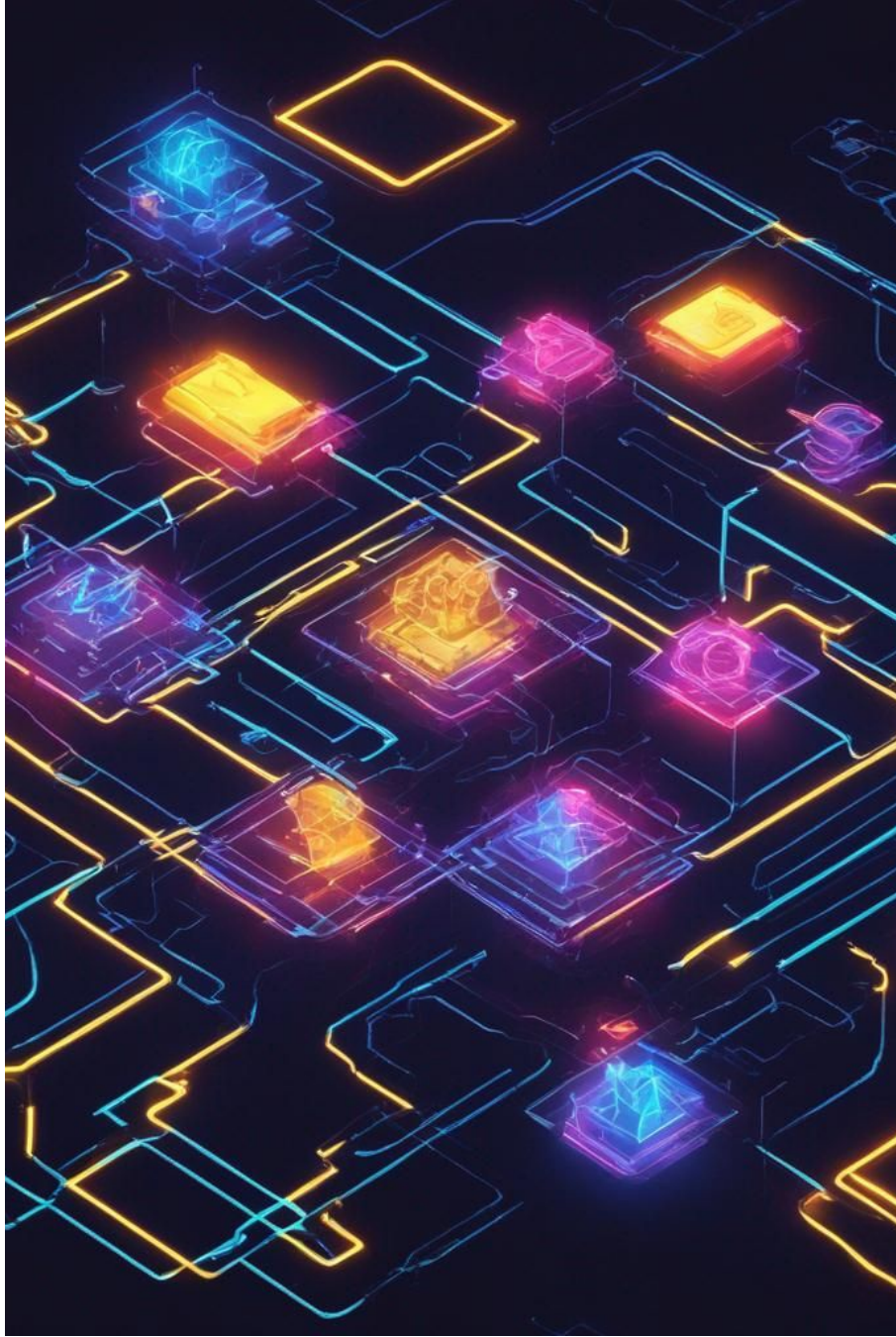
Securing Operations

A Comprehensive Guide to Operations Security and Beyond

CISSP Study Guide - VIII



Operations Security Core Concepts

Understanding Key Policies and Procedures

- Need-to-Know and Least Privilege Principle
- Separation of Duties
- Job Rotation
- Procedures for Sensitive Information
- Record Retention
- Monitoring of Special Privileges

Protecting Tangible and Intangible Assets

1. **Facilities:** Door Alarms, Fire Systems, Document Shredding

2. **Hardware:** Password Management, Access Restrictions, Use of Encrypted Tools like SSH

3. **Software:** Licensing Compliance, Protection of Information Assets (Trade Secrets, Product Plans)

Asset Management Strategies

- **Redundancy and Fault Tolerance:** Ensuring continuous availability
- **Backup and Recovery Systems:** Quick restoration capability
- **Identity and Access Management:** Preserving data integrity

Media Management - RAID Systems

Understanding RAID Levels

- **RAID 0:** Performance focus but without fault tolerance
- **RAID 1:** Disk mirroring for fault tolerance
- **RAID 3 and 5:** Striping with parity for a balance of performance and fault tolerance

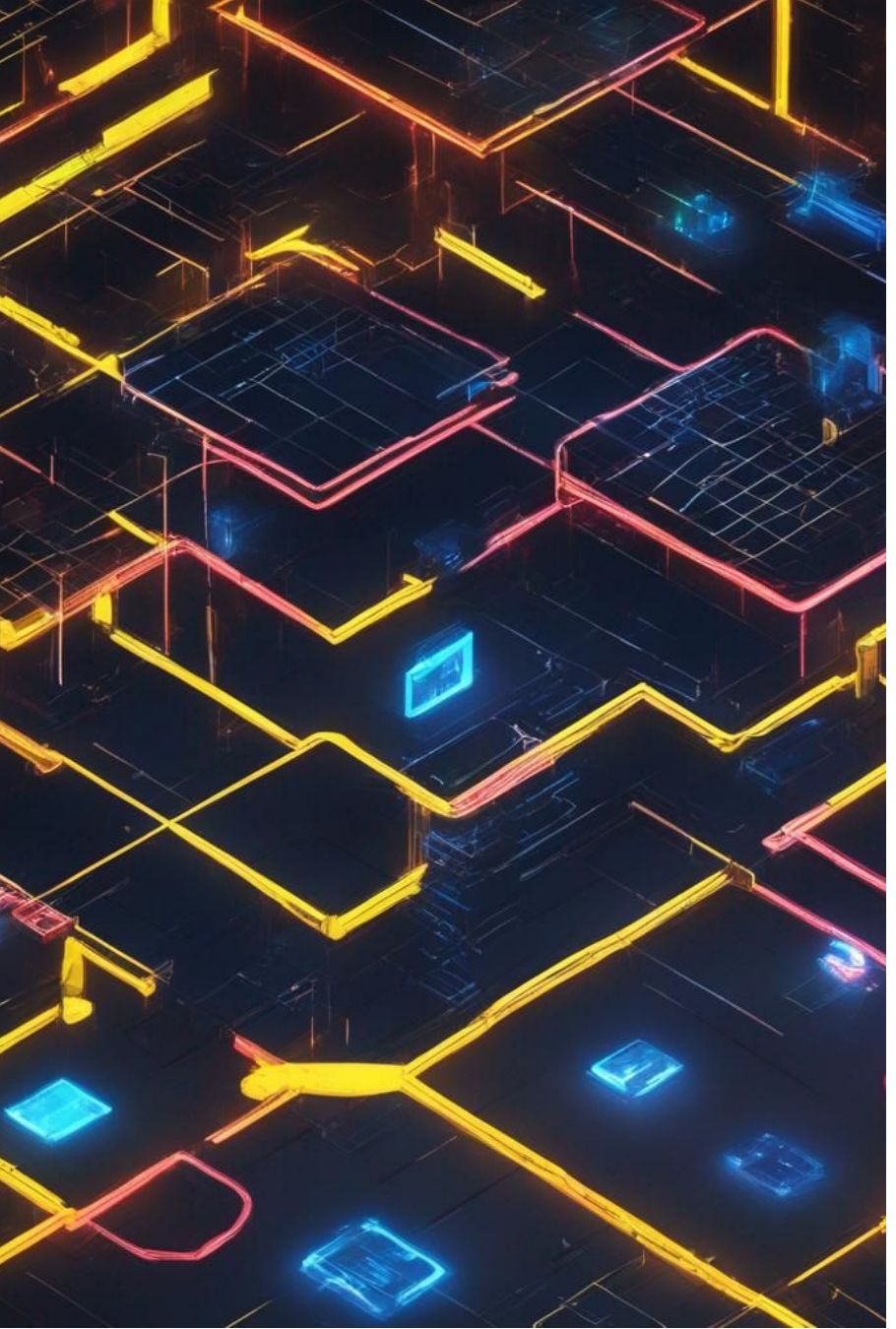
Advanced Storage Solutions

Comparing NAS and SAN

- **NAS:** LAN-based Ethernet-linked storage
- **SAN:** High-speed Fibre Channel storage infrastructure

Storage Management Considerations

- Hierarchical Storage Management (HSM)
- Accurate Media History and Labelling
- Safe Storage Environment for Media
- Temperature Control to Prevent Media Damage



Data Sanitization and Disposal Practices

1. **Data Purging:** Degaussing to eliminate forensic data recovery
2. **Data Clearing:** Making information irrecoverable
3. **Remanence:** Managing data remnants post-deletion

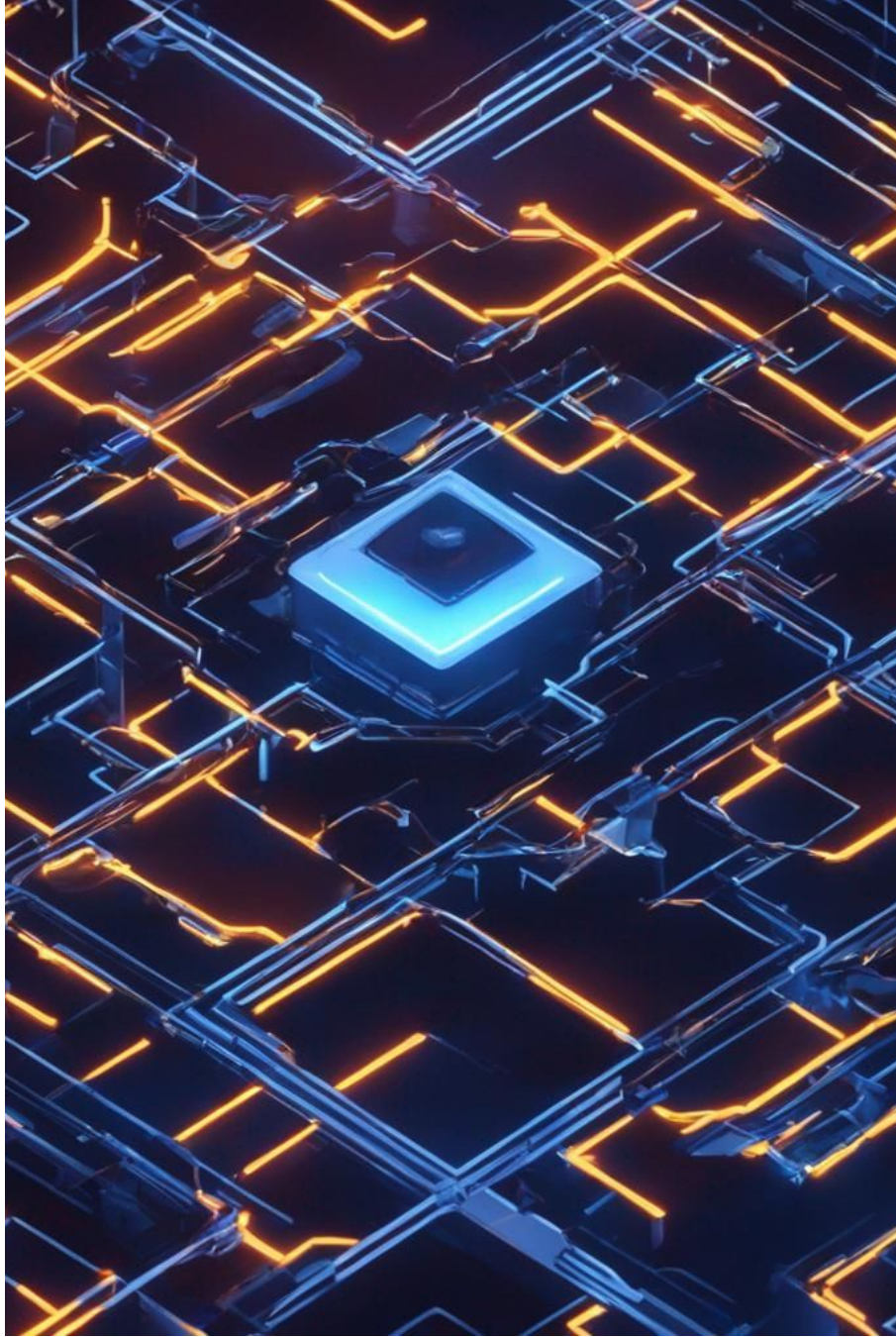
Network and Resource Administration

- Implementation of Redundant Hardware and Fault-tolerant Systems
- Adherence to SLAs for predictability
- Monitoring of MTBF and MTTR for planning
- Elimination of Single Points of Failure (SPOF)

Managing Incident Response

Incident Lifecycle

- Detection
- Response
- Reporting
- Recovery
- Remediation
- Review



The Change Management Process

- Formal Request and Analysis for Proposed Changes
- Reviewing Costs and Impacts
- Strategy Development with Fall-Back Planning
- Detailed Documentation and Management Reporting

Audit and Review Essentials

- Analyzing Control over Audit Trails
- Ensuring Separation of Duties in Audit Management
- Access Control to Log Files

Monitoring and Reporting Techniques

1. IDPS Updates and Effective Signature Management
2. Data Reduction in Monitoring for Requirements Fulfillment
3. Adaptable Reporting to Audience Technical Levels

Threats and Precautionary Measures

- Implementing Clipping Levels to Identify Anomalies
- Understanding Deviations from Standards
- Trusted Paths and Recovery for Secure System Operations

System Hardening and Maintenance

- Purging of Unnecessary Applications and Services
- Rigorous Management of External Device Connections
- Vulnerability Management Systems to Centralize Monitoring Operations

Information Security Buzz

Discover more at our InfoSec Knowledge Hub