Username LabUser

Pass Passw0rd!

Engineer is stealing IP (employee has not been authorized)

First thing we look for is proprietary information

copy and paste the task into the assignment

\*\* Be careful on the "HOW" this is not an SOP \*\*

\*\* Additional resources in the material for the chapter \*\*

A. Create an investigative plan of action based on forensic best practices or standards that your team will implement by doing the following:

1. Discuss the strategy that your team will use to both maximize the collection of evidence and minimize the impact on the organization.

Team needs briefed, expectation/level setting, the why. The team will need to identify the initial point of reporting. Identify

Brief the team, they will need a clear understanding of the task at hand prior to beginning any work. They need to understand as much about the scope of impact as possible. This will assist with preventing any scope creep during the initial investigation. Keeping the team aligned to a common goal enables to the team to work autonomously while striving for the same outcome.

2. Describe the tools and techniques your team will use in evidence gathering, preparation, and analysis.

Address the maximize of collection, right into secure the scene and chain of custody. Example we see login to two machines, take them off the network to isolate and contain. Minimizes the impact to the organization, they org now knows they have the rest of the network to work with.

Secure the scene – swiftly securing the scene allows for a more thorough collection of data and data artifacts. The more quickly a scene can be secured the better, preventing time for an attacker to have to clean up. This also helps to minimize the impact to the organization. By identifying the hosts that are impacted allows the teams to quickly identify what they are working with.

3. Describe how your team will collect and preserve required evidence, using standardized and accepted procedures.

Not here to get super technical. We know that the incident is going to need a memory acquisition, may need a write blocker to capture volatile mem, then hard drive. FTK for a bit-by-bit copy, don't take a chance with the data. Electron evidence examiner (e3Tool).

Conduct memory – write blocker – collect this information first

Move then to hard drives, copy with DD (bit by bit). Restress integrity (FTK works for this as well) Provide details for functionality at 30,000 feet, the why, not so much the how.

E3Tool to conduct analysis

Standardized and acceptable procedures.

4. Describe how your team will examine the seized evidence to determine which items are related to the suspected violation of company policy.

This step is a bit redundant; this is to preserve the chain of custody. E3Tool again, \*Key word search\* for proprietary information. Based upon research of additional resources. Based off claim of policy violation. Scientific manner, maintain integrity of drive, make sure no evidence corruption, ties back to secure the scene.

5. Discuss an approach that your team will use to draw conclusions based on the digital evidence that supports the claim of a policy violation.

Solidify the evidence, how does it prove anything.

Punctual, matter of fact.

Final write-up will need legal approval.

Then on to a power point for presentation.

6. Discuss how the case details and conclusions should be presented to senior management.

Who is senior management, target audience is non-technical, or less technical, needs to address who, what, where, when, why? Punctual and to the fact. Possibly need to run through HR to adhere to company policy, as this can have legal ramifications.

Acknowledgement of sources used, demonstrate professional communication.