CYBER RISK ASSESSMENT & THREAT INTELLIGENCE PLATFORM (CRATIP)

Technical Document

⇒ TABLE OF CONTENTS

	Page No.
ABSTRACT	
1: INTRODUCTION	**5-7**
1.1 Background & Motivation 1.2 Problem Statement 1.3 Objectives of the Project 1.4 Scope of the Project	
2: RELATED WORK	**8-12**
2.1 Introduction to Cyber Risk Assessment 2.2 Vulnerability Scanning Approaches 2.2.1 Network Scanning Using Nmap 2.3 Threat Intelligence Platforms 2.3.1 Shodan 2.3.2 VirusTotal 2.4 Vulnerability Scoring Systems 2.4.1 Common Vulnerability Scoring System (CVSS) 2.4.2 Exploit Prediction Scoring System (EPSS) 2.4.3 CISA Known Exploited Vulnerabilities (KEV) 2.5 Risk Assessment and Analytics Systems 2.6 Dashboards and Visualization in Cybersecurity 2.7 AI and Natural Language Processing in Cybersecurity 2.8 Research Gap and Motivation for CRATIP	
3: SYSTEM ARCHITECTURE & DESIGN	**13-17**
3.1 Overall System Architecture 3.2 Module Interaction Diagram 3.3 Data Flow Description 3.4 Technology Stack	
4: SYSTEM IMPLEMENTATION	**18-22**
4.1 Automated Vulnerability Scanning Engine 4.2 Threat Intelligence & Enrichment Engine 4.3 Risk Scoring & Analytics Engine 4.4 Dashboard & Visualization Module 4.5 Alert Generation & Notification System 4.6 AI-Based Risk Analysis Module	

5: TESTING & VALIDATION 23-26

5.1 Vulnerability Scanning Test Cases
5.2 Threat Intelligence Test Cases
5.3 Risk Scoring Test Cases
5.4 Severity-Based Validation (High / Medium / Low)

6: RESULTS & ANALYSIS 27-29

6.1 Risk Distribution Analysis
6.2 Alert Statistics
6.3 Dashboard Output Analysis

7: CONCLUSION & FUTURE WORK 30-32

7.1 Conclusion
7.2 Limitations of the System
7.3 Future Scope
7.3.1 Cloud Deployment and Scalability
7.3.2 Continuous Monitoring with Agents
7.3.3 Automated Remediation
7.3.4 Advanced Machine Learning Models
7.3.5 Compliance & Governance Mapping
7.3.6 SIEM & SOC Integration
7.4 Final Remarks

8: CONCLUSION 33-34

8.1 Summary of Work
8.2 Key Achievements
8.3 Impact of the System

9: FUTURE SCOPE 35

9.1 Cloud Deployment
9.2 Continuous Monitoring
9.3 Automated Remediation
9.4 Integration with SIEM Systems

10: REFERENCES 36

ABSTRACT

The rapid increase in cyber threats, network exposures, and software vulnerabilities has made traditional security assessment approaches insufficient for modern organizations. Existing cybersecurity solutions often generate fragmented, tool-specific outputs that are difficult to correlate, prioritize, and interpret, resulting in delayed and reactive security decisions. Furthermore, most systems rely on static severity metrics that fail to reflect real-world exploitability and future risk trends.

This project presents the **Cyber Risk Assessment & Threat Intelligence Platform (CRATIP)**, a comprehensive and automated cybersecurity assessment framework designed to identify, enrich, analyze, and prioritize cyber risks in an integrated manner. The platform combines **automated vulnerability scanning**, **real-time threat intelligence enrichment**, **dynamic risk scoring**, and **predictive analysis** into a unified system. Network assets are first analyzed using Nmap-based scanning techniques to identify open ports, services, and potential vulnerabilities. The identified findings are then enriched using trusted external threat intelligence sources such as **Shodan**, **VirusTotal**, **CISA Known Exploited Vulnerabilities (KEV)**, and vulnerability intelligence databases.

To overcome the limitations of static scoring systems, CRATIP implements a **risk-based scoring model** inspired by the **Exploit Prediction Scoring System (EPSS)**, enabling the platform to estimate the likelihood of exploitation over a defined time horizon. In addition, the system integrates **Artificial Intelligence (AI)** using GPT-based models to generate human-readable risk summaries, enabling both technical and non-technical stakeholders to understand security insights effectively. A **Streamlit-based interactive dashboard** provides real-time visualization of vulnerabilities, threat trends, alerts, and risk distributions.

The proposed platform enhances proactive security decision-making, reduces analysis overhead, and improves organizational cyber resilience. CRATIP demonstrates how the integration of automation, threat intelligence, predictive analytics, and AI-driven explanations can significantly improve modern cyber risk assessment practices.

1: INTRODUCTION

1.1 Background & Motivation

In recent years, the rapid expansion of digital infrastructure, cloud computing, and internet-facing services has significantly increased the cyber-attack surface of organizations. Enterprises today rely on complex networks consisting of servers, web applications, databases, and IoT devices, all of which are potential targets for cyber adversaries. At the same time, cyber threats have become more sophisticated, automated, and persistent, exploiting vulnerabilities at a much faster rate than traditional security mechanisms can respond.

Modern cybersecurity practices involve the use of multiple independent tools such as network scanners, vulnerability databases, and threat intelligence platforms. While these tools generate large volumes of security data, they often operate in isolation. Security analysts are required to manually correlate scan results, vulnerability scores, and threat intelligence feeds, which leads to increased operational complexity and delayed decision-making.

The motivation behind the Cyber Risk Assessment & Threat Intelligence Platform (CRATIP) is to address this challenge by providing a unified, automated, and intelligence-driven system that can discover vulnerabilities, enrich them with real-world threat data, and assess cyber risk in a proactive manner. By integrating automated scanning, threat intelligence, predictive risk analysis, and visualization into a single platform, CRATIP aims to reduce manual effort, improve accuracy, and enable informed cybersecurity decisions.

1.2 Problem Statement

Existing cybersecurity solutions suffer from several limitations that reduce their effectiveness in real-world environments:

- **Fragmented Security Data:** Vulnerability scanners, threat intelligence platforms, and monitoring tools generate data independently, making correlation difficult.

- **Static Risk Assessment:** Traditional scoring systems such as CVSS focus on technical severity but fail to capture real-world exploitability and attack trends.
- **Reactive Security Posture:** Most tools identify vulnerabilities only after they exist, offering little insight into which risks are most likely to be exploited in the near future.
- **Limited Contextual Awareness:** Security teams often lack contextual information such as exposure status, known exploitation, or threat reputation.
- **Complex Interpretation:** Raw technical outputs are difficult for non-technical stakeholders to understand, leading to communication gaps between security teams and management.

As a result, organizations struggle to prioritize vulnerabilities effectively, leading to inefficient remediation strategies and increased exposure to cyber threats.

1.3 Objectives of the Project

The primary objectives of the Cyber Risk Assessment & Threat Intelligence Platform (CRATIP) are as follows:

1. To design and implement an automated vulnerability scanning system capable of identifying open ports, running services, and potential attack surfaces.
2. To enrich discovered assets with real-time threat intelligence from trusted external sources such as Shodan, VirusTotal, Vulners, NVD, and CISA KEV.
3. To develop a dynamic risk scoring mechanism that evaluates vulnerabilities based on severity, exposure, and real-world exploitability.
4. To provide predictive insights by analyzing exploit trends and identifying vulnerabilities with high future risk potential.
5. To generate automated alerts for critical and high-risk security findings.
6. To present cybersecurity insights through an interactive dashboard that supports both technical and non-technical users.
7. To support audit-ready reporting and data export for compliance and documentation purposes.

1.4 Scope of the Project

The scope of the CRATIP project includes the design, development, and validation of a modular cybersecurity assessment platform with the following capabilities:

- Network-level vulnerability scanning using Nmap.
- Integration with multiple third-party threat intelligence APIs.
- Risk scoring and classification of assets into critical, high, medium, and low risk categories.
- Alert generation for high-risk and exploited vulnerabilities.
- Visualization of scan results, risk metrics, and alerts through a Streamlit-based dashboard.
- AI-based summarization of security findings for improved interpretability.
- Storage of scan results and alerts for historical analysis and reporting.

The project focuses on assessment and analysis rather than automated remediation. While the platform provides actionable insights and recommendations, the responsibility for applying patches or configuration changes remains outside the current scope. The system is designed to be extensible, allowing future integration with automated remediation tools, cloud platforms, and enterprise security solutions.

2: RELATED WORK

2.1 Introduction to Cyber Risk Assessment

Cyber risk assessment is a critical component of modern cybersecurity strategies. It involves identifying vulnerabilities, evaluating threats, and estimating the potential impact of cyber incidents on organizational assets. Traditional risk assessment methodologies primarily rely on periodic security audits and manual analysis, which are often insufficient in dynamic and large-scale network environments.

With the increase in cyber attacks such as ransomware, zero-day exploits, and advanced persistent threats (APTs), there is a growing need for automated and intelligence-driven risk assessment platforms. Researchers and industry practitioners have emphasized the importance of combining vulnerability assessment with real-world threat intelligence to improve risk prioritization and decision-making.

2.2 Vulnerability Scanning Approaches

Vulnerability scanning tools play a foundational role in identifying exposed services and potential weaknesses in networked systems.

2.2.1 Network Scanning Using Nmap

Nmap (Network Mapper) is one of the most widely used open-source tools for network discovery and security auditing. Several studies highlight Nmap's effectiveness in identifying open ports, running services, operating systems, and service versions.

Existing research demonstrates that:

- Port scanning helps define the attack surface of an organization.
- Service version detection is essential for mapping vulnerabilities to known CVEs.
- Automated scanning reduces human error and increases assessment frequency.

However, Nmap alone provides raw technical outputs without contextual risk interpretation. It identifies *what is open*, but not *how dangerous* it is in the real-world threat landscape.

2.3 Threat Intelligence Platforms

Threat intelligence provides contextual information about cyber threats, adversary behavior, and known exploitation activities.

2.3.1 Shodan

Shodan is a search engine for internet-connected devices. Research highlights its effectiveness in identifying:

- Publicly exposed services
- Misconfigured systems
- Industrial control systems (ICS)

Shodan data helps assess external exposure risk, which is critical for understanding attack vectors beyond internal scans.

2.3.2 VirusTotal

VirusTotal aggregates malware detection results from multiple antivirus engines and threat intelligence feeds. It is widely used for:

- IP reputation analysis
- Malware association checks
- Threat classification

Studies indicate that VirusTotal is effective in identifying malicious infrastructure but requires correlation with other data sources for accurate risk assessment.

2.3 Vulnerability Scoring Systems

2.3.1 Common Vulnerability Scoring System (CVSS)

CVSS is the most widely adopted standard for rating the severity of software vulnerabilities. It provides a numerical score based on metrics such as attack vector, attack complexity, privileges required, and impact.

While CVSS is useful for standardization, several researchers have identified limitations:

- CVSS scores are static and do not change over time.
- They do not consider whether a vulnerability is actively exploited.
- High CVSS scores do not always indicate high real-world risk.

As a result, organizations often struggle to prioritize vulnerabilities effectively when relying solely on CVSS.

2.3.2 Exploit Prediction Scoring System (EPSS)

EPSS is a probabilistic model developed to estimate the likelihood of a vulnerability being exploited in the wild. Unlike CVSS, EPSS focuses on *exploitability trends* rather than technical severity.

Recent studies show that:

- EPSS scores provide better prioritization for patch management.
- Combining EPSS with CVSS improves decision-making.
- Predictive models help shift security from reactive to proactive approaches.

CRATIP draws inspiration from EPSS by incorporating exploit probability and trend-based risk assessment into its scoring engine.

2.4.3 CISA Known Exploited Vulnerabilities (KEV)

The CISA KEV catalog lists vulnerabilities that are actively exploited in the wild. Research shows that vulnerabilities listed in KEV pose immediate and severe risk and should be prioritized regardless of CVSS score.

CRATIP leverages KEV data to automatically elevate risk scores for confirmed exploited vulnerabilities.

2.5 Risk Assessment and Analytics Systems

Several commercial and academic systems attempt to integrate scanning and analytics for cyber risk management. However, many existing platforms face the following challenges:

- Proprietary and closed architectures
- Limited explainability of risk scores
- High deployment and licensing costs
- Poor support for predictive analysis

Research suggests that modular architectures and open-source technologies provide greater flexibility and transparency. CRATIP follows a modular design that allows independent evolution of scanning, enrichment, and risk analysis components.

2.6 Dashboards and Visualization in Cybersecurity

Visualization plays a crucial role in security operations by enabling quick understanding of complex data.

Studies show that:

- Dashboards improve situational awareness for security teams.
- Visual risk categorization helps non-technical stakeholders.
- Interactive interfaces reduce cognitive load during incident response.

Streamlit and similar frameworks have gained popularity in research and prototyping due to rapid development capabilities. CRATIP adopts Streamlit to provide a centralized, interactive dashboard for security insights.

2.7 AI and Natural Language Processing in Cybersecurity

Recent research highlights the growing role of Artificial Intelligence and Generative AI in cybersecurity. AI-based systems are used for:

- Threat detection and classification
- Automated reporting and summarization
- Security recommendations

Generative AI models such as GPT have shown promise in converting technical security data into human-readable insights. CRATIP integrates AI-based summarization to bridge the gap between technical findings and executive-level understanding.

2.8 Research Gap and Motivation for CRATIP

Based on the literature review, the following research gaps are identified:

- Lack of unified platforms that combine scanning, threat intelligence, predictive risk scoring, and visualization.
- Over-reliance on static vulnerability scores without exploit trend analysis.
- Limited explainability of security findings for non-technical stakeholders.
- Insufficient integration of AI-driven insights in traditional security tools.

CRATIP addresses these gaps by providing an end-to-end, automated, and intelligence-driven cyber risk assessment platform that integrates multiple security dimensions into a single system.

3: SYSTEM ARCHITECTURE & DESIGN

3.1 Overall System Architecture

The Cyber Risk Assessment & Threat Intelligence Platform (CRATIP) follows a **modular, layered, and service-oriented architecture** designed to ensure scalability, maintainability, and ease of integration. The system is implemented using a client–server model, where the frontend dashboard interacts with a backend API responsible for executing security workflows and managing data processing.

The architecture is divided into the following major layers:

- **Presentation Layer**
  This layer provides the user interface for interacting with the platform. It is implemented using **Streamlit**, offering dashboards, charts, tables, and controls for initiating scans and viewing results.
- **Application Layer**
  The core business logic resides in this layer and is implemented using **FastAPI**. It orchestrates the execution of scanning, threat intelligence enrichment, risk scoring, alert generation, and AI analysis.
- **Processing Engines Layer**
  This layer consists of independent engines responsible for:
  - Automated Vulnerability Scanning
  - Threat Intelligence Enrichment
  - Risk Scoring and Analytics
- **Data Persistence Layer**
  A lightweight **SQLite database** is used to store scan results, risk scores, alerts, and audit logs in structured JSON format.
- **External Intelligence Layer**
  This layer integrates third-party threat intelligence sources such as **Shodan, VirusTotal, Vulners, NVD, and CISA KEV**, along with AI services accessed via the **OpenRouter API**.

This modular design ensures loose coupling between components, enabling independent development, testing, and future extension of individual modules without affecting the entire system.

3.2 Module Interaction Diagram

The interaction between modules in CRATIP follows a sequential and event-driven workflow. Each module consumes the output of the previous module and produces structured data for downstream processing.

Module Interaction Sequence

1. The user initiates a scan through the Streamlit dashboard.
2. The dashboard sends a request to the FastAPI backend.
3. The Vulnerability Scanning Engine performs network discovery and service identification.
4. The Threat Intelligence Enrichment Engine augments scan results with external intelligence data.
5. The Risk Scoring & Analytics Engine calculates asset-level and overall risk scores.
6. The Alerting Engine evaluates predefined thresholds and generates alerts.
7. Results are stored in the database and displayed on the dashboard.

(A module interaction diagram illustrating this flow should be included here in the final document.)

3.3 Data Flow Description

The data flow within CRATIP is designed to ensure consistency, traceability, and real-time visibility across all processing stages.

Step-by-Step Data Flow

1. **Input Acquisition**

   Users provide target IP addresses, domains, or CIDR ranges via the dashboard interface.

2. **Vulnerability Scanning Output**

   The scanning engine generates a structured JSON output containing:

   - Host identifiers
   - Open ports
   - Running services
   - Service versions
   - Preliminary vulnerability indicators

3. **Threat Intelligence Enrichment**

   The enrichment engine consumes the scan output and queries external APIs to retrieve:

   - Exposure details (Shodan)
   - Reputation scores (VirusTotal)
   - Known exploited vulnerabilities (CISA KEV)
   - CVE metadata (NVD, Vulners)

4. **Risk Scoring & Analytics**

   The enriched data is processed to compute:

   - Asset-level risk scores
   - Severity classification (Critical / High / Medium / Low)
   - Risk trends and exploit likelihood indicators

5. **Alert Generation**

   The system evaluates risk thresholds and generates alerts for critical conditions such as high-risk vulnerabilities or malicious IP detection.

6. **Visualization & Reporting**

   The final processed data is displayed on the dashboard and made available for export in CSV, Excel, and PDF formats.

This well-defined data flow ensures transparency and enables effective debugging, auditing, and future enhancements.

3.4 Technology Stack

The technology stack used in CRATIP was selected to balance performance, flexibility, and ease of development.

Programming Language

- **Python (v3.10+)**
  Chosen for its extensive ecosystem of security, data processing, and machine learning libraries.

Backend Framework

- **FastAPI**
  Provides high-performance asynchronous request handling, automatic API documentation, and background task execution.

Frontend Framework

- **Streamlit**
  Enables rapid development of interactive dashboards with minimal frontend complexity.

Security & Scanning Tools

- **Nmap** – Network discovery and service detection
- **python-nmap** – Python wrapper for Nmap

Threat Intelligence APIs

- **Shodan** – Internet exposure intelligence
- **VirusTotal** – IP and malware reputation analysis
- **Vulners / NVD** – CVE metadata and vulnerability information
- **CISA KEV** – Known exploited vulnerabilities catalog

Database

- **SQLite**

  A lightweight, serverless database suitable for local deployment and rapid prototyping.

Visualization & Analytics

- **Matplotlib / Plotly** – Graphs and visual analytics
- **Folium** – Geospatial visualization of assets

AI Integration

- **OpenRouter API (GPT-4)** – Natural language analysis and executive-level summaries

---

4: SYSTEM IMPLEMENTATION

This chapter explains the practical implementation of the Cyber Risk Assessment & Threat Intelligence Platform (CRATIP). Each subsystem is discussed in detail, covering its purpose, internal working logic, tools used, and how it integrates with other modules of the platform.

4.1 Automated Vulnerability Scanning Engine

The Automated Vulnerability Scanning Engine forms the foundational component of CRATIP. Its primary objective is to identify exposed network assets by discovering open ports, running services, and service versions across target systems.

This engine leverages **Nmap**, integrated using the python-nmap library, to perform network reconnaissance. The scanning engine supports multiple scan profiles to balance speed and depth of analysis, enabling flexible usage across different environments.

Implementation Details

- Accepts IP addresses, domains, or CIDR ranges as input.
- Executes Nmap commands programmatically from the backend.
- Parses scan results into structured JSON format.
- Extracts details such as:
    - Open ports
    - Protocols
    - Service names
    - Version information

The output of this module serves as the primary input for all downstream components, ensuring a standardized and machine-readable data format.

4.2 Threat Intelligence & Enrichment Engine

The Threat Intelligence & Enrichment Engine enhances raw scan results by correlating them with real-world threat intelligence data. This module transforms technical scan outputs into meaningful security insights.

Integrated Intelligence Sources

- **Shodan** – Identifies public exposure and internet-facing services.
- **VirusTotal** – Evaluates IP reputation and malicious activity.
- **Vulners & NVD** – Provides CVE metadata and vulnerability descriptions.
- **CISA KEV** – Confirms whether vulnerabilities are actively exploited in the wild.

Implementation Workflow

1. Receives scan results from the scanning engine.
2. Queries external APIs for each identified host or service.
3. Aggregates and normalizes threat intelligence data.
4. Appends enriched intelligence to the original scan JSON.

This enrichment process ensures that vulnerabilities are assessed in the context of real-world exploitability rather than isolated technical severity.

4.3 Risk Scoring & Analytics Engine

The Risk Scoring & Analytics Engine is responsible for prioritizing vulnerabilities and assets based on their likelihood of exploitation and potential impact.

Risk Scoring Logic

CRATIP implements a **dynamic, weighted risk scoring model** inspired by the Exploit Prediction Scoring System (EPSS). The engine considers:

- CVSS base score
- Asset exposure level
- Threat intelligence indicators

- Presence in CISA Known Exploited Vulnerabilities catalog

The final risk score is normalized to a **0–100 scale** and categorized as:

- Critical
- High
- Medium
- Low

Analytics Output

- Asset-level risk scores
- Overall organizational risk summary
- Severity distribution statistics
- Risk trend indicators

This module enables proactive security decision-making by highlighting vulnerabilities that pose immediate real-world threats.

4.4 Dashboard & Visualization Module

The Dashboard & Visualization Module provides a centralized interface for monitoring cybersecurity posture. It is implemented using **Streamlit**, allowing rapid development of interactive and responsive dashboards.

Key Dashboard Features

- Overview of scan status and risk posture
- Detailed vulnerability listings
- Threat intelligence summaries
- Risk score visualizations
- Interactive charts and tables

Visualization components such as **bar charts, pie charts, tables, and maps** are used to simplify complex security data, making it accessible to both technical and non-technical stakeholders.

4.5 Alert Generation & Notification System

The Alert Generation & Notification System continuously monitors risk analysis outputs and triggers alerts when predefined thresholds are exceeded.

Alert Conditions

- Critical risk score detection
- Presence of known exploited vulnerabilities
- Detection of malicious IP addresses
- Exposure of high-risk services (e.g., SSH, RDP)

Implementation Highlights

- Alerts are generated automatically after risk evaluation.
- Each alert contains severity, description, affected assets, and timestamp.
- Alerts are stored in the database for audit and tracking.
- Alerts are displayed prominently on the dashboard for immediate attention.

This module ensures timely awareness of critical security issues and supports rapid incident response.

4.6 AI-Based Risk Analysis Module

To bridge the gap between complex security data and decision-makers, CRATIP integrates an **AI-Based Risk Analysis Module** using **GPT-4 via OpenRouter API**.

Functionality

- Converts structured JSON risk data into natural language explanations.

- Provides executive-level summaries and remediation guidance.
- Explains vulnerability impact in simple, non-technical terms.

Example Use Case

The AI module can analyze a critical vulnerability and generate a summary such as:

“This vulnerability is actively exploited and could allow attackers to gain unauthorized access. Immediate patching is recommended.”

This module significantly enhances usability by making cybersecurity insights understandable to management and non-security professionals.

5: TESTING & VALIDATION

This chapter presents a comprehensive testing and validation strategy used to verify the correctness, reliability, and effectiveness of the Cyber Risk Assessment & Threat Intelligence Platform (CRATIP). The system was validated at each stage of processing to ensure accurate vulnerability detection, correct threat intelligence enrichment, reliable risk scoring, and appropriate severity classification.

Testing was conducted using controlled lab environments, known vulnerable services, and publicly documented malicious indicators.

5.1 Vulnerability Scanning Test Cases

The vulnerability scanning engine was tested using systems configured with known open ports and services. The objective was to validate accurate detection of exposed services, protocols, and service versions.

Test Case Table – Vulnerability Scanning Engine

TEST CASE ID	SEVERITY	INPUT SCENARIO	EXPECTED RESULT	ACTUAL RESULT	STATUS
VS-TC-01	High	SSH service running on port 22	Detection of SSH as high-risk service	SSH detected correctly	PASS
VS-TC-02	Medium	HTTP service on port 80	Identification of web service	Apache HTTP identified	PASS
VS-TC-03	Medium	Multiple open ports (80, 443, 3306)	All services detected	All services listed	PASS
VS-TC-04	Low	No open ports on target	No services detected	Zero open ports found	PASS

VS-TC-05	High	Exposed database port (3306)	Database exposure flagged	MySQL detected	PASS

These results confirm that the scanning engine accurately discovers network attack surfaces under various conditions.

5.2 Threat Intelligence Test Cases

Threat intelligence enrichment was validated using known malicious IP addresses, vulnerable services, and CVEs listed in trusted intelligence sources.

Test Case Table – Threat Intelligence Engine

TEST CASE ID	SEVERITY	INPUT SCENARIO	EXPECTED RESULT	ACTUAL RESULT	STATUS
TI-TC-01	High	IP listed in VirusTotal blacklist	Malicious reputation detected	IP flagged as malicious	PASS
TI-TC-02	High	CVE listed in CISA KEV catalog	Marked as actively exploited	Exploited status confirmed	PASS
TI-TC-03	Medium	Public-facing HTTP service	Exposure data from Shodan	Exposure details retrieved	PASS
TI-TC-04	Medium	Vulnerable service with CVE	CVE metadata enrichment	CVE details added	PASS
TI-TC-05	Low	Clean IP with no history	No threat indicators	No malicious flags	PASS

These tests validate that the enrichment engine correctly correlates scan data with real-world intelligence.

5.3 Risk Scoring Test Cases

The risk scoring engine was tested to ensure accurate calculation of risk scores and correct severity categorization based on multiple contributing factors.

Test Case Table – Risk Scoring Engine

TEST CASE ID	SEVERITY	INPUT SCENARIO	EXPECTED RISK LEVEL	ACTUAL RISK LEVEL	STATUS
RS-TC-01	Critical	CVE present in CISA KEV	Critical (90+)	Critical	PASS
RS-TC-02	High	High CVSS + exposed service	High (70–89)	High	PASS
RS-TC-03	Medium	Moderate CVSS, low exposure	Medium (40–69)	Medium	PASS
RS-TC-04	Low	Low CVSS, no exposure	Low (0–39)	Low	PASS
RS-TC-05	High	Malicious IP with open ports	High risk score	High	PASS

The results confirm the effectiveness of the dynamic risk scoring algorithm.

5.4 Severity-Based Validation (High / Medium / Low)

Severity-based validation was conducted to ensure consistent classification and prioritization of vulnerabilities across all modules.

Severity Classification Validation Table

SEVERITY LEVEL	VALIDATION CRITERIA	SYSTEM BEHAVIOR	VALIDATION RESULT
HIGH	Actively exploited, high exposure, malicious IP	Immediate alert generated	PASS
MEDIUM	Vulnerable service, limited exposure	Logged and monitored	PASS
LOW	Minimal risk, no exploit indicators	Informational entry only	PASS

> This validation ensures that CRATIP prioritizes threats correctly, enabling efficient risk mitigation and response.

Summary of Testing Outcomes

- All functional modules passed validation testing.
- Severity classification aligned with real-world threat behavior.
- Alerts were generated only for critical and high-risk conditions.
- The system demonstrated stable performance and reliable outputs.

6: RESULTS & ANALYSIS

This chapter presents a detailed analysis of the results generated by the Cyber Risk Assessment & Threat Intelligence Platform (CRATIP). The results demonstrate how the system processes raw vulnerability data, enriches it with real-world threat intelligence, and converts it into meaningful risk insights. The effectiveness of CRATIP is evaluated through risk distribution, alert statistics, and dashboard-based visualization outputs.

6.1 Risk Distribution Analysis

The risk distribution analysis illustrates how detected vulnerabilities are classified into different severity levels—Critical, High, Medium, and Low—based on the computed risk score.

Observed Risk Distribution

After executing multiple scans on controlled test environments and sample target assets, the following distribution pattern was observed:

- **Critical Risks**: Vulnerabilities associated with CISA KEV-listed CVEs and high EPSS probabilities.
- **High Risks**: Public-facing services with high CVSS scores and confirmed exposure.
- **Medium Risks**: Vulnerabilities with moderate severity and limited external exposure.
- **Low Risks**: Informational findings and low-impact services with minimal threat indicators.

Analytical Insights

- A smaller number of vulnerabilities accounted for the majority of overall risk.
- EPSS-based scoring successfully reduced false prioritization of low-impact CVEs.
- Actively exploited vulnerabilities were consistently ranked at the top.

This confirms that CRATIP effectively shifts vulnerability management from **quantity-based** to **risk-based** prioritization.

6.2 Alert Statistics

Alert statistics provide insight into how frequently the system generated alerts and the conditions under which they were triggered.

Alert Categorization

Alerts were classified into the following categories:

- **Critical Alerts**: Triggered when risk score exceeded 80 or a vulnerability was listed in CISA KEV.
- **High Alerts**: Generated for exposed services with high threat intelligence confidence.
- **Informational Alerts**: Logged for monitoring but did not require immediate action.

Alert Analysis Findings

- Critical alerts represented a small percentage but required immediate remediation.
- High alerts helped prioritize patching efforts effectively.
- Informational alerts improved visibility without overwhelming analysts.

The alerting system demonstrated a balanced approach, reducing alert fatigue while ensuring that critical threats were never missed.

6.3 Dashboard Output Analysis

The Streamlit-based dashboard acts as the primary interface for users to interact with CRATIP results. This section analyzes the effectiveness of the dashboard in presenting complex security data.

Dashboard Components Analyzed

- **Risk Overview Panel**: Displays aggregated risk scores and severity distribution.
- **Asset-Level Risk View**: Allows drill-down into individual IPs and services.
- **Alert Panel**: Shows real-time alerts with severity indicators.
- **AI-Generated Insights**: Provides natural language explanations of critical findings.

Evaluation Outcomes

- The dashboard enabled quick identification of high-risk assets.
- Visual risk indicators improved decision-making efficiency.
- AI-generated summaries bridged the gap between technical and non-technical stakeholders.

The dashboard successfully functioned as a **Single Pane of Glass**, consolidating scanning, intelligence, and risk insights into a unified view.

Summary of Results

- Risk prioritization aligned with real-world threat activity.
- Alert generation was accurate and severity-driven.
- Visualization improved usability and situational awareness.
- AI-based explanations enhanced interpretability of technical findings.

7: CONCLUSION & FUTURE WORK

7.1 Conclusion

The Cyber Risk Assessment & Threat Intelligence Platform (CRATIP) was successfully designed, implemented, and validated as a comprehensive solution for automated cybersecurity risk assessment. The primary objective of the project was to address the limitations of traditional vulnerability management systems, which often produce fragmented, static, and difficult-to-interpret security data.

CRATIP integrates multiple cybersecurity functions—including automated vulnerability scanning, threat intelligence enrichment, dynamic risk scoring, alerting, visualization, and AI-driven explanation—into a unified platform. By correlating internal scan results with trusted external intelligence sources such as Shodan, VirusTotal, and the CISA Known Exploited Vulnerabilities (KEV) catalog, the system provides a realistic and actionable view of cyber risk.

A key contribution of this project is the implementation of a **dynamic, risk-based prioritization model**. Unlike traditional approaches that rely solely on CVSS scores, CRATIP incorporates exploit likelihood indicators inspired by the Exploit Prediction Scoring System (EPSS). This enables the platform to distinguish between vulnerabilities that are theoretically severe and those that are actively exploited in real-world environments.

The inclusion of a Streamlit-based interactive dashboard ensures that security insights are presented clearly and intuitively. Additionally, the AI-based risk analysis module enhances accessibility by translating complex technical findings into simple, natural language explanations suitable for both technical and non-technical stakeholders.

Testing and validation results confirm that CRATIP accurately detects vulnerabilities, enriches findings with relevant threat intelligence, assigns appropriate severity levels, and generates timely alerts. The system demonstrated effectiveness in reducing alert fatigue while ensuring that critical risks were promptly highlighted.

Overall, CRATIP achieves its intended goals and demonstrates how automation, threat intelligence, predictive analytics, and artificial intelligence can be combined to significantly improve an organization’s cybersecurity posture.

7.2 Limitations of the System

While CRATIP delivers strong functionality, certain limitations were identified during development and testing:

- The platform currently relies on external APIs, which may be subject to rate limits or availability constraints.
- EPSS-based prediction accuracy depends on the quality and freshness of external datasets.
- The system performs on-demand scans and does not yet support continuous real-time monitoring.
- Automated remediation actions are not implemented in the current version.

These limitations provide clear directions for future enhancement.

7.3 Future Scope

The CRATIP platform is designed with extensibility in mind, allowing multiple enhancements in future versions. The following improvements are proposed:

7.3.1 Cloud Deployment and Scalability

The platform can be containerized using Docker and deployed on cloud platforms such as AWS, Azure, or GCP. This would enable large-scale scanning, multi-tenant support, and improved availability.

7.3.2 Continuous Monitoring with Agents

A lightweight endpoint agent can be developed to enable continuous vulnerability monitoring rather than periodic scanning. This would allow real-time detection of configuration changes and newly introduced vulnerabilities.

7.3.3 Automated Remediation

Integration with configuration management tools such as Ansible or Puppet can allow CRATIP to automatically remediate low- and medium-severity vulnerabilities, reducing manual intervention.

7.3.4 Advanced Machine Learning Models

Future versions may incorporate machine learning techniques to improve exploit prediction accuracy, anomaly detection, and risk trend forecasting.

7.3.5 Compliance & Governance Mapping

CRATIP can be extended to map vulnerabilities against compliance standards such as ISO 27001, NIST, and PCI-DSS, helping organizations meet regulatory requirements.

7.3.6 SIEM & SOC Integration

Integration with SIEM platforms like Splunk or ELK Stack would allow CRATIP to function as part of a Security Operations Center (SOC) ecosystem.

7.4 Final Remarks

The Cyber Risk Assessment & Threat Intelligence Platform (CRATIP) demonstrates how modern cybersecurity challenges can be addressed using a layered, intelligence-driven, and automation-focused approach. By shifting from reactive vulnerability management to proactive risk prediction, CRATIP provides a strong foundation for next-generation security assessment systems.

This project not only fulfills academic and technical objectives but also offers practical relevance for real-world cybersecurity environments, making it suitable for further research, development, and enterprise adoption.

8. CONCLUSION

8.1 Summary of Work

This project successfully designed and implemented the **Cyber Risk Assessment & Threat Intelligence Platform (CRATIP)**, a comprehensive system for automated vulnerability assessment, threat intelligence enrichment, and risk-based security analysis. The platform integrates multiple cybersecurity processes—including network scanning, external threat validation, dynamic risk scoring, alert generation, and visualization—into a unified and scalable solution.

The system follows a modular architecture consisting of an **Automated Vulnerability Scanning Engine**, **Threat Intelligence & Enrichment Engine**, **Risk Scoring & Analytics Engine**, and an **Interactive Dashboard with Alerting and AI-based analysis**. By correlating scan results with real-world threat intelligence sources and predictive scoring techniques, the platform moves beyond traditional static security assessments and provides actionable, prioritized insights.

8.2 Key Achievements

The key achievements of the CRATIP system are summarized as follows:

- Successful automation of **network vulnerability discovery** using Nmap with multiple scan profiles.
- Integration of **real-time threat intelligence** from trusted external sources such as Shodan, VirusTotal, CISA KEV, and NVD.
- Implementation of a **dynamic risk scoring model** that considers exploit probability, exposure, and threat context rather than relying solely on static CVSS scores.
- Development of a **user-friendly Streamlit dashboard** that visualizes risks, alerts, and trends in an intuitive manner.
- Implementation of **severity-based alert generation** for critical, high, medium, and low-risk vulnerabilities.
- Inclusion of an **AI-based analysis module** to translate technical findings into natural language insights for non-technical stakeholders.

- Validation of system functionality through **severity-based test cases**, ensuring reliability and correctness of each core module.

8.3 Impact of the System

The CRATIP platform significantly enhances an organization's cybersecurity posture by reducing manual effort, improving risk visibility, and enabling proactive decision-making. By prioritizing vulnerabilities based on real-world exploitability and exposure, the system helps security teams focus on the most critical threats first.

Additionally, the platform bridges the gap between technical security data and business-level understanding through AI-generated explanations and visual dashboards. This makes CRATIP suitable not only for security analysts but also for management and compliance teams, ultimately contributing to improved risk management and faster response times.

9. FUTURE SCOPE

The current implementation of CRATIP provides a strong foundation for cyber risk assessment. However, several enhancements can be incorporated to further extend its capabilities.

9.1 Cloud Deployment

The platform can be containerized using **Docker** and deployed on cloud platforms such as **AWS, Azure, or Google Cloud**. Cloud deployment would improve scalability, availability, and accessibility, enabling organizations to perform large-scale assessments across distributed environments.

9.2 Continuous Monitoring

Future versions can introduce **agent-based or scheduled scanning mechanisms** for continuous monitoring of assets. This would allow real-time detection of configuration changes, newly exposed services, and emerging vulnerabilities instead of relying solely on periodic scans.

9.3 Automated Remediation

The system can be enhanced by integrating with **configuration management and automation tools** such as Ansible or PowerShell scripts. Based on risk severity, CRATIP could automatically apply patches, disable vulnerable services, or enforce security configurations, reducing response time and manual intervention.

9.4 Integration with SIEM Systems

Integration with **Security Information and Event Management (SIEM)** platforms such as Splunk, QRadar, or ELK Stack would enable centralized logging, correlation with security events, and advanced incident response workflows. This would make CRATIP suitable for enterprise-grade security operations centers (SOCs).

10. REFERENCES

1. Scarfone, K., & Mell, P., *Guide to Vulnerability Scoring Systems (CVSS)*, NIST, USA.
2. First.org, *Exploit Prediction Scoring System (EPSS)*, https://www.first.org/epss
3. Nmap Project, *Network Mapper Documentation*, https://nmap.org
4. Shodan, *The Search Engine for the Internet of Things*, https://www.shodan.io
5. VirusTotal, *Malware and Threat Intelligence Platform*, https://www.virustotal.com
6. CISA, *Known Exploited Vulnerabilities Catalog*, https://www.cisa.gov/known-exploited-vulnerabilities-catalog
7. National Vulnerability Database (NVD), *CVE & CVSS Database*, https://nvd.nist.gov
8. FastAPI Documentation, https://fastapi.tiangolo.com
9. Streamlit Documentation, https://docs.streamlit.io
10. OpenAI / OpenRouter API Documentation, https://openrouter.ai