Dive into the world of cybersecurity incident detection and response.

Answer Key P2C4

Criteria / Asset	Account eve.lefevre@meditronique.com and local admin account	Backup server	Obsolete server
Ease of reconstruction	Medium	Complex	Simple
Ease of cleaning	Simple	Simple (investigation already done)	Complex
Security status before the incident	N/A	Good	Poor
Impact of unavailability	Low	Significant	Medium
Decision	**Cleaning**	**Cleaning**	**Reconstruction**

- The account eve.lefevre@meditronique.com is easy to clean: simply reset the password and verify the attribute changes. Reconstructing the account would mean giving Eve Lefevre a new account, which would require reconfiguring everything again, taking more time. So, the easiest option is to clean the account. The same applies to all other accounts retrieved by the attacker.
- The backup server has already been investigated, so part of the cleaning work has already been done. It is critical for backups, making it more complex to reinstall, and its unavailability would be more disruptive. Therefore, cleaning it is the simplest option.
- The obsolete server was vulnerable, so if you choose to clean it, you will also need to fix the vulnerability. No investigation has been carried out on it, making it easier to reinstall. Thus, the simplest option is to reconstruct it.