QUIZZ W0_ITW3 (INTERVIEW THIBAULT COULLET) (7/7 points)

Rappel : la valeur NA indiquée à la fin de chaque question correspond au nombre de réponses attendues.

Question W0.ITW3.1: the main role of a Security Operations Center (SOC) is to perform: (NA=1)

- ○ fault management
- ○ configuration management
- ○ accounting management
- ○ performance management
- ⦿ security management ✔

Question W0.ITW3.2: which management tool is used for collecting, indexing and correlating events and informations related to security? (NA=1)

- ○ IETF
- ⦿ SIEM ✔
- ○ TLS

Question W0.ITW3.3: in which of these cases do we have a false positive? (NA=1)

- ○ an intrusion detection system indicates no intrusion, while there is an intrusion.
- ⦿ an intrusion detection system indicates an intrusion, while there is no intrusion. ✔
- ○ an intrusion detection system indicates no intrusion, and there is no intrusion.
- ○ an intrusion detection system indicates an intrusion, and there is an intrusion.

Question W0.ITW3.4: the operational processes of the security operations center (SOC) rely on security norms, such as: (NA=2)

- ☑ ISO 27001
- ☐ IEEE 802.11i
- ☑ ITIL
- ☐ None

✔

Question W0.ITW3.5: the escalation of a security event consists in circumventing the security issue. (NA=1)

- ○ true
- ⦿ false ✔

Question W0.ITW3.6: digital forensics methods are used to support security management: (NA=1)

- ○ before an incident
- ⦿ after an incident ✔

Question W0.ITW3.7: a company cannot have both an infrastructure management team and a security management team. (NA=1)

- ○ true
- ⦿ false ✔

Vous avez utilisé 1 essais sur 3