




# Chapter 8 - Key Terms

 Term	 Page	 Description
<u>False Positive</u>	581	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. In other words, false positives are false alarms. They are also called benign triggers. False positives are problematic because by triggering unjustified alerts, they diminish the value and urgency of real alerts. If you have too many false positives to investigate, it becomes an operational nightmare, and you most definitely will overlook real security events.
<u>False Negative</u>	581	A 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.
<u>True Positive</u>	589	A term used to describe successful identification of a security attack or a malicious event.
<u>True Negative</u>	589	A term used to describe when the intrusion detection device identifies an activity as acceptable behavior and the activity is actually acceptable.
<u>Regular Expression</u>	586	A text string for describing a search pattern. Sometimes referred to as regex.
<u>Sniffer</u>	587	A full packet capture software.