




Chapter 15 - Key Terms

 Term	 Page	 Description
<u>Threat Hunting</u>	588	The process of iteratively looking for threats that could have probably bypassed security technology and monitoring capabilities. Threat hunters assume that an attacker has already compromised the network.
<u>Yeti</u>	590	An open-source tool used to organize and analyze threat intelligence.
<u>Caldera</u>	579	An open-source tool developed by MITRE to perform automated adversarial emulations.
<u>Atomic Red Team</u>	578	An open-source framework created by Red Canary that provides a list of machine-readable adversarial tactics and techniques that can be integrated with other tools to perform automated simulated attacks.