



# Major Project

## TrustCheck Reputation Assurance Platform

**Presented by:**  
**ARPITA KUMARI**  
**ARIHANT VARDHAN**  
**VIKASH KUMAR**  
**Vivek Singh Chandel**

**Guided by:**  
Dr. Akashdeep Bhardwaj  
Assistant Professor (SS)  
Systemics Cluster  
School of Computer  
Science

- Introduction
- Problem Statement
- Literature Review
- Objectives
- Methodology
- Pert Chart
- Output

# Introduction

- As defenders amplify their efforts to mitigate cyber threats, attackers correspondingly escalate their own capabilities, consistently striving to remain a step ahead in the digital confrontation. It soon became apparent that a new approach was needed to address this cat and mouse situation. The relentless advancements in cyber offense and defense soon clarified the urgent need for a paradigm shift to adeptly navigate this evolving standoff. As a strategic solution, the adoption of Threat Intelligence (TI) came to the forefront. Interestingly, the roots of Threat Intelligence stretch far back, being a cornerstone of military strategies for centuries, signifying its fundamental role in strategic forecasting and decision-making, now repurposed for cybersecurity resilience.
- Threat Intelligence (TI) equips organizations with the tools needed to stay ahead in the dynamic cybersecurity environment, aiming to identify and avert threats proactively. It achieves this by amassing critical information about potential adversaries, encompassing their strategies and operational tactics. Such actionable intelligence not only strengthens IT defenses but also supports strategic decision-making, enhancing overall security posture. This forward-looking approach is a key factor behind the growing reliance on Threat Intelligence across industries, as it enables organizations to take pre-emptive measures against cyber threats effectively.

# Problem Statement

The increasing sophistication and frequency of cyber threats pose significant challenges to organizations worldwide. Despite advancements in cybersecurity technology, many organizations struggle to effectively detect and mitigate these threats in a timely manner. Existing threat intelligence platforms often lack scalability, robust security measures, and user-friendly interfaces, hindering organizations' ability to proactively defend against evolving cyber threats.

# Literature Review

[1] Machine Learning has proven to be useful in detecting security threats, by analyzing security and log data to identify potential threats. Over the past decade ML techniques have been widely used to enable systematic learning and building of enterprise systems' normal profiles to detect anomalies and zero-day threats (Conti et al., 2018). ML includes a large variety of models in continuous evolution, presenting weak boundaries and cross relationships, and has already been successfully applied within various contexts in cybersecurity (Dua and Du, 2011; Ford and Siraj, 2014; Singh and Silakari, 2015; Buczak and Guven, 2016; Fraley and Cannady, 2017; Ghanem et al., 2017; Yadav et al., 2017; Apruzzese et al., 2018). The book by Dua and Du (2011) provides a comprehensive guide to how ML and data mining are incorporated in cybersecurity tools, and in particular, it provides examples of anomaly detection, misuse detection, profiling detection, etc. This study also provides a thorough analysis of where ML approaches can achieve maximum impact and a discussion of their limitations. The concluding chapters discuss emerging challenges and how ML and data mining can be used to effectively deal with them.

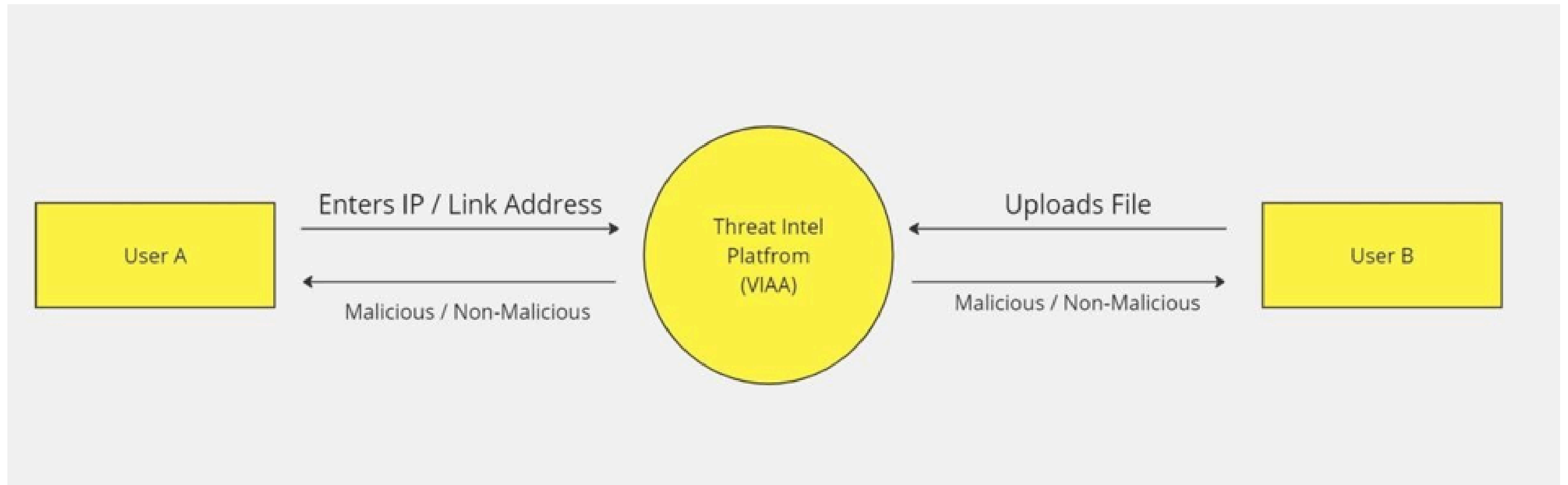
# Objective

1. Enhance Threat Detection Capabilities: Develop a comprehensive threat intelligence platform capable of accurately identifying and analyzing various types of cyber threats, including malicious URLs, IP addresses, and files.
2. Improve Scalability: Design the platform to scale horizontally, allowing for seamless integration of new data sources and accommodating increasing volumes of threat data without compromising performance.
3. Strengthen Security Measures: Implement stringent security protocols, including input validation for search URLs and robust file upload validation, to mitigate the risk of potential cyberattacks such as buffer overflow and malicious uploads.
4. Enhance User Experience: Create a user-friendly interface with intuitive dashboard features that provide users with easy access to threat analysis tools, actionable insights, and real-time threat alerts.



1. **Research and Analysis:** Conduct a comprehensive review of existing threat intelligence platforms, cybersecurity frameworks, and best practices to identify key requirements and challenges.
2. **Platform Design:** Collaborate with cybersecurity experts and software developers to design a scalable and secure threat intelligence platform architecture. Define the system's components, functionalities, and integration points.
3. **Development and Testing:** Utilize agile software development methodologies to iteratively build and test the platform's features and functionalities. Conduct rigorous testing to ensure the platform's reliability, scalability, and security.
  1. **Implementation and Deployment:** Deploy the developed platform in a controlled environment, collaborating with pilot users to gather feedback and fine-tune the system. Implement necessary enhancements and optimizations based on user feedback

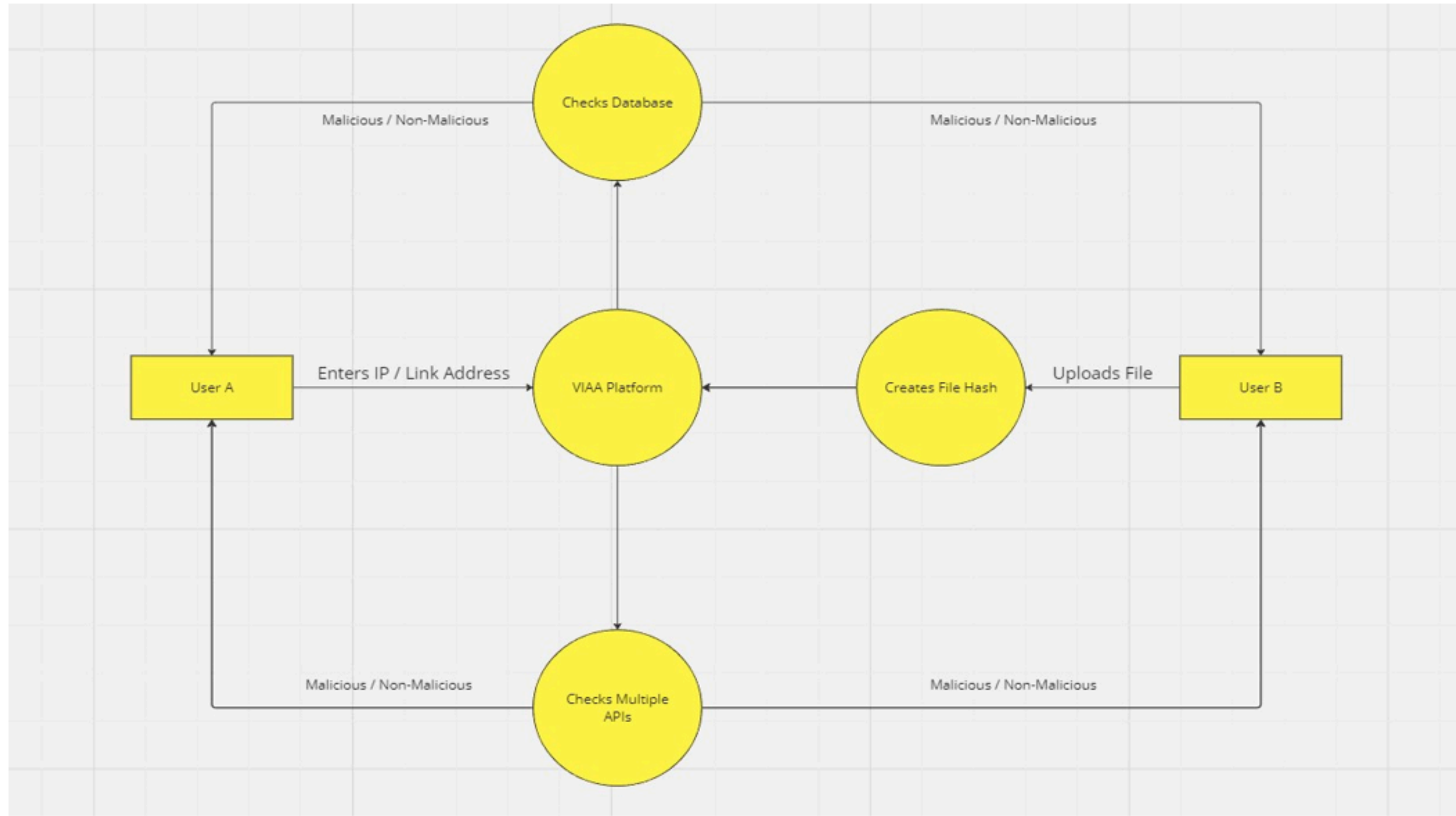
**a) D.F.D: Level 0**



*Fig [2.0] Zero Level DFD*



**b) Data flow Diagram: Level 1**



*Fig [2.1]: Level 1 DFD*

# PERT Chart

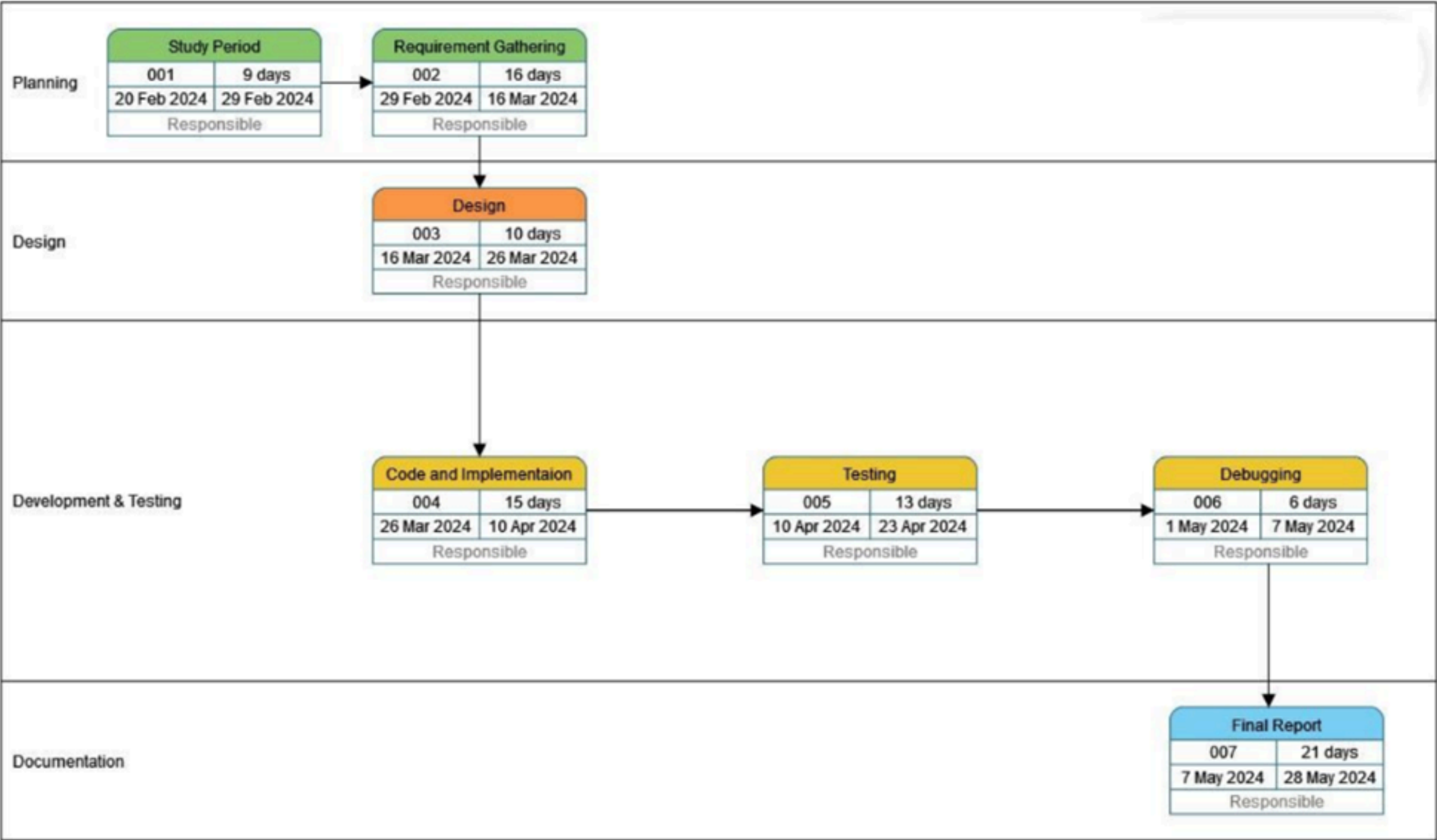
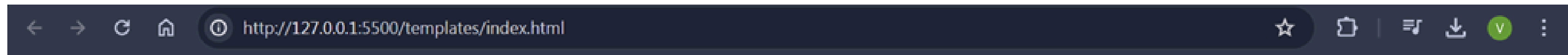


fig.10: Program Evaluation Review Technique Chart

# Output



## News

Check out the latest news

[Go to News](#)

## Check Reputation

Verify reputation

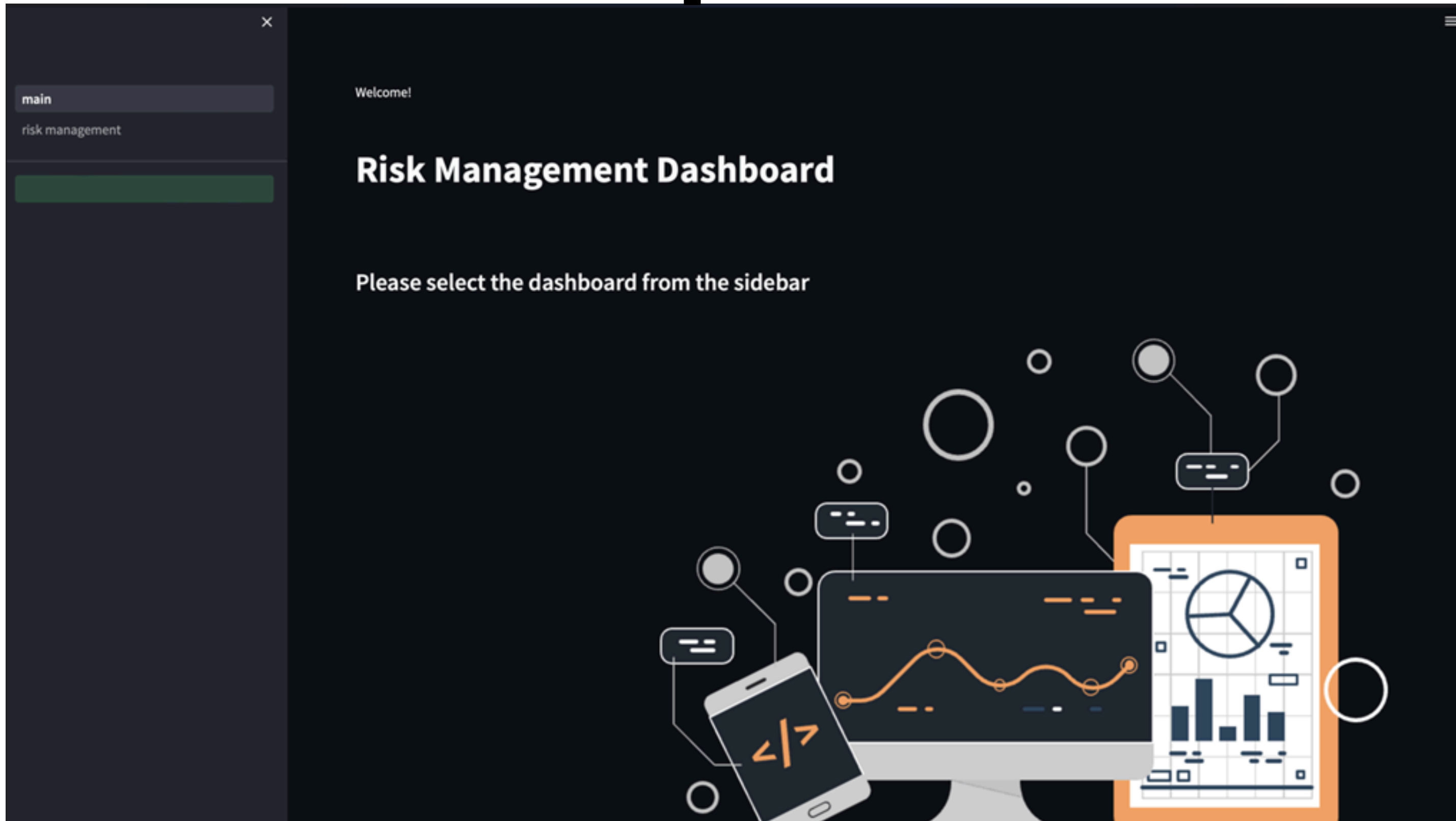
[Check Reputation](#)

## GRC Dashboard

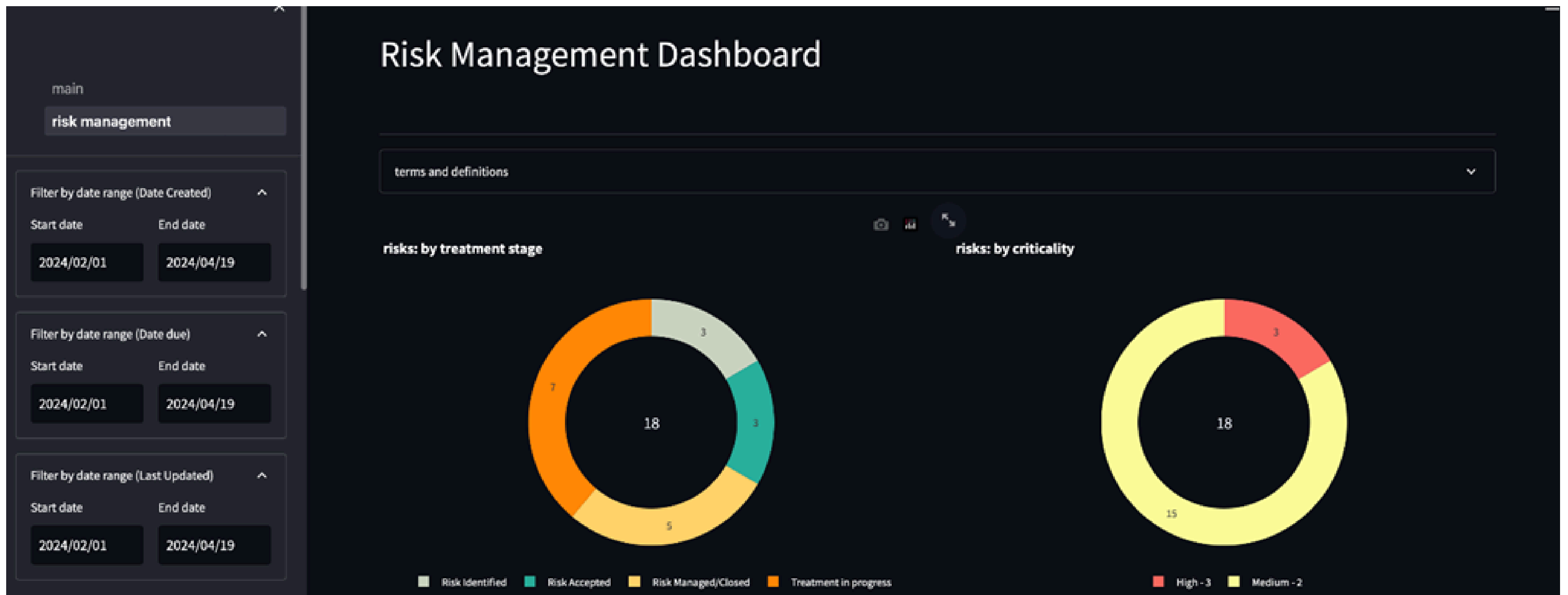
View GRC Dashboard

[Go to GRC Dashboard](#)

# Output








# Output





# Output

[Headlines](#) [Articles](#) [Sources](#) [Categories](#)


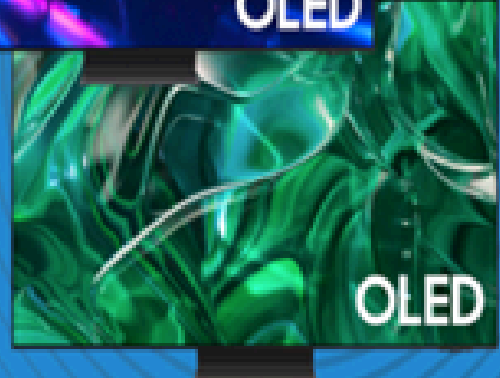

News Hub




**YouTube**  
**Can The Tesla Cybertruck Really Off-Road? - Top Gear**  
Can it jump? Rock crawl? Survive the whoops? Conquer the sand dunes? In short, can the Tesla Cybertruck REALLY off-road? Viral videos of it struggling on mi...  
 Author: None

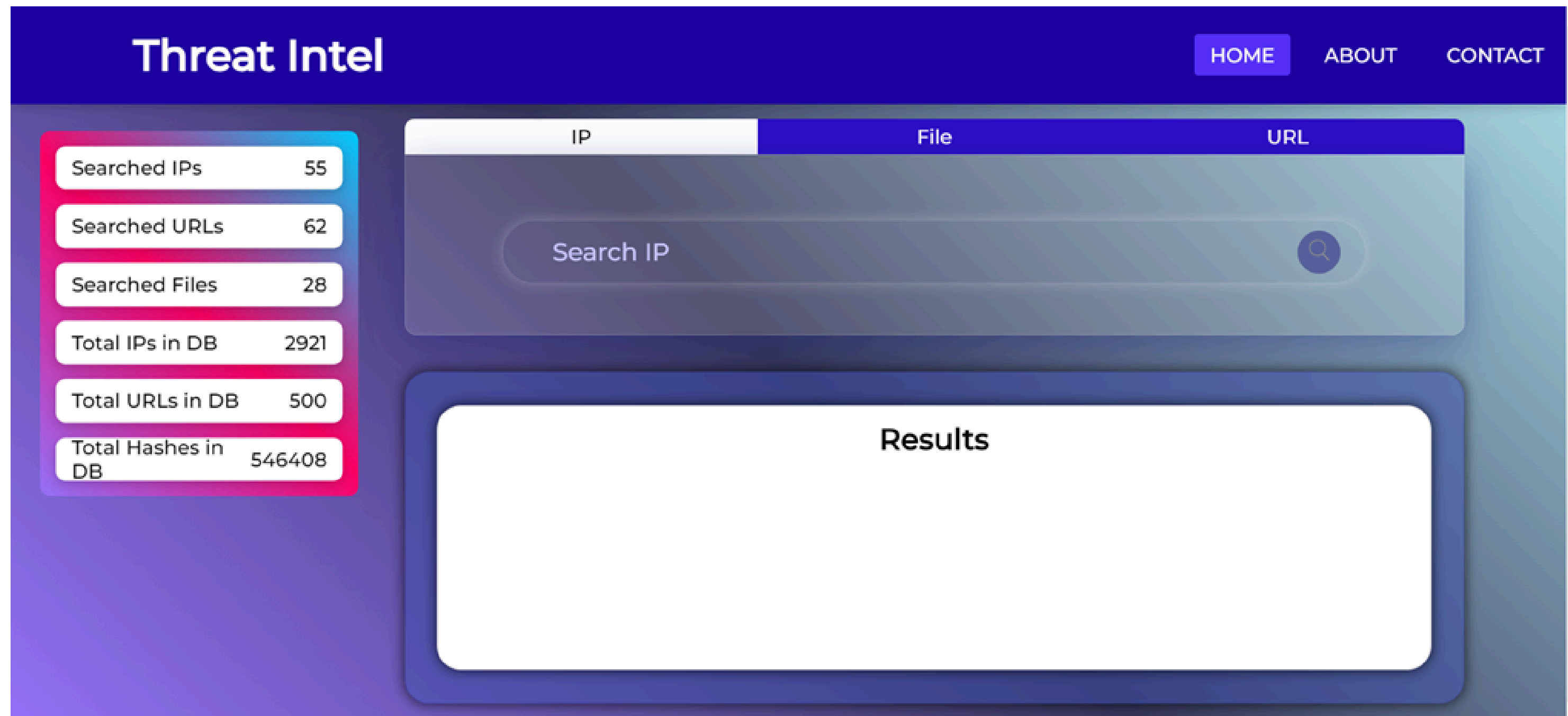


**The Verge**  
**The Delta emulator will soon turn your iPad into a giant Nintendo DS - The Verge**  
The next major version of Delta will bring iPadOS support and the developer says multi-phone multiplayer and Genesis emulation are on their way



**TechRadar**  
**Samsung OLED TVs are down to record-low prices - this is better than Black Friday - TechRadar**  
Save up to \$1,200 on Samsung's best OLED displays  
 Author: Mackenzie Frazier

# Output





# Output

Threat Intel

HOME

ABOUT

CONTACT

Searched IPs56

Searched URLs62

Searched Files29

Total IPs in DB2921

Total URLs in DB500

Total Hashes in DB546408

IPFileURL

1.10.241.225

Results

DatabaseNon-malicious IP

Abuse IP DBSafe

# Output

Threat Intel

HOMEABOUTCONTACT

Searched IPs56

Searched URLs62

Searched Files30

Total IPs in DB2921

Total URLs in DB500

Total Hashes in DB546408

IPFileURL

Screenshot 2024-04-29 at 9.07.08 PM.png

Upload

100%

File uploaded successfully.

Results

VirustotalSafe

KasperskyUndefined



Thank You