PHISHFACE

Walmart Global Tech

SecOps Dev Team / Project Manager / Scrum Master	Health			Original Deadline	Replanned Deadline
Ajay Gautam / Kyle Cloutier / Andrew Holcombe	Last 🟢	Current ⚫	Trend 🟢	1/26/25	N/A

PhishFace is a machine learning detection system designed to identify phishing attempts aimed at obtaining Walmart network credentials. This mechanism analyzes suspicious URLs detected on the Walmart network, captures screenshots, and notifies analysts for review when the screenshots resemble Walmart webpages.

Summary

Current Status:

- Facefetcher screenshotter service production deployment – In progress (12/16/24)
- Reporting Metrics – In progress
  - Establish KPI reporting pipelines (new campaign, targeted associate phishing, duplicates, False Positives, etc.) – In progress
  - PoC for reporting metrics – Complete
  - Developing for dev environment deployment – In progress
- PhishFace cases in Intel479 – In progress
  - Endpoint is established & prepared to be deployed with Facefetcher prod deployment.
  - Set up a mechanism for analysts' feedback. – In progress

Next Steps:

- Update to Intel479 to ingest new PhishFace cases.
- System to automate the training of new models based on new information.
- PhishFace production deployment in early January. (Changed due to customer requirements changing)

Risks/Issues/Dependencies

Risk:
- N/A
Dependency:
- N/A
Issue:
- Updates needed for alerting pending and due to Change Freeze dates PhishFace prod deployment has to wait until Change Freeze is over in early January, no impact to project end date.

Milestones	Start Date	End Date	Status
Implement New URL Intel Feeds	10/28/24	1/26/25	In Progress
Create PhishFace cases in Intel479 - Case Management	8/29/24	1/26/25	In Progress
Reporting Metrics	12/16/26	1/26/25	In Progress
ML Model Training Corpus Volume	12/30/24	1/26/25	Not Started
Goal 1 - Improve robustness of phishing detection ML model	7/29/24	1/12/25	In Progress
Goal 2 - Establish Semi-automatic labeling for training data based on alerts/feedback	7/29/24	1/12/25	In Progress
Goal 3 - Increase Scalability for Phishing Detection (100k/day)	5/6/24	8/09/24	Complete
Goal 4 – Enable the processing of URLs that have the potential to detect previously unmitigated phishes	10/28/24	1/12/25	In Progress
Goal 5 - Rearchitect System for Greater Engineering & Operational Excellence	10/28/24	1/26/25	In-Progress