Abstract to Accompany Diamond Model Poster

The Diamond Model is a novel understanding of intrusion analysis which establishes the foundational method of our discipline. The model establishes the basic atomic element of any intrusion activity, the event, composed of four core features present in all malicious activity: adversary, infrastructure, capability, and victim. These features are edge-connected representing their underlying relationships and arranged in the shape of a diamond. The Model further defines additional meta-features to support higher-level constructs such as the always present, and sometimes enduring, social-political relationship between adversary and victim as well as the technology enabling the capability and infrastructure.

By organizing the features by their inherit relationships in an edge-connected manner, it highlights the model's strongest feature: pivoting. Pivoting is the ability to derive new related information about malicious activity from a known feature. By organizing features by their fundamental relationships, the Diamond highlights pivoting opportunities which uncovers previously unknown features of the malicious activity.

The Diamond Model goes much further than the atomic event. Its features enable linking events together into activity threads describing their causal and temporal order which highlights opportunities for mitigation as well as knowledge gaps. These threads can then be combined with attack graphs into an Activity-Attack Graph which combines what has happened with what could happen allowing mitigation plans to encompass adversary preference and preempt adversary changes.

Analysts can go even further into coalescing events and threads into activity groups which can help address a myriad of higher-order questions such as identifying a common adversary between events, exploring trends and evolution of activity over time, and looking for a common capability developer.

These elements, the event, thread, and group all contribute to a foundational and comprehensive model of intrusion activity built around analytic processes. It captures the essential concepts of intrusion analysis and adversary operations while allowing the model flexibility to expand and encompass new ideas and concepts. This model establishes, for the first time, a formal method applying scientific principles to intrusion analysis – particularly those of measurement, testability, and repeatability – providing a comprehensive method of activity documentation, synthesis, and correlation. This scientific approach and simplicity produces improvements in analytic effectiveness, efficiency, and accuracy.

Ultimately, the model provides opportunities to integrate intelligence in real-time for network defense, automating correlation across events, classifying events with confidence into adversary campaigns, and forecasting adversary operations while planning and gaming mitigation strategies.