

An Active Defense Decision Model

Sergio Caltagirone - University of Idaho
scaltagi@acm.org

The currently available security and protection tools are both inefficient and ineffective against some of the most serious threats. Active defense would be a reasonable method of insuring a more efficient and effective means of mitigating these threats, but with it comes a number of serious problems, namely unknown risk. The model presented here provides a method to develop an active defense policy and escalation ladder which, during the most serious threats, can be used to determine the proper active defense actions that will mitigate the threat as well as provide a standard of legal and ethical due diligence.

The model is organized into two components, an active defense policy, and an escalation ladder. The active defense policy assists an organization with assessing their assets and risks, as well as providing a way to equate risk of threat to risk of action. The first step in the development of an active defense policy is the identification of the critical assets. Second, the organization should identify, to the best of their ability, every threat against each of the defined assets with respect to the classical security categories: availability, integrity, and confidentiality.

Next, the organization will develop a scoring chart. Which, by default, will include at least the categories: legal, financial, national security, and ethical consequences (additional categories can be added as needed by the organization). Each organization then assigns a perceived risk to each of the integers from 10 to -10, where the more positive represents a greater loss and 0 is neutral (no loss or gain).

Finally, the organization needs to identify each risk that is associated with each threat in the categories defined by the scoring chart. Each risk is then mapped to the scoring chart, which determines the base risk score. This base score is then multiplied by the probability of the risk manifesting itself during a successful threat. All of the risk scores associated with a threat are then summed to derive the risk score for the threat.

The next step in the development of the active defense policy is action evaluation. In this step, an organization needs to determine the protection goal of each threat – that is, at what state of protection can a threat be deemed eliminated. Then, for each threat, all of the potential actions that can be taken to mitigate that threat are enumerated, and the risks associated with taking the action are also listed. These risks are scored just as the threat risks were scored (with the addition of the perceived ethicalness of the action itself), multiplying their score by the probability of the manifestation of the risk. These risks are then summed to provide an action risk score. The actions are then ordered from 1 to n based on the probability of the action to successfully mitigate the threat alone.

After the development of the active defense policy, the organization is prepared to develop the escalation ladder. The escalation ladder is a weighted, directed acyclic graph with potential negative weights. Each threat is a different graph, and each action to mitigate the threat is a separate node with the weight $\text{Risk}(\text{Action}) - \text{Risk}(\text{Threat}) - \text{Success}(\text{Action})$. A standard shortest path algorithm is then used to traverse the graph, producing the best sequence of actions that an organization can take to minimize their risk, maximize the potential successfulness of their actions, and mitigate the threat.

If an organization is successful in developing an active defense policy and escalation ladder, they will have the ability to quickly, effectively, knowledgably, and potentially automatically respond to threats using active defense actions in a less risky manner.