Cheat Sheet for comprehensive CompTIA Secure Data Professional

Data Security Fundamentals

Data Classification

- **Types of Data:**
  - **Public:** Low-risk, no sensitive information.
  - **Internal:** Company-wide use, minimal risk.
  - **Confidential:** Sensitive, requires access controls.
  - **Restricted:** Highly sensitive, strict access controls.

Data Lifecycle

- **Creation:** Data entry, validation.
- **Storage:** Backup, encryption, access controls.
- **Usage:** Monitoring, auditing, compliance checks.
- **Archiving:** Long-term storage, retention policies.
- **Destruction:** Secure deletion, data sanitization.

Encryption and Key Management

Encryption Types

- **Symmetric Encryption:**
  - **Example:** AES (Advanced Encryption Standard)
  - **Key Management:** Single key for encryption and decryption.
- **Asymmetric Encryption:**
  - **Example:** RSA (Rivest-Shamir-Adleman)
  - **Key Management:** Public and private key pairs.

Key Management Best Practices

- **Key Generation:** Use strong, random algorithms.
- **Key Storage:** Secure vaults, hardware security modules (HSMs).

- **Key Rotation:** Regularly change keys to enhance security.
- **Key Revocation:** Immediate deactivation upon compromise.

Access Control and Identity Management

Access Control Models

- **Discretionary Access Control (DAC):** Owner controls access.
- **Mandatory Access Control (MAC):** System enforces access.
- **Role-Based Access Control (RBAC):** Access based on roles.
- **Attribute-Based Access Control (ABAC):** Access based on attributes.

Identity Management

- **Authentication Methods:**
  - **Multi-Factor Authentication (MFA):** Combines multiple factors (e.g., password + OTP).
  - **Single Sign-On (SSO):** Single credential for multiple systems.
- **Identity Lifecycle Management:**
  - **Provisioning:** Automated user account creation.
  - **Deprovisioning:** Automated account deactivation.

Data Protection and Privacy

Data Protection Techniques

- **Data Masking:** Redacts sensitive data in non-production environments.
- **Data Obfuscation:** Alters data to prevent unauthorized use.
- **Data Tokenization:** Replaces sensitive data with tokens.

Privacy Regulations

- **General Data Protection Regulation (GDPR):** EU data protection law.
- **California Consumer Privacy Act (CCPA):** California privacy rights.
- **Health Insurance Portability and Accountability Act (HIPAA):** US healthcare data protection.

Incident Response and Disaster Recovery

Incident Response Plan

- **Preparation:** Develop response teams, document procedures.
- **Detection and Analysis:** Identify incidents, assess impact.
- **Containment:** Limit spread, isolate affected systems.
- **Eradication:** Remove threat, clean affected systems.
- **Recovery:** Restore systems, verify functionality.
- **Lessons Learned:** Review process, update procedures.

Disaster Recovery Plan

- **Backup Strategies:**
  - **Full Backup:** Complete data copy.
  - **Incremental Backup:** Changes since last backup.
  - **Differential Backup:** Changes since last full backup.
- **Recovery Time Objective (RTO):** Maximum acceptable downtime.
- **Recovery Point Objective (RPO):** Maximum acceptable data loss.

Compliance and Auditing

Compliance Frameworks

- **ISO/IEC 27001:** Information security management.
- **NIST Cybersecurity Framework:** US government standards.
- **PCI DSS:** Payment card industry data security.

Auditing Best Practices

- **Regular Audits:** Schedule periodic audits.
- **Documentation:** Maintain detailed records of processes and controls.
- **Third-Party Audits:** Engage external auditors for unbiased reviews.

Tools and Technologies

Security Information and Event Management (SIEM)

- **Features:**

- Real-time monitoring.
- Log aggregation and analysis.
- Threat detection and alerting.

- **Examples:** Splunk, IBM QRadar, ArcSight.

Data Loss Prevention (DLP)

- **Features:**

- Content inspection.
- Policy enforcement.
- Endpoint monitoring.

- **Examples:** Symantec DLP, McAfee DLP, Cisco DLP.

Tips and Tricks

Security Awareness

- **Training:** Regular security awareness training for employees.

- **Phishing Simulations:** Conduct simulated phishing attacks to test awareness.

Best Practices

- **Regular Updates:** Keep systems and applications updated.

- **Strong Passwords:** Use complex passwords and change regularly.

- **Network Segmentation:** Divide network into segments to limit access.

Examples

Encryption Example

- **Scenario:** Encrypting sensitive customer data.

- **Solution:** Use AES-256 encryption with a secure key management system.

Incident Response Example

- **Scenario:** Ransomware attack.

- **Solution:** Isolate affected systems, restore from backups, update security measures.

Summary

- **Data Security:** Protect data at all stages of its lifecycle.

- **Encryption:** Use strong encryption methods and manage keys securely.

- **Access Control:** Implement robust access control models.

- **Incident Response:** Have a well-defined incident response plan.
- **Compliance:** Ensure adherence to relevant regulations and frameworks.

This cheat sheet provides a comprehensive overview of essential concepts and practices for the CompTIA Secure Data Professional certification.

By Ahmed Baheeg Khorshid

ver 1.0