Tab 1

https://www.youtube.com/watch?v=EjY26pq9yME

Based on the sources, the person is creating or conducting a **class (session) focused on cybersecurity incident response (IR)**.

Specifically, the current focus of the class is a **deep dive analysis and response process for phishing emails**. The session is titled "Mastering Phishing Email Analysis: Incident Response" and is uploaded on the YouTube channel "SIEM XPERT" [Source Title, 7].

Key aspects of this project/session include:

1. **Incident Focus:** The primary incident being analyzed is a **"possible fishing email delivered"** to an end user. This means the email Gateway failed to block or quarantine the email, allowing it to reach the recipient.
2. **Target Audience and Scope:** The content is primarily aimed at **Security Operations Center (SOC) analysts, especially L1 and L2 staff**, who perform incident response activities on a daily basis (24x7).
3. **Methodology (Analysis and Response):** The class covers the end-to-end process required to analyze and respond to such an incident. The steps discussed include:
    - **Context Identification:** Determining the source IP address, domain name, link, and attachment details.
    - **Evidence Collection:** Asking the user to forward the actual copy of the suspicious email (since it was delivered and is no longer available on the email Gateway for full content review).
    - **Historical Review:** Checking how many other users received the same email based on the source email ID, subject line, or attachment name using email Gateway logs.
    - **Threat Analysis:** Conducting technical checks on the email header, including IP address reputation, domain reputation (using tools like MX toolbox and VirusTotal), and checking for failed SPF, DMARC, and DKIM authentication mechanisms.
    - **Malware Analysis (Attachment/URL):** If the email contains an attachment, analyzing its hash value locally (using PowerShell) or uploading it to a sandbox/VirusTotal to determine if it is malicious (e.g., a Trojan). If it contains a URL, checking the URL and its associated domain/IP reputation.
    - **Action and Containment:** If the email is confirmed malicious, the response includes isolating the infected system from the network, disabling the network ID for unreachable users, asking users to permanently delete the email, and submitting the malicious file/hash to the antivirus vendor to update signatures.

In essence, the project is a **training module for cybersecurity professionals demonstrating the procedures for investigating and neutralizing a successful phishing attack**.

Based on the sources, the person is creating or conducting a **class (session) focused on cybersecurity incident response (IR)**.

Specifically, the current focus of the class is a **deep dive analysis and response process for phishing emails**. The session is titled "Mastering Phishing Email Analysis: Incident Response" and is uploaded on the YouTube channel "SIEM XPERT" [Source Title, 7].

Key aspects of this project/session include:

1. **Incident Focus:** The primary incident being analyzed is a **"possible fishing email delivered"** to an end user. This means the email Gateway failed to block or quarantine the email, allowing it to reach the recipient.


FORTIFY

The project is an **IOC Reputation Checker Tool**, designed primarily for **Security Operations Center (SOC) Analysts, specifically L1 and L2 personnel**, who perform the critical daily activity of incident response and deep-dive phishing analysis. The **why** for building this project is to automate and expedite the often repetitive process of analyzing Indicators of Compromise (IOCs) extracted from suspicious emails (such as the Source IP address, domain names, or attachment hash values). Since an analyst must confirm whether an email is malicious by checking multiple parameters and external reputation tools, this tool streamlines the process, transforming fragmented data into a cohesive and actionable summary that allows the analyst to quickly classify the incident and move forward with necessary containment steps, like isolating an infected system or blocking the malicious source.

The key features implemented in vanilla Python logic would include:

- **IOC Input Handling:** Accepting IP addresses, domains, URLs, or file hash values as input.
- **Reputation Lookup Simulation:** Simulating external checks (like those performed using MX Toolbox or VirusTotal conceptually) to determine if the IP or domain is flagged by threat intelligence feeds or blacklists.
- **Header Analysis Logic:** Checking for tell-tale signs of spoofing or maliciousness by analyzing simulated authentication mechanisms like SPF and DMARC failures, which are crucial indicators in phishing attempts.
- **Attachment Verification:** Using the hash value (e.g., SHA256 or MD5) to verify if the attached file is known malware, such as a Trojan.
- **Summary Generation:** Providing a final, clear conclusion on whether the indicator is malicious, based on the aggregated findings, to aid immediate decision-making.

Tab 2

Tab 3