What is Actionable Intelligence?

Cofense • Threat Intelligence,Internet Security Awareness | March 23, 2017

Do you know what is actionable intelligence? Do you know the difference between threat intelligence and actionable intelligence? If not, read on.

The term actionable intelligence has joined the ranks of threat intelligence, big data and more words that are used in well-meaning ways, but are ultimately meaningless.

Don't get us wrong, like many other vendors, we use these phrases to describe what we do. However, because there are so many companies out there using these terms with their own meanings attached to them, we feel the need to write this blog post and hopefully do right by the technology and service offerings that are transforming the way that we approach today's cyber threats.

In fact, there was a recent LinkedIn discussion on this very topic. A LinkedIn user posted this question:

What exactly is "actionable intelligence"? I see a lot of start-ups being created by MBA persons who have no background or credentials in IT security. The product they offer for big fees is known as "actionable intelligence". They are trying to duplicate for businesses what the NSA, CIA, FBI, and DHS are doing for, and within, the federal government. My question is: how can these companies have the manpower and the resources to provide services like the NSA, CIA, FBI, DHS. We all have heard of the failures in intel coming from the best intel services in the world, i.e. NSA, CIA, etc. Those big boys have failures. What should we expect from these start-ups and your companies that are jumping on the bandwagon.? And these companies do not know of the ordinary IT security practices like defense in depth,

hardening systems. They are providing intelligence about the “bad guys”. How do they go about getting this intelligence? It is so secretive how does a CISO know if it is worth anything?

As the following definition from businessdictionary.com provides, actionable intelligence is not relegated to security; maybe that’s why ‘MBA person with no security credentials’ feel they can use it or may actually know something about it from usage in a different field:

“Any intelligence can be used to boost a company’s strategic position against industry peers. The acquired intelligence must be transferred into real actions which can be used to either launch a preemptive strike or prepare a counter strategy. Examples include the competitors’ price range, marketing budget, target demographic, advertising campaign and strengths over a company’s own product.
Overly aggressive attempts to gather intelligence from competitors may be illegal and constitute corporate espionage.”

Now onto some of the other questions posited: Let’s get into the context of security. Here is one definition that’s pretty good:

“Actionable Security Intelligence is the real-time collection, normalization, and analysis of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise. The goal of Security Intelligence is to provide actionable and comprehensive insight that reduces risk and operational effort for any size organization.”

Not perfect, but not bad.

As for the vendors’ size, not everyone in the market of ‘threat intelligence’ is small – by the way, the industry analyst group The 451 estimates there will be $1.2B in spending this year and IDC thinks spending will be $1.8B. Symantec, Cisco,

Intel/McAfee, IBM and many other large traditional security vendors have acquired threat intelligence offerings.

As for the startups and whether or not they can compete, the question isn't one about manpower as you refer to with major security agencies; instead it's about their technology and its ability to provide value. If they can provide that value with one person their 'actionable intelligence' will be purchased. And yes, just like traditional defense in depth systems, threat intelligence is not a panacea for the woes of security. However, the reality of failures of current defense in depth, hardening and other current security techniques has to be acknowledged. Many organizations realize that 'defending' and 'responding' is no longer as effective as it used to be, and that being intelligence led is required. Why? The hackers, the bad guys, are winning more and more.

As for traditional security (defense in depth, hardening, Etc.), I don't think anyone would ever suggest that you not use these and other network defenses. And these threat intelligence vendors don't either. The traditional security systems and methods play a vital role in securing your network, even if they have their individual shortcomings. Their efficacy can be raised, however, when given the right kind of intelligence that has an immediate impact on network security. Threat intelligence can make these devices smarter and the security professionals who are too few and overworked, 'smarter' about how to stop and prevent attacks.

Cofense Intelligence

Cofense intelligence provides the combination of actionable threat intelligence and the understanding of the correlation between phishing attacks and their motivators which helps your team prioritize, investigate, and respond.

Key Benefits:

- Timely, Accurate, and Actionable Phishing Threat Intelligence
- Expert threat analysts to help operationalize threat intelligence and provide guidance
- Attack analysis and context to help make rapid, informed decisions
- Integrates with existing security solutions to speed phishing threat response

Cofense Intelligence is actionable because it is:

Consumable

Cofense Intelligence delivers threat intelligence in multiple forms. Machine-readable threat intelligence (MRTI) follows industry standards for quick integration with your existing security devices. Analysis reports in PDF and HTML format are optimized for threat analysts and incident response teams.

Reliable

Cofense Intelligence only notifies customers about confirmed threats that are vetted by our trained analysts, resulting in high-fidelity intelligence.

Timely

MRTI is published throughout the day as new attacks are confirmed. Strategic analysis reports are published weekly. The investigation app is available 24x7x365.

Fresh

Cofense Intelligence service derives threat intelligence from a variety of sources of malicious email and spam that are used to deliver dangerous payloads to your employees every day.

Contextual

Cofense Intelligence publishes threat intelligence that shows how individual elements of an attack are related and the relationships between seemingly disparate attacks.

User-friendly

We will help you operationalize the service and provide on-going support to make sure you are getting the most from the service.

With Cofense's unique security intelligence you are armed with the weapons you need to identify, block, and investigate threats hitting your enterprise daily.