Chapter 13 - Key Topics

Description	Element	Page	Summary
Describing Data Normalization	Paragraph	522	Data normalization is the process of capturing, storing, and analyzing data (security-related events, in this case) so that it exists in only one form. One of the main goals of data normalization is to purge redundant data while maintaining data integrity. The normalized data is protected by making sure that any manifestation of the same data elsewhere is only making a reference to the data that is being stored.
Understanding how to interpret common data values into a universal format	Paragraph	523	It is important that you have a way to interpret common data values into a universal format and have a good data model. Okay, so what's a data model? It is a hierarchically structured mapping of semantic knowledge about one or more data sets. Having a good data model for all your security event data allows you to build an assortment of specialized (and fast) queries of those data sets.
Identifying the five elements that make up the 5-tuple	Figure 13-2	524	Source IP Destination IP Source Port Destination Port Protocol
Defining what retrospective analysis is and how to identify malicious files	Paragraph	525	Cisco Advanced Malware Protection (AMP) for Networks and AMP for Endpoints provide mitigation capabilities that go beyond point-in-time detection. They use threat intelligence from Cisco TALOS to perform retrospective analysis and protection. Cisco AMP also provides device and file trajectory capabilities to allow the security administrator to analyze the full spectrum of an attack.

Description	Element	Page	Summary
Mapping threat intelligence with DNS & other artifacts	Paragraph	527	Security threat intelligence is extremely useful when you need to correlate events and gain an insight into what known threats are in your network. DNS intelligence and URL reputation are used in many security solutions such as the Cisco Firepower appliances, Cisco Firepower Threat Defense (FTD), the Cisco Web and Email security appliances, and Cisco Umbrella. For instance, you can correlate security events based on threat intelligence to identify communications to known malicious command and control (CnC orC2) servers and other malicious communication based on DNS information.
Contrasting probabilistic vs. deterministic analysis	Paragraph	527	**Deterministic Analysis** - All data used for the analysis is known beforehand. **Probabilistic Analysis** - Probabilistic analysis, on the other hand, is done assuming the likelihood that something will or has happened, but you don’t know exactly when or how.
Untitled			