Question 1: Explain the importance of analyzing indicators of application attacks to identify security threats. What are some common indicators of application attacks, and how can they help security teams detect and respond to potential breaches?

Answer: I would say it is very important to be able to analyze the indicators of attack. You must be able to understand how a threat actor can attack a system or framework. For example, if someone is attempting to execute an SQL injection you would see a SQL query/ expression show a form of Empty Input. Whereas with a legitimate query/ expression you would see a static field. This would allow you to understand that the threat actor is attempting to inject. In CSRF you would see some type of script appended to the URL. If you see this, you might be able to navigate or stay off the site it is attempting to re direct you to.

Question 2: Discuss the significance of analyzing indicators of web application attacks for organizations with online services. What are typical signs of a web application attack, and how can monitoring these indicators enhance the security posture of web applications? Provide an example of a web application attack indicator and explain its relevance in web application security.

Answer: Attackers can exploit vulnerabilities in server software and in client browser security to perform injection and session hijacking attacks that compromise data confidentiality and integrity. Typical signs of a web attack are usually located in the URL bar at the very end of the URL. If you can identify the web application attacks you increase security posture by not falling victim to a threat actor who may hijack your session or attempt to get a user to be directed to XSS. If you are able to inform other users around you about these attacks, you can prevent malicious activity and that increases security posture. A stored/ persistent Xss attack looks to insert a code into the back end of the database like the threat actor Mallory. The threat actor does this in order to apply malicious script in a message and then when the victim reads the message, the code executes. You may see this in the real world.