









Chapter 10 - Key Topics

 Description	 Element	 Page	 Summary
<u>Understanding network infrastructure & their sources</u>	Paragraph	373	Logs from network devices such as firewalls, routers, and switches can prove useful when you're proactively detecting or responding to a security incident. For example, brute-force attacks against a router, switch, or firewall can be detected by system log (syslog) messages that could reveal the suspicious activity. Log collectors often offer correlation functionality to help identify compromises by correlating syslog events.
<u>Understanding the importance of network time protocol in security monitoring & log management</u>	Summary	374	Before sending Syslog messages, you need to make sure networked devices have the correct time, otherwise it's useless. As a best practice, you should configure all network devices to use Network Time Protocol (NTP). Using NTP ensures that the correct time is set and that all devices within the network are synchronized.
<u>Analyzing traditional firewall logs</u>	Summary	378	Cisco ASA supports the following logging capabilities: Console Terminal Adaptive Security Device Manager (ASDM) Email External syslog server External SNMP server Buffered
<u>Analyzing syslog & logging in large-scale environments</u>	Summary	381	Large organizations use more scalable and robust systems for log collection and analysis. Examples, Splunk, Graylog, Elasticsearch, Logstash, & Kibana (ELK) stack

Aa Description	☰ Element	▼ Page	☰ Summary
<u>Analyzing next-generation firewall & next-generation IPS events</u>	Summary	385	<p>Next-generation firewalls, such as the Cisco ASA with FirePOWER services and Cisco Firepower Threat Defense, and next-generation IPS devices such as the Cisco Firepower Next-Generation IPS appliances provide a more robust platform known as the Cisco Firepower System which allows more granular monitoring of networks and access control policy enforcement. In a typical deployment, multiple managed devices installed on network segments monitor traffic for analysis and report to a Firepower Management Center (FMC). The FMC is the heart of all reports and event analysis.</p>
<u>Using the Cisco FMC to analyze next-generation firewall & next-generation IPS events</u>	Summary	390	<p>Next-generation firewalls and next-generation IPS systems via the FMC also support an incident lifecycle, allowing you to change an incident's status as you progress through your response to an attack. When you close an incident, you can note any changes you have made to your security policies as a result of any lessons learned. Generally, an incident is defined as one or more intrusion events that you suspect are involved in a possible violation of your security policies. In the FMC, the term also describes the feature you can use to track your response to an incident.</p>

Aa Description	☰ Element	▼ Page	☰ Summary
Understanding & analyzing NetFlow data	Summary	395	<p>NetFlow is a Cisco technology that provides comprehensive visibility into all network traffic that traverses a Cisco-supported device. Originally built for accounting and billing of network traffic. Now used for capacity planning, monitoring, reporting, investigations, and nonrepudiation. NetFlow network telemetry - See what is actually happening across the entire network, Identify DoS attacks, Quickly identify compromised endpoints and network infrastructure devices, Monitor network usage of employees, contractors, or partners, Obtain network telemetry during security incident response and forensics, Detect firewall misconfigurations and inappropriate access to corporate resources NetFlow IPv4/IPv6 Crucial Roles - Network planning, Network security, Network troubleshooting, Traffic engineering</p>
Understanding the different NetFlow versions	Table 10-4	401	<p>Version 1 (v1) [Obsolete]- the first implementation of NetFlow, limited to IPv4 without IP network masks and autonomous system numbers. Version 2 (v2) - never released Version 3 (v3) - never released Version 4 (v4) - never released Version 5 (v5) - This was a popular NetFlow version on many routers from different vendors. It was limited to IPv4 flows. Version 6 (v6) [Obsolete] - No longer supported Version 7 (v7) [Obsolete] - Like version 5, this version had a source router field. Version 8 (v8) [Obsolete] - This version had several aggregation forms, but only for information that is already present in v5 records. Version 9 (v9) - This version is template based and it is mostly used to report flows such as IPv6, Multiprotocol Label Switching (MPLS), and even plain IPv4 with Border Gateway Protocol (BGP) next hop. IPFIX - IPFIX is an IETF standard based on NetFlow v9 with several extensions.</p>

 Description	 Element	 Page	 Summary
<u>Understanding how Network Address Translation (NAT) & Port Address Translation (PAT) can introduce challenges for network security monitoring.</u>	Paragraph	405	Network Address Translation (NAT) can be a challenge for security monitoring. If you collect information after a network infrastructure device has “translated” the IP packets, you will only see the “translated address” in NetFlow records or packet captures. This scenario is more challenging if the infrastructure device is configured for Port Address Translation (PAT)
<u>Analyzing network packet captures</u>	Summary	414	Full packet capture can be very useful to see exactly what’s happening on the network however packet captures take up a lot of system resources. Sniffers - packet capture tools Pros/Cons - Packet captures provide a full historical record of a network transaction or an attack. It is important to recognize that no other data source offers this level of detail. Packet capture data requires understanding and analysis capabilities. Collecting and storing packet captures takes a lot of resources. Depending on your environment, this can be fairly expensive. Packet Capture Utilities - tcpdump, wireshark, netscout, solarwinds deep packet inspection & analysis
<u>Understanding basic network profiling</u>	Summary	418	Determining throughput, ports used, session duration, & address used can be used for basic network profiling.