OVERSEAS-BASED ORGANIZATION UNLEASHES XPATTERNS TO COMBAT GLOBAL CYBER ATTACKS

Situation Overview

An international organization operating overseas was relying on traditional point solutions, but were increasingly concerned that these appliances may be becoming obsolete. The organization believed these appliances suffered from system fatigue, and failed signature detection. Additionally, the organization only had a few analysts reviewing trouble tickets. Analysts were seeing more than 25,000 alerts per hour from packet flow monitoring, and given the growing volume of issues, the closure rates were getting worse, not better.

Their security posture was based on a simple model: See something, do something, which was inefficient..

- Saw something:
  - Identifying as potentially malicious took an average of six hours
  - Analyzing to determine if the identification was correct was an additional four hours

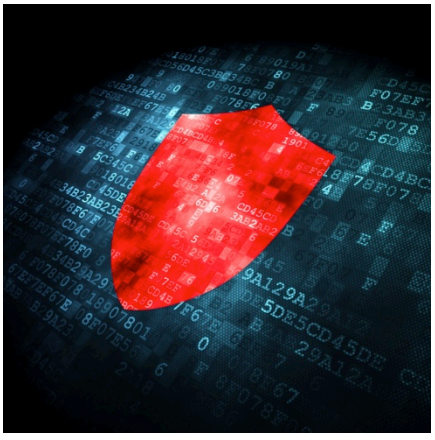
- Did something:
  - The time to develop a signature was two hours
  - The time to test the signature was three hours
  - The time to deploy the signature was at least eight hours

The organization initially set metrics at its peak response time, however, by the time the signature hit the street, that vector had been rotated out. In other words, the organization was thinking in weeks while their adversaries were thinking in hours. When attempting to address the matter, the challenges they confronted were:

- Lack of trained people
- Elongated workflows/closure rates that are acceptable for IT but not cyber security
- Inability train their way out of this
- Inability to secure the 10,000-plus analysts required to confront this problem using current techniques

COMBAT CYBER THREATS WITH 360-DEGREE SITUATIONAL AWARENESS ANALYSIS

xPatterns, built for fast implementation and highly relevant responses, deployed models trained to identify and prioritize items of interest for the organization. Once installed on the edge of the network, the xPatterns platform discovered over 36,000 risk candidates, and pinpointed a dozen highly critical items that required attention in milliseconds.



A simple model was then deployed to identify the number of distinct clients (IP addresses) visited by one machine in a day. If the count went above five, an automatic response would be triggered to decide whether or not to blacklist the IP address. In other words, xPatterns established a protocol for acceptable behavior and expected conduct on the network. When a machine exceeded the range outlined in the protocol, xPatterns either blocked it automatically or isolated the previously undetected in priority and scrutinized it to determine if it should be blocked. This put hours back on the clock and isolated items that needed to be analyzed.

Situation Outcome

In the wake of the events that occurred at this organization and recent global incidents, which underscored their need for dramatic change, they resolved to evolve rapidly and update their approach to cyber security.