Why is normalizing log data important in a centralized logging setup? **1 / 1 point**

- ○ Log normalizing detects potential attacks.
- ◉ Uniformly formatted logs are easier to store and analyze.
- ○ The data must be decrypted before sending it to the log server.
- ○ It's difficult to analyze abnormal logs.

Correct
Nice work! Logs from various systems may be formatted differently. Normalizing logs is the practice of reformatting the logs into a common format, allowing for easier storage and lookups in a centralized logging system.

2. What type of attacks does a flood guard protect against? Check all that apply. **1 / 1 point**

- ☐ Man-in-the-middle attacks
- ☐ Malware infections
- ☑ DDoS attacks

Correct
You got it! A flood guard protects against attacks that overwhelm networking resources, like DoS attacks and SYN floods.

- ☑ SYN floods

Correct
You got it! A flood guard protects against attacks that overwhelm networking resources, like DoS attacks and SYN floods.

3. What does DHCP Snooping protect against? **1 / 1 point**

- ○ Brute-force attacks

- ○ Data theft
- ◉ Rogue DHCP server attacks
- ○ DDoS attacks

Correct
Good job! DHCP snooping is designed to guard against rogue DHCP attacks. The switch can be configured to transmit DHCP responses only when they come from the DHCP server's port.

4. What does Dynamic ARP Inspection protect against? **1 / 1 point**

- ○ Rogue DHCP server attacks
- ○ DDoS attacks
- ○ Malware infections
- ◉ ARP poisoning attacks

Correct
That's exactly right! Dynamic ARP inspection protects against ARP poisoning attacks by watching for ARP packets. If an ARP packet doesn't match the table of MAC address and IP address mappings generated by DHCP snooping, the packet will be dropped as invalid or malicious.

5. What does IP Source Guard protect against? **1 / 1 point**

- ◉ IP spoofing attacks
- ○ Rogue DHCP server attacks
- ○ Brute-force attacks
- ○ DDoS attacks

Correct
Right on! IP Source Guard prevents an attacker from spoofing an IP address on the network. It does this by matching assigned IP addresses to switch ports, and dropping unauthorized traffic.

6. What does EAP-TLS use for mutual authentication of both the server and the client? **1 / 1 point**

- ○ Biometrics
- ○ Usernames and passwords
- ○ One-time passwords
- ◉ Digital certificates

Correct
Yep! The client and server both present digital certificates, which allows both sides to authenticate the other, providing mutual authentication.

7. Why is it recommended to use both network-based and host-based firewalls? Check all that apply. **1 / 1 point**

- ☑ For protection for mobile devices, like laptops

Correct
Nice job! Using both network- and host-based firewalls provides protection from external and internal threats. This also protects hosts that move between trusted and untrusted networks, like mobile devices and laptops.

- ☑ For protection against compromised hosts on the same network

Correct
Nice job! Using both network- and host-based firewalls provides protection from external and internal threats. This also protects hosts that move between trusted and untrusted networks, like mobile devices and laptops.

- ☐ For protection against DDoS attacks
- ☐ For protection against man-in-the-middle attacks