Building an Effective Cybersecurity Program – Test Question Bank (Sample)

1. Which of the following **BEST** describes the primary purpose of a Cloud Access Security Broker (CASB)?
   A. Monitor data traffic between on premise and a cloud service provider.
   B. Digitally enforce cloud security policies.
   C. Authenticate access to applications hosted by a cloud service provider.
   D. Provide billing metering for security services.

   Answer Key: **B**

2. A strategy used to lure bad actors into a constantly evolving faux enterprise environment is **BEST** referred to as:
   A. Dynamic deception.
   B. Passive threat monitoring.
   C. Honeynet.
   D. Honeypot.

   Answer Key: **A**

3. Which of the following is the **MOST** effective way to secure the physical hardware hosts in a vitalized enterprise?
   A. Secure the guest operating system.
   B. Harden the hypervisor.
   C. Apply existing information security controls.
   D. Apply virtualized controls to the physical host.

   Answer Key: **C**

4. What is the **MAIN** purpose of a purple security testing team?
   A. Defend against simulated hacker attacks.
   B. Emulate hackers to compromise systems.
   C. Perform both attacker and defender security testing roles.
   D. Oversee security testing and implement recommended improvements.

   Answer Key: **D**

5. What is the **BEST** definition of risk?

   A. Probability x Impact.
   B. Threat x Probability.
   C. Financial Impact x Probability.
   D. Impact x Threat.

   Answer Key: **A**

6. A cloud computing environment that is bound together by technology that allows data and applications to be shared between public and private clouds is **BEST** referred to as a:

   A. Community cloud.
   B. Private cloud.
   C. Hybrid cloud.
   D. Public cloud.

   Answer Key: **C**

7. An organization has decided to move their disaster recovery capability away from their hot site vendor. Which of the following is the **MOST** study to be conducted?

   A. A business impact study.
   B. A risk assessment.
   C. An RPO & RTO analysis.
   D. A threat and vulnerability assessment.

   Answer Key: **C**

8. What is the **BEST** approach to address a critical security operations center (SOC) staffing shortage?

   A. Contract with a Managed Security Service Provider (MSSP) to cover nights and weekends.
   B. Shift security monitoring to the network monitoring center.
   C. Reduce SOC operating hours.
   D. Reduce the number of events per second to increase productivity of existing SOC staff.

   Answer Key: **A**