Scenario: PHISHING
Inject 11

Role: ***INFORMATION TECHNOLOGY***

Detail:

- The incident responder's forensic review revealed the following information:
  - Finance received an email, purportedly from a trusted vendor, asking for a review of an invoice. An employee clicked on the link, causing a malicious file to be downloaded to the Organization's network.
  - The file remained undetected and was used by hackers to conduct reconnaissance and password stealing for several days before the hackers became operational.
  - Hackers used administrative privileges to execute their attack and gain access to the building automation system, phone system, and multiple computers on the network.

What do you do with this information?

CISA Cybersecurity Performance Goal:
Log Collection (2.T)