The Diamond Model of Intrusion Analysis

Sergio Caltagirone, Andy Pendergast, and Chris Betz

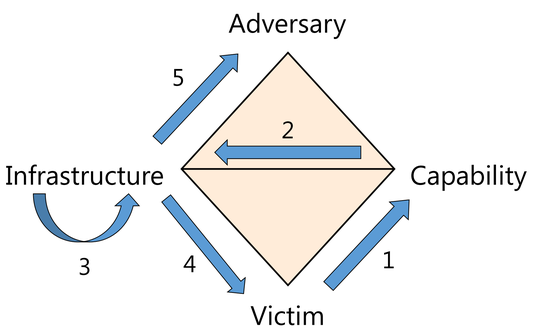
DiamondModel.org

About

The Diamond Model accurately details the fundamental aspects of all malicious activity as well as the core analytic concepts used to discover, develop, track, group, and ultimately counter both the activity and the adversary.

The Diamond is unique. It is at the same time formal and informal, simple and complex. It is simple and informal enough to be used by analysts daily in pursuit of the adversary. Yet, it is complex and formal enough to establish a mathematical framework upon which to apply advanced concepts such as clustering, classification, game theory, graph analysis, and others.

Pivoting

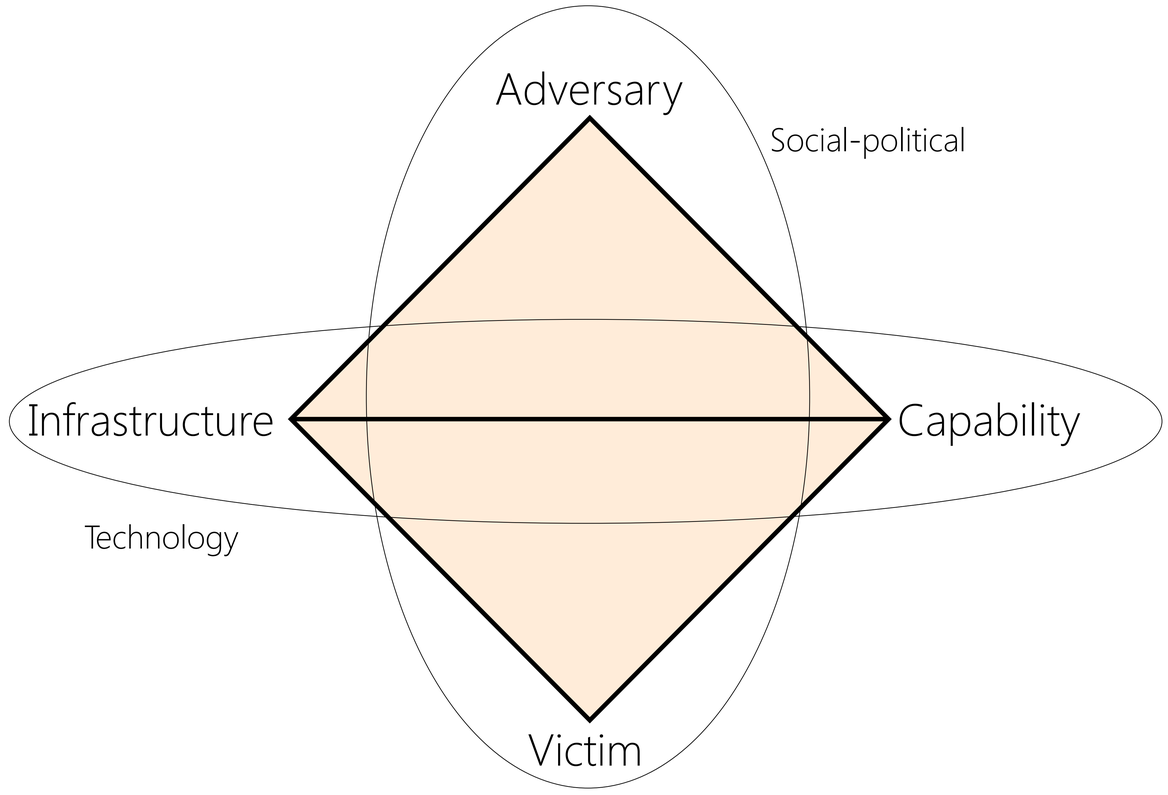


Pivoting is the analytic technique of extracting a data feature and exploiting that feature, in conjunction with data sources, to discover other related features. Pivoting success relies on the understanding of the relationship between features. The Diamond edges illustrate the relationship between features and highlight potential pivot opportunities.

Pivot Scenario

1. Victim discovers malware capability
2. Malware capability reversed to discover C2 domain
3. Domain resolved to C2 IP address
4. Firewall logs reveal further victims contacting C2 IP address
5. IP address ownership reveals adversary

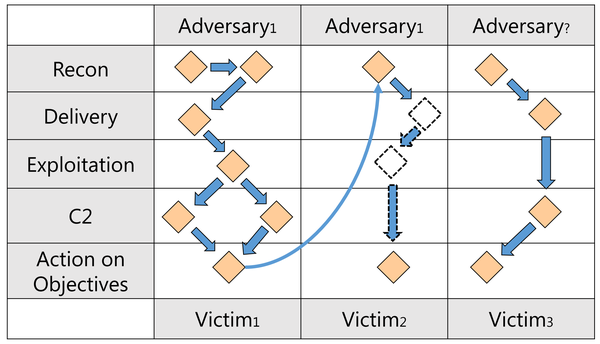
Diamond Event



The model establishes the basic atomic element of any intrusion activity, the event, composed of four core features: adversary, infrastructure, capability, and victim. It further defines two important meta-features, technology connecting the infrastructure and capability enabling operations and the social-political meta-feature describing the always-existing, and sometimes enduring, relationship between adversary and victim.

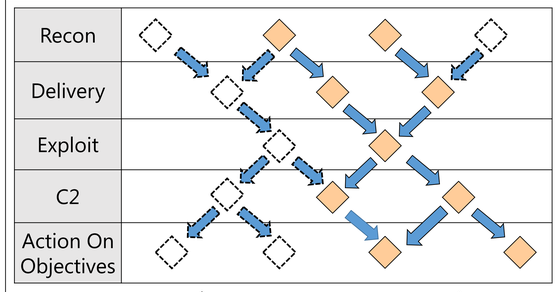
These features are edge-connected representing their underlying relationships and arranged in the shape of a diamond, giving the model its name: the Diamond Model. It further defines additional meta-features to support higher-level constructs such as linking events together into activity threads and further coalescing events and threads into activity groups.

Activity Threads



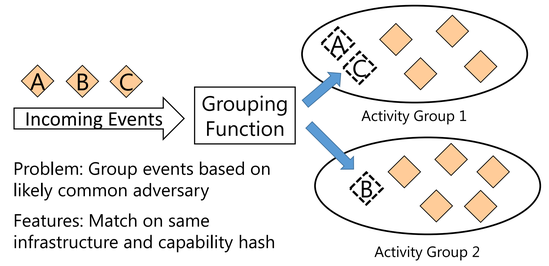
Events uncovered through pivoting are threaded into causal relationships using a n-phased approach. The chain of causal events between an adversary and victim is called an **activity thread**. The illustration shows the thread of events Adversary$_1$ took to achieve their objective against Victim$_1$. Further, Adversary$_1$ used Victim1 against Victim$_2$. Dashed events are hypotheses to be tested later. There is a third activity which has no known linkages to the other two and has an unknown adversary. Sub-graphs are known as **adversary processes** and are useful in identifying adversary behaviors.

Activity-Attack Graphs



The Diamond Model integrates the known malicious events of a activity thread with the postulated attack paths of an attack graph into a new form: the **Activity-Attack Graph**. This allows defenders to not only remediate what is known, but also preempt the adversary based on what is possible and informed by adversary preference.

Activity Groups



Diamond events, adversary processes, and activity threads can be grouped based on feature similarity – these are called **activity groups** and can answer many questions including:

- Identifying a likely common adversary between campaigns
- Identifying shared infrastructure and capabilities
- Trending adversary changes over time

Steps to establish an activity group

1. Define the problem
2. Feature selection
3. Create
4. Grow
5. Analyze
6. Redefine