Cyberspace Detection Engineering

Applying additive manufacturing to finding the unknown unknowns in cyberspace

by WO1 Jonathan Morey

The advent of 3D printing has been a revolution in manufacturing. This is due to the paradigm shift away from reductive manufacturing where you take a large piece of material and chisel away at it until you have created the part or component that you need. With 3D printing, you only add exactly the material that you need for the part or component to emerge. If we apply the same logic to cyberspace detection engineering, we see that it comes in both reductive and additive forms.

The most popular (and free) way to conduct network security monitoring is the Suricata intrusion detection system (IDS) with the Emerging Threats ruleset applied to it. It is common practice to download thousands of IDS rules and start funneling network traffic through them. This then requires an analyst to start tuning the IDS by looking at the massive amounts of alerts being generated. The analyst will then determine what alerts are false positives and then update the rule or configuration of the IDS to tune out the false positives. This approach to detection and threat hunting is reductive. The analyst is starting with a rule set that may or may not be a superset of the reality in each computer network—whittling away at the block of provided rules. By taking a reductive approach to detection engineering, analysts are focusing on the known knowns, and it is much more difficult (if not impossible) to find the unknown unknowns.

The additive form of detection engineering starts with an IDS that is a tabula rasa. When the IDS is introduced to the environment it should contain no rules. The analysts then focus on identifying and defining the directionality and conversational semantics that are what make up the correctness or well-behavedness of the environment in which they find themselves.

For directionality, the question to be answered is, for a given system, service, or otherwise, in what direction should the information be flowing, and from whom should the connection be initiated? For example, if there is an internally hosted web server, then the "correctness" of the directionality would be that defined clients within the network would be the ones initiating the connections to that server. Once this has been identified, an additive approach to detection engineering would then have the analyst craft the appropriate IDS rule that alerts on any connection that does not exhibit the correct directionality. To define the conversational semantics for this webserver, one would ask: Considering a connection that has the correct directionality, is the conversation being conducted over the correct port and protocol, and is the application layer data correct for what would be a legitimate conversation? This is then captured within an IDS rule that alerts only in the case that conversational semantics are violated.

Additive detection engineering is predicated on the analyst's ability to correctly identify normal and correct behavior in a given system, and the elegance of this approach is the emergence of the unknown unknowns. Consider the case when an analyst is alerted to something that upon further investigation is found to be a false positive because the analyst failed to identify the full set of correct directionality and conversational semantics. The analyst then updates the ruleset to more perfectly reflect the reality of a given system. Another possibility is that a misconfiguration has been made in the environment. The analyst would then alert the network administrators to this misconfiguration to the benefit of both the detection engineer and the network owner. The last possibility with the additive approach is that the IDS alert is something that is truly anomalous or malicious and warrants the full attention of the analyst.

>WO1 Morey is a Defensive Cyberspace Weapons Officer serving as the Cyber Planner for National Cyber Protection Team 81. He has previously deployed with the 13th MEU.

... cyberspace detection engineering ... comes in both reductive and additive forms ...