Why did we make this Diamond thing?  
ca. 2006... ZOMG APTz!!!

---

As a group of analysts, we needed a systematic, repeatable way to:
1. characterize organized threats
2. consistently track them as they evolve
3. sort one from another
4. and then figure out ways to counter them.
CURRENT USAGE

- Cognitive model used by hundreds of Intel, Threat Intel, DFIR analysts
- “Foundational” concepts for emerging cyber ontologies/standards/protocols e.g. STIX
- Set and Graph theory based model used as the “bones” within systems such as ThreatConnect
DIAMOND 101: EVENTS, EDGES, AND META FEATURES

Events=Diamonds
Each Event is characterized by and requires four Core Features (aka nodes, vertices):

- Badguy Persona: email addresses, handles, phone #’s
- Network Assets
- Malware
- Exploits
- Hacker Tools
- Stolen Certs

Meta-Features
- Timestamp
- Phase: e.g. Kill-Chain
- Result: Success, Failure, etc.
- Direction: i2v, i2i, a2i, etc
- Methodology: Class of Activity
- Resources: Necessary elements to carry out the event.

Unknowns and Uncertainty
Welcome...
Victim Discovers malware: $0606c10388c306f393128237f75e440f$

Malware contains C2 Domain: info.officelatest[.]com

C2 domain resolves to IP Address: 142.91.132.23

Domain WHOIS provides registrant: tommy.bibber1234321@ddd.com

NOTE: I did not limit myself to observables/indicators on my network. I left the victim space in the first pivot to DISCOVER more about the Adversary and his Capabilities and Infrastructure.
DIAMOND 121: EXTENDED DIAMOND

Social-Political Meta-Feature: A relationship always exists between the adversary and the victim.

Intent: You can use well defined Activity Groups to better understand this relationship and infer Intent.

Technology Meta-Feature: Represents the technology connecting & enabling the capability and infrastructure to operate.

Analyzing underlying technology w/o knowledge of specific infrastructure or capability can reveal malicious activity.
Working with the Cyber Kill-Chain™: Leveraging the Meta Features allows grouping of events into ordered, causal chains of activity separated by phases.

Vertical Correlation: IR Process of identifying causal events in an Activity Thread.

Directed Arcs allow for “looping” events through phases.

Hypothesis generation is supported (note the dashed-diamond in Incident 2).

Horizontal Correlation: Correlations between Activity Threads (Incidents here) can be made to enable grouping.
TYPICALLY used initially to identify a common Adversary. But not limited to this. Some Other Examples:

- Trending
- Intent Deduction
- Adversary Capabilities and Infrastructure
- Cross-Capability Identification
- Adversary Campaign Knowledge Gap Identification
- Automated Mitigation Recommendation
- Common Capability Development Deduction
- Center of Gravity Identification

Activity Group: common/similar malicious events, adversary processes, and threads.
Define the Problem: “I want to define a common adversary behind events and threats using similarities in infrastructure and capabilities.”

Other ways this may manifest:
What makes APT1 activity APT1?,
What makes Rocra malwareRed October and not someone else?
Does PoisonIvy, PlugX, 9002 = the same APT?

Feature Selection: Define what combination of elements (Ips, Domains, Malware, Processes) are criteria for grouping and select your data set(s) to search for this criteria. Criteria can be confidence weighted.

Steps to Create an Activity Group

1. Define the Problem
2. Feature Selection
3. Create
4. Grow
5. Analysis
6. Redefine
DIAMOND 201: CREATING ACTIVITY GROUPS

Create: The feature selection you chose can be used cognitively for clustering or it can be applied in a group creation function.

Grow: Once created, the Activity Groups can be grown by iterating the group creation function over newly available data.
DIAMOND 201: CREATING ACTIVITY GROUPS

Analysis: Now that we have a healthy Activity Group, growing as things change; I can fill knowledge gaps, define new problems like:

- **Trending**: How has an adversary’s activity changed over time and what is the current vector to infer future change?
- **Intent Deduction**: What is the intent of the adversary?
- **Adversary Capabilities and Infrastructure**: What is the complete set of observed capabilities and infrastructure of the adversary?
- **Cross-Capability Identification**: Which capabilities have been used by multiple adversaries?
- **Adversary Campaign Knowledge Gap Identification**: What are the organization’s knowledge gaps across an adversary’s campaign?
- **Automated Mitigation Recommendation**: When an event is detected which adversary is behind the event and what action can/should be taken?
- **Common Capability Development Deduction**: Which capabilities show evidence of common authors/developers?
- **Center of Gravity Identification**: Which resources and processes are the most common and critical to an activity and/or campaign?

Or... **Redefine**: through knowledge learned I may want to go back and revisit my grouping function.
**ADVANCED DIAMOND: ACTIVITY-ATTACK GRAPHS FOR MITIGATION**

*Attack Graphs* identify and enumerate paths an adversary *could* take. They are exhaustive.

*Activity Threads* define paths an adversary *has* taken.

If you overlay what *could* happen with what *has* happened you get an *Activity-Attack Graph*.

**Key Benefits:**
- It highlights attacker preferences alongside possible alternative paths.
- Enable better Mitigation Strategies by mitigating current threat and taking into account reactions or alternate adversary tactics.
USE WITH THE CYBER KILL CHAIN™
Highly Complementary, How?

Activity-Attack Graph

Activity Group

Single Activity Thread

Victim 1

Victim 2

CYBER KILL CHAIN™ Coarse of Action Matrix

<table>
<thead>
<tr>
<th>Activity</th>
<th>Detect</th>
<th>Deny</th>
<th>Disrupt</th>
<th>Degrade</th>
<th>Deceive</th>
<th>Destroy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recon</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actions on Obj</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CONCLUSIONS

This is just a primer, learn more here:


Also, look out for an upcoming full SANS CTI Course based on the Diamond and the Kill-Chain.

THANK YOU

Special thanks to Sergio and Chris for being Super Heroes.
Also to the entire Cyber Squared team for their constant support and assistance.

Andy Pendergast, apendergast@threatconnect.com