Soaring Budgets & The New Era of Rapid Detection

Do you lose sleep over the true efficiency of your cyber security's ability to protect your valuable data and private information? Cyber adAPT can help you regain these valuable lost hours.

The totality of the saying 'an ounce of prevention is equal to a pound of cure' is very much applicable in the development of security strategies here at Cyber adAPT. Prevention is a tremendous strategy that can radically reduce the chances you'll get infected. It is easier and less expensive than treatment (cure); that is why we all have made investments in preventative measures and perimeter technologies such as firewalls, intrusion detection/prevention systems, endpoint malware agents, sandboxes, email filters, URL filters and the like.

However, while these are all prudent measures that should not be eliminated, they are not 100% effective in preventing us from getting infected. In fact, Gartner recently published a research paper that may be prophetic in this regard: "Malware Is Already In Your Organization; Deal With It," stating that "By 2020, 60% of enterprise information security budgets will be allocated to rapid detection and response approaches – up from less than 10% in 2014."

That is an astounding prediction! Even if this is only directionally true, say perhaps 30-40% of our security budgets instead of 60%, are we ready for this?

From a strategic/budgeting perspective, this means we will have to figure out how to spend LESS on the traditional prevention activities, people, and systems, and MORE on the detection side of the equation – unless you believe IT budgets will swell to absorb these much higher costs.

Rapidly rising budgets means our information systems need to be refocused to detect bad behavior or malware attacks so we can do something about it before it's too late. "Too late" meaning our data has already been exfiltrated, modified, or stolen, and/or our IT systems and networks have been disrupted or otherwise compromised.

Of course, we may have a few years to get there, but it will turn out to be an incredibly difficult journey for those CIO's and CSO's that don't start planning now. The new strategy will require new tools that can run in the network core, at very high speeds, are passive, (not in-band), able to learn, and most importantly, able to recognize potentially abnormal, ("interesting"), activities by looking at multiple layers of EVERY packet to see what it is and what it is doing. Ideally, again, such a tool would correlate these interesting activities over long periods of time, (months or years if necessary), until a configurable level of confidence is reached so we can "alarm" our incident response team(s) to let them know an attack is in progress.

There are many elegant aspects of such a strategy:

- It operates without agents, and without disruption of network traffic
- It is invisible to normal network discovery, as it lives passively on the core, (think fiber tap)
- It is agnostic to malware sources, types, variants, authors and methods of initial infection
- It does not rely on KNOWN malware types
- It focuses on the TACTICS and METHODOLOGY of the intrusion, (i.e., the "kill chain")
- It can reliably detect and correlate over arbitrarily long timeframes
- It can use its learning and confidence building capabilities to radically reduce 'false positives'
- It's in the core, "where the action is", or at least where many, or most, of our precious IP assets live

The newest addition to our product line Cyber adAPT does all of these things and a lot more. It's also designed to augment and complement many of the security investments you may already have in place.

If you think it's time to start thinking about what your security architecture should look like in 2020, we'd love to talk to you.