Chapter 15 - Key Topics

Description	Element	Page	Summary
Understanding who performs threat hunting	Summary	554	The hunting process requires deep knowledge of the network and often is performed by SOC analysts (otherwise known as investigators, threat hunters, tier 2 or tier 3 analysts, and so on).
Threat Hunting vs. Traditional SOC Operations vs. Vulnerability Management	Section	555	**Vulnerability Management** - the process of patching vulnerabilities across the systems and network of your organization, including cloud-based applications in some cases. **Traditional SOC Operations** - A reactive process based on detecting and responding to security incidents. **Threat Hunting** - Threat hunters assume that an attacker has already compromised the network. Subsequently, they need to come up with a hypothesis of what is compromised and how an adversary could have performed the attack. For the threat hunting to be successful, hunters need to be aware of the adversary tactics, techniques, and procedures (TTPs) that modern attackers use. This is why many organizations are using MITRE’s ATT&CK framework to be able to learn about the tactics and techniques of adversaries.

Description	Element	Page	Summary
Understanding the threat-hunting process	Summary	556	1. Threat hunting starts with a trigger based on an anomaly, threat intelligence, or a hypothesis (what could an attacker have done to the organization?). From that moment you should ask yourself: "Do we really need to perform this threat-hunting activity?" or "What is the scope?" 2. Then you identify the necessary tools and methodologies to conduct the hunt. 3. Once the tools and methodologies are identified, you reveal new attack patterns, TTPs, and so on. 4. You refine your hunting tactics and enrich them using data analytics. Steps 2–3 can take one cycle or be iterative and involve multiple loops (depending on what you find and what additional data and research need to be done). 5. A successful outcome could be that you identify and mitigate the threat. However, you need to recognize that in some cases this may not be the case. You might not have the necessary tools and capabilities, or there was no actual threat. This is why the success of your hunting program depends on the maturity of your capabilities and organization as a whole.
Defining the MITRE ATT&CK for Matrix for Enterprise & PRE-ATT&CK.	Paragraph	558	**ATT&CK** - (https://attack.mitre.org) is a collection of different matrices of tactics and techniques. **PRE-ATT&CK** - (https://attack.mitre.org/tactics/pre) includes the tactics and techniques that adversaries use while preparing for an attack, including the gathering of information (open-source intelligence [OSINT], technical and people weakness identification, and more).
The Life of a Cyber Attack, PRE-ATT&CK, & ATT&CK	Figure 15-7	558	See page for visual

Description	Element	Page	Summary
Automated Adversarial Emulation	Section	563	**Caldera** - MITRE, and others in the industry have created several open-source tools to provide automated adversary emulation that can also help with some aspects of threat hunting. Caldera is one of those tools. Caldera was originally created by MITRE, but many security experts across the industry contribute to it. You can download Caldera from https://github.com/mitre/caldera. **Caldera Components** - Caldera Core services (TTPs, command & control, other capabilities), Plug-ins, Agents (Linux, Windows, macOS) See page for a visual diagram. **Atomic Red Team** - is another tool/ecosystem that can be used to perform automated adversary emulation. Atomic Red Team is a collection of adversarial techniques mapped to MITRE's ATT&CK documented in GitHub (https://github.com/redcanaryco/atomic-redteam).
Threat Hunting, Honeypots, HoneyNets, and Active Defense	Section	571	For many years, security professionals have used honeypots and honeynets to help detect attacks and learn adversary TTPs. **Honeypot** - a decoy system. **HoneyNet** - a collection of decoys. **honeypotting as a service** - essentially, you can buy on-demand honeypot services that reduce the time and effort required to set up and monitor a honeypot. **Active Defense** - involves actively responding to adversaries once detected. The nature and scope of the response can vary. It could be that you enhance your monitoring capabilities or that you isolate attackers to one area of your network to learn their TTPs. Some people confuse honeypots/honeynets and active defense with threat hunting.
Untitled			