Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model: a comparison of cyber intrusion analysis models

Francesco Maria Ferazza

Technical Report

RHUL–ISG–2022–5

11 April 2022

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

ABSTRACT

Every day Advanced Persistent Threats become more sophisticated and aggressive, and so do their attacks and intrusions. Many intrusion analysis models and frameworks exist to help defenders and analysts in their efforts to understand and counter advanced adversarial campaigns.

This dissertation analyses the three most renowned and widely used models, Lockheed Martin's Cyber Kill Chain, MITRE's ATT&CK framework, and the Diamond Model.

A method to compare them, based on the differences between their purposes, designs, and levels of abstraction, will be presented and used.

This comparison will highlight the ontological and eschatological differences between the models and will illustrate how the three of them can be harmoniously used in a complementary, integrated way.

KEYWORDS:

CYBER KILL CHAIN | MITRE ATT&CK | DIAMOND MODEL | APT | INTRUSION ANALYSIS | INTELLIGENCE ANALYSIS | DEFENSIVE GAP ASSESSMENT | CYBER SECURITY ONTOLOGY