1. Which of the following would be implemented on a server to BEST protect documents stored at rest?

A File integrity monitoring.

B File encryption.

C Traffic encryption.

D Anti-malware software.

1. Which of the following statements is TRUE for the process of mutual authentication?

A Two remote systems authenticate each other at the same time.

B Two remote systems authenticate each other in sequence.

C Three or more remote systems authenticate each other at the same time.

D Three or more remote systems authenticate each other in sequence.

1. A user who does not usually do remote working needs to work on some documents over the weekend. They have been given permission to copy the documents onto a USB stick to take home. Which of the following would be the BEST solution to ensure any files saved to the USB stick are not compromised in the event it is lost?

A Removable media encryption.

B Data loss prevention.

C Trusted platform module

D File encryption.

1. An appropriate level of which of the following would BEST provide protection against a man-in-the-middle attack?

A File encryption.

B Device encryption.

C Traffic encryption.

D Database encryption.

1. A public facing website using HTTPS is likely to first deter a potential attacker at which stage of the MITRE ATT&CK chain?

A Initial access.

B Execution.

C Persistence.

D Exfiltration.

1. Educating users to guard against spear phishing is an example of a defence against which stage of the MITRE ATT&CK chain?

A Initial access.

B Privilege escalation.

C Defence evasion.

D Credential access.

1. When selecting a payment processor to take credit card payments, which accreditation would be MOST important for the processor to hold?

A.ISO-27001:2013.

B Cyber Essentials +.

C CREST.DPCI-DSS.

1. A supplier is ISO27001 certified. Which of following are they LEAST LIKELY to have in place ?

A The ability to securely take card payments.

B An annual penetration testing programme.

C An appropriate process controlling user authentication.

D Antivirus software that updates daily.

1. Which of the following, if not enabled, could lead to a man-in-the-middle attack?

A Network firewall.

B Traffic encryption.

C DNS filtering.

D Data loss prevention.

1. Which of the following is MOST LIKELY to be a benefit of an open source security solution?

A Products are more scalable.

B Products are more stable.

C Products have better support.

D Products are highly editable and configurable.