Chapter 8 - Key Topics

Description	Element	Page	Summary
Understanding the incident response process at detailed in the NIST SP 800-61 revision 2.	Tip	299	https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
Understanding the differences between security events & security incidents	Summary	299	**NIST SP 800-61 Events** - An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. **NIST SP 800-61 Security Incident** - a computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
Exploring the incident response plan	Summary	301	Incident response plan elements defined in **NIST SP 800-61**: 1. Incident response plan's mission 2. Strategies & goals of the incident response plan 3. Senior management approval of the incident response plan 4. Organizational approach to incident response (playbooks, orchestration, automation) 5. How the incident response team will communicate with the rest of the organization and with other organizations 6. Metrics for measuring the incident response capability and its effectiveness 7. Roadmap for maturing the incident response capability 8. How the program fits into the overall organization
Exploring the incident response process	Summary	302	**NIST Special Publication 800-61 Phases** - Preparation, Detection & Analysis, Containment, Eradication, & Recovery, Post-Incident (Postmortem)
Understanding information sharing & coordination	Summary	304	**Financial Services Information Sharing and Analysis Center (FS-ISAC)** - Information Sharing and Analysis Centers (or ISACs) are private-sector critical infrastructure organizations and government institutions collaborating and sharing information. During the investigation and resolution of a security incident, you may also need to communicate with outside parties regarding the incident. Examples include, but are not limited to, contacting law enforcement, fielding media inquiries, seeking external expertise, and working with Internet service providers (ISPs), the vendor of your hardware and software products, threat intelligence vendor feeds, coordination centers, and members of other incident response teams.
Exploring the VERIS schema & related tools	Paragraph	305	The **VERIS** schema is divided into the following five main categories: 1. Incident Tracking 2. Victim Demographics 3. Incident Description 4. Discovery & Response 5. Impact Assessment

Description	Element	Page	Summary
Listing the different types of incident response teams	List	307	**Product Incident Response Team (PSIRT) National CISRTs & Computer Emergency Response Team (CERT) Coordination Center Incident response teams of security vendors & managed security service providers (MSSP)**
Reviewing the FIRST CSIRT & PSIRT services framework	Tip	309	The Forum of Incident Response and Security Teams (FIRST) has a comprehensive resource called the "Computer Security Incident Response Team (CSIRT) Services": www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1. Similarly, a services framework for PSIRTs is available at www.first.org/standards/frameworks/psirts.
Understanding CVSS	Summary	310	Maintained by FIRST. 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.
Exploring national CSIRTs & computer emergency response teams	Summary	314	Numerous countries have their own Computer Emergency Response (or Readiness) Teams (CERTs). The Forum of Incident Response and Security Teams (FIRST) website includes a list of all the national CERTS and other incident response teams at www.first.org/members/teams. **US-CERT** (www.us-cert.gov) **Indian Computer Emergency Response Team** (www.cert-in.org.in) **CERT Australia** (https://cert.gov.au) **Australian Computer Emergency Response Team** (www.auscert.org.au/).
Defining what coordination centers are	Summary	315	Several organizations around the world also help with the coordination of security vulnerability disclosures to vendors, hardware and software providers, and security researchers.
Surveying incident response providers and managed security service providers (MSSP)	Summary	315	Cisco, along with several other vendors, provides incident response and managed security services to its customers. These incident response teams and outsourced CSIRTs operate differently because their task is to provide support to their customers. **Cisco's Incident Response Service** - This service provides Cisco customers with readiness or proactive services and post-breach support. **Cisco's managed security service** - The Cisco ATA service offers customers 24-hour continuous monitoring and advanced-analytics capabilities, combined with threat intelligence as well as security analysts and investigators to detect security threats in customer networks.

Description	Element	Page	Summary
Exploring the common artifact elements & source of security events	Summary	316	IP Addresses/Hostnames, Event Metadata (timestamps, event/alert severity), URIs/URLs, Client & Server Port Identities, Detailed System Information (Process Information, Information About Files, Registry Entries, Hashes, System API Calls)
Defining the 5-Tuple	Summary	317	IP address, Destination IP address, source port, destination port, protocol
Using file hashes	Summary	320	File hashes are also a key component of many security event logs. For example, the Cisco Advanced Malware Protection (AMP) for Networks and Cisco AMP for Endpoints examine, record, track, and send files to the cloud. The Cisco AMP for Networks creates a SHA-256 hash of the file and compares it to the local file cache. If the hash is not in the local cache, it queries the Cisco FMC.
Tips on building your own lab	Summary	321	The Cyber Ops Associate exam requires you to identify the 5-tuple in packet captures and recognize different application and operating system logs. 1. Start by simply downloading free virtualization platforms like Virtual Box 2. Download any of the popular penetration testing Linux distributions such as Kali, WebSploit, Parrot, or Black Arch (more on that later in this section) and install it on a virtual machine. 3. Download an intentionally vulnerable application or a target VM. 4. To monitor the network and learn how to analyze packet captures, system logs, and use tools like Snort (https://snort.org), download a Linux distribution such as Security Onion (https://securityonion.net).
What are false positives, false negatives, true positives, true negatives	Summary	326	**False Positive (benign triggers)** - is a broad term that describes a situation in which a security device triggers an alarm but no malicious activity or actual attack is taking place. **False Negatives** - term used to describe a network intrusion device's inability to detect true security events under certain circumstances—in other words, a malicious activity that is not detected by the security device. **True Positive** - is a successful identification of a security attack or a malicious event. **True Negative** - occurs when the intrusion detection device identifies an activity as acceptable behavior and the activity is actually acceptable.
What are regular expressions?	Summary	327	A regular expression (sometimes referred to as regex) is a text string for describing a search pattern. Is considered a swiss army knife.
Understanding protocols, protocol headers, & intrusion analysis	Summary	330	Traditional IDS and IPS and next-generation IPS can perform protocol analysis; for example, TCP, HTTP, TLS, Ethernet. Can make sure protocols are compliant. **Packet Capture Utilities (Sniffers)** - one of the best ways to get familiar with packets traversing the network & protocol analysis

Description	Element	Page	Summary
Mapping security event types to source technologies	Summary	333	**Intrusion Detection & Prevention** - Signature-Based Detection, Analysis of Protocol Metadata and Packet Content, Dynamic Cloud-Based Binary Analysis and Advanced Malware Protection (AMP), Sample Products: Cisco Next-Generation IPS Firepower Appliances and Snort. **Anomaly Detection** - Look for Unusually Frequent, Large, or Lengthy Network Sessions, Look for Connections to Suspicious IP Geo-Locations, Each Flow Data Record Contains IPS, Ports, Duration, and Bytes Transferred, Does Not Require as Much Storage Space as Full Packet Capture, Sample Products: Cisco Lancope, Cognitive Threat Analytics **Malware Analysis** - Detects and Blocks Malicious or Zero-Day Exploits, Detonates Suspicious Files (Sandboxing), Analyzes File Behavior (Captures Malicious Network Communication, Dropped Files, Registry/OS Changes, etc.), Sample Products: Cisco Advanced Malware Protection (AMP) for Networks and for Endpoints **Full Packet Capture** - Used for Event Research and Analysis, Confirms True Positive Signature Alerts, Stores All Network Traffic, Including Packet Payload, Requires Large Amounts of Storage Space, Sample Products: Moloch, Wireshark, Netwitness **Protocol Metadata** - Contains Only Packet Metadata, No Payload, Used for Event Research and Analysis, Useful for Alerting in Siem Reports, Does Not Require as Much Storage Space as Full Packet Captures, Sample Technologies and Products: NetFlow, IPFIX, Cisco Tetration, QOSMOS
Untitled			