From the Executive Director's Desk

I have argued in the past that one of the biggest challenges that the security community has to overcome is regaining the connection with our inner hacker. Before we began professionalizing the modern Internet-aware security role, offensive and defensive actions were generally conducted by the same people. Hackers and defenders demonstrated similar skill sets, their activities characterized by the context that they operated in at one point in time and the results of the activity. We were adventures, explorers, and puzzle solvers, inherently curious and indifferent to boundaries.

In February, I focused a good amount of time examining characteristics of the security practitioner, professional, and executive. What I found from my conversations with folks at each level is that we all yearn to be more effective. Whether it is to detect attacks quicker, integrate advanced cyber technologies that can improve the enterprise security architecture, fill long-open positions with quality talent, or conduct better informed long-term strategic planning, we are struggling to cut through the noise to make progress towards a brighter tomorrow.

While professionalization of the security role constrains our inner hackers, the puzzles that we are trying to solve have become more complex. The ACSC is rebalancing the playing field by promoting a stronger community defense that will aid the individual business and mission objectives of ACSC members by harnessing the power of our collective knowledge, experiences, and perspectives. In addition to our now monthly Cyber Tuesday meeting for front-line defenders, our addition of the ACSC Collaboration Platform and a soon-to-be-announced Executive Forum represents the next steps to improving the New England information sharing environment. I welcome your feedback as we continue this journey together.

Michael Figueroa, Executive Director

By The Numbers

10 - The number of member organizations on the new ACSC Collaboration Platform.

Any employee of ACSC member organizations may join the conversation and even invite their trusted security advisors from non-member organizations by sending email to slack-request@acscenter.org.

Thoughts and Trends

Taken from conversations with community members.

"We've started giving tests to vendors to get through the snake oil."

"It's challenging to have the cloud conversation with regulators."

"We've learned that we need to act fast on good candidates because they are gone so quickly."

"More attention is on protecting customer interface points."

"We all have the same problems, but our resources are so different from some of these other companies."

Collaboration Focus

At our February Cyber Tuesday meeting, ACSC member participants focused on Security Operations Analytics, Top Threats for 2017, Building Malware Playgrounds, and DDoS Situational Awareness. The ACSC Executive Director posted some background behind the discussion on LinkedIn. Here is a snippet from that post, "The Case for Analytics Architecture For Security Operations":

"'Data is coming from 100 different sources in 200 different formats.'

Building a security operations capability is much easier said than done. At our monthly Cyber Tuesday meeting last week, ACSC members took a deep dive into the challenges of building a strong analytics capability to inform enterprise-level security operations functions. Whereas the security industry tends to focus on the data problem, our discussion went beyond the technology to assess effective practices of using what information an organization has at its disposal.

I have said in various forums that our ability to collect data far outweighs our ability to effectively process it in an actionable timeframe. Leading Security Information and Event Management (SIEM) tools often have non-trivial learning curves for effective use. But, even once an organization feels that it has mastered the tools that it has available to it, questions remain around how to ask the right questions to gain valuable intelligence from the data and who should be asking the questions.

For example, a SIEM tool jockey may be able to write rules and automate workflows, but building a strong intelligence capability demands that questions and data be architected. Doing so requires a completely different analytical skill set than what is needed to operate a SIEM tool. Effective security operations analytics is more about the approach than the tools. Security professionals and executives need to be mindful that standard reports will only give you the facts. The context to support decision-making requires that the organization do more. Our discussion highlighted the tools that our members are using, some practices that have worked for them, challenges and obstacles that they have faced, and even touched on efforts to make some data available outside of security operations to build collaboration channels with business units."

The entire post is available here: https://www.linkedin.com/pulse/case-analytics-architecture-security-operations-figueroa-cissp.

Media Focus

ACSC Executive Director Michael Figueroa is scheduled to be a guest on the Security Startup Weekly podcast with Paul Asadoorian and Michael Santarcangelo on Friday, March 17. You can catch the episode live at http://securityweekly.com/category/ssw/ or get it on-demand through any leading podcaster.