LM *Intel Driven Defense*™ white paper clippings

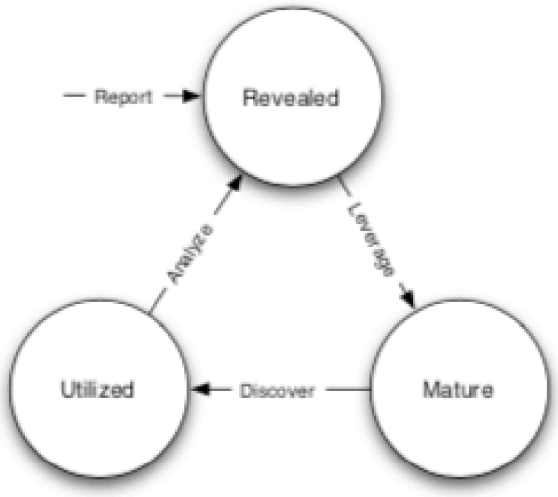


Figure 1: Indicator life cycle states and transitions

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

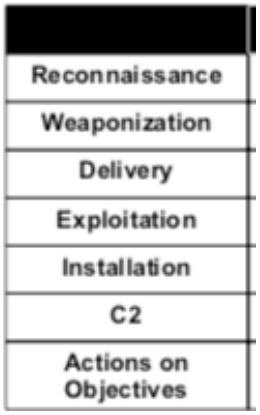
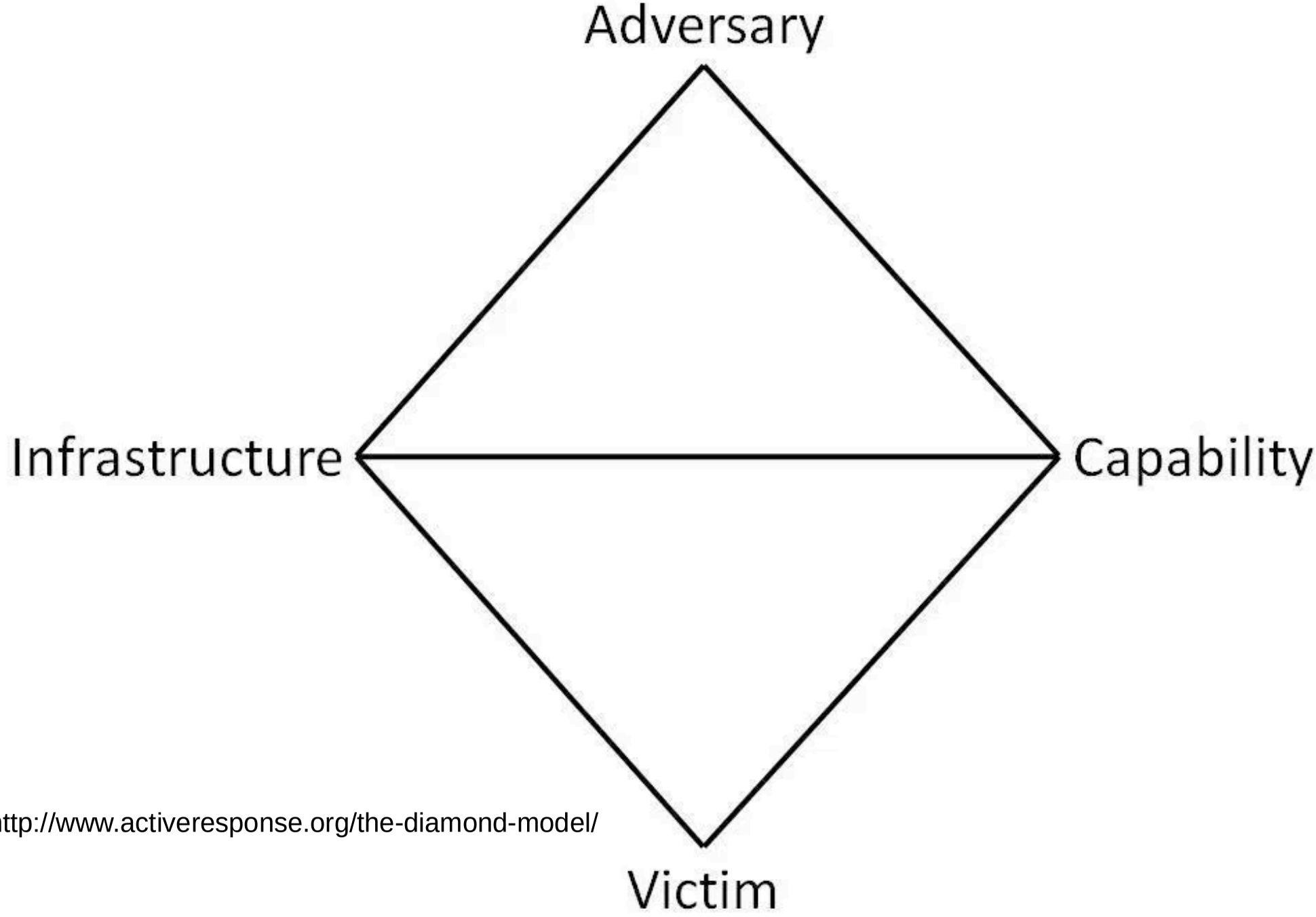


Figure 4: Earlier phase detection

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Eric M. Hutchins∗, Michael J. Cloppert†, Rohan M. Amin, Ph.D.‡Lockheed Martin Corporation

https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf



http://www.activeresponse.org/the-diamond-model/

Diamond Model Axia

1	For every intrusion event there exists an adversary taking a step towards an intended goal by using a capability over infrastructure against a victim to produce a result.
2	There exists a set of adversaries (insiders, outsiders, individuals, groups, and organizations) which seek to compromise computer systems or networks to further their intent and satisfy their needs.
3	Every system, and by extension every victim asset, has vulnerabilities and exposures.
4	Every malicious activity contains two or more phases which must be successfully executed in succession to achieve the desired result.
5	Every intrusion event requires one or more external resources to be satisfied prior to success.
6	A relationship always exists between the Adversary and their Victim(s) even if distant, fleeting, or indirect.
7	There exists a sub-set of the set of adversaries which have the motivation, resources, and capabilities to sustain malicious effects for a significant length of time against one or more victims while resisting mitigation efforts. Adversary-Victim relationships in this sub-set are called persistent adversary relationships.

http://www.activeresponse.org/diamond-model-axioms/

ACH – Psychology of Intelligence Analysis Chapter 8 Heuer

Step-by-Step Outline of Analysis of Competing Hypotheses

1. Identify the possible hypotheses to be considered. Use a group of analysts with different perspectives to brainstorm the possibilities.

2. Make a list of significant evidence and arguments for and against each hypothesis.

3. Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the "diagnosticity" of the evidence and arguments--that is, identify which items are most helpful in judging the relative likelihood of the hypotheses.

4. Refine the matrix. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.

5. Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove the hypotheses rather than prove them.

6. Analyze how sensitive your conclusion is to a few critical items of evidence. Consider the consequences for your analysis if that evidence were wrong, misleading, or subject to a different interpretation.

7. Report conclusions. Discuss the relative likelihood of all the hypotheses, not just the most likely one.

8. Identify milestones for future observation that may indicate events are taking a different course than expected.

https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/art11.html

Courses of Action Matrix

	Passive COAs				***Active COAs***		
LMCKC™	Disc	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Recon							
Weap							
Deliv							
Expl							
Inst							
C2							
Actions							

LMCKC™ and CoAs from LM Intelligence Driven CND paper

Enhanced by Rob M. Lee for FOR578