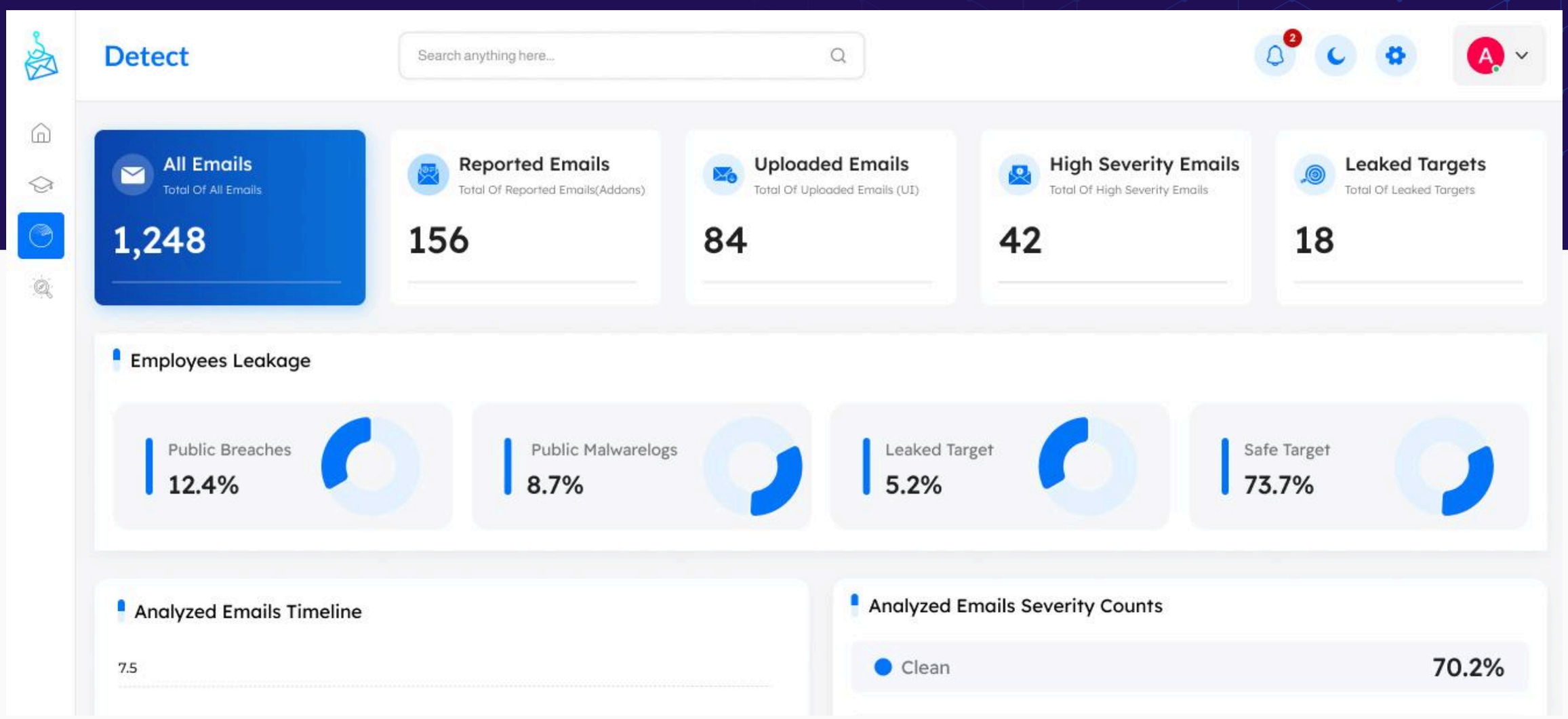
# Detect-Phish

A platform that enables organizations to detect, report, and respond to phishing threats using AI, threat intelligence, and customizable detection rules.

dPhish




## Overview

**Detect-Phish,** a Reported Emails Analysis & Response Platform, which analyzes reported emails, identifies phishing, and responds to the entire phishing campaign as an additional layer of security.

## The Challenge

Statistically, employees report from tens to hundreds to thousands of suspicious emails per month- depending on whether the organization is small, medium, or enterprise - creating a significant analysis workload. Yet, over 90% of these reports are non-malicious, the SOC analysts must review every case, which consumes valuable time and effort

## dPhish's Approach

**01.**
**Detect-Phish** automatically classifies 85% of non-malicious emails and applies the required actions, reducing analysts' workload by 76.5%.

**02.**
**Accurately** identifies 80% of phishing emails reported by employees, providing an additional 8% reduction and achieving a total of 84.5% less analyst effort.

**03.**
**The remaining** 14.5% is supported by detailed automated analysis reports, cutting review time from ten minutes to about one minute per email.

## Feature Matrix

| Features | Value |
|---|---|
| **Email ingestion methods** | • Manual upload (EML/MSG)<br>• API integration<br>• Outlook & Gmail plugins |
| **Detection engines** | • Enriched Object Detection (Logic rules)<br>• IOC feeds integration<br>• Advanced AI classification engine<br>• YARA signature detection |
| **Automated remediation** | • Campaign scoping<br>• Email quarantine<br>• Malicious email deletion |
| **Reporter notifications** | • Real-time preliminary analysis feedback<br>• Final verdict notification to reporter |
| **Reporting & Dashboard** | • Unified analyst dashboard<br>• Trend & behavior analytics<br>• CSV, Excel, PDF exports<br>• Campaign timeline view |
| **Integrations** | • SIEM integration<br>• REST API (SOAR)<br>• LDAP/Active Directory<br>• Single Sign On (SSO)<br>• Web Proxy<br>• Email Gateway<br>• DNS Security |
| **Phishing reporter plugin** | • Outlook<br>• Gmail |
| **Deployment** | • SaaS (Cloud)<br>• On-Premises |

## Key Values

### 01. High Detection Efficiency

- Accurate identification of real phishing attempts by Advanced AI, logic-based rules, YARA signature detection, and threat-intelligence IOCs..

### 02. Reduce SOC Analyst Effort

- Up to 88.5% reduction in manual email analysis workload.

### 03. Easy & Fast Investigation

- Automated analysis reduces investigation time to under a minute.

### 04. Automated Remediation

- Automatically scope, quarantines or removes malicious emails.

### 05. Real-Time Awareness Feedback

- Reporters instantly see the preliminary analysis result.

### 06. Final Verdict Notifications

- Reinforces awareness by sending the final analysis verdict to the reporter.

### 07. Dark Web Intelligence Integration

- Identifies compromised credentials and uncovers unreported phishing activity.

### 08. Unified Dashboard & Insights

- Centralized view for analysts to track trends, user behavior, and incidents.

### 05. SIEM Integration

- Integrate analysis results with your SIEM to generate alerts for phishing-classified reported emails.

### 10. Compatible With Existing Email Security Solutions

- Enhances rather than replaces the current email gateway.