ENERGYSEC CONNECTED

News From the EnergySec Community

October 2016

In this Issue:

President'sReport

Building the Future

Growing the Workforce

As Summer fades into Fall, the memories of harvest remain fresh in my mind; tomatoes picked ripe off the vine, grapes, berries, and apples plucked at their peak, a welcome reward for efforts long since past. Surely, the harvest would not have come if not for hard work in the months and years preceding. It is that truth that drives EnergySec's workforce program. The current and future need for security professionals will not be met without hard work, diligently pursued, with an eye to the future.

An example of this vision is presented in this month's newsletter. Recently, EnergySec was privileged to produce a one-day event focused on introducing high-school age students to technology and security, with a goal of encouraging the pursuit of careers in this field. The event was produced in partnership with 1NTERRUPT, a non-profit organization based in Worcester, MA. Although the event was planned to accommodate 50 students, overwhelming demand forced us to stretch the capacity to 56, making the event an unqualified success. More details on this event are presented in the body of this newsletter.

Beyond this event, we continue to build capability and capacity, pursue and grow relationships in the academic community, and seek out industry partnerships to address this important issue. Almost daily we hear of the shortage of qualified security professionals. At the same time, cyber attacks continue to grow in number and sophistication. While we cannot single-handedly correct this situation, we can make a decided impact, and help to position our industry as a destination of choice for new security professionals.

We've made the development of the current and future workforce a cornerstone of our strategy to support security efforts in this industry. You can learn more about our current activities and future plans by visiting the workforce section of our website, http://www.energysec.org/workforce-development/. Or, contact us at workforcedev@energysec.org.

We hope you'll consider partnering with us in this effort.

-SHP

RealityCheck

But That's Really Unlikely

by Jack Whitsitt, Security Strategist, EnergySec

Over the past few weeks, I've had the opportunity to spend a little time doing some actual risk analysis work. Invariably, there are smart folks at the table who know their business far better than I do. Invariably, that knowledge is insufficient to identify and evaluate actual cyber security risk. This blindness, I've found, happens most often as a result of "Engineer's Blindness" or "Inadvertent Head in the Sand" syndromes.

In the first case, those most familiar with a system are often least able to see its vulnerabilities and other weaknesses. This happens most often simply because our familiarity with our own work blurs the edges of our vision. We know what we expect a system to do, we know what we built the system to do, and if we could see how it could be made to do more or less than it should, we would have fixed it already.

In the second case, as human beings, we often unconsciously feel that if something were happening, we would have known about it or seen some evidence of it. This effect is easy to see when talking to lay people about cybersecurity. They simply can't believe there are so many breaches, yet those breaches are reported in all of the major news sources they consume. If it's not a part of your world, it often remains outside of your conscious awareness.

In combination, these two problems make us collectively pretty bad at threat modeling and risk management. We do not think like "Hackers," whose mindset and talents center around their attention to detail, their ability to see actual vs. expected utility, and their ability to chain together small steps to move mountains.

So, when you are evaluating your cyber security program at any level (whether determining how best to tune IDS's or how to build your audit program), consider two things:

1. Invite many different viewpoints to the table and listen to them. Get all of the pieces on the table before you judge them. There is a lot of knowledge in your organization that is pertinent to understanding what your exposure and risks are and many of them are *not* in your local group or chain of command. Making too many assumptions is a common error.

2. Separate out "possible" from "likely" in your threat modeling efforts. Often what we feel is "unlikely", because of our various blind spots, is simply a mistaken impression or would be more likely in a slightly different context. Once we know what is possible (threat modeling) we can evaluate what is most probably (risk management).

And, obviously, implicit in this article is the need to do both organizational threat modeling and risk management as discrete efforts – above and beyond and outside of – your information security program. But you knew that already, right?

About the Columnist

Jack Whitsitt, security strategist for EnergySec, brings a breadth of cyber security knowledge and thought leadership to any project. His unusual combination of hard technical, public/private partnership development, facilitation, and national risk management experience allow him to provide particular insight into and leadership of strategic organizational, sector, and national cyber security initiatives and educational endeavors.

A participant in the national critical infrastructure protection dialogue for seven years, Jack has provided regular advice, insight, and thought leadership to all levels of government and industry and has been responsible for several successful sector-level initiatives

CommunityReport

INTERRUPT - PDX Style

An overflow crowd of 14-22 year old students

Seven-thirty on Saturday morning, October 1st, found EnergySec staff and volunteers at Mt. Hood Community College preparing for the inaugural INTERRUPT PDX event, setting up registration tables, organizing classrooms and preparing the Treasure Hunt.

Although we had planned for 50, the overwhelming interest from the students in the schools we reached out to led us to expand the registration to 56 with students still on a waitlist.

The day began with Dr. Wayne Machuca from Mt. Hood Community College speaking to the students about the need for cybersecurity workers and the importance of that work. Marc Blackmer, founder of INTERRUPT, spoke about the origins and purpose of the event. Our morning keynote speaker, Jeff Bryner, gave insight into Mozilla's Bug Bounty program, demonstrating that students could work in the cybersecurity field right now.

Next, the students participated in four breakout sessions which taught the basics of networking, ethics, hardware hacking, and web security. Two advanced courses were also added, Malware Analysis, taught by Jeff Bryner, Director of Enterprise Information Security at Mozilla, and Introduction to Cryptography, taught by Steve Parker, EnergySec President.

After lunch, keynote speaker, Gene Kim (Tripwire Founder), talked with the students about the pathways into cybersecurity, relating his own experiences as a cybersecurity professional. Next, the Treasure Hunt! Marc related the scenario — a team of penetration testers has been hired by a small utility to check their networks for technical and human vulnerabilities. The students divided into teams and the fun began!

EnergySec wants to thank our sponsors, Archer Security Group and Galois, for their financial support of this event, Mt. Hood Community College for the venue, and Archer News, Kerry Tomlinson, for reporting on the event.

The event earned rave reviews from students, and parents as well, with statements such as, "Just a note to say a huge thank you for getting Isaiah into the event today! He had so much fun and hasn't stopped talking about it since we picked him up." "[Our son] is so excited about this (and he is NEVER excited

about anything!)"

EnergySec is looking forward to the next INTERRUPT event!

Supply Chain Security Panel Review

Prominent components of our 12th Annual Summit were panel discussions

by Brandon Workentin, EnergySec Staff

With the recent FERC Order in supply chain security, the topic has been a major focus of industry. EnergySec has also focused on this topic. At the 2015 EnergySec Security and Compliance Summit, we featured a workshop focused on how to achieve and improve supply chain security. At this year's Security and Compliance Summit, we featured a panel of vendor representatives who discussed the topic of supply chain security from the vendor perspective. Dave Lewis, of Akamai, moderated the panel. He was joined by James McQuiggan of Siemens, Dennis Gammel of SEL, Bryan Owen of OSISoft, and David Foose of Emerson.

The discussion began with the topic of default passwords. They talked about how they, as vendors, can help customers to deal with, or change, default passwords.

Dennis Gammel spoke about the benefits that he sees from allowing customers to come onsite to the vendor in order to engage with the Research & Development team and give input in how products can be improved. David Foose spoke about responding to a series of natural disasters at a manufacturing plant, and how they had to work with their customers to prioritize who received orders when they were below their normal manufacturing capacity.

Like all of the panels at the Summit, this one included time for questions from the audience. A theme of the questions, and the panel as a whole, was the need for an organization to have a personal relationship with their vendors so that when problems, such as Heartbleed, arise you will know who you can talk to and who you should be calling with any questions you have. Summit moderator Patrick Miller also walked the vendors through the process their organizations go through in responding to vulnerabilities in their software, from how researchers could notify them to what the organization does to respond and notify their customers.

Volunteering - What's In It For Me?

But I don't have time to volunteer…

Have you heard those words before? Said them? Then you're not alone. According to the U.S. Bureau of Labor Statistics news release in February, the volunteer rate dropped .4% in 2015 to 24.9% (http://www.bls.gov/news.release/volun.nr0.htm). So why should ***you*** volunteer? Here are three great personal benefits that volunteering provides.

1. Improved Health. According to an article in *Science Direct,* research has shown that volunteering improves mental and physical health. It also encourages participants to develop better health habits and lowers mortality risks. (http://www.bls.gov/news.release/volun.nr0.htm)

2. Time Management. Forbes magazine's article "5 Surprising Benefits of Volunteering" states that those who volunteer their time feel that they have more time or are less time-constrained. (http://www.forbes.com/sites/nextavenue/2015/03/19/5-surprising-benefits-of-volunteering/2/#1d1e5c656810)

3. Develop new skills. Teachers (or managers) know that the best way to learn something new is to teach it to others. When you teach a new skill, your own learning becomes more focused.

(https://hbr.org/2012/11/how-to-master-a-new-skill)

Are you ready to improve your health? Have more time? Hone those new skills? EnergySec's Volunteer Co-ordinator, Mary Parker (a volunteer herself), is ready to connect you to a variety of volunteer opportunities, a chance for you to share your knowledge and skills with your community. For more information on ways you can get involved, email us at volunteer@energysec.org.

EnergySec Webinars

Hosted Webinars - Educational and Product-based

by Brandon Workentin, EnergySec Staff

EnergySec regularly hosts webinars, focused both on improving the security of our industry and making the job of achieving and showing compliance a little bit easier. Our most recent webinar covered the topic of how to leverage open source intelligence in order to improve security. Silobreaker's Charlotte Goring and Darrell Johnston joined EnergySec's Sean Maloney to demonstrate Silobreaker's open source intelligence gathering tool which EnergySec has been using in a proof-of-concept capacity and has found to be very beneficial in collecting and organizing the many sources of information out on the Internet.

(http://www.energysec.org/events/webinar-replay-hiding-in-plain-sight/)

In September, we hosted a webinar with Tim Erlin of Tripwire and Bill Kearson, the Director of Information Security at JEA. This webinar included tips on best practices for baselining and whitelisting, as well as how to make it easier to maintain proof of your organization's compliance. Bill Kearson discussed how Tripwire products have helped him in his job, which includes managing both security and compliance at JEA.

(http://www.energysec.org/events/webinar-replay-keep-your-guard-stay-compliant-and-be-secure/)

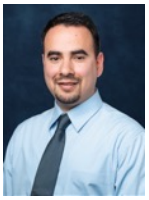
Our next webinar will include Kelly Brazil, of ProtectWise, and, if his schedule allows it, another utility participant. They will discuss ways that a smaller utility, without the budget to hire a large security staff, can use technology to develop a more proactive security approach, becoming able to be the hunter, not the hunted. This webinar will be on October 26th, at 11:00am PT / 2:00pm ET.

(http://events.energysec.org/events/empowering-a-small-security-team-to-act-proactively/)

EnergySec produces webinars as a service to our community and members. But, there's more to hosting a webinar than just 60 minutes and a GotoWebinar account. EnergySec works with our webinar partners to tailor content to the needs of our community. We assist in identifying panelists, and often provide our own staff experts to add to the conversation. We promote the webinar to our extensive contact list, record and archive the webinar, and provide a followup survey to registered participants. Webinars are just one more way we fulfill our educational mission.

Meet our Staff - Andrew Zambrano

Andrew Zambrano, Cybersecurity Analyst



Andrew Zambrano joined the EnergySec team full time in mid-September. Andrew, a former Marine, attended Mt. Hood Community College where he earned an AA degree. Andrew began as an intern at EnergySec in April 2015. When asked why he pursued a degree in the cybersecurity field, he said, "I like to protect and serve. (The) cybersecurity field (seemed) like a natural fit and there was/is a need…I picked the Energy sector because it is actually protecting something besides a monetary bottom line…"

Andrew is a part of EnergySec's Shared Analyst program, designed to help smaller organizations supplement their security posture and operational needs, including best practices, log analysis, intel gathering, etc. He also contributes to the EnergySecConnected newsletter, writing articles about security products on the market.

Andrew creates and administers all of our customer and industry surveys to ensure relevant and quality offerings to our community. He is a part of the development team for the EnergySec online community that includes the EnergySec Vendor Resource Center which displays nearly all the security tool options for utilities on the market today. This allows our commercial partners the ability to showcase their best solutions to our members big and small.

Upcoming Events

February 22-23, 2017
2nd Annual Hawaii Education Series
Waikiki Beach, Honolulu, Hawaii

WorkforceDevelopment

INTERRUPT PDX

Why do we do it?

Multiple phone conversations, building of materials, printing flyers, countless emails, finding a venue, testing the VMs, retesting, rebuilding, more phone calls, personal visits — why did the EnergySec staff put their time, energy, and resources into INTERRUPT PDX?

Simple answer: To make a difference.

The cybersecurity world is exploding with reports on the workforce shortage, or more specifically, the talent shortage of cybersecurity professionals. Papers are written, surveys are organized, research is conducted — all leading to the same result, a growing fear of the generations to come and a lot of discussion on what should be done.

How will this talent shortage be managed? EnergySec believes it will be managed by making a difference in our own community. Our staff is determined to be people of action — to not only recognize the need, but to do what we can to fix it.

INTERRUPT gave us the opportunity to do, not to discuss. Was it risky? Yes. Ask Marc Blackmer, founder of INTERRUPT. Ask the EnergySec staff who jumped in to a new venture. And we need more people willing to step out and take on the risks of positively affecting the next generation.

That's why EnergySec did it — to encourage and train and know this Generation Z. When we accepted the risk, we found this next generation to be engaging, smart, dedicated, and willing learners/participants.

What do they need from us? Knowledge! They are willing to learn but they need us to interact with them so they can know what the cybersecurity profession is and the opportunities it presents to them.

Would we do it again? Absolutely! As Marc says, "This is not a one and done event." We want to continue to engage these students and they are excited about continuing their cybersecurity quest.

Next steps? A week-long camp, PDX Cyber Camp 2017.

What do we hope to accomplish? The training of a generation of cybersecurity professionals to protect our critical infrastructure.

Are you interested in organizing or participating in this or similar events in your area? Drop us a note at workforcedev@energysec.org.

ProfessionalEducation

Low Impact Onsite Workshops

A one-day training brought directly to you

As 2017 approaches, there has been a noticeable increase in interest regarding the low impact requirements of CIP V6. which begin taking effect on April 1, 2017. EnergySec has been ahead of the curve on this with its launch of a 1-day course focused on the low impact requirements and related compliance activities. We offer this course regularly at public events throughout the country.

We have now added an option to host this course as an onsite workshop for a flat rate with unlimited participants. This workshop style event is well-suited to individual power plants and small entities that need to provide CIP education to a diverse group of individuals, and for whom travel is logistically or financially impractical. The workshop is based on our 1-day course curriculum, adapted as needed for the particular entity, and led by one of our highly qualified and experienced CIP instructors.

For more information or to schedule a workshop, contact us at education@energysec.org.

Professional Education Staff Profile - Brent Castagnetto

Meet one of our NERC CIP Instructors

Brent most recently served as Manager, CIP Audits and Investigations for the Western Electricity Coordinating Council (WECC), the organization charged with compliance oversight for the Western Interconnection. Brent has more than 6 years direct experience auditing the CIP standards and helping the industry with compliance.

Brent teaches our newest CIP course, the NERC CIP Audit Workshop, where his expertise as an auditor is evident in the in-depth material presented.

2017 Schedule

A look ahead to next year

We are currently developing our course schedule for 2017. We will offer two formats for courses this year. In some cities, we will offer multiple courses in two concurrent tracks. In other cities we will offer a 5-day form including both our NERC CIP Bootcamp and our Audit Workshop running consecutively. This will allow individuals to take both courses the same week.

Registration is currently open for the following cities and dates:

Phoenix, AZ | January 23-26
Nashville, TN | Feb 20-24

Additional planned cities are:

- Atlanta, GA | April
- Kansas City, MO | June
- Portland, OR | July
- New England | Sep
- Austin, TX | Nov
- San Diego, CA | Dec

InformationSharing andAnalysis

Silobreaker: Bringing Relevance Back to Big Data

Open Source intelligence gathering resource

By Andrew Zambrano, EnergySec

How do you get your threat intelligence? Do you rely on email alerts from sources that may or may not be relevant? Silobreaker takes a simple, yet very useful, approach to bringing all the relevant data to one interface while allowing you to highly customize how that data is displayed and used.

Silobreaker Quick Facts

- Founded in 2005.
- Headquarters in London, United Kingdom
- Engineering Team in Stockholm, Sweden

- Collect open source intelligence (OSINT) from over 200,000 sources including news, blogs, forums, feeds and social media.

Although many of the features are explained on Silobreaker's website, I want to discuss the Silobreaker dashboard which includes customization of both the look and feel, as well as the actual data returned and how the data can be displayed in a meaningful manner. Silobreaker does offer their "Silobreaker API" for automation and increased productivity as well as their "Silobreaker Software" if you prefer a more customizable local client.

The Dashboard

At first glance the Silobreaker dashboard can appear to be a bit busy, but one must remember that with the hundreds of thousands of sources being pulled in, it is quite impressive. The first thing you see on the display are the various widgets that are designed to bring the relevant data to the forefront. The ability to quickly add, remove, reorganize, and customize each widget by dragging and dropping makes it easy to put the widgets you prefer on display. Each widget also has customizable features.

Search Bar: The search bar is especially useful to quickly search for virtually any subject immediately. Suggestions are given to help refocus the search into key phrases, people, organizations, places, or publications. This is really key to successfully finding the data in which you are interested. Another handy tool within the search bar is the wizard and the advanced search options. The ability to limit or expand upon a predetermined list of variables brings more clarity to a search that could otherwise be inefficient and wasteful. Your search can be executed through a "360 Degrees, Network, Hot Spots, Time Series, or Word Cloud" lens, so-to-speak.

The **360 search** is a full coverage search, returning results including entities, top stories, content organized by media type, and focus. The **Network** search places a chosen variable in the center of the network map and a web of relevant data points is mapped with connections between the data points. Simply hovering over variables will show terms in context. In addition, hovering over the lines between points will show the two data points are related, again in context. The network tool helps an organization spend less time trying to determine how intel relates.

The **Hot Spot** search shows red dots on a world map that shows where the data is relevant geographically. This can be filtered by date. Hovering over each dot will bring up the contextual data. The **Time Series** search allows you to view your information as a timeline plot and/or a bar graph which again can be customized by date as easy as hovering over the interesting dates to view in context. The **Word Cloud** is a collage of terms, with the literal size of the word correlating to the the number of data points or relevance; the bigger the word the more information and relevance to your search.

Customizing and Sharing Data

 www.littlebobbycomic.com

Obviously, the most crucial part of bringing all of this data in is the ability to customize how you view and share the data that matters to you.

Tabs: There are two main pieces to the tab bars. First, any new tabs you create are displayed first and, just like a browser, creating a new tab is just one click. The second series of tabs are assembled by Silobreaker as an added service to help an organization get started with base-line intel. One nice feature is that you can make a tab personal to your login or share it with the "**share as collaborative**" button. This allows everyone on your team to view the tab you created, saving time and reducing wasted man hours. "**Make a Copy**" is way to build upon a particular tab without having to start from scratch. Other tab features like **export** (HTML, DOCX, RTF, and XML), **Share as Read-Only, Edit tab,** and **Create Email alert** are a perfect touch to getting the data where you need it to be as well as staying in the know with email alerts.

Widgets The widgets are separated into three categories: content, analytical tools, and social media. When you create or edit a new tab you are able to add widgets from a list of items from those three categories.

Once your widget has been created, it is very easy to customize or edit each widget individually. Customization options include feed (RSS feed), export, and edit.

The last feature is the ability to hover over any variable or source and add it to a read-only **report** which can be shared and exported. Here you can build a useful report and share it within minutes.

Silobreaker's ability to put its results in context is key to saving potentially days in the traditional gather and sorting of intel. Bottom line, any organization (especially small ones) that says it takes threat intel seriously should take a look at using Silobreaker.

Shared Analysts

"Fractional ownership"

We've all received that offer of a free vacation weekend only to learn that it involves enduring a hard-nosed pitch for a timeshare. Well, we can't offer you a vacation, but we do have a "time-share" offering that you may find compelling. EnergySec is launching a "shared analyst" program intended to enable small to mid-size utilities (or even large ones), to obtain additional resources without the cost and expense of adding new FTEs.

This program has a simple model. Simply decide on the fraction of an FTE you need, select the individual you'd like to work with, and you have a new resource for your team. A unique aspect of this service is that organizations are not just buying a bucket of time tied to some nameless, faceless individual on the other end of a phone line. EnergySec shared analysts are individuals assigned to client organizations. The intent is that client organizations will form a long-term relationship with their named analyst, who will become an extension of their team, even making regular onsite visits if desired.

In addition to the services of the named analyst, EnergySec backs up all our clients with the full resources of our organization. We have experienced, senior level staff that support and assist our analysts in meeting their client's needs using a "teaching hospital" approach. We also have established relationships with the Department of Homeland Security and other agencies, and participate in many information sharing forums. We continue to grow our capabilities as we establish our services in accordance with the emerging ISAO model.

To learn more, drop us a note at info@energysec.org, or call us at (503) 905-2920.