National Forensic Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Email-based Data Exfiltration Through Insider Threat Detection

MINOR PROJECT

Faculty Advisor : Mr. Dharmesh Dave

Disha Sharma
240103002014
9th May 2025

TABLE OF CONTENTS

SR. NO.	TOPIC	DESCRIPTION
1.	Introduction	Motivation and Scope of the Project
2.	Theoretical Background	Research Findings and Comparative Analysis
3.	Proposed Model	Problem Statement Revisited, Framework, Methodology
4.	Empirical Result Analysis	Experimental Setup, Evaluation Metrics, Testing/Implementation
5.	Conclusion	Future Scope. Progress Report, References

01 : INTRODUCTION

MOTIVATION

The Reasons :

- Complicated IT Environment
- Inadequate Security Measures
- Lack of Employee Training and Awareness
- Weak Enforcement Policies

The Numbers :

- 83% of Organizations reported at least one Insider Threat. (IBM)
- 67% of insiders are likely to email sensitive data externally. (Teramind)
- 36% organizations only had effective access control solutions in place. (IBM)
- 54% of insiders already have credentialed access. (StationX)
- 44% insiders use applications that can leak data eg Email (StationX)

SCOPE OF THE PROJECT

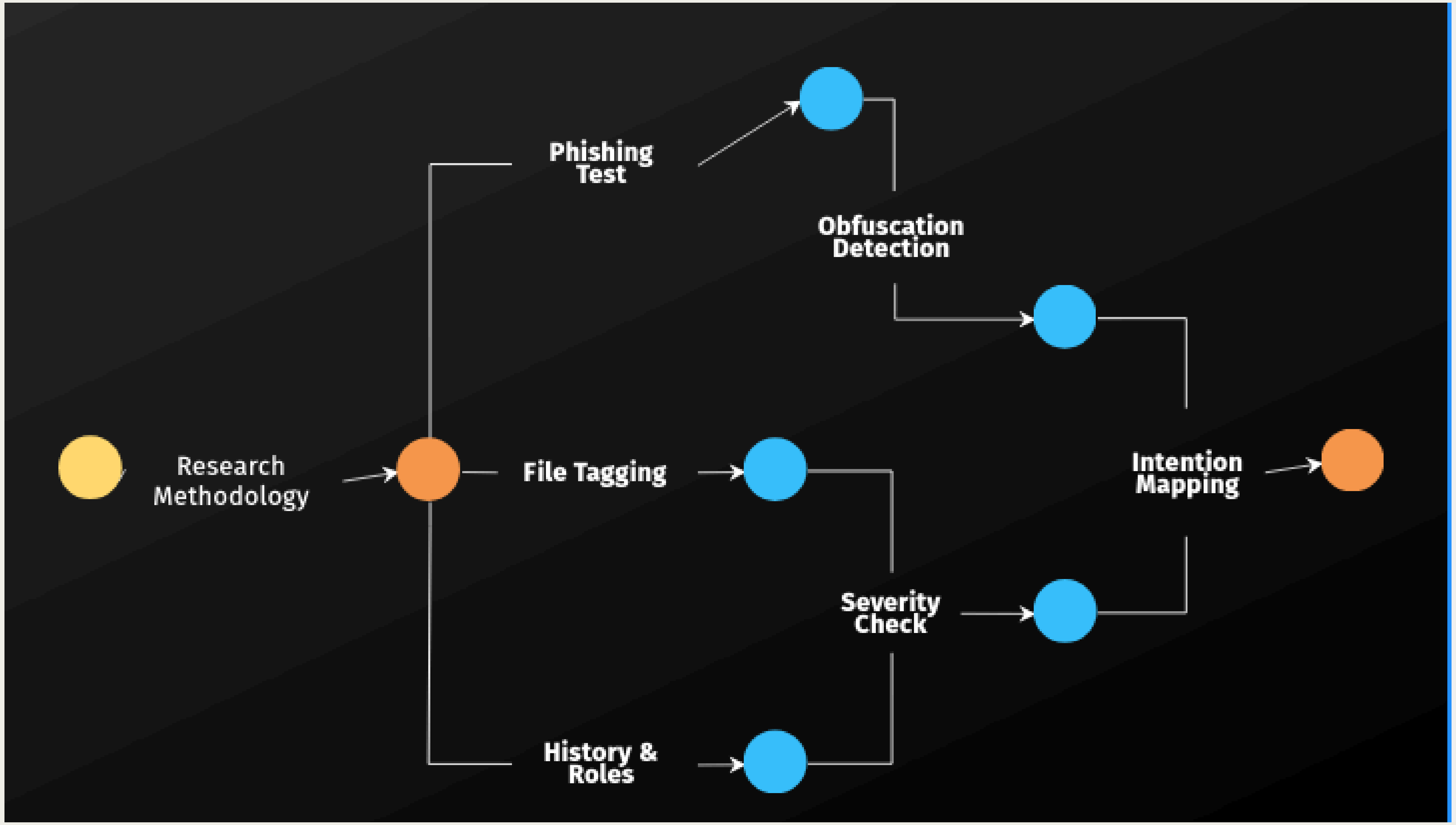


Figure 01 : A PERT chart created to organize the scope and roadmap of the project.

02 : THEORETICAL BACKGROUND

RESEARCH FINDINGS

Detection Approach	Signature Based VS Anomaly Based
Suitability	Static Analysis VS Behavioral Analysis
Customization & Extensibility	Small-scale VS Large-scale
Alerting & Logging	CLI VS GUI

Table 01 : Findings From Literature Review

COMPARATIVE ANALYSIS

Feature	Snort	OSSEC	Security Onion
Detection Type	Signature-based	Log-based + Rule-based	Hybrid (Signature, Anomaly, Log)
Real-time Monitoring	Yes	Yes	Yes
Alerting Mechanism	Real-time alerts via syslog/snmp	Email, Syslog, Custom Scripts	GUI alerts, ELK Stack integration
Type of Data Monitored	Network packets	System logs, file integrity, registry	Network traffic, logs, full packet capture
Custom Rule Support	Strong (custom Snort rules)	Custom rules and decoders	Supports Snort/Suricata rule customization
Ease of Setup	Moderate (requires configuration)	Easy to moderate	Complex (multiple tools, VMs, config)

Table 02 : Comparative Analysis of Existing Tools

03 : PROPOSED MODEL

PROBLEM STATEMENT

This project aims to develop a custom, real time threat detection system tailored for small and medium sized organizations, enhancing security visibility against email-based insider threads.

Keywords : Email Communication, Intent Classification, Rule-based model, Real-time alerting

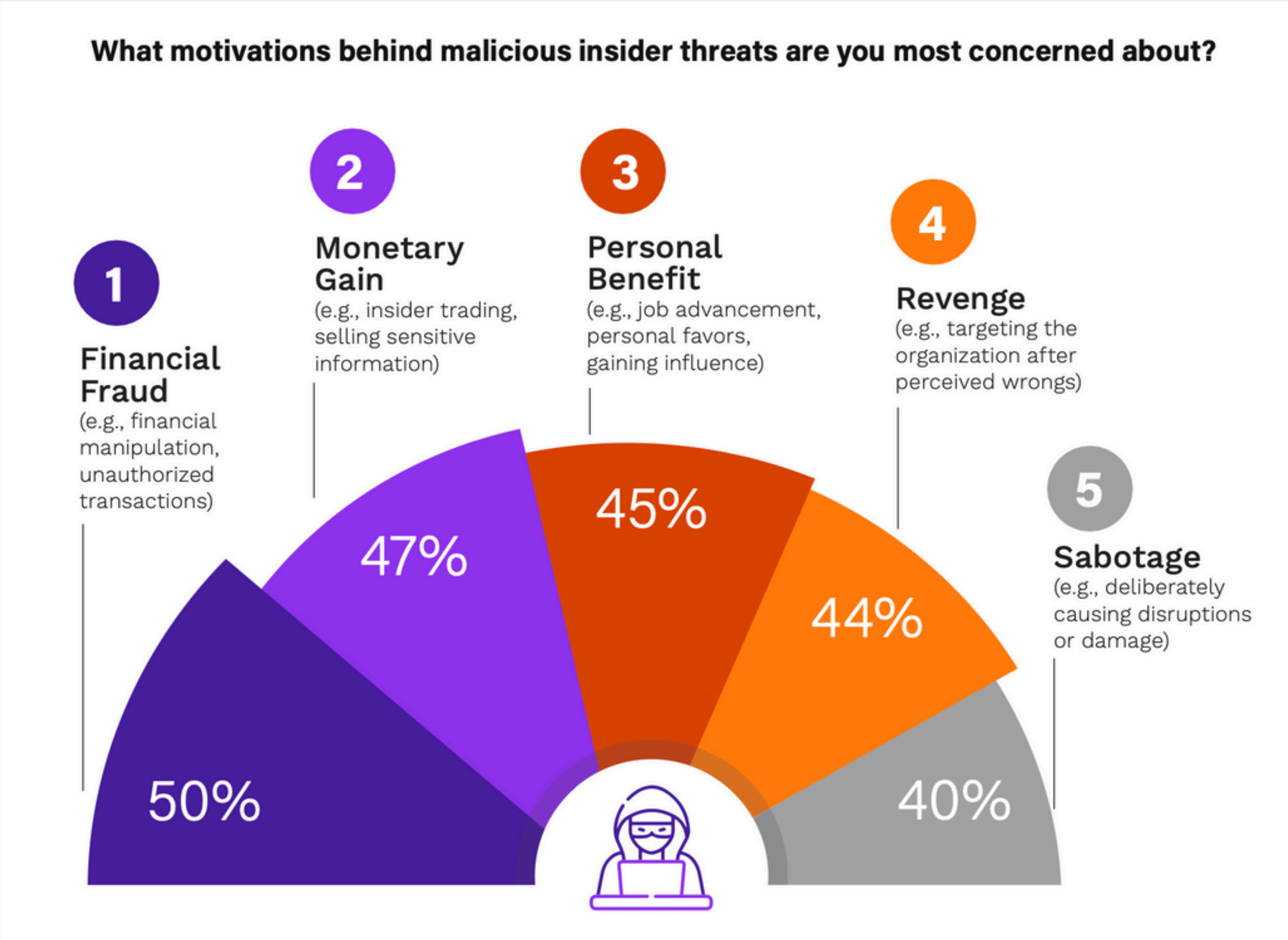


Figure 02 : Motivation Behind Malicious Attackers

“Understanding the Shifting Perceptions of Insider Threats over External Cyber Attacks.” Securonix, 25 Jan. 2024, www.securonix.com/blog/shifting-perceptions-of-insider-threats-vs-external-cyber-attacks/.

FRAMEWORK

Email Monitoring Schedule

Gmail API, Email Headers, Drafts, Forwarded Emails, Signature Attachments

Content & Attachment Analyzer

Static rules engine, File tagging and hashing module, NLP Engine

Behavioral Analysis

Frequency, User Roles, User History, Repeated Actions

Threat Classification

Careless Insider, Malicious Insider, Normal Communication, Severity - High, Medium, Low

Alert & Logging System

CLI, Centralized logging, Real-time

Dashboard/Interface

Incident History, User Activity, Real-time Alerts and Logs

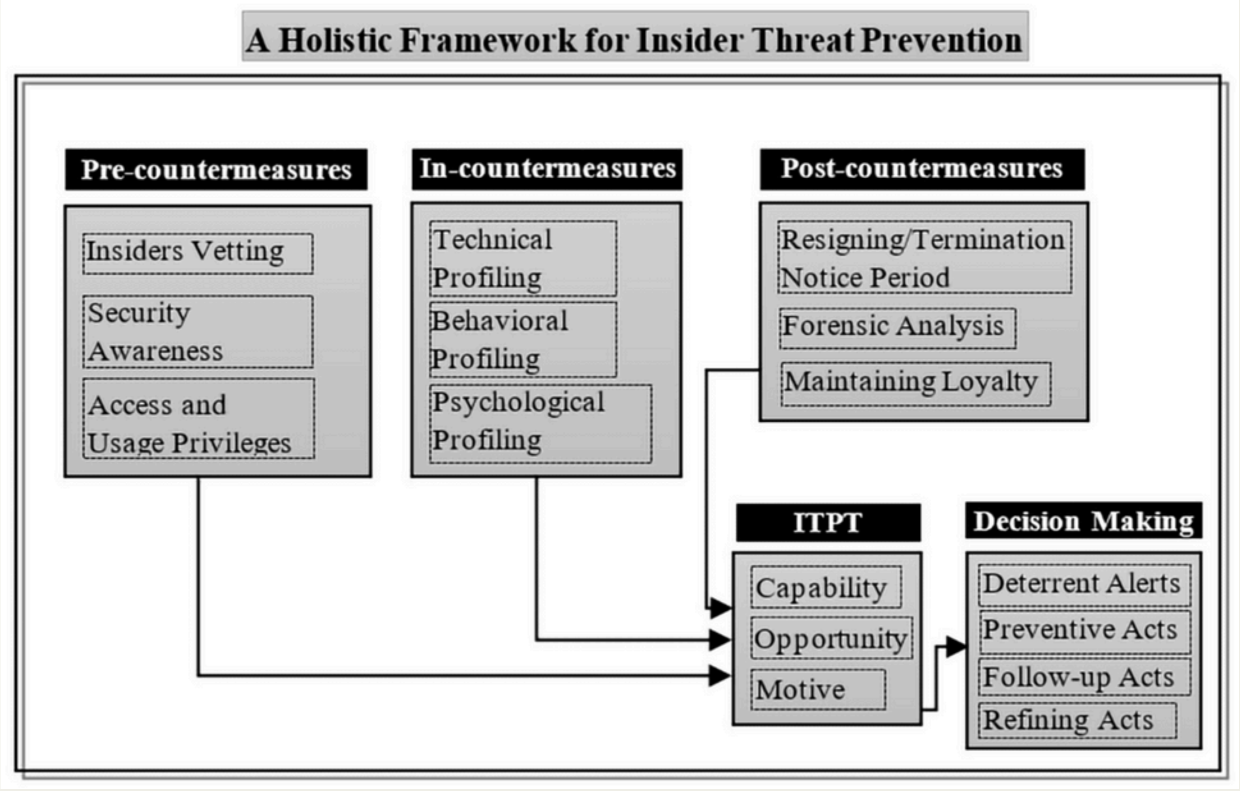


Figure 03 : System Model

Alsowail, Rakan A., and Taher Al-Shehari. “A Multi-Tiered Framework for Insider Threat Prevention.” MDPI, Multidisciplinary Digital Publishing Institute, 22 Apr. 2021, www.mdpi.com/2079-9292/10/9/1005.

METHODOLOGY

Email Monitoring

Sender/Recipient Analysis

Timestamp

Subject

Email Body Attachments

Rule-Based

Static Detection

Phishing Attempts

Misaddressed Emails

Unauthorized File Uploads

File Tagging

Confidentiality

Cross References

Access Control

Signature Protection

Content Matching

Fuzzy Hashing

Hash Database

NLP Based

Classification

Intention - Accidental or Intentional

Severity - High, Medium, Low

User Behavior Analysis

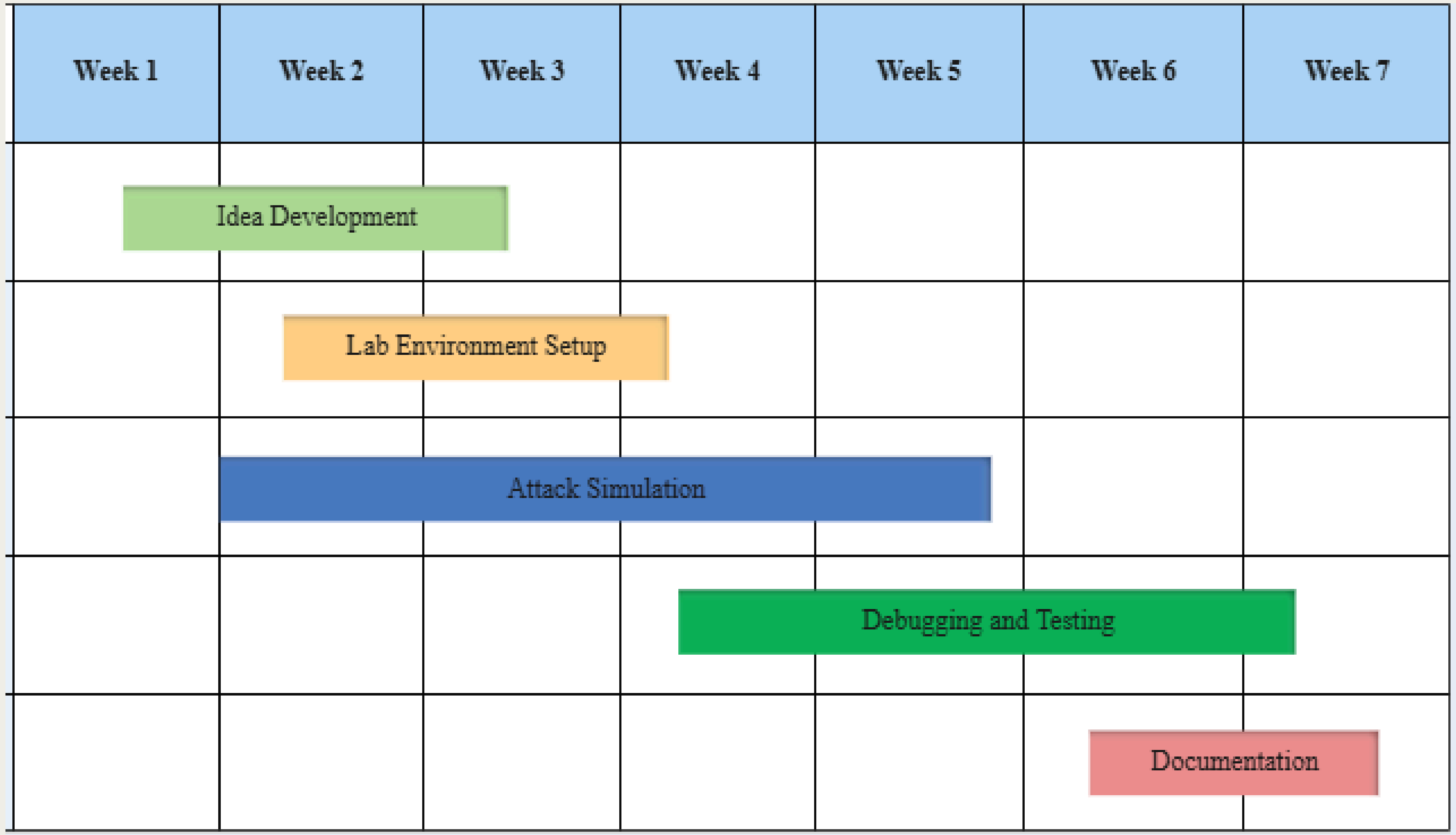


Figure 04 : Gantt Chart

04 : EMPIRICAL RESULT ANALYSIS

EXPERIMENTAL SETUP

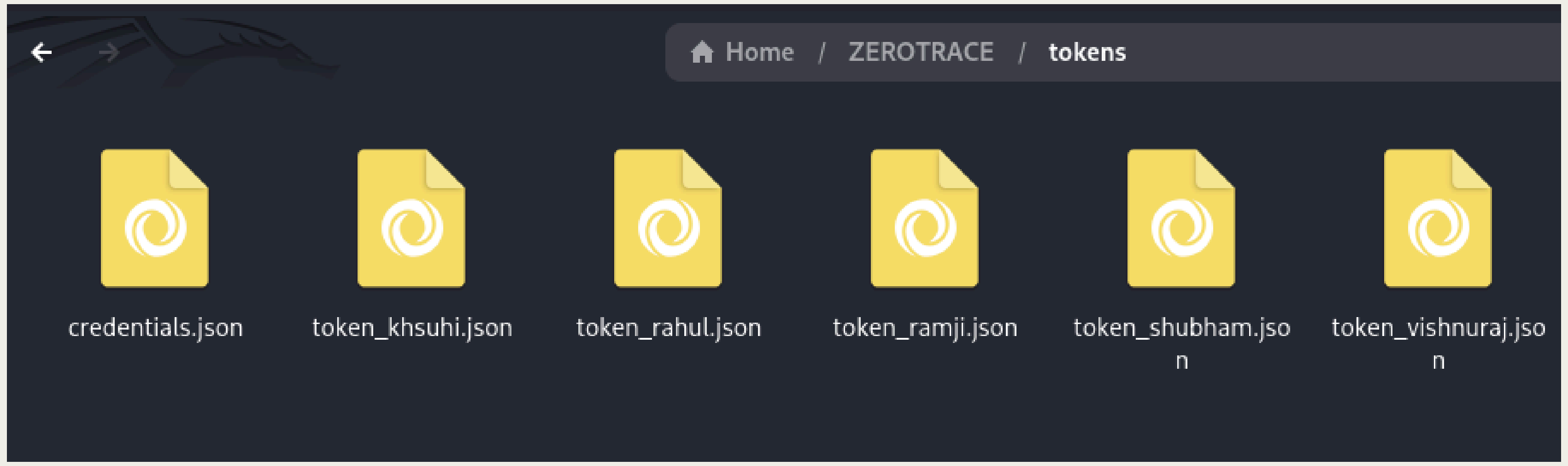


Figure 05 : Authorizing Users

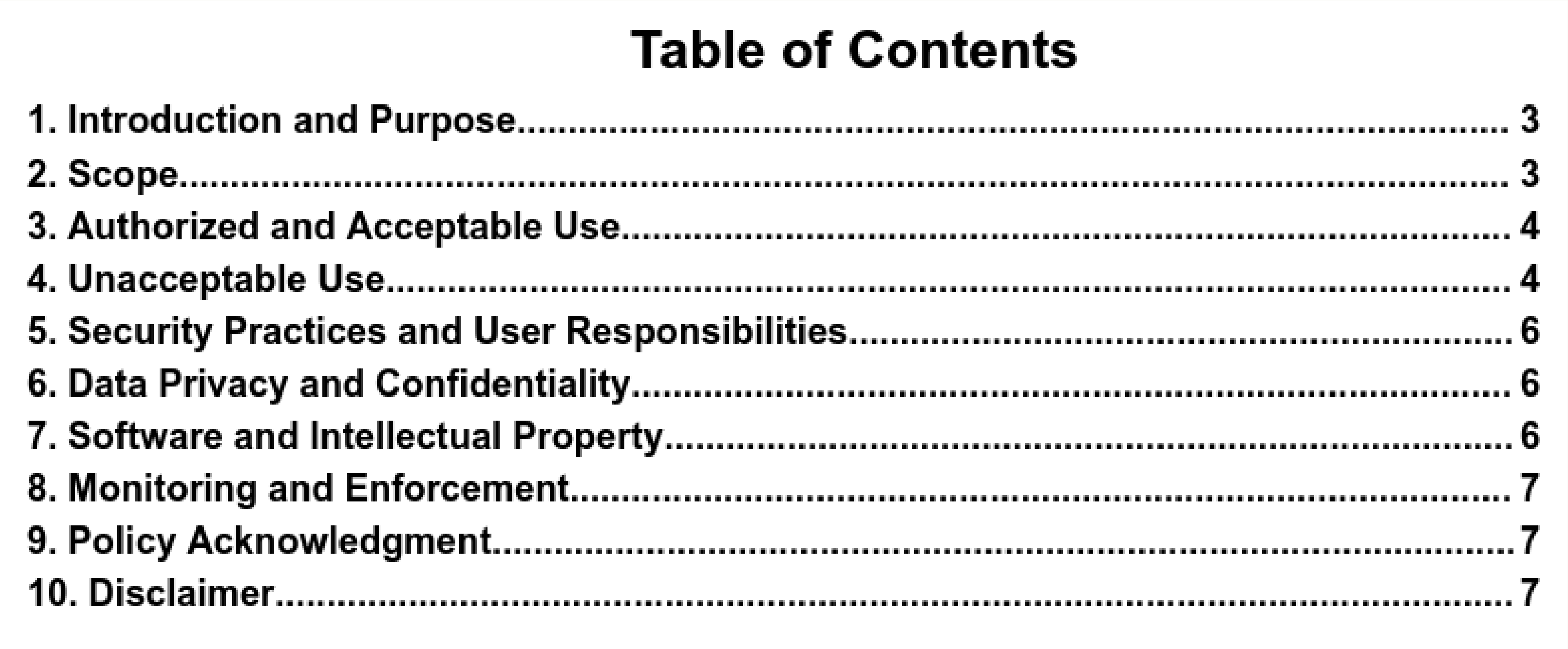


Table of Contents

Figure 06 : Zerotrace Acceptable Usage Policy

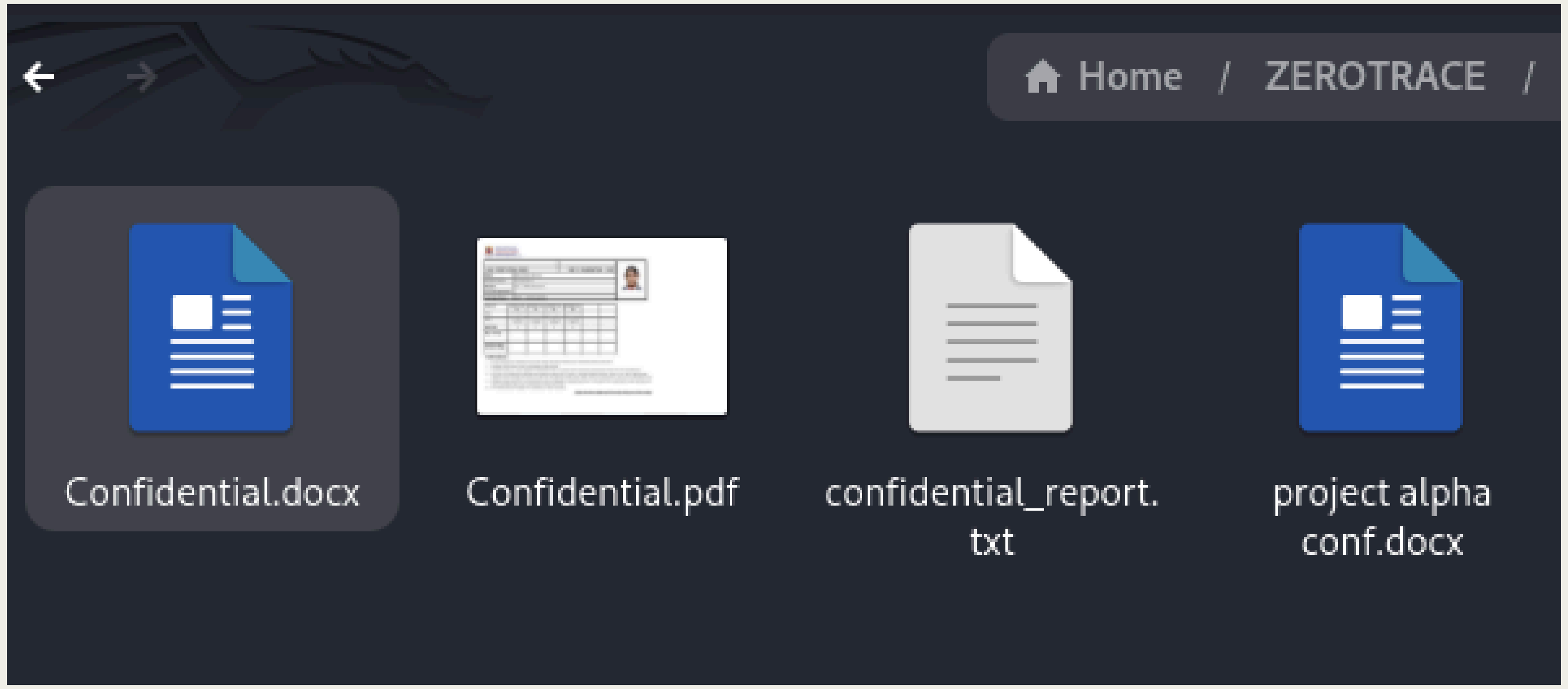


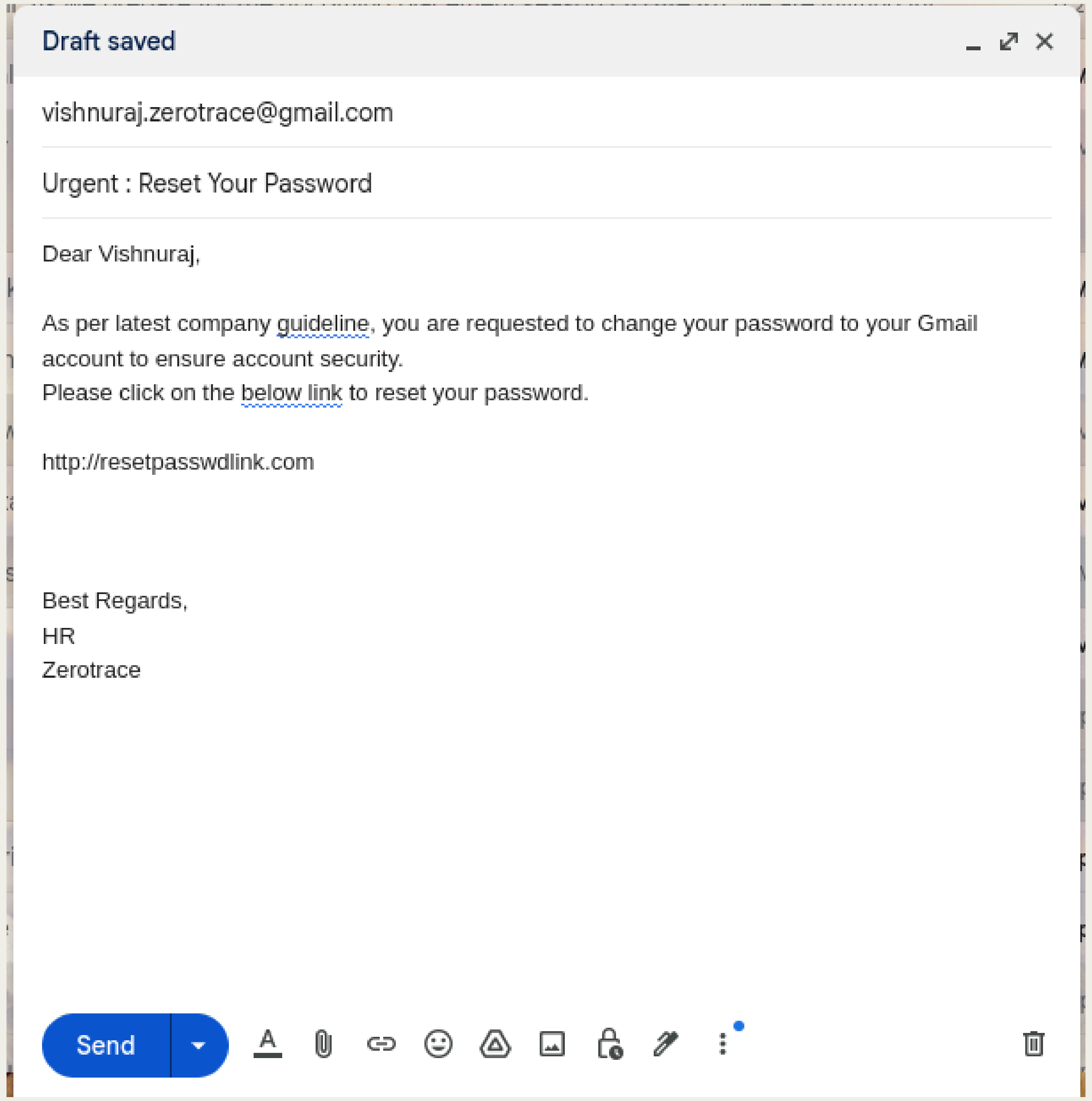
Figure 07 : Confidential Attachments

EVALUATION METRICS

Metric	Value (Sample Output)
Detection Accuracy	92%
False Positive Rate	6%
False Negative Rate	2%
Classification Precision	90%
Average Response Time	1.5 seconds
Severity Scoring Accuracy	95%

Table 03 : Evaluation Criteria and Results

EDGE CASE #1



vishnuraj.zerotrace@gmail.com

Urgent : Reset Your Password

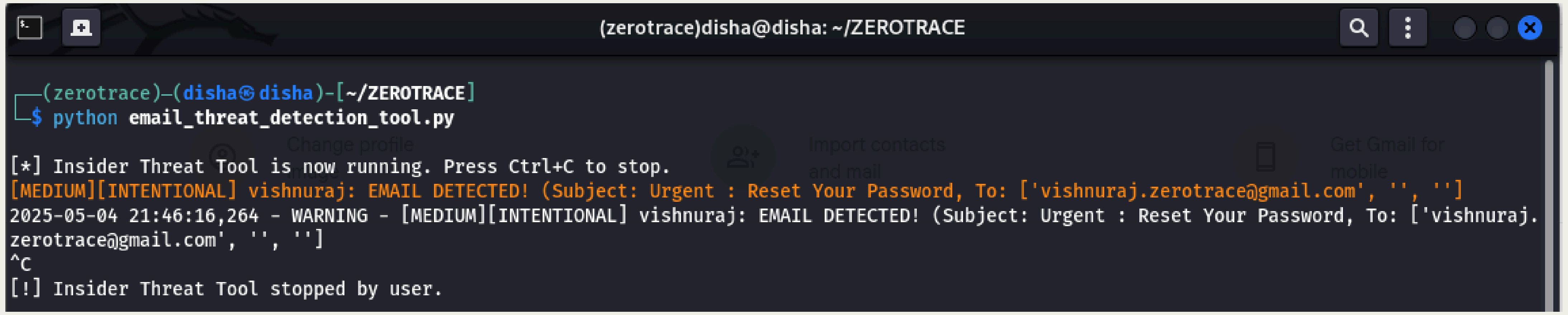
Dear Vishnuraj,

As per latest company guideline, you are requested to change your password to your Gmail account to ensure account security.
Please click on the below link to reset your password.

http://resetpasswdlink.com

Best Regards,
HR
Zerotrace

Figure 08 : Phishing Email



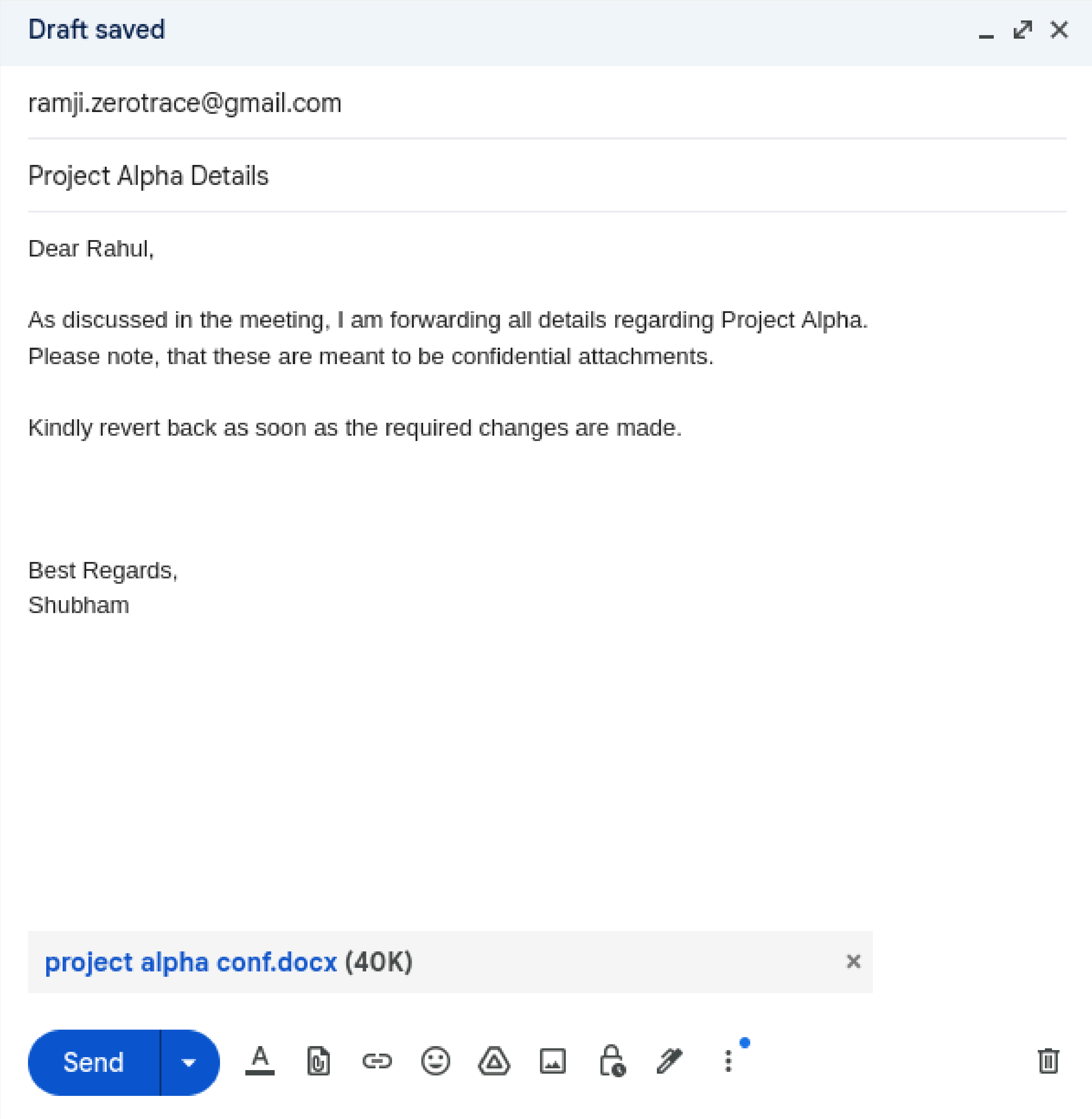
```
┌──(zerotrace)─(disha㉿disha)-[~/ZEROTRACE]
└─$ python email_threat_detection_tool.py

[*] Insider Threat Tool is now running. Press Ctrl+C to stop.
[MEDIUM][INTENTIONAL] vishnuraj: EMAIL DETECTED! (Subject: Urgent : Reset Your Password, To: ['vishnuraj.zerotrace@gmail.com', '', '']
2025-05-04 21:46:16,264 - WARNING - [MEDIUM][INTENTIONAL] vishnuraj: EMAIL DETECTED! (Subject: Urgent : Reset Your Password, To: ['vishnuraj.
zerotrace@gmail.com', '', '']
^C
[!] Insider Threat Tool stopped by user.
```

Figure 09: Alert Detected

Why? - To detect accidental of incidental phishing attempts. External Email, Internal Forwards (repeated), Obfuscation, Encoding

EDGE CASE #2



Draft saved

ramji.zerotrace@gmail.com

Project Alpha Details

Dear Rahul,

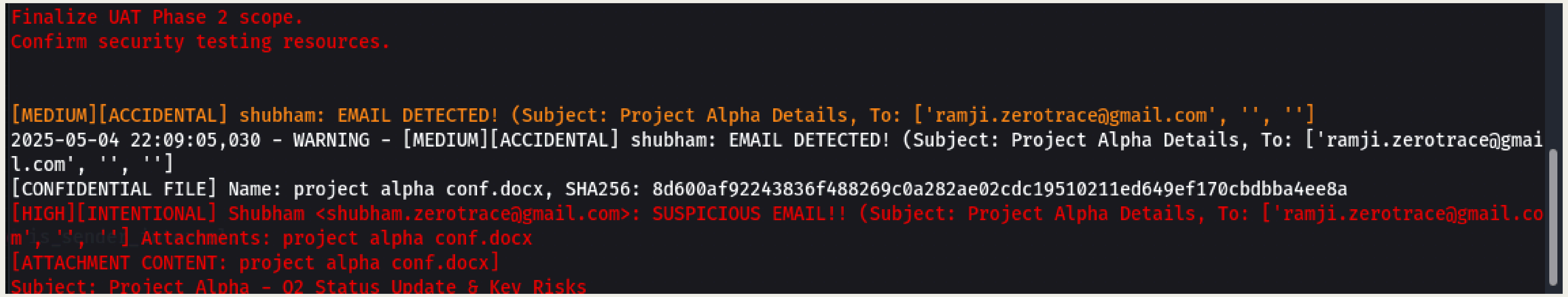
As discussed in the meeting, I am forwarding all details regarding Project Alpha.
Please note, that these are meant to be confidential attachments.

Kindly revert back as soon as the required changes are made.

Best Regards,
Shubham

project alpha conf.docx (40K)

Figure 10 : Misaddressed Email



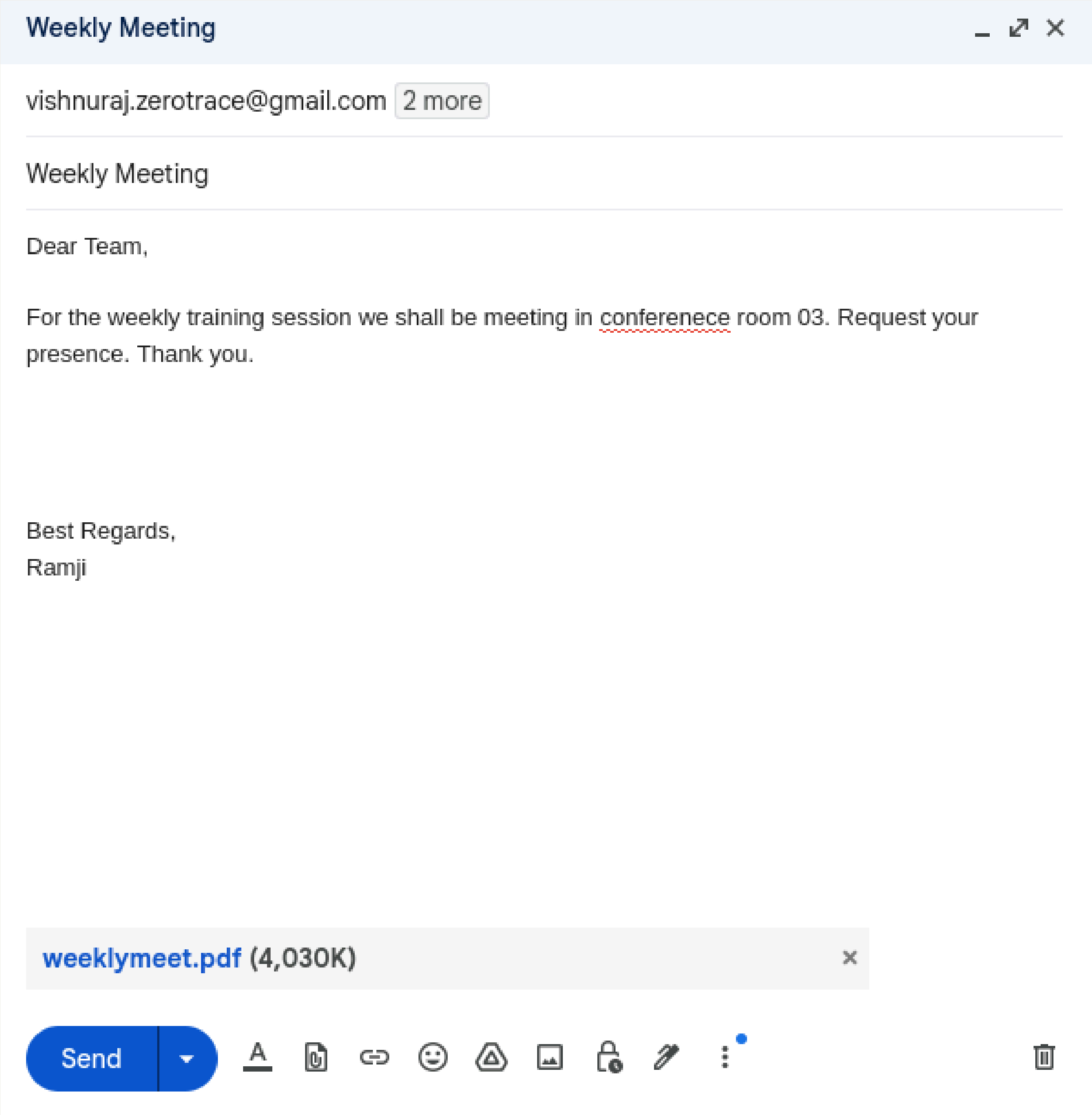
```
Finalize UAT Phase 2 scope.
Confirm security testing resources.


[MEDIUM][ACCIDENTAL] shubham: EMAIL DETECTED! (Subject: Project Alpha Details, To: ['ramji.zerotrace@gmail.com', '', '']
2025-05-04 22:09:05,030 - WARNING - [MEDIUM][ACCIDENTAL] shubham: EMAIL DETECTED! (Subject: Project Alpha Details, To: ['ramji.zerotrace@gmai
l.com', '', '']
[CONFIDENTIAL FILE] Name: project alpha conf.docx, SHA256: 8d600af92243836f488269c0a282ae02cdc19510211ed649ef170cbdbba4ee8a
[HIGH][INTENTIONAL] Shubham <shubham.zerotrace@gmail.com>: SUSPICIOUS EMAIL!! (Subject: Project Alpha Details, To: ['ramji.zerotrace@gmail.co
m', '', ''] Attachments: project alpha conf.docx
[ATTACHMENT CONTENT: project alpha conf.docx]
Subject: Project Alpha - Q2 Status Update & Key Risks
```

Figure 11: Alert Detected

Why? - To detect misaddressed emails (accidental), personal email uploads (intentional), Confidential Attachments, ZIP Attachments

EDGE CASE #3



Weekly Meeting

vishnuraj.zerotrace@gmail.com 2 more

Weekly Meeting

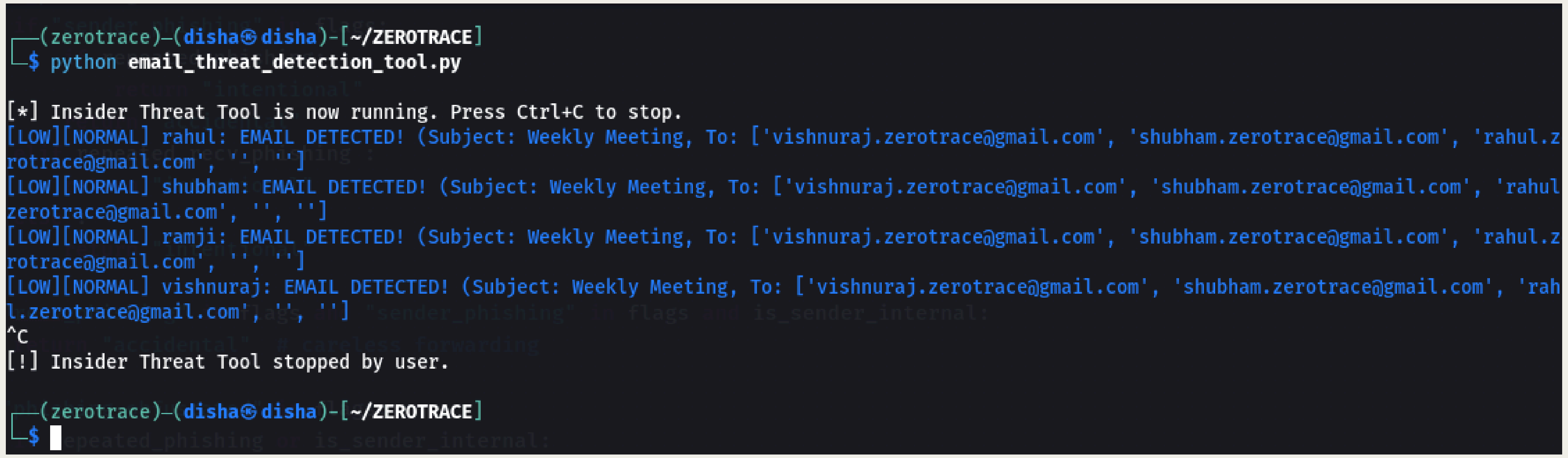
Dear Team,

For the weekly training session we shall be meeting in conferenece room 03. Request your presence. Thank you.

Best Regards,
Ramji

weeklymeet.pdf (4,030K)

Figure 12 : Normal Email



```
┌──(zerotrace)─(disha㉿disha)-[~/ZEROTRACE]
└─$ python email_threat_detection_tool.py

[*] Insider Threat Tool is now running. Press Ctrl+C to stop.
[LOW][NORMAL] rahul: EMAIL DETECTED! (Subject: Weekly Meeting, To: ['vishnuraj.zerotrace@gmail.com', 'shubham.zerotrace@gmail.com', 'rahul.z
rotrace@gmail.com', '', '']
[LOW][NORMAL] shubham: EMAIL DETECTED! (Subject: Weekly Meeting, To: ['vishnuraj.zerotrace@gmail.com', 'shubham.zerotrace@gmail.com', 'rahul
zerotrace@gmail.com', '', '']
[LOW][NORMAL] ramji: EMAIL DETECTED! (Subject: Weekly Meeting, To: ['vishnuraj.zerotrace@gmail.com', 'shubham.zerotrace@gmail.com', 'rahul.z
rotrace@gmail.com', '', '']
[LOW][NORMAL] vishnuraj: EMAIL DETECTED! (Subject: Weekly Meeting, To: ['vishnuraj.zerotrace@gmail.com', 'shubham.zerotrace@gmail.com', 'rah
l.zerotrace@gmail.com', '', '']
^C
[!] Insider Threat Tool stopped by user.

┌──(zerotrace)─(disha㉿disha)-[~/ZEROTRACE]
└─$ 
```

Figure 13: Alert Detected

Why? - To distinguish normal emails from suspicious ones, False Positives

FINAL THOUGHTS

- Distinguishes and Classifies Intention
- Customizable according to Organization’s needs
- Lightweight and Resource Intensive

FUTURE SCOPE

- Machine Learning Integration
- Behavioral Baseline Profiling
- Advanced NLP Techniques
- Multi-Channel Monitoring
- SIEM Integration
- Macro Parsing
- Automated Response

REFERENCES

- Gelman, H., & Hastings, J. D. (2025). Scalable and Ethical Insider Threat Detection through Data Synthesis and Analysis by LLMs. arXiv preprint arXiv:2502.07045. https://arxiv.org/abs/2502.07045
- Koli, L., Kalra, S., Thakur, R., Saifi, A., & Singh, K. (2025). AI-Driven IRM: Transforming Insider Risk Management with Adaptive Scoring and LLM-Based Threat Detection. arXiv preprint arXiv:2505.03796. https://arxiv.org/abs/2505.03796
- Kantchelian, A., Neo, C., Stevens, R., Kim, H., Fu, Z., Momeni, S., … & Poletto, M. (2024). Facade: High-Precision Insider Threat Detection Using Deep Contextual Anomaly Detection. arXiv preprint arXiv:2412.06700. https://arxiv.org/abs/2412.06700
- Gayathri, R. G., et al. (2024). FedAT: Federated Adversarial Training for Distributed Insider Threat Detection. arXiv preprint arXiv:2409.13083. https://arxiv.org/abs/2409.13083
- Zhang, Y., Wang, H., & Li, X. (2023). Insider Threat Detection Based on User Behavior Modeling and Anomaly Detection Algorithms. Applied Sciences, 9(19), 4018. https://www.mdpi.com/2076-3417/9/19/4018

Thank you!

PRESENTED BY : DISHA SHARMA

Enrollment Number : 240103002014

: https://www.linkedin.com/in/disha-sharma-0b9601218/

: https://github.com/Disha0611