#interviewtips

CYBERSECURITY INTERVIEW QUESTIONS & ANSWERS

KNOW YOUR NIST CONTROLS

Swipe to know →

@thecyberhat

ACCESS CONTROL

What is the purpose of Access Control (AC) in the NIST 800-53 framework?

Access Control (AC) is designed to manage user access to resources within an organization's information systems, ensuring that only authorized users can access specific data or perform certain actions.

What does AC-2: Account Management entail?

AC-2: Account Management involves the processes and procedures for creating, modifying, disabling, and removing user accounts within an organization's information systems, ensuring that only authorized individuals have access to system resources.

Explain the concept of AC-6: Least Privilege?

AC-6: Least Privilege principle dictates that users should be granted the minimum level of access necessary to perform their job functions, reducing the risk of unauthorized access and potential misuse of privileged resources.

@thecyberhat

CONFIGURATION MANAGEMENT

How does Configuration Management (CM) contribute to information security?

Configuration Management (CM) ensures that information systems are configured securely and consistently, reducing the risk of vulnerabilities arising from misconfiguration or unauthorized changes.

Explain the purpose of CM-3: Configuration Change Control?

CM-3: Configuration Change Control governs the process of managing and documenting changes to the configuration of information systems, ensuring that changes are authorized, tested, and implemented in a controlled manner to mitigate risks.

What does CM-6: Configuration Settings involve?

CM-6: Configuration Settings focuses on establishing and maintaining secure configuration settings for hardware, software, and firmware components of information systems to minimize security risks and ensure operational integrity.

@thecyberhat

IDENTIFICATION & AUTHENTICATION

How does Identification and Authentication (IA) contribute to information security?

A: Identification and Authentication (IA) verifies the identity of users and devices accessing information systems, ensuring that only authorized entities can gain access and reducing the risk of unauthorized activities.

What does IA-2: Identification and Authentication (Organizational Users) encompass?

A: IA-2: Identification and Authentication (Organizational Users) involves the processes and mechanisms used to uniquely identify and authenticate organizational users before granting access to information systems, ensuring accountability, and preventing unauthorized access.

Describe the significance of IA-3: Device Identification and Authentication?

IA-3: Device Identification and Authentication focuses on verifying the identity of devices attempting to connect to information systems, ensuring that only trusted and authorized devices can access organizational resources.

@thecyberhat

INCIDENT RESPONSE

How does Incident Response (IR) contribute to information security?

A: Incident Response (IR) prepares organizations to effectively detect, respond to, and recover from security incidents, minimizing the impact of incidents on information systems and organizational operations.

Explain the role of IR-5: Incident Monitoring in information security?

A: IR-5: Incident Monitoring involves the continuous monitoring and analysis of information system activities and events to detect and respond to security incidents in a timely manner, reducing the likelihood and impact of successful attacks.

What is the purpose of IR-8: Incident Response Plan?

A: IR-8: Incident Response Plan establishes the organization's strategies, procedures, and responsibilities for responding to security incidents effectively, ensuring a coordinated and structured approach to incident management.

@thecyberhat

Security Assessment & Authorization

How does Security Assessment and Authorization (CA) contribute to information security?

Security Assessment and Authorization (CA) ensures that information systems undergo thorough assessment and authorization processes to verify compliance with security requirements and mitigate risks to organizational assets and operations.

What activities are involved in CA-2: Security Assessments?

CA-2: Security Assessments involve conducting comprehensive evaluations of information systems to assess their security posture, identify vulnerabilities, and evaluate compliance with security controls and requirements.

What is the significance of CA-7: Continuous Monitoring in information security?

CA-7: Continuous Monitoring involves the ongoing surveillance and assessment of information systems to detect and respond to security threats and vulnerabilities in real-time, ensuring continuous compliance with security requirements and prompt remediation of issues.

@thecyberhat

Did you like the post?

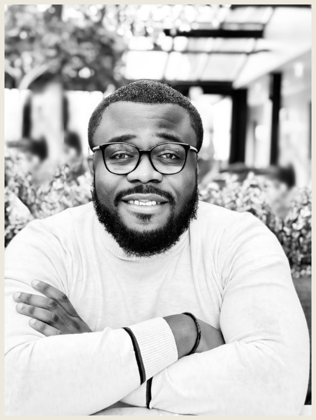
follow for more!

Like

Comment

Share

Save



Emmanuel Owusu-Kyereko
@thecyberhat

MSc | CISM | CISA | PMP | ISSO | AWS SOLUTIONS ARCHITECT | CMMC | SEC+ | THIRD PARTY VENDOR RISK MANAGEMENT | ISO 27001 LEAD AUDITOR