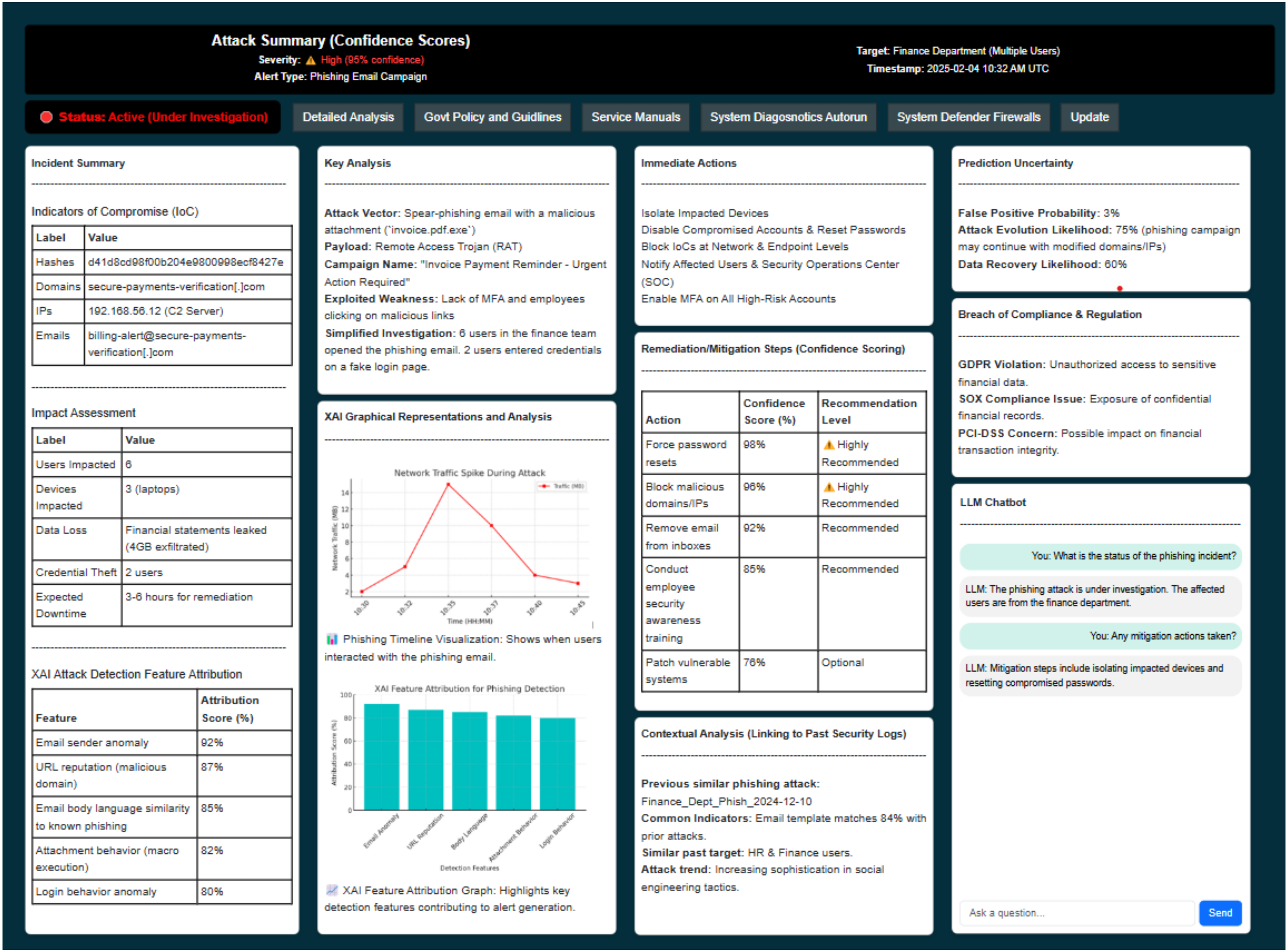

Attack Summary (Confidence Scores)

Severity: ⚠ High (95% confidence)

Alert Type: Phishing Email Campaign

Target: Finance Department (Multiple Users)

Timestamp: 2025-02-04 10:32 AM UTC

● **Status: Active (Under Investigation)**

Incident Summary

Indicators of Compromise (IoC)

Label	Value
Hashes	d41d8cd98f00b204e9800998ecf8427e
Domains	secure-payments-verification[.]com
IPs	192.168.56.12 (C2 Server)
Emails	billing-alert@secure-payments-verification[.]com

Impact Assessment

Label	Value
Users Impacted	6
Devices Impacted	3 (laptops)
Data Loss	Financial statements leaked (4GB exfiltrated)
Credential Theft	2 users
Expected Downtime	3-6 hours for remediation

XAI Attack Detection Feature Attribution

Feature	Attribution Score (%)
Email sender anomaly	92%
URL reputation (malicious domain)	87%
Email body language similarity to known phishing	85%
Attachment behavior (macro execution)	82%
Login behavior anomaly	80%

Key Analysis

Attack Vector: Spear-phishing email with a malicious attachment ('invoice.pdf.exe')
Payload: Remote Access Trojan (RAT)
Campaign Name: "Invoice Payment Reminder - Urgent Action Required"
Exploited Weakness: Lack of MFA and employees clicking on malicious links
Simplified Investigation: 6 users in the finance team opened the phishing email. 2 users entered credentials on a fake login page.

XAI Graphical Representations and Analysis

📊 Phishing Timeline Visualization: Shows when users interacted with the phishing email.

📈 XAI Feature Attribution Graph: Highlights key detection features contributing to alert generation.

Immediate Actions

Isolate Impacted Devices
Disable Compromised Accounts & Reset Passwords
Block IoCs at Network & Endpoint Levels
Notify Affected Users & Security Operations Center (SOC)
Enable MFA on All High-Risk Accounts

Remediation/Mitigation Steps (Confidence Scoring)

Action	Confidence Score (%)	Recommendation Level
Force password resets	98%	⚠ Highly Recommended
Block malicious domains/IPs	96%	⚠ Highly Recommended
Remove email from inboxes	92%	Recommended
Conduct employee security awareness training	85%	Recommended
Patch vulnerable systems	76%	Optional

Contextual Analysis (Linking to Past Security Logs)

Previous similar phishing attack: Finance_Dept_Phish_2024-12-10
Common Indicators: Email template matches 84% with prior attacks.
Similar past target: HR & Finance users.
Attack trend: Increasing sophistication in social engineering tactics.

Prediction Uncertainty

False Positive Probability: 3%
Attack Evolution Likelihood: 75% (phishing campaign may continue with modified domains/IPs)
Data Recovery Likelihood: 60%

Breach of Compliance & Regulation

GDPR Violation: Unauthorized access to sensitive financial data.
SOX Compliance Issue: Exposure of confidential financial records.
PCI-DSS Concern: Possible impact on financial transaction integrity.

LLM Chatbot

You: What is the status of the phishing incident?

LLM: The phishing attack is under investigation. The affected users are from the finance department.

You: Any mitigation actions taken?

LLM: Mitigation steps include isolating impacted devices and resetting compromised passwords.