Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 21 of the official CISSP study guide. Here are the top things you need to know from this chapter on malicious code and application attacks. Understand the propagation techniques used by viruses. Viruses use four main propagation techniques file infection, service injection, boot sector infection and macro infection to penetrate systems and spread their malicious payloads. You need to understand these techniques to effectively protect systems on your network from malicious code.

Explain the threat posed by ransomware. Ransomware uses traditional malware techniques to infect a system and then encrypts data on that system using a key known only to the attacker. The attacker then demands payment of a ransom from the victim in exchange for providing the decryption key.

Know how antivirus software packages detect known viruses. Most antivirus programs use signature-based detection algorithms to look for telltale patterns of known viruses. This makes it essential to periodically update virus definition files in order to maintain protection against newly authored viruses as they emerge. Behavior-based detection monitors target users and systems for unusual activity and either blocks it or flags it for investigation.

Understand how user and entity behavior analytics UEBA functions. UEBA tools develop profiles of individual behavior and then monitor users for deviations from those profiles that may indicate malicious activity and or compromised accounts. Be familiar with the various types of application attacks that attackers use to exploit poorly written software. Application attacks are one of the greatest threats to modern computing. Attackers exploit buffer overflows, back doors, time-of-check to time-of-use vulnerabilities and root kits to gain illegitimate access to a system. Security professionals must have a clear understanding of each of these attacks and associated countermeasures.

Understand common web application vulnerabilities and countermeasures. As many applications move to the web, developers and security professionals must understand the types of attacks that exist in this environment and how to protect against them. The two most common examples are cross site scripting and SQL injection attacks.