









# Chapter 1 - Key Topics

Aa Description	≡ Element	▼ Page	≡ Summary
<u>Cybersecurity vs. Information Security (InfoSec)</u>	Section	8	<p><b>InfoSec</b> - In the past, information security programs and policies were designed to protect the confidentiality, integrity, and availability of data within the confines of an organization.</p> <p><b>Cybersecurity</b> - Is the process of protecting information by preventing, detecting, and responding to attacks. Builds upon traditional InfoSec &amp; includes: <i>Cyber risk management, threat intelligence &amp; information sharing, threat hunting (proactively looking for potential compromise), third-party organization, software, &amp; hardware dependency management.</i></p>
<u>What is a threat?</u>	Paragraph	10	<p><b>Threat</b> - A threat is any potential danger to an asset.</p> <p><b>Latent/Unrealized Threat</b> - If a vulnerability exists but has not yet been exploited—or, more importantly, it is not yet publicly known—the threat is latent and not yet realized.</p> <p><b>Malicious Actor</b> - The entity that takes advantage of the vulnerability is known as the malicious actor. <b>Threat Agent/Threat Vector</b> - The path used by a malicious actor to perform the attack is known as the threat agent or threat vector.</p>
<u>What is a vulnerability?</u>	Paragraph	11	<p><b>Vulnerability</b> - A vulnerability is a weakness in the system design, implementation, software, or code or the lack of a mechanism.</p>
<u>What is an exploit?</u>	Paragraph	13	<p><b>Exploit</b> - An exploit refers to a piece of software, a tool, a technique, or a process that takes advantage of a vulnerability that leads to access, privilege escalation, loss of integrity, or denial of service on a computer system. <b>Zero-day exploit</b> - Sometimes no one may even know the vulnerability exists, and it is exploited. That is known as a zero-day exploit.</p>
<u>Threat Intelligence</u>	Section	17	<p><b>Threat Intelligence</b> - Threat intelligence is referred to as the knowledge about an existing or emerging threat to assets, including networks and systems. Threat intelligence includes context, mechanisms, indicators of compromise (IoCs), implications, and actionable advice. <b>Threat Intelligence Process</b> - Planning &amp; Direction → Collection → Processing → Analysis &amp; Production → Dissemination</p>

Aa Description	≡ Element	▼ Page	≡ Summary
<u>White, Black, &amp; Gray Hat Hackers</u>	Figure 1-5	18	<p><b>White Hat</b> - These individuals perform ethical hacking to help secure companies and organizations. Their belief is that you must examine your network in the same manner as a criminal hacker to better understand its vulnerabilities. <b>Black Hat</b> - These individuals perform illegal activities, such as organized crime. <b>Gray Hat</b> - These individuals usually follow the law but sometimes venture over to the darker side of black hat hacking. It would be unethical to employ these individuals to perform security duties for your organization because you are never quite clear where they stand.</p>
<u>Threat Intelligence Standards (STIX, TAXII, CybOX, OpenIOC, etc.)</u>	List	19	<p><b>Structured Threat Information eXpression (STIX)</b> - This express language is designed for sharing cyberattack information. STIX details can contain data such as the IP addresses or domain names of command and control servers (often referred to as C2 or CnC), malware hashes, and so on. STIX was originally developed by MITRE and is now maintained by OASIS. You can obtain more information at <a href="http://stixproject.github.io">http://stixproject.github.io</a>. <b>Trusted Automated eXchange of Indicator Information (TAXII)</b> - This open transport mechanism standardizes the automated exchange of cyber threat information. TAXII was originally developed by MITRE and is now maintained by OASIS. You can obtain more information at <a href="http://taxiiproject.github.io">http://taxiiproject.github.io</a>. <b>Cyber Observable eXpression (CybOX)</b> - This free standardized schema is used for specification, capture, characterization, and communication of events of stateful properties that are observable in the operational domain. CybOX was originally developed by MITRE and is now maintained by OASIS. You can obtain more information at <a href="https://cyboxproject.github.io">https://cyboxproject.github.io</a>. <b>Open Indicators of Compromise (OpenIOC)</b> - This open framework is used for sharing threat intelligence in a machine-digestible format. <b>Open Command &amp; Control (OpenC2)</b> - This language is used for the command and control of cyber-defense technologies. OpenC2 Forum was a community of cybersecurity stakeholders that was facilitated by the U.S. National Security Agency. OpenC2 is now an OASIS technical committee (TC) and specification. You can obtain more information at <a href="http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=openc2">www.oasis-open.org/committees/tc_home.php?wg_abbrev=openc2</a></p>





 Description	 Element	 Page	 Summary
<a href="#">Threat Intelligence Platform</a>	Section	19	<b>Threat Intelligence Platform</b> - Many organizations deploy their own threat intelligence platforms (TIPs) to aggregate, correlate, and analyze threat intelligence information from multiple sources in near real-time. <b>Threat Intelligence Platforms support the following</b> - Threat intelligence collection, Data correlation, Enrichment and contextualization, Analyze, Integrations with other security systems, Act.
<a href="#">SQL Injection</a>	Section	21	<b>SQL Injection</b> - SQL injection (SQLi) vulnerabilities can be catastrophic because they can allow an attacker to view, insert, delete, or modify records in a database. In an SQL injection attack, the attacker inserts or injects, partial or complete SQL queries via the web application. The attacker injects SQL commands into input fields in an application or a URL to execute predefined SQL commands. <b>In-band SQL injection</b> - With this type of injection, the attacker obtains the data by using the same channel that is used to inject the SQL code. This is the most basic form of an SQL injection attack, where the data is dumped directly in a web application (or web page). <b>Out-of-band SQL injection</b> - With this type of injection, the attacker retrieves data using a different channel. For example, an email, a text, or an instant message could be sent to the attacker with the results of the query. Alternatively, the attacker might be able to send the compromised data to another system. <b>Blind (inferential) SQL injection</b> - With this type of injection, the attacker does not make the application display or transfer any data; rather, the attacker is able to reconstruct the information by sending specific statements and discerning the behavior of the application and database.
<a href="#">Command Injection</a>	Section	22	<b>Command Injection</b> - A command injection is an attack in which an attacker tries to execute commands that she is not supposed to be able to execute on a system via a vulnerable application. Command injection attacks are possible when an application does not validate data supplied by the user (for example, data entered in web forms, cookies, HTTP headers, and other elements). The vulnerable system passes that data into a system shell.
<a href="#">Identifying authentication-based vulnerabilities</a>	List	22	Credential brute forcing Session hijacking Redirecting Exploiting default credentials Exploiting weak credentials Exploiting Kerberos vulnerabilities

Aa Description	☰ Element	▼ Page	☰ Summary
<u>Cross-site Scripting</u>	Section	25	<p><b>Reflected XSS</b> - Reflected XSS attacks (nonpersistent XSS) occur when malicious code or scripts are injected by a vulnerable web application using any method that yields a response as part of a valid HTTP request. An example of a reflected XSS attack is a user being persuaded to follow a malicious link to a vulnerable server that injects (reflects) the malicious code back to the user's browser. <b>Stored/Persistent XSS</b> - Stored, or persistent, XSS attacks occur when the malicious code or script is permanently stored on a vulnerable or malicious server, using a database. These attacks are typically carried out on websites hosting blog posts (comment forms), web forums, and other permanent storage methods. <b>Dom-based XSS</b> - In a DOM-based XSS attack, the attacker sends a malicious URL to the victim, and after the victim clicks on the link, it may load a malicious website or a site that has a vulnerable DOM route handler. After the vulnerable site is rendered by the browser, the payload executes the attack in the user's context on that site. <b>XSS typical locations</b> - Search fields that echo a search string back to the user, HTTP headers, Input fields that echo user data, Error messages that return user-supplied text, and hidden fields that may include user input Applications (or websites) that display user-supplied data.</p>
<u>Cross-Site Request Forgery</u>	Section	27	<p><b>Cross-site request forgery (CSRF or XSRF)</b> - attacks occur when unauthorized commands are transmitted from a user who is trusted by the application. CSRF attacks are different from XSS attacks because they exploit an application's trust in a user's browser. CSRF vulnerabilities are also referred to as <b>one-click attacks</b> or <b>session riding</b>.</p>
<u>OWASP Top 10</u>	Section	29	<p><b>Open Web Application Security Project (OWASP)</b> - is a nonprofit charitable organization that leads several industrywide initiatives to promote the security of applications and software. <b>OWASP Top 10</b> - OWASP lists the top 10 most common vulnerabilities against application at the following address:  <a href="http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project">www.owasp.org/index.php/Category:OWASP_Top_Ten_Project</a></p>

 Description	 Element	 Page	 Summary
<u>Network firewalls</u>	Paragraph	31	<p><b>Network firewalls</b> - Network-based firewalls provide key features that are used for perimeter security, such as Network Address Translation (NAT), access control lists, and application inspection. The primary task of a network firewall is to deny or permit traffic that attempts to enter or leave the network based on explicit preconfigured policies and rules.</p> <p><b>Network firewall techniques</b> - Simple packet-filtering techniques, Application proxies, Network Address Translation, Stateful inspection firewalls, Next-generation context-aware firewalls</p>
<u>Access control lists (ACLs)</u>	Paragraph	31	<p><b>Access Control Lists (ACL)</b> - Are a collection of permit and deny conditions, called rules, that provide security by blocking unauthorized users and allowing authorized users to access specific resources. <b>Access Control Entry (ACE)</b> - Each entry of an ACL is referred to as an access control entry (ACE). <b>ACE packet classification</b> - Layer 2 protocol information such as EtherTypes, Layer 3 protocol information such as ICMP, TCP, or UDP, Layer 3 header information such as source and destination IP addresses, Layer 4 header information such as source and destination TCP or UDP ports</p>
<u>Extended ACLs</u>	Section	34	<p><b>Extended ACLs</b> - the most commonly deployed ACLs.</p> <p><b>Extended ACLs classify packets</b> - Source and destination IP addresses, Layer 3 protocols, Source and/or destination TCP and UDP ports, Destination ICMP type for ICMP packets</p>
<u>Application Proxies</u>	Paragraph	35	<p><b>Application proxies</b> - Application proxies, or proxy servers, are devices that operate as intermediary agents on behalf of clients that are on a private or protected network. Clients on the protected network send connection requests to the application proxy to transfer data to the unprotected network or the Internet.</p>
<u>Network Address Translation (NAT)</u>	Section	36	<p><b>Network Address Translation (NAT)</b> - Several Layer 3 devices can supply Network Address Translation (NAT) services. The Layer 3 device translates the internal host's private (or real) IP addresses to a publicly routable (or mapped) address. By using NAT, the firewall hides the internal private addresses from the unprotected network and exposes only its own address or public range.</p>

Aa Description	≡ Element	▼ Page	≡ Summary
<u>Port Address Translation (PAT).</u>	Section	37	<b>Port Address Translation (PAT)</b> - Typically, firewalls perform a technique called Port Address Translation (PAT). This feature, which is a subset of the NAT feature, allows many devices on the internal protected network to share one IP address by inspecting the Layer 4 information on the packet. This shared address is usually the firewall's public address;
<u>Static Translation</u>	Paragraph	37	<b>Static Translation</b> - A different methodology is used when hosts in the unprotected network need to initiate a new connection to specific hosts behind the NAT device. You configure the firewall to allow such connections by creating a static one-to-one mapping of the public (mapped) IP address to the address of the internal (real) protected device. For example, static NAT can be configured when a web server resides on the internal network and has a private IP address but needs to be contacted by hosts located in the unprotected network or the Internet.
<u>Demilitarized Zones (DMZs).</u>	Paragraph	38	<b>Demilitarized Zones (DMZs)</b> - Firewalls can be configured to separate multiple network segments (or zones), usually called demilitarized zones (DMZs). These zones provide security to the systems that reside within them with different security levels and policies between them.
<u>Application-Based segmentation &amp; Micro-segmentation</u>	Section	39	<b>Cisco Application Centric Infrastructure (ACI)</b> - Provide micro-segmentation capabilities. Micro-segmentation in Cisco ACI can be accomplished by integrating with vCenter or Microsoft System Center Virtual Machine Manager (SCVMM), Cisco ACI API (controller), and leaf switches. <b>Endpoint Groups (EPGs)</b> - Cisco ACI allows organizations to automatically assign endpoints to logical security zones called endpoint groups (EPGs). <b>µSeg EPGs</b> - A micro-segment in ACI. You can apply policies to these segments based on attributes. Applying attributes to µSeg EPGs enables you to apply forwarding and security policies with greater granularity than you can to EPGs without attributes. Attributes are unique within the tenant.

Description	Element	Page	Summary
<a href="#"><u>Understanding global threat correlation capabilities</u></a>	Paragraph	50	<b>Cisco Global Threat Correlation Capabilities</b> - Cisco NGIPS devices include global correlation capabilities that utilize real-world data from Cisco Talos. Cisco Talos is a team of security researchers who leverage big-data analytics for cybersecurity and provide threat intelligence for many Cisco security products and services. Global correlation allows an IPS sensor to filter network traffic using the “reputation” of a packet’s source IP address. The reputation of an IP address is computed by Cisco threat intelligence using the past actions of that IP address. IP reputation has been an effective means of predicting the trustworthiness of current and future behaviors from an IP address.
<a href="#"><u>Advanced Malware Protection (AMP)</u></a>	Paragraph	50	<b>Advanced Malware Protection</b> - Cisco provides advanced malware protection capabilities for endpoint and network security devices.
<a href="#"><u>Cisco Web Security Appliance (WSA)</u></a>	Paragraph	54	<b>Cisco Web Security Appliance (WSA), Cisco Security Management Appliance (SMA), and Cisco Cloud Web Security (CWS)</b> . These solutions enable malware detection and blocking, continuous monitoring, and retrospective alerting. A Cisco WSA uses cloud-based intelligence from Cisco to help protect an organization before, during, and after an attack. <b>Attack Continuum</b> - The life cycle of an attack including before, during, & after.
<a href="#"><u>Cisco Email Security Appliance (ESA)</u></a>	Paragraph	58	<b>Cisco Email Security Appliance (ESA)</b> - Users are no longer accessing email only from the corporate network or from a single device. Cisco provides cloud-based, hybrid, and on-premises solutions based on the Email Security Appliance (ESA) that can help protect any dynamic environment. <b>ESA features</b> - Access control, antispam, network antivirus, Advanced Malware Protection (AMP).
<a href="#"><u>Cisco Identity Services Engine (ISE)</u></a>	Paragraph	60	<b>Cisco Identity Services Engine (ISE)</b> - The Cisco Identity Services Engine (ISE) is a comprehensive security identity management solution designed to function as a policy decision point for network access. It allows security administrators to collect real-time contextual information from a network, its users, and devices.
<a href="#"><u>Security cloud-based solutions</u></a>	Paragraph	62	Cisco Cloud Email Security (CES) Cisco AMP Threat Grid Cisco Threat Awareness Service Umbrella (formerly OpenDNS) Stealthwatch Cloud CloudLock





 Description	 Element	 Page	 Summary
<a href="#"><u>Cisco AMP Threatgrid</u></a>	Paragraph	62	<b>Cisco AMP Threatgrid</b> - Cisco integrated Cisco AMP and Threat Grid to provide a solution for advanced malware analysis with deep threat analytics. The Cisco AMP Threat Grid integrated solution analyzes millions of files and correlates them with hundreds of millions of malware samples. This provides a look into attack campaigns and how malware is distributed.
<a href="#"><u>Umbrella (OpenDNS)</u></a>	Paragraph	63	<b>OpenDNS</b> - Cisco acquired a company called OpenDNS that provides DNS services, threat intelligence, and threat enforcement at the DNS layer. OpenDNS has a global network that delivers advanced security solutions (as a cloud-based service) regardless of where Cisco customer offices or employees are located. This service is extremely easy to deploy and easy to manage.
<a href="#"><u>Stealthwatch Cloud</u></a>	Paragraph	63	<b>Stealthwatch Cloud</b> - Stealthwatch Cloud is a Software as a Service cloud solution. You can use Stealthwatch Cloud to monitor many different public cloud environments, such as Amazon's AWS, Google Cloud Platform, and Microsoft Azure.
<a href="#"><u>CloudLock</u></a>	Paragraph	64	<b>CloudLock</b> - Cisco acquired a company called CloudLock that creates solutions to protect customers against data breaches in any cloud environment and application (app) through a highly configurable cloud-based data loss prevention (DLP) architecture. Policy driven actions: File-level encryption, Quarantine, End-user notifications
<a href="#"><u>Cisco Netflow</u></a>	Paragraph	64	<b>Netflow</b> - NetFlow is a Cisco technology that provides comprehensive visibility into all network traffic that traverses a Cisco-supported device. NetFlow was initially created for billing and accounting of network traffic and to measure other IP traffic characteristics such as bandwidth utilization and application performance. NetFlow has also been used as a network capacity planning tool and to monitor network availability. <b>Netflow in a security context</b> - used as a network security tool because its reporting capabilities provide nonrepudiation, anomaly detection, and investigative capabilities. As network traffic traverses a NetFlow-enabled device, the device collects traffic flow data and provides a network administrator or security professional with detailed information about such flows.







Aa Description	≡ Element	▼ Page	≡ Summary
<u>Data Loss Prevention (DLP).</u>	Paragraph	65	<b>Data Loss Prevention (DLP)</b> - Data loss prevention is the ability to detect any sensitive emails, documents, or information leaving your organization. Cisco ESA → RSA email DLP for outbound email traffic Cisco Cloud Email Service & the Cisco Hybrid Email Security → own DLP. Cisco WSA → can redirect outbound traffic to a third-party DLP solution.
<u>The Principles of the Defense-in-Depth Strategy.</u>	Section	66	<b>Defense-in-Depth Strategy</b> - Layered and cross-boundary “defense-in-depth” strategy is what is needed to protect your network and corporate assets. <b>Nontechnical activities</b> - Nontechnical activities such as appropriate security policies and procedures and end-user and staff training. <b>Physical Security</b> - including cameras, physical access control (such as badge readers, retina scanners, and fingerprint scanners), and locks. <b>Network Security</b> - Network security best practices, such as routing protocol authentication, control plane policing (CoPP), network device hardening, and so on. <b>Host Security</b> - Host security solutions such as advanced malware protection (AMP) for endpoints, antiviruses, and so on. <b>Application Security</b> - Application security best practices such as application robustness testing, fuzzing, defenses against cross-site scripting (XSS), cross-site request forgery (CSRF) attacks, SQL injection attacks, and so on. <b>Data network traversal</b> - you can employ encryption at rest and in transit to protect data. <b>Role-based network security approach</b> - When applying defense-in-depth strategies, you can also look at a roles-based network security approach for security assessment in a simple manner. Each device on the network serves a purpose and has a role; subsequently, you should configure each device accordingly. <b>Management plane</b> - This is the distributed and modular network management environment. <b>Control plane</b> - This plane includes routing control. It is often a target because the control plane depends on direct CPU cycles. <b>User/Data plane</b> - This plane receives, processes, and transmits network data among all network elements. <b>Services plane</b> - This is the Layer 7 application flow built on the foundation of the other layers. <b>Policies</b> - The plane includes the business requirements. Cisco calls policies the “business glue” for the network. Policies and procedures are part of this section, and they apply to all the planes in this list.

Aa Description	≡ Element	▼ Page	≡ Summary
<u>SDN and the traditional management, control, &amp; data plane</u>	Paragraph	68	<p><b>Software-defined networking</b> - Software-defined networking introduced the notion of a centralized controller. The SDN controller has a global view of the network, and it uses a common management protocol to configure the network infrastructure devices. The SDN controller can also calculate reachability information from many systems in the network and pushes a set of flows inside the switches. The flows are used by the hardware to do the forwarding. Here you can see a clear transition from a distributed “semi-intelligent brain” approach to a “central and intelligent brain” approach. <b>Control &amp; Data Plane changes</b> - the big change was in the control and data planes in software-based switches and routers (including virtual switches inside of hypervisors). For instance, the Open vSwitch project started some of these changes across the industry. <b>Management Pane changes</b> - These benefits are in both physical switches and virtual switches. SDN is now widely adopted in data centers. A great example of this is Cisco ACI.</p>
<u>Confidentiality, Integrity, &amp; Availability: The CIA Triad</u>	Section	69	<p><b>Confidentiality</b> - The ISO 27000 standard has a very good definition: “confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.” <b>Integrity</b> - Integrity is the ability to make sure that a system and its data have not been altered or compromised. It ensures that the data is an accurate and unchanged representation of the original secure data. <b>Availability</b> - Availability means that a system or application must be “available” to authorized users at all times. According to the CVSS Version 3 specification, the availability metric “measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability.”</p>

Aa Description	☰ Element	▼ Page	☰ Summary
<u>Risk &amp; risk Analysis</u>	Section	70	<p><b>Risk</b> - In the world of cybersecurity, risk can be defined as the possibility of a security incident (something bad) happening. <b>Federal Financial Institutions Examination Council (FFIEC)</b> - developed the Cybersecurity Assessment Tool (Assessment) to help financial institutions identify their risks and determine their cybersecurity preparedness. <b>FFIEC-Inherent Risk Profile and Cybersecurity Maturity</b> - The Inherent Risk Profile identifies the institution's inherent risk before implementing controls. Cybersecurity includes domains, assessment factors, components, and individual declarative statements across five maturity levels to identify specific controls and practices that are in place. <b>FFIEC-The International Organization for Standardization (ISO) 27001</b> - This is the international standard for implementing an information security management system (ISMS). ISO 27001 is heavily focused on risk-based planning to ensure that the identified information risks (including cyber risks) are appropriately managed according to the threats and the nature of those threats. <b>ISO/IEC 27005 Information technology—Security techniques—Information security risk management</b> - Establish the risk management context, Quantitatively or qualitatively assess risks, Treat risks, Keep stakeholders informed, Monitor &amp; review risks <b>Common Weakness Scoring System (CWSS)</b> - A methodology for scoring software weaknesses. CWSS is part of the Common Weakness Enumerator (CWE) standard. <b>Common Misuse Scoring System (CMSS)</b> - A standardized way to measure software feature misuse vulnerabilities. More information about CMSS is available at <a href="http://scap.nist.gov/emerging-specs/listing.html#cmss">http://scap.nist.gov/emerging-specs/listing.html#cmss</a>. <b>Common Configuration Scoring System</b> - More information about CCSS can be found at <a href="http://csrc.nist.gov/publications/nistir/ir7502/nistir-7502_CCSS.pdf">http://csrc.nist.gov/publications/nistir/ir7502/nistir-7502_CCSS.pdf</a>.</p>
<u>Defining PII</u>	Paragraph	72	<p><b>PII</b> - According to the Executive Office of the President, Office of Management and Budget (OMB), and the U.S. Department of Commerce, Office of the Chief Information Officer, PII refers to "information which can be used to distinguish or trace an individual's identity." <b>Examples of PII</b> - An individuals name, social security number, biological or personal characteristics, date &amp; place of birth, mothers maiden name, credit card numbers, bank account numbers, driver's license, address information (email, street, telephone numbers).</p>

 Description	 Element	 Page	 Summary
<u>Defining PHI</u>	Paragraph	72	The Health Insurance Portability and Accountability Act (HIPAA) requires healthcare organizations and providers to adopt certain security regulations for protecting health information. The Privacy Rule calls this information “protected health information,” or PHI. <b>Examples of PHI</b> - An individual's name (that is, patient's name), All dates directly linked to an individual, including date of birth, death, discharge, and administration, Telephone and fax numbers, Email addresses, and geographic subdivisions such as street addresses, ZIP codes, and county, Medical record numbers and health plan beneficiary number, Certificate numbers or account numbers, Social security number, Driver license number, Biometric identifiers, including voice or fingerprints, Photos of the full face or recognizable features, Any unique number-based code or characteristic, The individual's past, present, and future physical or mental health or condition, The provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual
<u>Principle of Least Privilege</u>	Section	73	<b>Principle of Least Privilege</b> - all users—whether they are individual contributors, managers, directors, or executives—should be granted only the level of privilege they need to do their jobs, and no more. Also known as "need to know".
<u>Separation of Duties</u>	Section	73	<b>Separation of Duties</b> - Separation of duties is an administrative control dictating that a single individual should not perform all critical- or privileged-level duties. The goal is to safeguard against a single individual performing sufficiently critical or privileged actions that could seriously damage a system or the organization as a whole.

Aa Description	☰ Element	▼ Page	☰ Summary
<u>Security Operations Centers (SOCs)</u>	Section	74	<p><b>Security Operations Centers (SOCs)</b> - are facilities where an organization's assets, including applications, databases, servers, networks, desktops, and other endpoints, are monitored, assessed, and protected. <b>SOCs address security questions</b> How can you detect a compromise in a timely manner? How do you triage a compromise to determine the severity and the scope? What is the impact of the compromise to your business? Who is responsible for detecting and mitigating a compromise? Who should be informed or involved, and when do you deal with the compromise once detected? How and when should you communicate a compromise internally or externally, and is that needed in the first place? <b>SOCs need to be effective</b> Executive sponsorship. SOC operating as a program. Organizations should operate the SOC as a program rather than a single project. A governance structure. Effective team collaboration. Access to data and systems. Applicable processes and procedures. Team skill sets and experience. Budget (for example, will it be handled in-house or outsourced?).</p>
<u>Playbooks, Runbooks, &amp; Runbook Automation (RBA)</u>	Section	75	<p><b>Playbooks, Runbooks, and Runbook Automation (RBA)</b> - Organizations need to have capabilities to define, build, orchestrate, manage, and monitor the different operational processes and workflows. <b>Runbook</b> - A runbook is a collection of procedures and operations performed by system administrators, security professionals, or network operators. According to Gartner, "the growth of RBA has coincided with the need for IT operations executives to enhance IT operations efficiency measures." <b>Metrics to measure effectiveness</b> - Mean time to repair (MTTR), Mean time between failures (MTBF), Mean time to discover a security incident, Mean time to contain or mitigate a security incident, Automation of the provisioning of IT resources <b>Examples</b> - Rundeck</p>

 Description	 Element	 Page	 Summary
<u>Digital Forensics</u>	Section	76	<b>Digital/Computer/Cyber Forensics</b> - Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts. (The word forensics means “to bring to the court.”) Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive. <b>Examples</b> - Computers, smartphones, tablets, network infrastructure devices, network management systems, printers, IoT devices.
<u>Understanding chain of custody.</u>	Paragraph	76	<b>Chain of custody</b> - Chain of custody is how you document and preserve evidence from the time you started a cyber forensics investigation to the time the evidence is presented at court or to your executives (in the case of an internal investigation).
<u>Untitled</u>			