# Chapter 14 - Key Topics

| Description | Element | Page | Summary |
|---|---|---|---|
| Understanding the Diamond Model of Intrusion | Summary | 532 | The Diamond Model is designed to represent a cybersecurity incident and is made up of four parts. **Adversary** - Active intrusions start with an adversary who is targeting a victim. **Capabilities** - Capabilities can be various forms of tools, techniques, and procedures and will use along some form of infrastructure. **Infrastructure** - The adversary will use various capabilities along some form of infrastructure to launch an attack against the victim. **Victim** - An adversary targetes a victim. See page for visual. |
| The Extended Diamond Model of Intrusion | Figure 14-2 | 534 | The Diamond Model can be expanded further by adding two additional meta-features that establish connections between relations. **Technology** - The technology meta-feature connects capabilities and infrastructure by describing the technology used between these two parts of the model. **Social-Political** - The social-political meta-feature represents the relationship between the adversary and victim. See page for visual. |
| MITRE's ATT&CK & the Diamond Model of Intrusion | Summary | 535 | You can also combine the Diamond Model of Intrusion methodology with MITRE's ATT&CK to learn more about the adversary's tactics, techniques, and procedures (TTPs). **Activity Threads** - The relationships between diamonds are known as activity threads, which can spread across the same attack as well as connect other attacks, depending on gathered intelligence that meets activity group requirements. |

| Description | Element | Page | Summary |
|---|---|---|---|
| Developing an Activity Thread | Figure 14-8 | 538 | **Activity Threads** - The relationships between diamonds are known as activity threads, which can spread across the same attack as well as connect other attacks, depending on gathered intelligence that meets activity group requirements. **Attack Graph** - Once the incident management team builds a decent-sized activity group mapping out multiple incidents, the team can better analyze the data to fill in missing knowledge gaps and start to potentially predict future attack paths. This can be built into an attack graph. **Activity Threats** - Are paths the adversary has already taken. **Activity-Attack Graph** - Combining the attack and activity data gives the team an activity-attack graph, which is useful for highlighting the attacker's preferences for attacking the victim as well as alternative paths that could be used. This gives the incident response team a way to focus efforts on defending against the adversary, by knowing where to likely expect the attack as well as being aware of other possible risks to the victim. See page for visual example. |
| Understanding the phases of the Kill Chain Model | List | 539 | Reconnaissance Weaponization Delivery Exploitation Installation Command & Control (C2 or CnC) Actions on objectives |
| Early and Late Detection in the Kill Chain Example | Figure 14-10 | 540 | **Early Detection** Example - Early detection could be identifying the website attempting to exploit the host. **Late Detection** Example - The network IPS identifying an internally breached host system with ransomware installed that's communicating out to a remote server that will initiate the encryption handshake process. See page for visual example |

| Description | Element | Page | Summary |
|---|---|---|---|
| The Kill Chain vs. MITRE's ATT&CK | Section | 548 | **MITRE's ATT&CK Blue Team** - Blue Team = defenders. Blue teamers use to better understand adversary techniques to protect their organization. To perform threat hunting. **MITRE's ATT&CK Red Team** - Red Team = Offensive security, mock adversary. Red teamers use it to perform adversarial attack emulation and simulations. **MITRE ATT&CK Tactics -** Initial Access, Execution, Persistence, Privilege Escalation, Credential access, Discovery, Lateral movement, Collection, Command & control, Exfiltration, Impact **MITRE ATT&CK Matrices** - PRE-ATT&CK, Windows, Linux, MacOS, Mobile, Cloud, ICS |
| Untitled | | | |