WRITING SAMPLE

No Threat is an Island

The Diamond Model of Intrusion Analysis

You've collected plenty of data via sharing and purchased feeds, but now you have to figure out what it all means. One piece of data doesn't tell a story by itself; it has to be evaluated in relation to other data in order to be useful. The Diamond Model of Intrusion Analysis offers a way to look at those relationships between data points to gain a deeper understanding of the threats against your organization.

Imagine a diamond shape. It has pointed corners connected by edges. Now imagine that each corner of the diamond contains one type of event –adversary operations, adversary capabilities, infrastructure, or victims.

If you just look at a single corner, you'll see a narrow view that isn't very useful. For instance, if you look only at adversary operations you'll learn about what the bad actors are doing, but not what actions, technology, or types of organizations they might target next.

However, if you connect each corner of the diamond to all of the others, a sharp picture of your threats will emerge. From any point on the diamond (adversary, capability, infrastructure, victim), you can 'see' another view of the threat -- who, how, possibly why, and what's likely to happen next. The action of moving from one point to another to gain a different view is called **analytic pivoting** – or just **pivoting**.

For example, you've probably discovered some malware on your network. Reverse the pivot and the command-and-control domain can be exposed. Resolve the domain and the underlying IP address of the malware controller's host is revealed. Examine firewall logs to discover which other hosts in your network have been compromised. Then the IP address registration can be used to potentially identify the attacker. Now you know the who, what, how, and maybe the why of your event, so you have a better chance of predicting the what-next.

There are different ways of using the Diamond Model. **Centered approaches** are based on different corners and edges of the diamond. They can be used alone or in conjunction with each other to gain a more complete picture of threats, and thus determine more effective actions. Some common approaches include:

Victim-centered approach

Most organizations take this approach through network and host monitoring, detection, and defense operations. In the victim-centered approach, data related to a victim is used to learn about an adversary. Threat activities against a victim reveal the adversary's capabilities and infrastructure. In some cases, analysts have watched an attack in action in order to see how the adversary operates; this can allow organizations to predict who might be targeted next

Capability-centered approach

This approach, most commonly used by anti-virus manufacturers, looks at a specific capability. By focusing on a known capability, analysts can determine potential new victims, as well as the infrastructure and technology that support the capability. Also, analysts can gather clues to related capabilities and possible clues to the adversary's identity.

Infrastructure-centered approach

Focusing on the adversary's infrastructure reveals the victims that are in contact with the infrastructure, the capabilities controlled by the infrastructure, any related infrastructures, and possible clues to the adversary.

Adversary-centered approach

This is possibly the most difficult of the centered approaches to utilize. It requires direct monitoring of an adversary's activities in order to learn about their infrastructure and capabilities, so it's limited by the need for access to their operations.

Social-political-centered approach

This approach does not lead directly to new elements or indicators. Rather, it uses an expected adversary-victim relationship to hypothesize who might be a victim and who is likely to attack that victim, or who might be an adversary and who that adversary might

attack. For instance, organizations in one country might be targeted by a rival country with which it is at war.

Technology-centered approach

This approach looks at potential misuse or peculiar use of a technology. For instance, peculiar activity might indicate that adversaries are trying to find and exploit a vulnerability. The techniques they use can then be used to deduce which infrastructure and capabilities will be used to conduct a future attack.