Bustillos, Rey-mark G. ClassCode:40458

Scenario 6:

I understand this scenario involves a Chief Information Security Officer (CISO) deploying a honeypot with a baseline configuration to uncover possible system vulnerabilities. This strategy is used to observe real-world cyberattacks and gather valuable insights without risking actual production systems.

One major advantage of this approach is the ability to collect real-time threat intelligence. By using a system with default or standard settings, the CISO can observe how attackers exploit common vulnerabilities. This helps the security team improve their defenses, update intrusion detection systems, and better understand attacker behavior. A honeypot can also serve as a decoy, drawing attackers away from real systems.

However, there are also disadvantages. Honeypots need constant monitoring and skilled professionals to manage and analyze the data. They only attract certain types of attackers, so the information collected may not reflect all possible threats. There are also legal and ethical concerns if the honeypot is used to launch further attacks. Additionally, relying too much on honeypots may give a false sense of security.

In conclusion, deploying a honeypot with a baseline configuration is a smart and useful method for detecting vulnerabilities and studying threats. Still, it should be used alongside other security tools and strategies. With proper planning and monitoring, a honeypot can greatly improve an organization’s ability to defend against cyberattacks.