1. To ensure network connection events are detected in a Windows Active Directory, what technology COULD be used?

A IPS module on an internal firewall.

B Antivirus on the user device.

C HIDS agent on the Domain Controller.

D Network traffic monitoring.

1. Which of the following provides the BEST integrity when implementing a Full Disk Encryption (FDE) solution for an end-user laptop?

A Trusted Platform Module (TPM).

B Hardware Security Module (HSM).

C Public Key Infrastructure (PKI).

D Advanced Encryption Standard (AES).

1. Which of the following would be the BEST method of receiving confidential documents from a number of clients where confidentiality is the main concern?

A E-mail.

B SFTP server.

C Drop Box.

DFileShare.

1. An internal web server requires only HTTPS access from the internet. Protecting the server from unauthorised access attempts to other services would BEST be achieved by which of the following?

A Locating the web server inside a DMZ.

B Configuring the perimeter firewall.

C Installing antivirus on the web server

D Enabling multi-factor authentication on the web server.

1. Session management is a mitigation for which of the following risks which can be exploited in the collection stage of the MITRE ATT&CK model?

A Man-in-the-browser.

B SSH hijacking.

C Forced authentication.

D Multi-layer encryption.

1. Which of the following should be restricted internally as it is MOST LIKELY to be exploited in the lateral movement stage of the MITRE ATT&CK chain?

A Remote access tools.

B Commonly used port.

C Windows Remote Management.

D Uncommonly used port.

1. Which ofthe following would a cyber security professional require a CREST certification to be qualified to do?

A Configure a network firewall.

B Operate a SIEM.

C Deploy e-mail security

.D Conduct a penetration test.

1. What is the biggest disadvantage of IPS when compared with IDS?

A It is passive in nature.

B It is reactive in nature.

C It does not take action based on alerts.

D It can take action based on false positives.

1. For a public facing website to be compromised, which of the following is MOST LIKELY to be absent or poorly configured?

A Network traffic monitoring.

B Web application firewall.

C DNS filter.

D Traffic encryption.

1. Which of the following is MOST LIKELY to be a disadvantage of an open source security solution when compared to an equivalent commercial product?

A Products are not easily configurable.

B Products do not offer auditing facilities.

C Products are only community supported.

D Products are expensive to license.