

Survey on Explainable Security Threat Alerts

This is a 15-20 minute survey to understand how security analysts investigate cybersecurity threats and how **Explainable AI (XAI)** can enhance their workflows as well as threat analysis. The insights from this survey will help shape research on integrating XAI into security dashboards for **better threat detection, response, and mitigation**.

What is Explainable AI (XAI)? Explainable AI (XAI) refers to AI systems that provide **human-readable explanations** for their decisions, helping security teams **understand why an alert was triggered and what analysis can be performed to address the alert**.

Example: Imagine a security tool flags an email as phishing. Instead of just labeling it "Phishing," an XAI-powered system explains:

1. **Feature 1:** The email sender domain is suspicious (92% confidence).
2. **Feature 2:** The URL in the email body is linked to past phishing campaigns (87% confidence).
3. **Feature 3:** The language in the email resembles previous phishing emails (85% confidence).

This level of transparency **helps analysts validate alerts faster** and **reduce false positives**.

Your insights are crucial in shaping the development of more efficient and user-friendly security alert systems. We aim to reduce the complexity of alert handling and support security teams to make faster, more informed decisions.

We value your expert opinion and would appreciate your feedback on the following questions:

* Indicates required question

1. Email *

2. What is your job title? *

3. Name *

4. What is your experience in SOC operations or as a Security Analyst, in number of years? *

Mark only one oval.

- ☐ 1-2 years
- ☐ 2-5 years
- ☐ 5-10 years
- ☐ More than 10 years

Incidence Response and Workflow

5. What are first **3-5 steps** after detecting a cybersecurity alert? Please be elaborate on how you perform root cause analysis and mitigate the threat. *

6. How long does it take on an average to resolve a critical threat? *

7. How do you prioritize alerts? *

Check all that apply.

- ☐ Severity
- ☐ Asset Criticality
- ☐ Past Incidents
- ☐ Threat Intelligence
- ☐ Manual Review
- ☐ Other: _____

Security Tools and Workflows

8. What **security tools** do you currently use? *

Check all that apply.

- ☐ SIEM
- ☐ XDR
- ☐ EDR
- ☐ IDS/IPS
- ☐ SOAR
- ☐ Other: _____

9. What is your **biggest frustration** with your current security tools? *

Explainable AI in Security

10. Have you used **any XAI-powered tools** in your security investigations? *

Mark only one oval.

- ☐ Yes
- ☐ No

11. If yes, which **XAI tools** have you used? (if no say n/a) *

12. If no, what kind of **explainability features** would be helpful? *

Check all that apply.

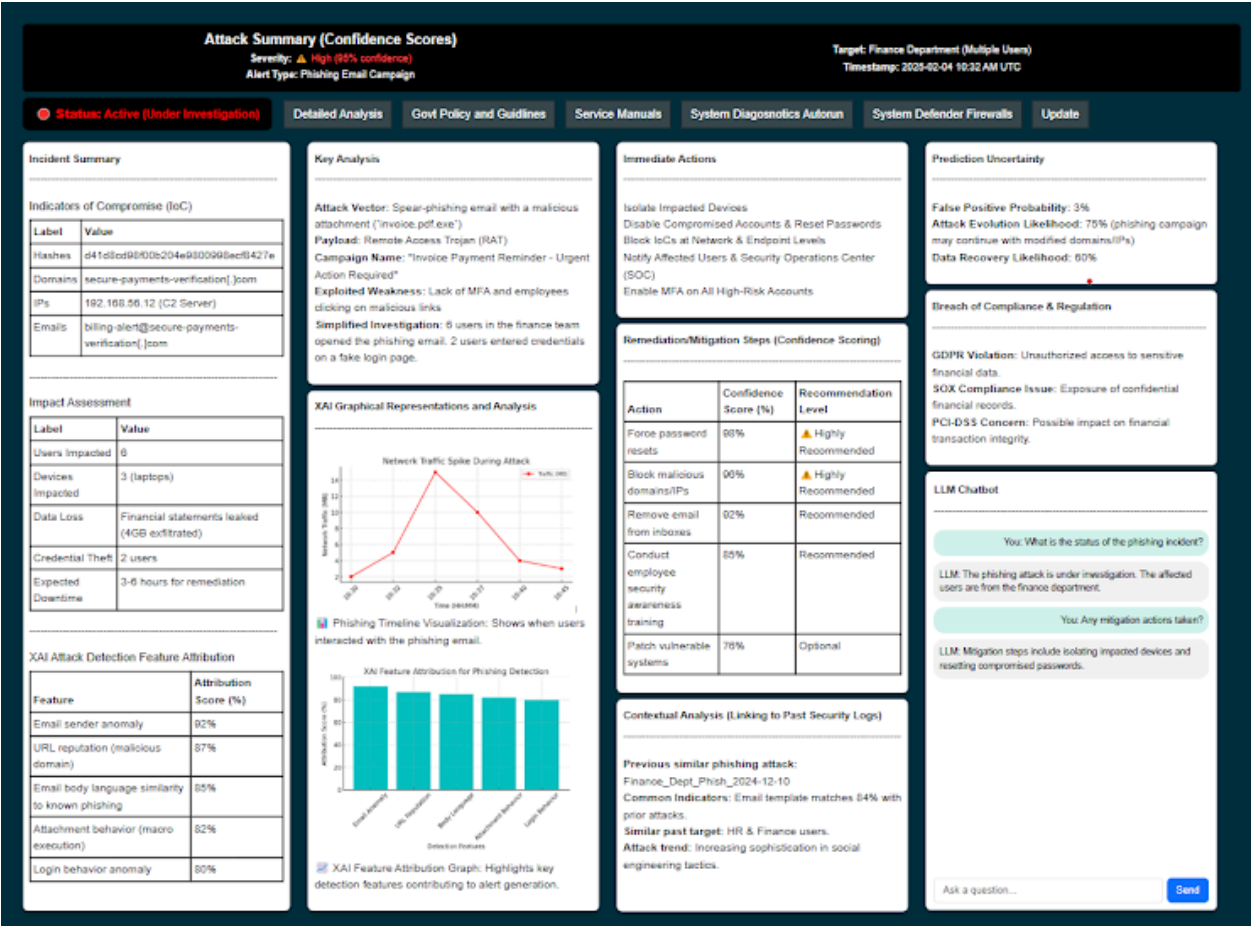
- ☐ Confidence Scores
- ☐ Attack Attribution
- ☐ Alternative Explanations
- ☐ Feature Contribution
- ☐ Other

Feedback on XAI enabled Dashboards

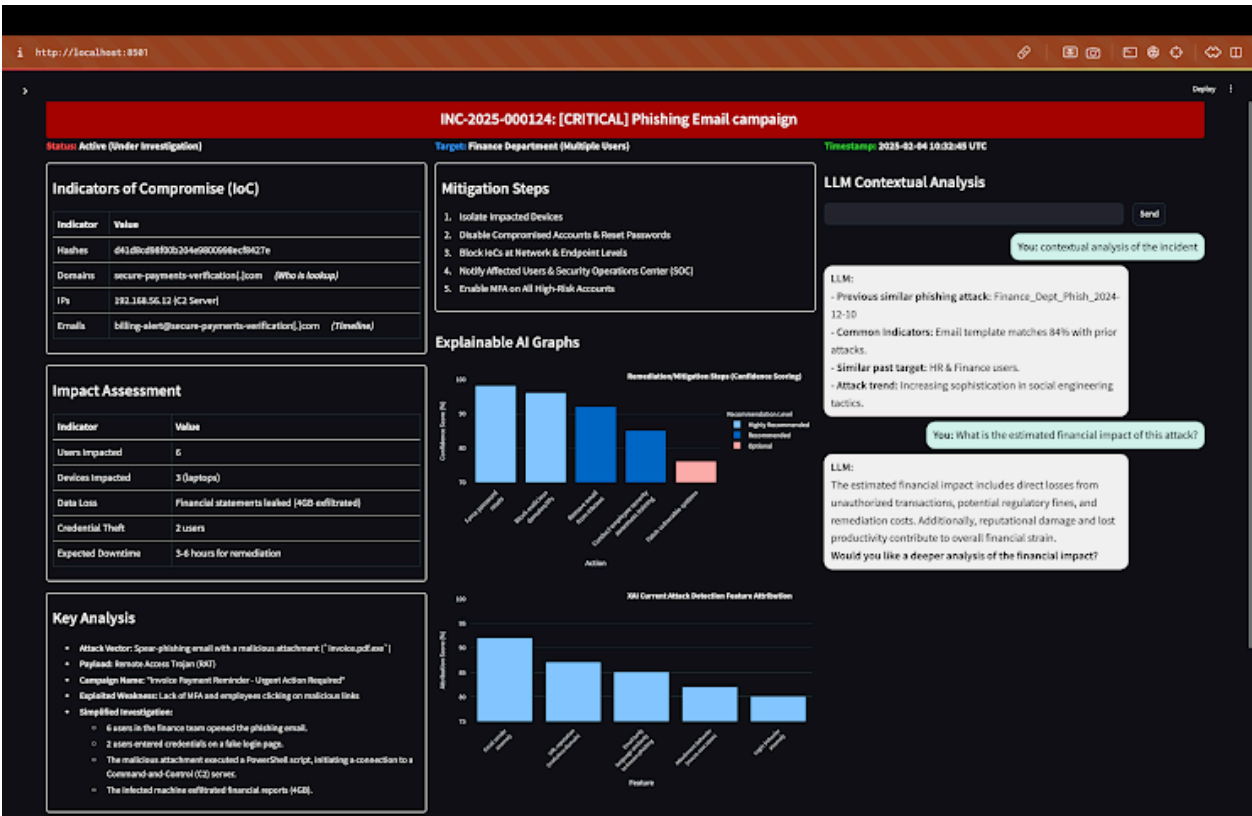
Below are 2 dashboards we've designed for you to envision how XAI can be integrated into a SOC workflow. For example, the XAI Graph Representation and analysis shows important features when phishing is recognized on a client machine.

13. See a SOC dashboard 1 below that we've designed to integrate XAI into your workflows. Which explanations do you prefer and why?

★



14. See a SOC dashboard -2 below. Which explanations do you prefer and why? *



Insights on XAI

15. What challenges do you face when **understanding AI-driven security alerts**? *

16. What are your biggest **concerns** about using AI in cybersecurity? *

17. Will you be open to have a short 30 minute follow-up call with our research team? *

This content is neither created nor endorsed by Google.

Google Forms