Dive into the world of cybersecurity incident detection and response.

Answer Key P2C1

The questions to ask to qualify Charlie Dupont's login attempts are, in order of priority:

- "Are there any ongoing investigations regarding Charlie Dupont?" "Or concerning the IP address used for the login attempts?"
- "Can I contact Charlie Dupont within 5 minutes to confirm if it's really him logging in?" Directly calling Charlie can help clarify quickly.
- "Has Charlie Dupont recently changed his password?" Recent password changes can be quickly checked in the SIEM system.
- "What is the IP address associated with the login attempts?" This might give you some context, but it's not a high priority.
- For this type of alert, you don't need much additional context. The key question is: is Charlie the one logging in?

2. To assess Alice Martin's impossible travel alert, first verify the details and any ongoing investigations concerning the alert:

- "Does this user typically connect from this country?"
- "Are there any alerts or investigations involving the same IP address?"
- "Any alerts with the account alice.martin@meditronique.com?"
- "What do these two IP addresses correspond to?" A possible explanation could be the use of a VPN. "Is the French IP address from the VPN?"

- "What devices are connected? Is it the same device Alice usually uses to connect?"
- A quick look at Alice's schedule might help determine if she is indeed in Morocco. She might have also informed her management or Human Resources about her trip.
- However, don't start analyzing her workstation or other data sources. If necessary, it means you need to investigate the incident!

3. To determine if the suspicious software should be investigated:

- "Are there any alerts or investigations involving the same suspicious file name?"
- "Is the suspect program known to the IT department?" Check the context provided by the IT team.
- "Are there similar alerts or investigations on this server?"
- "Are any operations planned by the IT department on this server?" Review the scheduled operations and any related server information.
- If none of these checks provide a conclusion, an investigation is necessary to find out more.
- Here too, don't start analyzing the code or searching through the SIEM—this is the purpose of an investigation!

After completing these steps within about 10 minutes, you've identified:

- that Charlie Dupont changed his password before going on vacation and indeed forgot it;
- that Alice Martin and her entire department are on a corporate seminar in Morocco. She likely connected via Méditronique's VPN while simultaneously connecting on another device (such as a phone). You may opt to launch an investigation with reduced urgency to confirm this;
- that the suspicious software has not been identified, so you initiate an investigation with high priority.