Take-aways from the CyberMaryland Conference

Posted At : October 15, 2013 12:15 PM | Posted By : John Slye

Related Categories: Critical Infrastructure Protection, Information Security, Big Data/Analytics, Cybersecurity

October is Cybersecurity Awareness Month and so there are numerous events happening around the region. With the partial federal shut-down, several have been postponed or cancelled, but not the CyberMaryland Conference in Baltimore, where I had the opportunity attend and to present Deltek's Federal Cybersecurity market outlook and forecast in one of the sessions.

The annual two-day **CyberMaryland Conference** draws people from industry and education as well as from inside and outside federal, state and local government. The event also hosts the Maryland Cyber Challenge competition for High School, College and Professional teams to compete in a real-world environment.

The conference's proximity to Ft. Meade, home of the National Security Agency (NSA) and Defense CYBERCOM, helps to bring folks from those organizations to speak and network. But while there were those in uniform in the crowd, the speaking podium was almost completely void of government representation. Chalk it up to the shut-down.

Here are just a few of the comments and take-aways from the various sessions as well as some conversations I had with fellow attendees:

- **Fighting Malware** – Simply chasing the malware is ineffective. You need to chase the person developing and inserting the malware to anticipate, predict their actions. You need to understand the tactics, techniques, and procedures well to defeat them before they hit you.
- **Maximizing the value of threat intelligence feeds** – Everyone is building their TI filters from the same available data feeds. Whatever the source you have, you need to evaluate and establish for yourself the fidelity of the information you're getting. Keep track of the reputation of the feeds you get so you know their value to you over time.
- **Using "Big Data" for cybersecurity** – Scientific analysis is foundational to an effective defense and to do this you need raw, unfiltered data. Use your big data platform to build a threat intelligence repository and take a deep dive into the threat data to maximize your understanding and the data's value. Use it to pivot off data points and make connections. Bring critical thinking to bear. Big data analytics is a science and intelligence analysis is an art. You need to combine the two to be effective.
- **Information sharing for cybersecurity effectiveness** – Often, sharing within a particular industry community begins as an informal process among people you know, through established relationships. Operationalizing wider sharing becomes more about the data – is it useful, trustworthy. The data needs to fit easily into your analysis processes and framework. This is not always the case for some feeds, e.g. STIX is a CSV file, so it doesn't flow automatically into systems.
- **Outsourcing security** – The trend of outsourcing an organization's security knowledge base to a 3rd party can have the effect of "dumbing down" security. As we leverage externally-provided knowledge bases more and more we are letting go of internal comprehension of the local security terrain, at the same time the necessary skills are increasing. This is dangerous. Organizations need to maintain some in-house core capabilities in security analysis and build a measure of advanced analysis capabilities to maintain security effectiveness.
- **Offensive cyber-capabilities** – These need to be distinct enough from known threats in order to get past current protections. Stuxnet would have never gotten through the perimeter if it matched any of the known profiles. Otherwise, it would have been detected and prevented. So when it comes to developing effective offenses, you really have to come up with something new.

These are just some of what I jotted down during sessions or in reflection on conversations with others. Even with limited interaction with our federal counterparts in the cybersecurity community there was plenty of useful exchange of information, networking and camaraderie.   The challenge to secure data, systems and networks seems only to be growing and collaboration will continue to be a key to success.

---

*Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about **GovWin FIA**. Follow me on Twitter **@GovWinSlye**.*