The following correction applies to page 167 of the *CISM® Review Questions, Answers & Explanations Manual 8th Edition*. Justification B has been bolded to indicate that B is the correct answer.

S2-203 Which of the following approaches would be **BEST** to address significant system vulnerabilities that were discovered during a network scan?

A. All significant vulnerabilities must be mitigated in a timely fashion.
B. Treatment should be based on threat, impact and cost considerations.
C. Compensatory controls must be implemented for major vulnerabilities.
D. Mitigation options should be proposed for management approval.

B is the correct answer.

Justification:
A. Some vulnerabilities may not have significant impact and may not require mitigation.
B. The treatment should consider the degree of exposure and potential impact and the costs of various treatment options.
C. Compensatory controls are considered only when there is a viable threat and impact, and only if the primary control is inadequate.
D. Management approval may not be required in all cases.

S2-204 How does a security information and event management (SIEM) solution **MOST** likely detect the existence of an advanced persistent threat (APT) in its infrastructure?

A. Through analysis of the network traffic history
B. Through stateful inspection of firewall packets
C. Through identification of zero-day attacks
D. Through vulnerability assessments

A is the correct answer.

Justification:
A. Advanced persistent threat (APT) refers to stealthy attacks not easily discovered without detailed analysis of behavior and traffic flows. Security information and event management (SIEM) solutions analyze network traffic over long periods of time to identify variances in behavior that may reveal APTs.
B. Stateful inspection is a function of some firewalls, but is not part of a SIEM solution. A stateful inspection firewall keeps track of the destination IP address of each packet that leaves the organization's internal network. Whenever the response to a packet is received, its record is referenced to ascertain and ensure that the incoming message is in response to the request that went out from the organization.
C. Zero-day attacks are not APTs because they are unknown until they manifest for the first time and cannot be proactively detected by SIEM solutions.
D. A vulnerability assessment identifies areas that may potentially be exploited, but does not detect attempts at exploitation, so it is not related to APT.