Attack Frameworks and Identifying Attacks

Incident responders frequently need ways to describe attacks and incidents
using common language and terminology.

MITRE's ATT&CK

Includes detailed descriptions, definitions, and examples for the complete threat lifecycle from initial access through execution, persistence, privilege escalation, and exfiltration.

At each level, it lists techniques and components, allowing threat assessment modeling to leverage common descriptions and knowledge.

ATT&CK matrices include pre-attack, enterprise matrices focusing on Windows, macOS, Linux, and cloud computing, as well as iOS and Android mobile platforms.

It's the most comprehensive freely available database and it has broad support in a variety of security tools

http://attack.mitre.org/

Diamond Model of Intrusion Analysis

The Diamond Model of Intrusion Analysis describes a sequence where an adversary deploys a capability targeted at an infrastructure.

capability here means any tool, technique, resource..

Specific Terms

Core Features for an event, which are the adversary, capability, infrastructure, and victim (the vertices of the diamond)

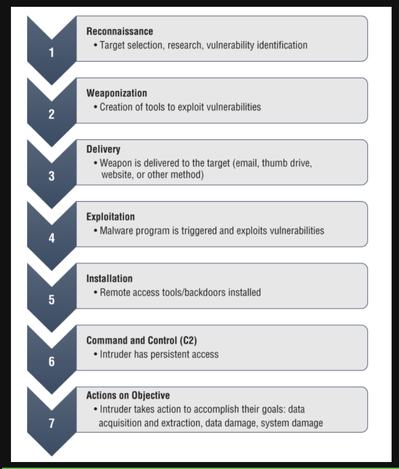
The Meta-Features, which are start and end timestamps, phase, result, direction, methodology, and resources, which are used to order events in a sequence known as an activity thread, as well as for grouping events based on their features

A Confidence Value, which is undefined by the model but that analysts are expected to determine based on their own work

The Diamond Model focuses heavily on understanding the attacker and their motivations, and then uses relationships between these elements to allow defenders to both understand the threat and think about what other data or information they may need to obtain or may already have available.

http://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

Lockheed Martin's Cyber Kill Chain



7-Step process

Reconnaissance

Attacker
Plan their attack and gather information about the target including open source intelligence or active scanning

Defender
Gather data about reconnaissance activities and prioritize defenses based on that information

Weaponization

Attacker
Build and acquire a weponizer, which combines a malware and an exploit into a payload that can be delivered to the target

Defender
Conduct full malware analysis to understand what payload is being dropped and how the exploit was made

Build detections for weponizers and look at the timeline of when the malware was created and whether it's widely shared or closely held

Delivery

Attacker
Deploy the payload whether by dropping it directly or by sending it through an email or other techniques

Defender
Observe how the attack was delivered and what was targeted and then try to infer what the adversary is intending to accomplish

Exploitation

Attacker
Uses the payload to gain access

Defender
Focus on user awareness, secure coding, vulnerability scanning, etc... to ensure that the organization have strong security and very limited attack surface

Installation

Attacker
Focus on persistent backdoor access

Defender
Monitor typical artifacts of a persistent remote shell or other remote access methodologies

Command and Control (C2)

Attacker
Allow 2 way communication and continued control of the remote system using C2

Defender
Detect C2 by hardening the network, deploying detection capabilities, and conducting ongoing research to ensure awareness of new C2 technologies

Actions on Objective

Attacker
Achieving the goal of the mission

Defender
Establish incident response playbook

http://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf