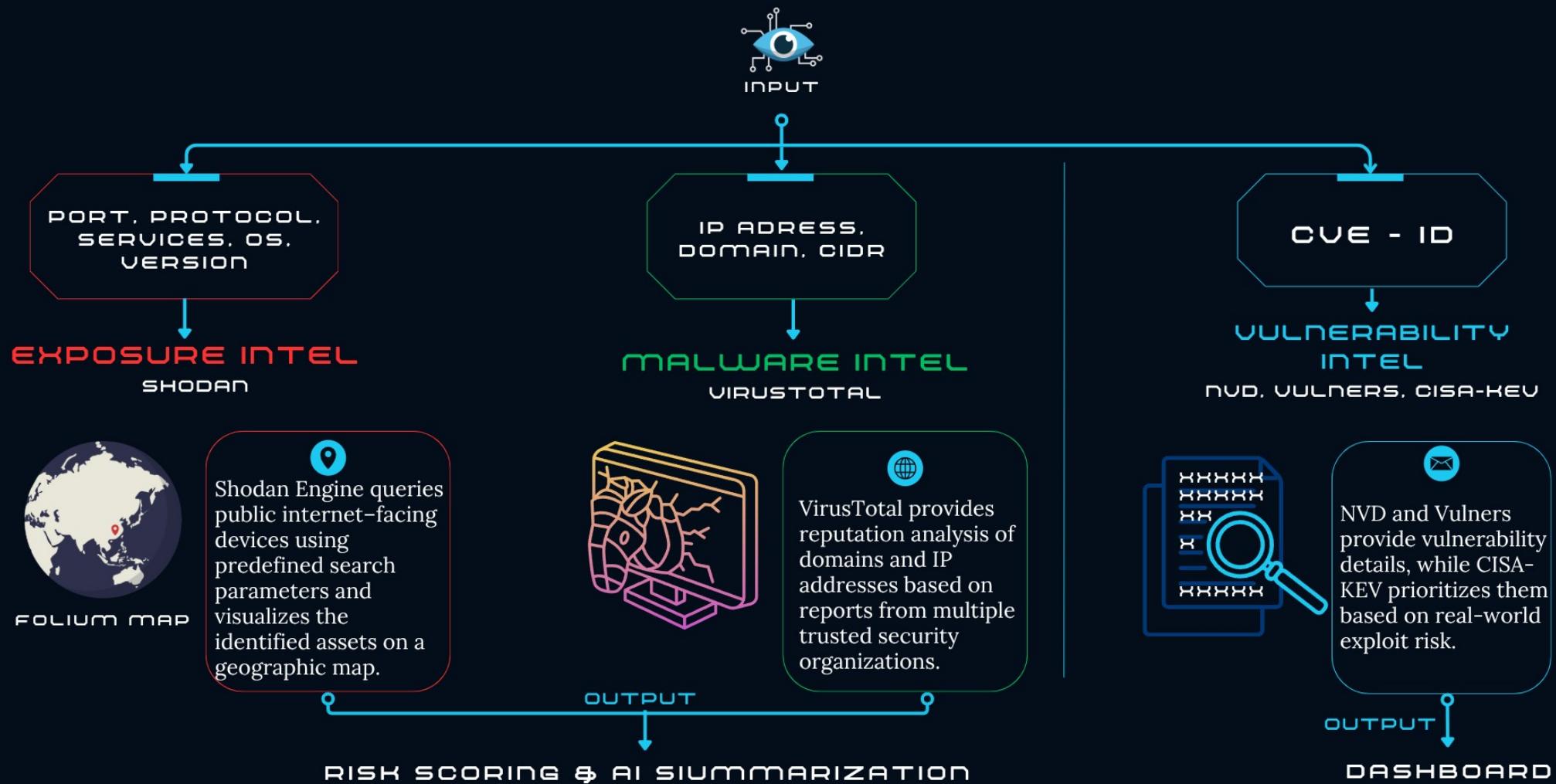
MALWARE INTELLIGENCE

- Evaluates IPs and domains using VirusTotal
- Detects malicious history and trust level

VULNERABILITY INTELLIGENCE

- Enriches detected CVEs using NVD & Vulners
- Prioritizes critical risks using CISA-KEV

INTERNAL WORKFLOW



RISK SCORING ENGINE



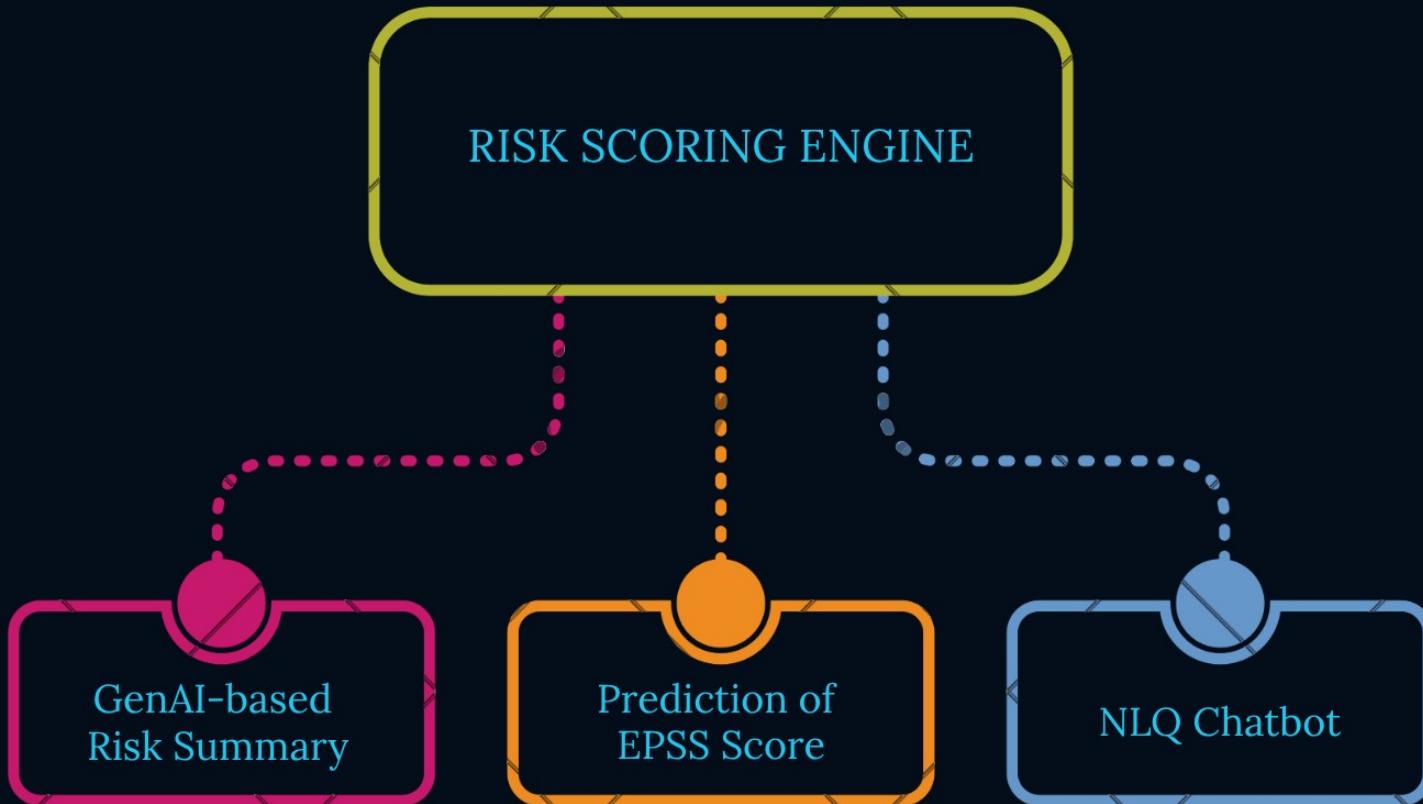
WHY RISK SCORING ENGINE ?

- Risk Scoring Engine that transforms raw vulnerability and threat intelligence data into prioritized cyber risk to support effective security decision-making.

APPROACHES :

- Combines CVSS severity scores with EPSS exploit probability
- Applies risk analytics to rank vulnerabilities based on real-world impact
- Produces actionable risk insights instead of raw technical data

RISK SCORING ENGINE INTEGRATION



GenAI-based
Risk Summary:

Summarize about json data
from threat intelligence

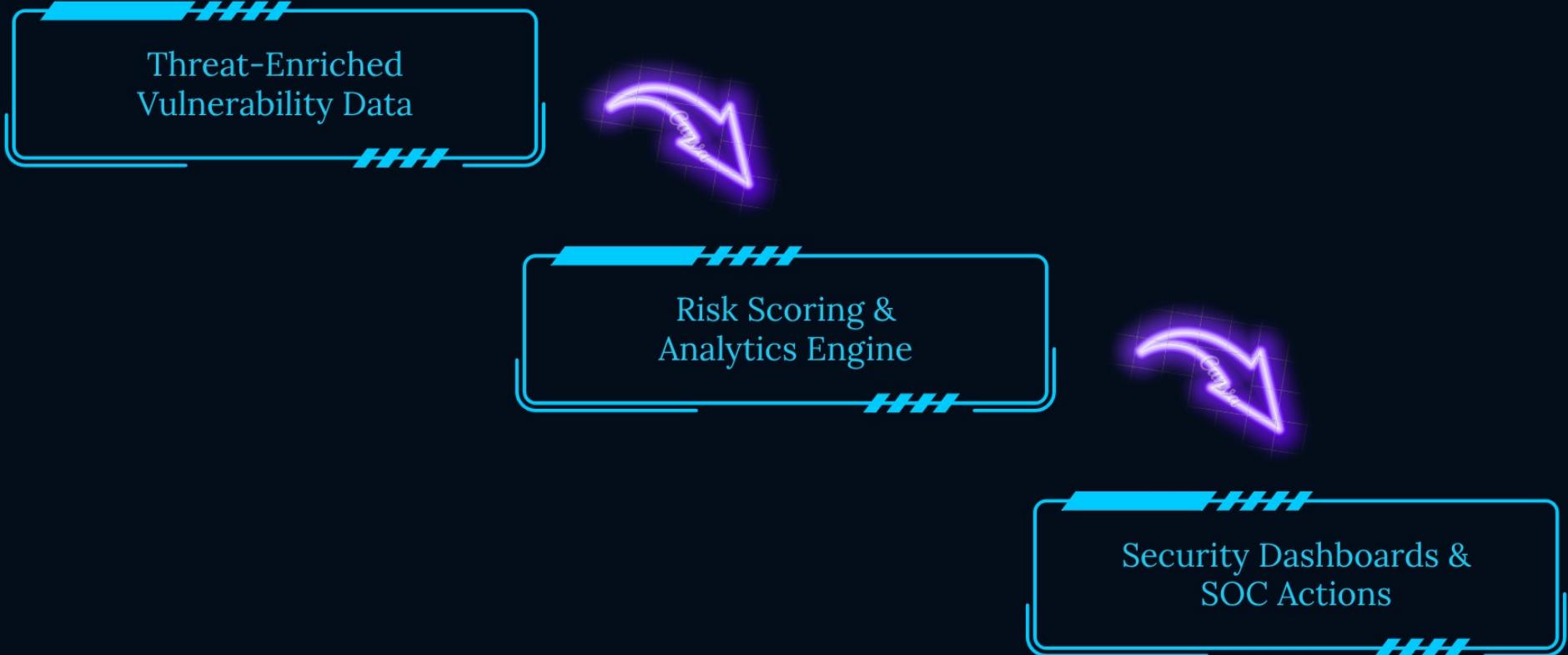
Prediction of
EPSS Score:

Exploitability of vulnerability

NLQ (Natural Language
Queries):

Chatbot interface

RISK SCORING ENGINE WORKFLOW



DASHBOARD

Intention by dashboard layer

User-facing interface of the platform

Visualizes outputs from all backend layers



- Scan monitoring
 - Risk & threat analysis
 - Alert viewing and reporting
- Does not perform scanning or risk computation

Approach Used

API-driven, Modular Dashboard Architecture

Key Design Principles

- **Separation of Concerns**
 - Backend handles scanning, threat intel, risk scoring
 - Frontend handles only Visualization and interaction
- **Layer-aware Design**
 - Each dashboard tab maps to a backend layer
- **Reusable Components**
 - Common data loader (`data_loader.py`) used across all tabs

Technology Stack

- **Streamlit** – UI framework
- **Python** – Core language
- **Pandas** – Data transformation
- **Plotly** – Interactive visualizations
- **REST APIs (FastAPI backend)** – Data communication

Working



- User enters target details, ports, and scan profile
- Frontend sends scan request to backend API
- Backend runs scans, analyzes data, and stores results
- Frontend fetches results using multiple APIs
- Data is visualized using charts, tables, and metrics



WATCH THE LIVE ACTION!

Theme

Mode

Dark

Light

Scan Inputs

Targets (IP / Host / CIDR)

scanme.nmap.org

Ports (optional)

22,80,443 or 1-1000

Upload target file (.txt)

Drag and drop file here

Limit 200MB per file + TXT

[Browse files](#)

Scan Profile

Normal

[Run Scan](#)

[Reset All Tabs](#)

Cyber Risk Assessment Dashboard

Scan Profile: nmap | 20:25:47

[Overview](#) [Nmap](#) [Vulnerability Insights](#) [Threat Summary](#) [Threat Intel](#) [Risk Analysis](#) [Alerts](#) [AI Analyst](#)

Overview

Scan Type: nmap | Scan Time: 2026-01-19T14:53:24.619916

Total Hosts	Total Findings	Threat Score	Risk Level
1	3	19	Low

Findings Severity Distribution

Severity	Percentage
High	33.3%
Medium	33.3%
Low	33.3%
Critical	0%

Cyber Risk Assessment Dashboard

Scan Profile: nmap | 20:25:47

[Overview](#) [Nmap](#) [Vulnerability Insights](#) [Threat Summary](#) [Threat Intel](#) [Risk Analysis](#) [Alerts](#) [AI Analyst](#) [Reports](#)

Global Threat Intelligence

Leaflet | Tiles © Esri — Source: Esri, Maxar, Earthstar Geographics, GIS User Community

FUTURE SCOPE OF CRATIP

PERSONALIZATION SUPPORT

- Role-based dashboards (Admin, Analyst, Manager)
- Custom risk thresholds and alerts
- Organization-specific security policies

REAL-TIME MONITORING & ALERTS

- Continuous scanning instead of periodic scans
- Real-time alerts for critical vulnerabilities
- Email / SMS / webhook notifications

AUTOMATED THREAT RESPONSE (SOAR)

- Auto-isolate vulnerable systems
- Automated ticket creation for incidents
- Suggested mitigation steps using AI



THANK YOU!

