Chapter 7 - Key Topics

Description	Element	Page	Summary
Identity & account management life cycle management phases	List	235	**Registration & Identity Validation** - A user provides information and registers for digital identity. The issuer will verify the information and securely issue a unique and non-descriptive identity. **Privileges provisioning** - The resource owner authorizes the access rights to a specific account, & privileges are associated with it. **Access Review** - Access rights are constantly reviewed to avoid privilege creep. **Access Revocation** - Access to a given resource may be revoked due, for example, to account termination.
Password Management	Section	236	**Password Creation** - Organizations should have policies and standards for password creation: strength, age, reusability. **User-generated passwords** - Users generate their own passwords which are simple to remember but easy to guess and often re-used across multiple systems. **System-generated passwords** - Generated by the system, are strong and compliant with security policy but can be difficult to remember and users tend to write them down. **OTP & token** - Passwords are generated by an external entity & synced with an internal resource. Users don't need to remember complex passwords, this method requires more infrastructure and the software & hardware required generates deployment & maintenance costs.

Description	Element	Page	Summary
Multifactor Authentication	Section	239	The process of authentication requires a subject to supply verifiable credentials, these credentials are referred to as factors. In **multifactor-authentication** two or more factors are presented. In **multilayer authentication** more than one of the same type of factor is used. **Identification** is establishing identity. **Authentication** is about proving identity.
Single Sign-On System	Figure 7-6	244	A user is accessing resources on Server B; for example, the user sends an HTTP GET request for a web page (step 1). SSO is used to provide authentication service for Server B. When Server A receives the request for a web page, it redirects the user to the SSO server of the organization for authentication (steps 2 and 3). The user will authenticate to the SSO server, redirecting the user back to Server B with proof of authentication—for example, a token (steps 4 and 5). Server B will validate the proof of authentication and grant access to resources.
Security Events & Log Management	Section	251	**Event** (NIST SP 800-61r2) - An event is any observable occurrence in a network. **Security Incident** - An event that violates the security policy of an organization. **Event Management** - includes administrative, physical, & technical controls that allow the proper collection, storage, and analysis of events. Many compliance frameworks such as ISO & PCI DSS mandate log management controls & practices.
Log Collection, Analysis, & Disposal	Section	251	Log storage critical for maintaining log confidentiality & integrity. **Information Collected via Logs** - User ID, system activities, timestamps, successful or unsuccessful access attempts, configuration changes, network addresses & protocols, file access activities **NIST SP 800-92** - Defines three categories of logs of interest for security professionals. **Logs**

Description	Element	Page	Summary
			generated by security software - Antivirus/antimalware, IPS/ICD, Web Proxies, remote access software, authentication servers, vulnerability management software, infrastructure devices (firewalls, routers, switches, wireless access points) **Logs generated by the operating system** - System events, audit logs **Logs generated by the applications** - Connection & session info, usage info, significant operational action **Syslog (RFC 5424)** - Event notification protocol with three main entities (originator - the entity that generates a Syslog message, collector - the entity that receives that info about an event in Syslog format, relay - an entity that can receive messages from originators and forward them to other relays or collectors). Uses TCP or UDP port 514 **Syslog Facility** - Kernel Messages (0), User-level messages (1), Mail system (2), System daemons (3), Security/Authorization messages (4), Messages generated by Syslogd (5), Line printer subsystem (6), Network news subsystem (7), UUCP subsystem (8), Clock daemon (9), Security/authorization messages (10), FTP daemon (11), NTP subsystem (12), Log Audit (13), Log alert (14), Clock daemon (15), Local use 0-7 (16-23) **Syslog Severity** - Emergency: the system is unusable (0), Alert: Action must be taken immediately (1), Critical: Critical conditions (2), Error: Error conditions (3), Warning: Warning conditions (4), Notice: Normal but significant condition (5), Informational: informational messages (6), Debug: Debug-level messages. **Syslog Header** - Priority (PRI) where facility x 8 + severity, timestamp, hostname, application name, process ID

Description	Element	Page	Summary
Security Information & Event Manager (SIEM)	Section	255	**Log Collection** - This includes receiving information from devices with multiple protocols and formats, storing the logs, and providing historical reporting and log filtering. **Log normalization** - This function extracts relevant attributes from logs received in different formats and stores them in a common data model or template. This allows for faster event classification and operations. Non-normalized logs are usually kept for archive, historical, and forensic purposes. **Log aggregation** - This function aggregates information based on common information and reduces duplicates. **Log Correlation** - This is probably one of the most important functions of a SIEM. It refers to the ability of the system to associate events gathered by various systems, in different formats and at different times, and create a single actionable event for the security analyst or investigator. Often the quality of an SIEM is related to the quality of its correlation engine. **Reporting** - Event visibility is also a key functionality of a SIEM. Reporting capabilities usually include real-time monitoring and historical base reports. **SIEM Examples** - HP ArcSight, BlackStratus, EiQ Networks, Hawk Network Defense, Log Rhythm, NetIQ, IBM QRadar, RSA, Splunk, Symantec, TrustWave

Description	Element	Page	Summary
SIEM Capabilities	List	256	**Log Collection** - is the process of collecting and organizing logs for analysis. A log collector is a software that is able to receive logs from multiple sources and in some cases offers storage capabilities and log analysis functionality. **SIEM** - is a specialized device or software for security event management. It increases the normal log collector functionality by providing log collection, normalization, aggregation, correlation, and reporting capabilities.
Security Orchestration, Automation, & Response (SOAR)	Section	257	Security Orchestration, Automation, and Response (SOAR) is a set of solutions and integrations designed to allow organizations to collect security threat data and alerts from multiple sources. SOAR platforms take the response capabilities of a SIEM to the next level. SOAR solutions supplement, rather than replace, the SIEM. They allow the cybersecurity team to extend its reach by automating the routine work of cybersecurity operations. Unlike traditional SIEM platforms, SOAR solutions can also be used for threat and vulnerability management, security incident response, and security operations automation.

Description	Element	Page	Summary
Summary of asset management phases	List	258	**Asset Management** - refers to policies, processes, & technology to manage and protect an organization's assets during their lifecycle. **Asset Inventory** - deals with collecting and storing information about assets, such as location, security classification, & owner. **Asset acceptable use and return policies** - specify how users can use an asset and how an asset should be returned when it is not needed anymore. **Asset Ownership** - is the process of assigning an owner to an asset. Each asset within the organization needs an owner. The owner is responsible for the security of the asset during its life cycle. **Asset Classification** - is the process of evaluating the risk of an asset in terms of confidentiality, integrity, and availability and assigning a security classification to an asset. **Asset Labeling** - is the process of assigning a label to an asset that includes its security classification. **Asset Handling** - refers to procedures and technologies that allow for the secure storage, use, and transfer of an asset. **Media management** - deals with the secure management of the media life cycle, which includes media access, media marking, media storage, media use, media transport, media downgrading, and media sanitization and disposal.

Description	Element	Page	Summary
Threats to organizations using BYOD	List	261	BYOB Threats - Defined in **NIST SP 800-124** **Lack of physical security controls** - The risk of being stolen is much higher. **Use of untrusted devices** - Personal devices can be rooted or jailbroken, increasing the risk of compromise. **Use of untrusted networks** - Risk of usage of compromised networks increased. **Use of untrusted applications** - 3rd party applications may be untrusted and dangerous. **Interaction with other systems** - Interactions with systems outside the control of your org, increasing the risk of data loss. **Use of untrusted content** - Mobile devices can access content in more ways, QR codes, for example, increases risk. **Use of location services** - Can help attackers locate an asset or person and use this to build an attack.

Description	Element	Page	Summary
Enterprise mobile management phases	List	262	Five-phase life cycle - **NIST 800-124 Initiation** - This phase includes the activities an organization needs to perform before designing a mobile solution. Include selecting the strategy for implementation, determining how the strategy matches the organization's mission, developing a mobile device security policy, etc. **Development** - In this phase, the technical characteristics and deployment plan of the mobile solution are specified. It includes which authentication or encryption strategy will be used, the type of mobile brands that will be allowed, and so on. **Implementation** - In this phase, mobile devices are provisioned to meet the security policy requirements. This phase includes the testing and production deployment of the solution. **Operation & Maintenance** - This phase includes ongoing security tasks that need to be performed during the mobile device's life cycle. Examples are reviewing access controls, managing patches, handling threat detection and protection, and so on. **Disposal** - Includes activities around media disposal.

Description	Element	Page	Summary
Capabilities of a Mobile Device Management (MDM) system	List	263	**Restrict Access** - restrict user or application access to mobile device hardware, cameras, network interfaces, GPS, and services or native applications such as the built-in web browser or email client. **Limit or Prevent** - access to organization resources based on the device profile and security posture. **Monitor, alert, & report** - on policy violations. **Encrypt** - data communications between the device and the org as well as data stored on the device. **Remote Wipe** - In case of lost or stolen. **Enforce strong passwords** - This includes password strength policies, clipping level, and so on. **Remote Lock** - remotely lock and remotely reset the password. **DLP** - Enforce Data Loss Prevention (DLP) solutions on mobile. **Restrict Installs** - restrict types of applications that may be installed.
Comparing Cloud-based MDM & On-Premises MDM	Figure 7-6	264	**Cloud-Based MDM Characteristics** - Deployed as a service & operated by a third party, lower cost, flexibility, fast deployment, scalability. easier to maintain. **On-premises MDM Characteristics** - Deployed and managed within org, higher control, intellectual property retention, regulatory compliance
Configuration management & terminology	List	268	**Configuration Management** - concerned with all policies, processes, & technologies used to maintain the integrity of the configuration of a given asset. **Change Management** - concerned with all policies, processes, and technologies that handle a change to an asset's life cycle.

Description	Element	Page	Summary
Configuration Management	Section	268	**NIST SP 800-128 Definition** - defines configuration management as a set of activities used to maintain organizational resource integrity through the control of processes for initializing, changing, and monitoring the resource configuration. **Configuration Item (CI)** - the identifiable part of a system that is the target of the configuration control process. **Baseline Configuration** - set of attributes & CIs related to a system, which has been formally reviewed & approved.
Secure configuration mangement (SecCM) phases	List	269	**Planning** - Includes the definition of SecCM policies and procedures and the integration of these procedures within the IT and information security policy of an organization. **Identifying & implementing the configuration** - Includes the development and establishment of security baseline configuration and the implementation of the baseline on CIs. **Controlling the configuration changes** - Includes the management of changes to keep the baseline configuration secure. **Monitoring** - Used to validate and ensure that the CIs are compliant with the organization's security policy and to maintain a secure baseline configuration.
Configuration & change management definitions	List	270	**Standard change** - A common change that has already been authorized and is low risk. This type of change might not need to follow a formal change management process. **Emergency change** - A change that needs to be implemented on an urgent basis. This type of change usually has a separate procedure. **Normal change** - A change that is not a standard change or an emergency change. This is the type of change that will go through the full change management procedure.

Description	Element	Page	Summary
ITIL Change Management Process	Figure 7-16	272	**Create Request For Change (RFC)** - RFC is created. **Record RFC** - RFC is recorded in the change management system. **Review RFC** - RFC is reviewed to see whether it is complete and if the change can be approved. **Assess & Evaluate Change** - Determine the risk and benefit associated with the change. **Authorize Change Build & Test** - Authorize the change and build test plan. **Coordinate Change Build & Test** - Implement the test plan & report the results. **Authorize Change Deployment** - Authorize the deployment of a change. **Coordinate Change Deployment** - Implement the change. **Review & Close Change Record** - Verify that the change is working, and update all relevant systems (change management system, configuration management system, etc.)

Description	Element	Page	Summary
Change security impact analysis	List	272	Defined in **NIST SP 800-128** 1. **Understand the change** - Develop a high-level view of what the change will look like. 2. **Identify vulnerabilities** - This step includes looking for information on vulnerabilities from the vendor or other vulnerability information providers. This step might also include performing a security analysis of the code. 3. **Access risks** - This step includes identifying possible threats and calculating the impact and likelihood of the threats exploiting the system vulnerabilities identified in the previous step. The risk can be accepted, mitigated with the use of additional countermeasures, or avoided, in which case the change request is rejected. 4. **Access the impact on existing security controls** - This includes the evaluation of how the change would impact other security controls. For example, a deployment of a new application on a server might require a change to a firewall rule. 5. **Plan safeguards & countermeasures** - This step deals with any safeguards and countermeasures that need to be put in place to mitigate any risk determined by the change request.
Vulnerability Management Phases	Figure 7-17	273	Vulnerability Identification → Vulnerability Analysis & Prioritization → Vulnerability Remediation
Vulnerability identification & CVE	Paragraph	274	Common Vulnerabilities and Exposures (CVE) from MITRE is a dictionary of vulnerabilities and exposures in products and systems. It is an industry-standard method for identifying vulnerabilities. Each vulnerability is identified by a CVE identifier (CVE-ID).

Description	Element	Page	Summary
Vulnerability Scan	Section	276	A popular method for identifying vulnerabilities in systems and devices. There are two types, active & passive scanning. **Active Scanner** - This type of scanner sends probes to the system and evaluates a vulnerability based on the system response. An active scanner can be used together with some type of system credentials or without them. **Passive Scanner** - Deployed on the network, a passive scanner observes network traffic generated by a system and determines whether or not the system may be affected by a specific vulnerability. **Network vulnerability scanners** - focus on network infrastructure. **Web vulnerability scanners** - work on the application layer and probe web services. **Workflow of vuln. scan usage** - Identify systems as targets, alert owners, users, stakeholders of the system, run the scanner, perform report analysis
Penetration Testing (Ethical Hacking) Assessments	Section	277	Also referred to ethical hacking or white hats, a penetration test, or pen test, goes one step further and is used to test an exploit of a vulnerability. **Vulnerability chaining** - is the process of exploiting vulnerabilities in sequence so that the exploitation of the first leads to the exploitation of the second.

Description	Element	Page	Summary
Types of penetration testing assessments	List	277	**White box** - With this approach, the pen tester has access to inside information and has the possibility to receive documentation about systems, system versions and patch levels, and so on. In some cases, the tester may also get information on the source code of applications or credentials to access some systems. This approach is generally used to simulate an insider threat. **Black Box** - This approach is the opposite of white box, and the pen tester does not have any information about the system he is trying to breach. This is more accurate in simulating an external attack. This type of test, however, is less complete than a white box approach because the pen tester needs to find by himself all the information needed to prepare the attack. Because these activities are performed during a limited amount of time, not all the security gaps are usually found. **Gray Box** - This is halfway between a white box and a black box approach. In this approach, the pen tester has some information available but not all.
Comparing Vulnerability Scan & Penetration Assessment	Table 7-7	278	**Vulnerability Scan** - works by assessing known vulnerabilities, can by fully automated, minimal impact on the system, main goal is to report known vulnerabilities. **Penetration Testing** - can find unknown vulnerabilities, mixture of automated & manual process, may disable the system, main goal is to compromise the system.
Coordinated Disclosure	Section	279	**Full Disclosure** - All details about a vulnerability are disclosed. **Coordinated Disclosure** - Relevant information about the vulnerability is disclosed; however, information that could help an attacker build an exploit is omitted.

Description	Element	Page	Summary
Common Vulnerability Scoring System (CVSS)	Paragraph	283	Common Vulnerability Scoring System is an industry-standard used to convey information about the severity of vulnerabilities. In CVSS, a vulnerability is evaluated under three aspects, and a score is assigned to each of them. **Base** - The Base group represents the intrinsic characteristics of a constant vulnerability over time and does not depend on a user-specific environment. This is the most important information and the only mandatory information to obtain for a vulnerability score. **Temporal** - The temporal group assesses the vulnerability as it changes over time. **Environmental** - The environmental group represents the characteristic of a vulnerability taking into account the organization's environment.
Vulnerabilities workarounds & mitigations	Paragraph	287	**Vulnerability workaround** - a technical solution that can avoid an exploit of a vulnerability without affecting the service or feature that is affected by the vulnerability itself. For example, the process of creating an access list on a device and dropping a specific malicious packet that triggers the vulnerability is considered a workaround. **Mitigations** - are technical solutions that limit the exposure or the impact of a vulnerability. Limiting the number of hosts that can send the affected packet via an access control list is an example of a mitigation.

Description	Element	Page	Summary
Patch Management Steps	List	288	**1. Identify the systems** - This is where the patch should be installed. **2. Prioritize the systems that need to be patched** - Some systems need to be patched immediately because they are mission-critical or because they are highly exposed to the vulnerability covered by that patch. Other systems might need to be patched, but there is no immediate danger. **3. Evaluate countermeasures** - In some cases, additional compensative controls can be deployed while the patch request goes through the change management process. **4. Start the change process** - Filing a request for change formally starts the change process to request the installation of a patch. Include: Review of RFC, assess whether the patch deployment needs to follow the formal process, test the patch, perform security impact analysis, authorize and deploy the patch, verify that the system works correctly. **5. Update configuration records** - Once the patch has been deployed and successfully verified, the configuration record database needs to be updated with the information about the new patch installed and related documentation (such as the time and date for completion, service-level agreement [SLA] milestones, issues found during the deployment, and so on).

Description	Element	Page	Summary
Patch deployment methods	List	289	**Agent-based** - This model uses an agent, which is software installed on the system that communicates with a patch management server. **Agentless** - This model includes one device that constantly scans the infrastructure and determines which host to patch. A lighter touch than the agent method. **Passive network monitoring** - This model uses network traffic monitoring to determine which version of the operating system a host is running. This is the least intrusive method, but it's the least reliable as well. Because it does not require any privileges on the system, it is generally used to check systems that are not under the control of the organization (for example, visitor systems).
Patch Deployment Prioritization	Figure 7-21	290	See page for visual flow.
Patch deployment approaches	List	290	**Update all or phased deployment** - the patch can be deployed at once to all that require it, or a phased approach can be used based on prioritization and risk assessment. **Pull or push deployment** - the patch can be pushed to a system (enterprise patch management using an agent-based method), or can be asked to install. **Manual or automatic deployment** - The patch is pushed and installed automatically, or the user may be asked to choose to install the patch manually or semi-manually.
Untitled			