Dive into the world of cybersecurity incident detection and response.

Answer Key P2C2

In the initial stages of the investigation, you must first understand what is happening and whether the activity is truly malicious. To achieve this, identify what the software aims to do, where it originates from, and whether it attempts to conceal its actions:

- What is the purpose of the suspicious program?
  - You can test it in a sandbox to verify if its actions match those of the legitimate program.
- How was this program executed?
  - Is it automatic or manual? Is this the usual method of executing this program?
  - What account launched the program?
- Are there any attempts to conceal its execution?

Focus on these key questions!

In the next phase, you need to understand:

- What damage has already been inflicted on the organization?
  Look through **application logs** (in this case, the backup system) to check if the attacker modified or accessed sensitive data within the backups.
- How did the attacker gain access to the server?
  Review system logs to determine how the program was launched, by whom, and how the user connected.
- How did the attacker penetrate the information system (SI)?
- Trace the connections through **network equipment and directory logs** to understand the attacker's entry point.
- Did the attacker affect other systems?
- Check **the EDR or SIEM for IoCs** (Indicators of Compromise) you have identified.

By following these threads, you can determine the potential ongoing impacts the attacker could leverage and assess their level of access.

It's more effective to follow the leads you have rather than searching aimlessly across the entire SI. Your detection mechanisms will assist in identifying malicious behaviors linked to your investigation.

Investigation Outcome

By tracking these paths, you discover that:

- The malicious software's objective is to steal credentials from other users connected to the machine.
- The attacker accessed the server using the local administrator's account, which was stolen from another compromised server.
- This other server was compromised through a known vulnerability.
- The attacker entered the SI via VPN, using the account eve.lefevre@meditronique.com, whose passwords had leaked online.