Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 17 of the official CISSP study guide. Here are the top things that you need to know from this chapter on preventing and responding to incidents. List and describe the incident management steps. The CISSP security operations domain lists incident management steps such as detection, response, mitigation, reporting, recovery, remediation and lessons learned. After detecting and verifying an incident, the first response is to limit or contain the scope of the incident while protecting evidence. Based on governing laws, an organization may need to report an incident to official authorities and if PII is effective, individuals need to be informed. The remediation and lessons learned stages include root cause analysis to determine the cause and recommend solutions to prevent a recurrence.

Understand basic preventive measures. Basic preventive measures can prevent many incidents from occurring. These include keeping systems up to date, removing or disabling unneeded protocols and services, using intrusion detection and prevention systems, using anti-malware software with up to date signatures and enabling both host-based and network-based firewalls. Know the difference between whitelisting and blacklisting. Software whitelists provide a list of approved software and prevent the installation of any other software not on the list. Blacklists provide a list of unapproved software and prevent the installation of any software on the list.

Understand sandboxing. Sandboxing provides an isolated environment and prevents code running in a sandbox from interacting with elements outside of the sandbox. Know about third party provided security services. Third-party security services help an organization augment security services provided by internal employees. Many organizations use cloud-based solutions to augment their internal security.

Know about denial-of-service DoS attacks. DoS attacks prevent a system from responding to legitimate requests for service. A common DoS attack is the SYN flood attack, which disrupts the TCP three-way handshake. Even though older attacks are not as common today, because basic precautions block them, you may still be tested on them, because many newer attacks are variations on older methods. Smurf attacks employ an amplification network to send numerous response packets to a victim, ping of death attack send numerous oversized ping packets to the victim causing the victim's system to freeze, crash or reboot.