Cybersecurity Certifications

Colleagues,
Are you debating whether or not to get a cybersecurity certification? Do you already have a cybersecurity certification and are wondering if you should get another one? Are you looking for some help to convince your employer to support your efforts to obtain a cybersecurity certification?

So why should you get a cybersecurity certification? What good are they? There are numerous reasons to pursue certifications. One of the most common reasons to pursue a cybersecurity certification is to help you in your current job. The Information Week August 14, 2016, article on “8 Cybersecurity Certifications to Boost Your IT Career” states: “Cybersecurity skills are in high demand across all industries. These certifications can help IT managers boost their security know-how and protect their organizations.”

Another common reason to pursue a certification is to help you be more competitive for a new job or a promotion. According to the 18 Jun 2016, Foote Partners News Release: “Market values for 76 Information Security certifications have been on a slow and steady upward path for two years”. The News Release also states: “Strong performing certifications in the first three months of 2016 were those in IT security management and architecture, penetration testing, forensics, and cybersecurity.”

A cybersecurity certification can also be an important consideration for pay. Four of the top six certifications on the Global Knowledge “15 Top Paying Certifications for 2017” are cybersecurity certifications: CRISC, CISM, CISSP, and CISA. And each of those four were also in the top six of the 2016 list.

The IT and cybersecurity career fields are extremely dynamic. We’re exposed to new technologies, new techniques, and new exploits all the time. How do you keep up with it all?

What you learned in an Associate’s or Bachelor’s degree can rapidly become old, outdated knowledge. A cybersecurity certification provides the opportunity to improve your currency and relevancy, and can help you keep pace with the ever-changing IT/cybersecurity environment.

Alternatively, a cybersecurity certification provides the opportunity for career broaden-
Will Vault7 Shake Infosec Like Snowden?


The Wikileaks ‘Vault7’ release from earlier this month reignited the reality of state-sponsored espionage, and what our governments know about us.

The revelations were that Wikileaks had a cache of CIA material consisting of several hundred million lines of computer code that has been “circulated among former US government hackers and contractors in an unauthorized manner.” These were leaked to the whistle-blowing website and demonstrated abilities to hack mobile phones and bypass the encryption used by messaging services like Signal, WhatsApp and Telegram.

Wikileaks later announced plans to work with affected manufacturers to help them push out fixes, but according to Motherboard, Julian Assange sent an email to Apple, Google, Microsoft and all the companies mentioned in the documents asking the companies to sign off on a series of conditions before being able to receive the technical details to deploy patches. These apparently included a 90-day disclosure deadline, which would compel companies to commit to issuing a patch within three months.

The whole situation served as a reminder of 2013, when Edward Snowden revealed the reality of mass surveillance by global governments. I recently caught up with F- Secure chief research officer Mikko Hypponen to talk about the impact of this fresh revelation on government spying.

“The biggest surprise to me is that it happened, but I am surprised that they let somebody steal all of that information,” Hypponen said, referring to the fact that this was leaked by an insider.

Asked if Wikileaks’ reputation for activity within the presidential election, along with Assange’s self-imposed exile, had changed views of the whistle-blowing website, Hypponen said that he “didn’t think that they leaked anything that has turned out to be fake”, so should be trustworthy.

“The reasons for leaking may be suspect but I don’t think they have been duped, and I don’t think anyone has ever proved them to be fake – so Vault7 is real. Also, no one has been caught by leaking through Wikileaks which is remarkable. Manning got caught because of his own chats, Snowden revealed himself, and they have proven that they do have the know-how and capability to not get their sources compromised, and that is remarkable.”

Mikko made a very relevant point about fresh ‘leakers’ - mainly ‘where are the leakers around the world’?

“Particularly with intelligence leaks focused around Five Eyes intelligence, we’ve seen very little coming from countries doing really bad stuff and that is clearly out of balance,” he said.

“Also, the issue with the leaking is that someone could just walk away with the laptop and all of that data, previously data was stored on paper and it would have been 10 truckloads of paper and that is hard to drive out of any organization. Take the tiniest memory card and fill a shipping container with them and ship it from Europe to the USA, it will be a million times more than what the internet can do right now, even though it will take days.”

Back at Infosecurity Europe 2014, Hypponen said that “Leaking can be done by employees and insiders” and “if an employee knows they can leak information without getting caught, you only have one option left: do no evil.”

When asked why he felt this was the right time to reveal this cache, Mikko said he was unsure of the timing and motivation, as they specifically chose a time and thought of a reason for it, and coming so soon after the SHA -1 collision disclosure, he said that story would have persisted longer had the Vault7 release not appeared.

“Of course there is a big difference between the NSA and CIA, as CIA does mass surveillance. NSA looks at your data and CIA – mainly ‘where are the leakers’ – feels the NSA and CIA, as CIA does mass surveillance. NSA looks at your data and CIA probably does not and that is the same for most people. The CIA does intelligence and its targets are very few and targeted, and the vast majority of its targets are being intercepted as NSA do mass surveillance and these leaks were very bad for both NSA and CIA as, with regards to CIA’s targets: extremists and terrorist organizations, rogue nations and these guys are now running around in circles trying to find CIA things on their network based on the information that was made public by Wikileaks.”

Read the rest here: https://www.infosecurity-magazine.com/news-features/will-vault7-shake-infosec-like/
We are holding steady on our membership—~481 members as of the end of March. Overall, we are maintaining our membership with renewals and new memberships—both general and students/Freemiums. Kudos to everyone who referred a student or general member. Keep those renewals and new members coming in! Remember that for each referral you make, you are entered into the ISSA International quarterly drawing for various prizes.

It was great to see so many members at the Cyber Focus Day. Lots of interesting presentations and tons of opportunities for networking. Thanks to all the members who helped make this a successful event. One area that was mentioned during the day was the ISSA Fellows program. This includes Senior Members, Fellows, and Distinguished Fellows. I would really like to recommend that members who meet the requirements for these honors seriously consider submitting applications. The requirements can be found on the ISSA website at http://www.issa.org/?page=FellowProgram. Recognition of this type is not only personally rewarding but it can also be a good item to have on your resume. Also, it helps improves the recognition of the Chapter within the greater ISSA community. While it does take a little effort to put your package together there are plenty of people who have done it that can provide examples, reviews and other assistance. Once your package is submitted, it’s relatively painless after that. Your dues stay the same, you aren’t required to run for any offices, you still get free lunch (or dinner) and you still get all the other benefits of regular membership. So, please, at least think about it and feel free to contact me if you want to discuss it.

The Freemium program is alive and well. We’ve added a couple of new Freemium members under the new official ISSA program. Eligibility rules governing the program remain the same: Full time students, not fully employed in Cybersecurity, etc. Rather than being a separate membership type (as it was during the trial) we will provide a chapter unique payment code for them to use in the payment block when they join as a “Student” member. Students who don’t meet the Freemium criteria can still enroll as “Student” members, too. However, they will have to pay the current student membership rate of $55. If you know of students who might be eligible have them contact me. I will capture the information required to confirm eligibility and then I can provide them the payment code so they can join for free.

Finally, I would like to welcome our new members on behalf of the Chapter! When you’re participating in Chapter activities, please take a moment to introduce yourself to members of the board, me, and other members. Don’t forget to identify yourself as a new member and feel free to ask for help or information. Thanks for joining the Chapter and don’t forget to look for opportunities to lend your expertise to improve the Chapter. We’re always open to new ideas and suggestions.

David Reed
Membership Committee Chairman
dreed54321@comcast.net

(Continued from page 1)

ing. Look for a certification in an area that may augment your current knowledge and experience. Make yourself more valuable to your current employer by expanding your depth and breadth of knowledge. Consider a certification in auditing, cloud security, penetration testing, forensics, or secure programming, to stay competitive with your peers and prepared for the future.

There are many reasons to consider becoming certified, or to continue your professional growth by obtaining additional certifications. Our Chapter offers Security+ and CISSP Exam Prep Review Seminars and we’ve formed study groups for other certifications. If there’s interest, we may be able to form a new study group to help review certification material to ensure you’re prepared for the exam. Training for certifications can also be obtained from commercial companies in the local area.

Reach out to a Board member, our Training Committee, or our Mentoring Committee if you have any questions or would like to talk to someone about pursuing a certification.

Colleen
The planned release of NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Systems and Organizations (Initial Public Draft), on March 28 has been delayed. The publication is still undergoing internal review. We hope to be able to release the publication in the very near future. Here are a few highlights from the Notes to Reviewers that will give you a preview of what to expect in Revision 5--

"...This update to NIST Special Publication 800-53 embarks on a proactive and systemic approach to develop and make available to a broad base of public and private sector organizations, a comprehensive set of safeguarding measures for all types of systems, including general purpose computing systems, cyber-physical systems, cloud and mobile systems, industrial/process control systems, and IoT devices. Those safeguarding measures include security and privacy controls to protect the critical and essential operations and assets of organizations and the personal privacy of individuals. The ultimate objective is to make the systems we depend on more penetration resistant to attacks; limit the damage from attacks when they occur; and make the systems resilient and survivable.

"Revision 5 of this foundational NIST publication represents a one-year effort to develop the next generation security and privacy controls that will be needed to accomplish the above objectives. It includes significant changes to make the controls more consumable by diverse groups including, for example, enterprises conducting mission and business operations; engineering organizations developing systems and systems-of-systems; and industry partners building system components, products, and services. The major changes to the publication include:

- Making the security and privacy controls more outcome-based by changing the structure of the controls;
- Fully integrating the privacy controls into the security control catalog creating a consolidated and unified set of controls for systems and organizations;
- Separating the control selection process from the actual controls, thus allowing the controls to be used by different communities of interest including systems engineers, software developers, enterprise architects; and mission/business owners;
- Eliminating the term information system and replacing it with the term system so the controls can be applied to any type of system including, for example, general purpose systems, cyber-physical systems, industrial/process control systems, and IoT devices;
- Deemphasizing the federal focus of the publication to encourage greater use by nonfederal organizations;
- Promoting integration with different risk management and cybersecurity approaches and lexicons, including the Cybersecurity Framework;
- Clarifying the relationship between security and privacy to improve the selection of controls necessary to address the full scope of security and privacy risks; and
- Incorporating new, state of the practice controls based on threat intelligence and empirical attack data, including controls to strengthen cybersecurity and privacy governance and accountability…"

We will continue to keep you updated on the progress of the internal review and the anticipated release date.

Status of NIST SP 800-53, Revision 5
NDSU team works to create cybersecurity systems for self-driving cars

By Helmut Schmidt, Forum News Service, March 25, 2017

A group of North Dakota State University students is developing software to ensure that when self-driving cars tool down our roads, they will be safe from cyberattacks.

“You really want to make sure that how you protect this is thought of very early in the game,” said Jerry Straub, an assistant professor of computer science who is guiding the effort.

“This is the type of technology where you don’t want to wait for the attacker” to make his attack, he said.

Some people might see hacking the operating system of a vehicle or transportation system as a thrill or a symbol of prestige, with deadly consequences.

“If a car is hacked, you might have someone seriously injured or dying within minutes,” Straub said.

The push for autonomous vehicles is accelerating and the U.S. is expected to be a huge market, though there is much work and coordination to be done by automakers, governments and other firms.

Elon Musk, Tesla’s founder, has said fully autonomous Teslas could be ready by 2018 and gain government approval by 2021.

Volkswagen, Audi, Toyota, Honda, BMW, Chrysler, General Motors, Ford and other automakers are working on self-driving vehicles. Google is also developing autonomous vehicles.

Uber CEO Travis Kalanick said on Twitter he expects his firm’s fleet to be fully autonomous by 2030.

John McMillan, a sophomore from Vadnais Heights, Minn., is one of a handful of students on the NDSU software design team. Each student works on a different aspect of cybersecurity, including management of vehicles if there is an accident; identifying and dealing with emergency vehicles; control among vanets (groups of vehicles) and identifying attacks; security systems for individual cars; and security for roadside units or towers that coordinate the transit system.

The challenge is magnified by the fact that there are no fixed systems in place. But that is also the allure, McMillan said.

“To really be the first people to research into this was super appealing,” he said. “We’re defining this as we go and defining questions no one has looked at yet.”

Read the rest here:
DHS finalizing best practices for notifying victims of major cyber breaches

By Nicole Ogrysko, Federal News Radio, March 6, 2017

The Homeland Security Department is finalizing best practices that agencies, state and local governments and other organizations involved in a cyber breach can use to notify victims. The guidance lends suggestions on the decision-making process for notifying impacted individuals, preparing and delivering notices, concerns about “over-notifying” and additional support for victims. The DHS Data Privacy and Integrity Advisory Committee drafted the document after former DHS Chief Privacy Officer Karen Neuman asked the committee in September 2015 to develop written best practices for notifying data breach victims.

The committee made minor changes to and approved a final draft of best practices (http://1yxsm73j7aop3qc9y5ifaw3.wpengine.netdna-cdn.com/wp-content/uploads/2017/03/Best-Practicesfor-Data-Breach-Notification-1.19.17_FINAL-DRAFT.pdf) at a committee meeting Feb. 21.

“We can get to work on our important work so that unfortunately that I’m afraid, the next time this will happen, we’ll be ready for it and we can respond quickly and appropriately,” Jonathan Cantor, acting chief privacy officer for DHS, said during the department’s meeting last month.

Decision-making process

When deciding whether and how to notify impacted individuals of a cyber breach, the DHS committee first suggests conducting a risk analysis.

The organization should think about the nature of the data that was compromised and its sensitivity. Breaches where Social Security or medical information was stolen, for example,

“The analysis leading to a decision about notification must be conducted rapidly, since both legal requirements and the interests of those affected necessitate prompt notification, the final draft said. “It is important to seek a balance between the need for speed and the need for accurate information in the notice.”

To achieve that balance, the organization should think about whether the details of the breach are already public and if details of the scope of the attack are known.

“An overly broad notification may unnecessarily alarm people who, upon further investigation, may be found not to have been affected,” the final draft document said. “But it may not be possible to achieve perfect knowledge and a long delay in notifying can result in greater harm to more people.”

Preparing and delivering notices

The DHS committee suggests that organizations create template notification letter that it can modify depending on the scenario. Organizations should send notification letters through the first-class mail, which is more likely to reach the intended recipient, the committee said.

The letters or emails themselves shouldn’t look like junk mail or like correspondence from an unfamiliar source. They should be written in plain language with few acronyms and little jargon.

Organizations should also make sure that notifications don’t include too much information and only the details that a victim might need to have a basic understanding of what happened,” The DHS Data Privacy and Integrity Committee said.

“When more than one entity was involved in the breach, such as a breach that occurred at a third-party vendor, the source of the notice (the name on the letterhead) should be the entity that is most directly known to the recipients,” the DHS draft said. “The signature on the notice should be of a fairly high-level person in the notifying entity to indicate the seriousness with which the incident is regarded.”

Over-notifying

It is possible to notify breach victims too often, as the Federal Trade Commission has discovered.

As more states have enacted their own cyber breach notification laws, FTC has noticed that recipients tend to ignore multiple notices, some with important information.

"Individuals affected by a data breach are in the best position to determine the importance of a given incident and its potential for harm to them,” the final draft said. “To reduce the likelihood that individuals would become desensitized to notices, the language and format of the notice should make it easier for recipients to understand what the notice is, make an assessment of their own risk and take appropriate action.”

Read the rest here: http://federalnewsradio.com/cybersecurity/2017/03/dhs-finalizing-best-practices-notifying-victims-major-cyber-breaches/
Automated Next Gen Cybersecurity Will be Based on Intent

By Ken McAlpine, Securityweek, March 09, 2017

Over the last few months, I’ve written about a number of technologies impacting cybersecurity and how in a perhaps idealistic world, these security systems can all interact with each other, share information about the devices in our networks, and take mitigating actions, as required. So where does that leave us for improving our overall approach to information security as it relates to rapidly evolving networked systems?

Ultimately, it’s all about information – our ability to automatically and effectively determine what’s new, what’s important, and what’s unusual, regardless of where across the distributed network it exists. A term I’ve started hearing recently that I like refers to this as intent-based network security (IBNS.)

What do we mean by this term? In short, intent-based network security is the process of applying analytics to the information generated by all of the deployed security devices on a network. Individual security solutions are already capable of delivering significant amounts of independent, unrelated data. As we build out homogenous, interconnected security fabrics, however, we can begin to correlate the enormous amounts of information being generated. This integration is the secret sauce to IBNS, as it allows us to reduce these informatics mountains into molehills, which allows us to automatically refine security in real time as our network and threat landscapes change.

Another thing that such an integrated approach will hopefully result in is a consistent method for correlating and organizing this information with such things as common naming, reliable data, effectively ranking threats, etc.

This is only the first step. Before we can do anything with respect to implementing IBNS, we really need a way to understand and define which data is important, and have a consistent, universal method for describing it.

There are two very different methods of looking at IBNS.

The first is from the perspective of the business owner or the person responsible for security policy. This person needs to be able to simply define or update business intent, and the security policy and related infrastructure needs to interpret that information and automatically implement a reasonable and sufficient response. For example, security policies should be able to automatically limit systems to the information and services that they should have access to. Of course, this requires us to be more exact in our network designs. If we continue with the Wild West free-for-all approach to networks that we’ve been using, the challenge, of course, will be that much larger.

The second, and newer method involves rethinking how we solve the security problem. A key component of building an integrated and responsive security fabric is to implement security tools that can automatically assess and determine if a system is performing activities that are normal or intended – hence the emergence of a set of security practices referred to as intent-based. Again, a somewhat simplified description of such an approach is that it is able to address and automatically respond to the following question: Is the system doing things that are likely intended by that user on that system or not?

There are many things that need to go into creating a system that can truly be defined as providing intent-based network security:

- Knowing what the system is from a physical perspective
- Knowing what the system is normally used for
- Knowing what the system has historically done
- Knowing what the system is doing now
- Knowing who is currently using the system
- Knowing when the system changes

As we deploy security more holistically, our ability to understand and observe in real time the activity of a system is improved significantly over a traditionally isolated, perimeter-only security deployment.

The migration to virtual systems and containers, in particular, also makes the ability to implement intent-based network security more straightforward, as the number of things that a given system are expected (intended) to do is reduced and they become simpler and more granular.

A similar concept can be applied to Internet of Things (IoT) systems, as they typically only have a very limited set of behaviors and/or intended communications. Understanding these should allow us to observe changes away from this behavior. For example, PoS systems normally only communicate to a handful of systems within a corporate environment or within a given region. If all of a sudden those same end systems begin communicating to other remote geographies, then that behavior is worth initially preventing and launching a subsequent investigation.

Read the rest here:
http://www.securityweek.com/automated-next-gen-cybersecurity-will-be-based-intent
Experts: Cybersecurity in city set to surge

By Helen Robinson, Colorado Springs Business Journal, March 24, 2017

Colorado Springs ranks 16th nationally in the new Best Cities for Cybersecurity Professionals report, and experts say it is uniquely placed for a surge in growth and recognition as a cybersecurity hub.

Personal finance website GoodCall.com analyzed data from 221 cities for the report, highlighting Colorado Springs’ excellent cybersecurity job prospects and desirable lifestyle — ahead of cities including San Francisco, Seattle, Santa Monica, Washington, D.C., and Denver.

What makes Colorado Springs outstanding for cybersecurity professionals? The list is long.

Local cybersecurity leaders point to the large military and government presence, the National Cybersecurity Center, Catalyst Campus, academic institutions active in cyber education and industry partnerships, cross-sector collaboration, broad political support for cybersecurity development, innovative local companies, workforce development efforts and low cost of living.

National Cybersecurity Center CEO Ed Rios said Colorado Springs stands out for the quality and depth of its cyber jobs market.

“We have within 65 miles of Colorado Springs six different military installations and one major government organization, all that are very dependent on cyber,” he said.

“That not only has its own organic needs, but it has created private sector support and companies and entrepreneurs that are necessary in order to present capabilities to those government and military installations.

“That in turn obviously creates opportunity and that’s a large reason why we see demand and — between here and Denver — over 10,000 cyber-related job vacancies.”

Rios said cyber professionals in Colorado Springs are working to match the fast pace of the industry and its challenges.

“What we bring is business accelerators … and business entrepreneurial opportunities that really are competitive to the rest of the nation and even to Denver,” he said. “We have tremendous growth opportunities and plenty of demand.”

Frank Backes, vice president of business development for RT Logic and Kratos, said Colorado Springs’ market leadership base is also a draw.

“There’s a confluence of demand and very high-end expertise that comes together in Colorado Springs in a way that other communities just don’t have,” Backes said.

He said critical components of the market leadership and customer base include Air Force Space Command, which develops cybersecurity strategy and is headquartered in Colorado Springs, Schriever Air Force Base’s satellite command and control infrastructure and market presence, as well as private companies driving the need for cybersecurity infrastructure.

COLLABORATION CULTURE

Much of Colorado Springs’ outsized cybersecurity success stems from synergy and collaboration at a level not seen in other cities, leaders said.

“If you want to be a mover and shaker in this town when it comes to information technology and cybersecurity, you’ve got to see who’s doing what, you’ve got to talk to them, partner with them, and you’ve got to help people solve problems,” said Shawn P. Murray, cybersecurity engineer and chief academic officer with Springs-based Murray Security Services & Consulting.

“What’s happening here is not the old humdrum stuff.”

Murray praised the Southern Colorado Technology Alliance’s work in examining government contracts and matching local companies to required skill sets.

“They’re saying, ‘Your company could go after this portion of it if you partner with this other company; we’ll help you write the proposal,’” Murray said.

“That’s innovative. That’s what’s unique about what Colorado Springs is doing. I travel all over the U.S. doing consulting and training, and I don’t see this anywhere else.”

Andrew Vance, principal cyber technology consultant at Vance Rodriguez Consulting, said “real, visible partnerships” across sectors are key to the city continuing to strengthen its position as a cybersecurity hub.

Vance said he had felt confident locating and developing his business in Colorado Springs because of the city’s public-private cybersecurity partnerships and the level of involvement of UCCS, the Air Force Academy, Catalyst Campus, the private sector and the legislature in supporting those relationships.

“That was enough for me to say not only is this great for Department of Defense professionals, but also for Millennials coming out of the academic institutions — they can see this is a good place to live and work,” Vance said.

Murray pointed to CyberWorx at the Air Force Academy, root9B and SecureSet as examples of Springs-based groups making their mark by keeping up with ever-changing skill sets, taking real world problems and reaching faster, more creative solutions.

Read the rest here: http://www.csbj.com/2017/03/24/experts-cybersecurity-in-city-set-to-surge/
Poor Security Practice

By Dr. Shawn Murray, ISSA-COS, March 31, 2017

Key Focus Areas: Project Management, Change Management, Communication and Risk Management

It was just before lunchtime one day; I was plugging away at developing a new policy for continuity of operations in our organization. I sat in a cubicle next to Mike, my program’s network engineer. Mike was one of the better NEs that I have had the pleasure of working with over the years. He had a reputation for having a clean and organized work area and was very methodical in following established processes. I overheard him talking to one of his computer screens which displayed a dashboard for health and status of the network and he sounded concerned. I heard him state, “this can’t be right” as he got up and headed in the direction of the primary data center. In the data center, our team was removing a bunch of systems used to support a previous program that had been decommissioned. The program was fairly large and required a lot of various nodes to be powered down, removed from racks and submitted for disposition. The nodes being decommissioned were collocated with other hardware that was being used to support programs that were still operational. It was some of the operational systems that Mike was concerned with, as they had dropped off the network without warning.

Upon investigation, it was discovered that two of the systems administrators which were part of the decommissioning project, had decided to take a shortcut by taking a pair of scissors and cut through an entire band of fiber optic communication cables hanging from the cable tray. They had inaccurately thought that the cables were only supporting the decommissioned systems in the rack and had not followed the procedures as developed by the project team, which articulated instructions to disconnect each cable from each node, tie them off and hang from the cable tray. Mike was understandably miffed and the operational network supporting the mission was taken offline for several hours. The customer, data owners and subsequent stakeholders had to be notified of the incident and the team received a monetary penalty fee on the contract due to the error.

This scenario identifies and describes areas that could use some improvement. When we analyze the scenario, we have to look at the areas where tasks could have been accomplished with better oversight so as to reduce risk. The organization had a solid change management process where key stakeholders were briefed regarding the tasks and procedures to be performed in each phase of the decommissioning project. The procedures were also documented and communicated to the team members responsible for executing them. If the SAs had followed the procedures as written, then the cables would not have been cut with a pair of scissors. The SAs argued that they should have been informed that some of the cables connected equipment that was still supporting operational as well as decommissioned systems. The chief engineer for the project countered with, “at no time was there a task in a procedure that required any person to use a pair of scissors to cut through the fiber cables”. It was further explained that even if the SAs had followed the procedures and inadvertently disconnected each cable from each node in the racks and somehow a production system was taken off line, then the recovery time would have been less because the re-connection could have been made much quicker. This was compared to the action of having to run new fiber cables because the ones that were cut were damaged beyond use.

It is important for procedures to be vetted by the team developing them as well as any stakeholders that may be impacted by them if not followed correctly. Risk should be identified when analyzing the possibility of errors happening and a mitigation strategy should be developed to reduce these risks. One of the most important things that needs to take place is the socialization of the procedure by those tasked with executing them. This is important to ensure that the procedures are understood and are able to be executed as written. If a person believes that efficiency can be achieved with a different approach, then it should be presented back to the project team for approval before execution. This allows risk to be reassessed and stakeholders to agree and approve the new approach.
Carnegie Mellon's CyLab challenges high school students to give hacking a try

By Staff, Carnegie Mellon, March 27, 2017

Carnegie Mellon University aims to build a talent pipeline into the cyber workforce by introducing computer security skills to middle and high school students through picoCTF, a free, online hacking contest that starts March 31, 2017. Now in its third year, the virtual game of capture the flag (CTF) has previously drawn nearly 30,000 people.

"Right now, we're facing a tremendous shortfall in computer security experts," says David Brumley, project lead for picoCTF, the director of CyLab and a professor of Electrical and Computer Engineering. "The root of the problem is that most people don't even know that computer security is a field they can go into. Building awareness is a major goal of picoCTF."

This year, players will be competing for over $30,000 in prizes, thanks to this year's corporate sponsors. Anyone may register to play, but only U.S. students in grades 6-12 are eligible for prizes. Registration will remain open until the end of the competition, and there is no penalty for registering after the competition's official start date, March 31.

For two weeks beginning on March 31, participants will learn to reverse engineer, break, hack, decrypt or do anything necessary to solve a series of challenges that are centered around a unique storyline. Challenges start out easy and become increasingly difficult.

"To get started, you just need critical thinking skills," Brumley says. "We lead you throughout the game to develop more and more sophisticated notions of computer security so that by the end, you're solving real crypto problems and performing at a high level."

Tim Becker, an undergraduate student studying computer security at Carnegie Mellon, played picoCTF in 2013 as a high school student and uncovered a talent he never knew he had.

"I competed with some friends for fun, but none of us expected to do that well," Becker says. "But we ended up finishing in 3rd place, and that's how I ended up getting into this field."

Fast forward four years, and Becker is now a captain on Carnegie Mellon's student hacking team, the Plaid Parliament of Pwning (PPP). The team has won DefCon's Capture the Flag competition—informally known as the "Super Bowl of Hacking"—three times in the past four years.

Read the rest here: https://phys.org/news/2017-03-carnegie-mellon-cylab-high-school.html#jCp

Update Your Profile!

Don’t forget to periodically logon to www.issa.org and update your personal information.
IoT Devices are Dramatically Expanding Your Digital Footprint

By Adam Meyer, Security Week, March 24, 2017

IoT devices are the rage for consumers and business alike. While sound business has always been data-driven, consumers have latched onto data and remote control capabilities. IoT devices are convenient, giving us access and availability to things previously not possible unless you were physically in front of the device. They also can produce useful data for us to process and use to make better decisions.

IoT devices are giving me a sense of Déjà vu… like I have had to deal with this before … a few times.

Circa 2000-2005 when Virtual Machines started to become the go-to technology of the time, many a CIO was raising their fist in victory by consolidating physical hardware into a virtualized environment and claiming cost savings. Only the cost savings were negligible or non-existent when you factored in the massive expansion of the digital footprint that now had to be secured and managed.

Fast forward to the 2009’ish timeframe and a magical term called BYOD started to show up. “Hey look!” said the CIO, “we can let people use their own devices and save on our hardware costs”. Except now we are explicitly co-mingling data that needs to be protected with personal devices. Ever had to do e-discovery on a BYOD device? Fun times. I was a CISO when this BYOD trend hit the street and instead of jumping at the bit to be a first-adopter, I took a wait and see approach. I’ve lost count of how many horror stories I heard about early day BYOD adoption problems.

Just like VM’s and BYOD/Mobile, IoT devices can also create a major risk for organizations - by dramatically expanding their level of presence. All of these devices create more opportunities for cybercriminals to exploit. And I’ve read many reports projecting the number of “smart” devices to double or triple within the next four years. Most of these devices are consumer-based, lack basic cybersecurity features and are not under centralized management. Just look around your office and what do you see?

In this pie chart, (see the article on-line) my threat intelligence analyst team at SurfWatch Labs has looked at the threat data over the last year and aggregated all of the targeted IoT devices to put some more color to this risk. Needless to say, there are a lot of new avenues for cybercriminals to exploit to gain unauthorized access to more important systems and information.

Not only are there more devices expanding your digital footprint, business and personal devices, apps and data are being co-mingled more than ever. What this all adds up to is potentially the largest digital footprint that is NOT under proper security management.

Cybercriminals recognize this!

When looking at the threat landscape and bad actors, the value of good cyber threat intelligence is that it can help provide critical insights on cybercriminals’ motivations and intent, capability and opportunity. What organizations can control is the opportunity presented to the bad guys. And right now there is huge opportunity to cause harm via IoT devices, which is why I wrote that we will see more increasingly creative IoT attacks in the coming year. This forecast was based on the expanding deployment and use of IoT devices, the ability of cybercriminals to turn these devices into powerful botnets as proven in the second half of 2016 with Mirai, and the “as-a-service” capabilities that have been observed on the Dark Web.

The latest IoT-related threat to emerge in 2017 is Imeij, which has been detected in the wild targeting equipment made by Taiwanese manufacturer AVTech. Proof of concepts are also occurring with researchers highlighting how PLC controllers can be hacked and potentially taint water supply.

The reality is that IoT devices will continue to grow and be used by more individuals and businesses. The challenge is to account for these devices in your overall security and risk management process. Here are some recommendations to get visibility and some management around these devices:

Read the rest here:
http://www.securityweek.com/iot-devices-are-dramatically-expanding-your-digital-footprint
2017 Fellows Cycle Now Open

The Colorado Springs ISSA Chapter has over 400 current members. Many of you have been members for several years and may qualify for the ISSA fellow program. The Fellow Program recognizes sustained membership and contributions to the profession. If you think you or another ISSA associate may qualify in the fellow program, please contact Shawn P. Murray at 5871charlois@gmail.com or at 719-362-0666 to coordinate the process. Shawn is the chair of the chapter awards committee and will help you through the steps. Below are some additional details on the ISSA Fellow Program. Qualification information is also presented below:

No more than 1% of members may hold Distinguished Fellow status at any given time. Fellow status will be limited to a maximum of 2% of the membership.

Nominations and applications are accepted on an annual cycle. The current cycle opened December 2, 2016 and applications will be accepted until July 10, 2017, at 5:00pm Eastern Time. Following the application period, there will be a ten week review period followed by the notification and presentation process. Fellows and Distinguished Fellows will be recognized at the 2016 ISSA International Conference. Submissions received after August 1, 2016 will be considered in the following cycle.

Familiarize yourself with the Fellow Program, and the submission guidelines (http://c.ymccdn.com/sites/www.issa.org/resource/resmgr/Fellow_Program/Fellow_Policies_Revised_June.pdf). If you have questions, contact Shawn or The ISSA Fellow Manager (fellow@issa.org) or call 866 349 5818 (US toll free) extension 4082.

To Become a Senior Member

Any member can achieve Senior Member status. This is the first step in the Fellow Program. What are the criteria?

- 5 years of ISSA membership and 10 years relevant professional experience
- All Senior Member applications require an endorsement from their home chapter to qualify.

For your convenience, please feel free to use this Senior Member Application Check-list to confirm eligibility and completion of application

To access the Senior Member application go to: https://www.issa.org/?Senior_member_App
For the Senior Member endorsement form go to: https://www.issa.org/?Senior_Mem_Endorse

To Become a Fellow or Distinguished Fellow

Have you led an information security team or project for five or more years? Do you have at least eight years of ISSA membership and served for three years in a leadership role (as a chapter officer or Board member or in an International role)? You may be eligible to become an ISSA Fellow or Distinguished Fellow. Please contact Shawn and become familiar with the Fellow Program Guidelines and use the current forms to ensure you comply with all requirements.

- 8 years of association membership, 3 years of volunteer leadership in the association and 5 years of significant performance in the profession such as substantial job responsibilities in leading a team or project, performing research with some measure of success or faculty

(Continued on page 13)
ISSA Nametags

Do you want an ISSA nametag for your very own to wear to meetings, conferences, and events? You can now order/pick up yours directly from:

Blue Ribbon Trophies & Awards

245 E Taylor St (behind Johnny’s Navajo Hogan on North Nevada)

Colorado Springs

(719) 260-9911

Although their hours are officially Monday through Friday until 5:30 pm, they are occasionally in the shop on Saturdays. This is a small business so cash/check would be appreciated. Email wbusovsky@aol.com to order.

devolving and teaching courses.

- All Fellow applications require a nomination to qualify

To access the Fellow application go to:

https://www.issa.org/?Fellow_App

To nominate a Fellow go to:

https://www.issa.org/?Fellow_Nom

To submit a Fellow letter of recommendation go to:

https://www.issa.org/?Fellow_Recommend

- 12 years association membership, 5 years of sustained volunteer leadership in the association, and 10 years of documented exceptional service to the security community and a significant contribution to security posture or capability.

- All Distinguished Fellow applications require a nomination to qualify.

To access the Distinguished Fellow application go to:

https://www.issa.org/?Distinguished_Fellow

To nominate a Distinguished Fellow go to:

https://www.issa.org/?D_Fellow_Nom

To submit a Distinguished Fellow letter of recommendation go to:

https://www.issa.org/?Fellow_Recommend

Please help us identify candidates that we can recognize in our chapter! Please contact:

Shawn P. Murray, Chapter Recorder
5871charlois@gmail.com, 719-362-0666
A funny thing happened on the way to "Cyber Pearl Harbor." The Russians attacked, but few noticed - at least at first.

The Russian government, of course, has succeeded in waging information warfare campaigns against numerous countries, many of which worried about defending themselves against a military-style cybersecurity first strike that might, for example, have crashed power grids and the internet as a prelude to a ground invasion.

But few seemed to have plans in place for defending against having their democratic processes getting hijacked by leaking stolen data to "dox" targets or seeding fake news.

Now, the Russian government appears to be doubling down on its success, publicly confirming for the first time that is has a "cyber army" designed to wage a propaganda war, according to a report from Russian news agency TASS, which is owned by the Russian government.

"The information operations forces have been established, that are expected to be a far more effective tool than all we used before for counter-propaganda purposes," Russia's Defense Minister, Sergey Shoigu, told Russian lawmakers last week, TASS reported.

"Propaganda should be smart, competent and effective," he added.

Russia's Information Warfare Superiority

Russia has well-honed - and constantly evolving - information warfare expertise. "They rightly claim that they're superior to their adversaries, something that is obvious to any observer," says the security researcher known as the Grugq in a Tumblr post.

Indeed, the story of how Russian information warfare efforts added a large dollop of chaos into last year's U.S. presidential election, and potentially influenced the election - "an amazing influence operation entirely within the cyber domain," according to the Grugq - is now well known. The operation counted among its victims the Democratic National Committee, Hillary Clinton's campaign chairman John Podesta and former Secretary of State Colin Powell.

"Last year, there is no doubt in my mind that the Russian government tried to undermine and influence our elections. They broke into political institutions, invaded the privacy of private citizens, spread false propaganda and created discord in the lead up to a historic vote," U.S. Rep. Michael McCaul, R-Texas, the chairman of the House Homeland Security Committee and an original co-chair of the Cybersecurity Caucus, said in a keynote speech earlier this month at RSA Conference 2017 in San Francisco.

"I was briefed on the situation starting in the springtime," he said. "I pushed both the Obama Administration and then candidate Trump to take public and forceful stands on the issue. But I was disappointed in their response. The crisis was the biggest wake-up call yet that cyber intrusions have the potential to jeopardize the very fabric of our republic."

Muddled Response

But it's unclear how, exactly, targets of Russian propaganda should respond. To date, for example, U.S. cybersecurity defense planning hasn't included counting the country's media outlets as a piece of critical infrastructure that might be disrupted by foreign governments for political effect.

Such questions aren't limited to the United States. In recent months, there have been reports that Russia has been targeting France, Germany and other countries.

"European officials across the board are saying that they're seeing Russian intelligence agencies hacking into political parties; that they're using bots, fake identities on social media, to spread and propagate disinformation to affect their election outcomes," former U.S. counterterrorism official Richard Clarke told NPR on Feb. 17. "This is happening in France every day. It's happening in Germany. And we're seeing reports from other countries of Russian hacking, including Norway and Poland and of course Ukraine."

Read the rest here:

http://www.govinfosecurity.com/blogs/no-shock-russia-confirms-cyber-war-efforts-p-2401?rf=2017-02-28_ENEWS_SUB_GIS_Slot1&mkt_tok=eyJpIjoiTlRoa09UZGxObU5rWkRGaSIsIlNQi05b2k2cnBvT241MiNwcVRIeGlIQ2FJOWiLyQk1kSno0WjUIU5jemuVYUNFVeDmWZ2FiT2hSNnpYQ21pWnppJWV1CZnM3UFZLSU2qbUdaaJjZURQOGRxQ1wvZUtralluSTdcL1ZYRUsT1dqbGE0d0RieXpEaWIsY0txaXFMNVA2Nlp1n0%3D
Proposed Legislation Would Give Legal Right to Hack Back

By Kevin Townsend, Security Week, March 22, 2017

Hacking back is a perennial and contentious issue. Its latest instance comes in the form of a 'Discussion Draft' bill proposed by Representative Tom Graves (R-GA): The Active Cyber Defense Certainty Act. Graves claims it is gaining bipartisan support, and he expects to present it to the House of Representatives for vote within the next few months.

The Draft Bill is an amendment to the Computer Fraud and Abuse Act (CFAA). The CFAA is a deterrent to hacking through potentially severe sanctions; but it has not been effective in preventing cybercrime, and it has made hacking back illegal. The new bill would remove those parts of the CFAA that effectively prevent private business from taking their own action against hackers: "It is a defense to a prosecution under this section that the conduct constituting the offense was an active cyber defense measure."

Noticeably, the bill uses the term 'active cyber defense' throughout, and never once mentions the term 'hacking back'. Active cyber defense is defined by SANS as "The process of analysts monitoring for, responding to, and learning from adversaries internal to the network." It is discussed in detail and expanded in the study titled Into the Grey Zone: The Private Sector and Active Defense against Cyber Threats published by the George Washington University in October 2016.

The George Washington University report warns, "Today, when active defense is discussed, too often the discussion shifts to 'hacking back' -- offensive cyber measures that are beyond the scope of what we define as permissible activity in this report." This has clearly happened with the Graves proposal: it conflates active defense with hacking back.

The proposed Act will provide a CFAA defense when a 'victim' organization responds in a manner "consisting of accessing without authorization the computer of the attacker to the victim's own network to gather information in order to establish attribution of criminal activity to share with law enforcement or to disrupt continued unauthorized activity against the victim's own network."

This is limited by a requirement not to destroy information, not to cause physical injury, and not to create a threat to public health or safety. Nevertheless, it fundamentally gives victim organizations the right to access the attackers' computer without authorization... to disrupt the hackers' action -- and this is hacking back.

Hacking back already happens under limited circumstances. Law enforcement does it, and often uses the expertise of security firms to help.

"To a limited extent," comments security researcher David Harley, "this Act would formalize a cooperative framework that already exists between security companies and law enforcement agencies." This relationship gives law enforcement security expertise and capacity, while offering some legal protection to the security firms.

But, he adds, "I would have to worry about a framework that extended this protection to companies that don't often have that expertise and may be motivated to misuse that protection for competitive advantage... Apart from the ethical issues, I suspect that the quality of those investigations might in many cases be severely compromised."

So, two immediate problems with allowing hacking back is that a lack of expertise could either compromise forensic evidence, or accidentally cause actual harm to the attackers’ supposed computers. Without adequate expertise, the supposed servers might not even be the attackers’ servers. "Because of (compromised) proxies," comments F-Secure's security advisor Sean Sullivan, "hacking back/active defense is complicated and it’s quite unlikely that the US Congress would be able to properly define what should be allowed or not."

Read the rest here:
http://www.securityweek.com/proposed-legislation-would-give-legal-right-hack-back

GET A JOB!

Colorado Springs ISSA chapter member Melody Wilson maintains a “Jobs” page at Cyberjoblist.com. There is no charge. The jobs are set to remain listed for 30 days. Job listing originators re-post them again for another 30 days. It is designed for Colorado Springs, but once in awhile a job is listed outside the area.

You can also sign-up on the Cyberjoblist.com site for Job Alerts to be notified when a new job listing is posted!
A simple command allows the CIA to commandeer 318 models of Cisco switches

By Dan Goodin, ArsTechnica, March 20, 2017

Cisco Systems said that more than 300 models of switches it sells contain a critical vulnerability that allows the CIA to use a simple command to remotely execute malicious code that takes full control of the devices. There currently is no fix.

Cisco researchers said they discovered the vulnerability as they analyzed a cache of documents that are believed to have been stolen from the CIA and published by WikiLeaks two weeks ago. The flaw, found in at least 318 switches, allows remote attackers to execute code that runs with elevated privileges, Cisco warned in an advisory published Friday. The bug resides in the Cisco Cluster Management Protocol (CMP), which uses the telnet protocol to deliver signals and commands on internal networks. It stems from a failure to restrict telnet options to local communications and the incorrect processing of malformed CMP-only telnet options.

"An attacker could exploit this vulnerability by sending malformed CMP-specific telnet options while establishing a telnet session with an affected Cisco device configured to accept telnet connections," the advisory stated. "An exploit could allow an attacker to execute arbitrary code and obtain full control of the device or cause a reload of the affected device."

Compounding the risk, vulnerable switches will process CMP-specific telnet options by default, "even if no cluster configuration commands are present on the device configuration," the advisory warned. The vulnerability mostly affects Cisco Catalyst switches but is also found in Industrial Ethernet switches and embedded services. Cisco plans to release a fix at an unspecified date.

While Friday's advisory said there are "no workaround that address this vulnerability," it did say the vulnerability was active only when buggy devices were configured to accept incoming telnet connections. Disabling telnet as a means for receiving incoming connections eliminates the threat, and Cisco has provided instructions for disabling telnet. Cisco switch users who aren't willing to disable telnet can lower the risk of exploits by using an access control list to restrict the devices that are permitted to send and receive telnet commands.

Read the rest here:

Is Social Engineering the New Alternative to Ransomware?

By Brien Posey, Redmond Magazine, March 14, 2017

Hardly a day goes by lately when I don't read or hear something about the threat of ransomware. In fact, I think that most consumers probably view ransomware as being the single biggest threat to their data. Personally, I agree that ransomware is a huge problem. I know several people who have fallen victim to ransomware and I am, by no means, trying to downplay the seriousness of this threat. Even so, I can't help but wonder if the threats are starting to change.

Before I explain, I want to point out that once a piece of malware makes it into the wild, the odds are pretty good that the malware will never be completely eradicated. Last year, for example, I performed a deep scan on my file server and found an infected file. The interesting part is that according to my logs, that particular file had not been accessed in over 17 years. Hence, there was an ancient, presumably extinct piece of malware lying dormant on my file server. My point is that even if ransomware does eventually fall out of favor with malware authors, the problem will never completely go away because there is so much ransomware that already exists.

So how could anyone in their right mind think that ransomware is about to be replaced by social engineering? Well, consider an incident from a few days ago.

Someone in my family was attempting to go to Target's Web site to do some shopping. They accidentally typed the URL incorrectly and ended up on a presumably malicious Web page. This page displayed a message saying that the PC had been infected with a virus and that the full contents of the hard disk would be permanently lost unless "technical support" is contacted within the next five hours.

My relative tried to call me, but I was busy and didn't answer the phone. My relative then called the supposed tech support number, but hung up when the "technician" asked to take control of his PC. My relative tried calling me again, and this time I was able to answer the phone. After hearing the story, I took a look at the infected PC. Now here is where things get weird. The malicious Web site did not damage the PC in any way. It didn't even so much as access in over 17 years. Hence, there was an ancient, probably extinct piece of malware lying dormant on my file server. My point is that even if ransomware does eventually fall out of favor with malware authors, the problem will never completely go away because there is so much ransomware that already exists.

My relative tried to call me, but I was busy and didn't answer the phone. My relative then called the supposed tech support number, but hung up when the "technician" asked to take control of his PC. My relative tried calling me again, and this time I was able to answer the phone. After hearing the story, I took a look at the infected PC. Now here is where things get weird. The malicious Web site did not damage the PC in any way. It didn't even so much as request any of the browser's settings. Multiple malware scans using a variety of different products also failed to detect any sort of an infection.

Read the rest here:
https://redmondmag.com/articles/2017/03/14/social-engineering-the-new-alternative-to-ransomware.aspx
By Jim Finkle, Reuters, March 16, 2017

A North Korean hacking group known as Lazarus was likely behind a recent cyber campaign targeting organizations in 31 countries, following high-profile attacks on Bangladesh Bank, Sony and South Korea, cyber security firm Symantec Corp said on Wednesday.

Symantec said in a blog that researchers have uncovered four pieces of digital evidence suggesting the Lazarus group was behind the campaign that sought to infect victims with "loader" software used to stage attacks by installing other malicious programs.

"We are reasonably certain" Lazarus was responsible, Symantec researcher Eric Chien said in an interview.

The North Korean government has denied allegations it was involved in the hacks, which were made by officials in Washington and Seoul, as well as security firms.

U.S. Federal Bureau of Investigation representatives could not immediately be reached for comment.

Symantec did not identify targeted organizations and said it did not know if any money had been stolen. Nonetheless, Symantec said the claim was significant because the group used a more sophisticated targeting approach than in previous campaigns.

"This represents a significant escalation of the threat," said Dan Guido, chief executive of Trail of Bits, which does consulting to banks and the U.S. government.

Lazarus has already been blamed for a string of hacks dating back to at least 2009, including last year's $81 million heist from Bangladesh's central bank, the 2014 hack of Sony Pictures Entertainment that crippled its network for weeks and a long-running campaign against organizations in South Korea.

Guido, who reviewed Symantec's finding, said that it was troubling to see a hacking group focus on attacking banks using increasingly sophisticated techniques.

"This is a dangerous development," he said.

Symantec, which has one of the world's largest teams of malware researchers, regularly analyzes emerging cyber threats to help can defend businesses, governments and consumers that use its security products.

The firm analyzed the hacking campaign last month when news surfaced that Polish banks had been infected with malware. At the time, Symantec said it had "weak evidence" to blame Lazarus.

Read the rest here: http://www.reuters.com/article/cyber-northkorea-symantec-idUSL2N1GT09O

Please Note:
Address Change

Should you have a submission for the ISSA-COS Newsletter there has been an address change.

Submissions should now be sent to doncreamer@outlook.com. My old "q.com" account is no more.
Defense-in-Depth has Failed Us. Now What?

By Marc Solomon, Security Week, March 16, 2017

Defense-in-depth. It’s a philosophy we’re all familiar with: layering defenses so that if one fails, another layer is there to stop the attack. Sounds like a great approach, and it has become standard practice for the vast majority. The problem is that, frankly, it has not worked. For years we have been bombarded with a slew of headlines about compromises and breaches. And the velocity is increasing. In spite of all its layers of protection, defense-in-depth has failed us.

Why the Failure

There are various reasons why defense-in-depth has failed, stemming from the fact that each layer of defense has been a point product – a disparate technology that has its own intelligence and works within its own silo. This results in three key challenges. First, silos make it extremely difficult to share that intelligence – between tools or even teams – in any real way. Second, management complexity grows exponentially as you add additional management consoles for an already stretched security team. Third, these silos of technology just create an obstacle course for the attacker. But as the adage goes, “every obstacle is an opportunity,” and attackers capitalize on that. They successfully navigate this obstacle course every day to accomplish their mission – whether it is to steal, disrupt or damage what’s not theirs. Over time adversaries have evolved and so too have the technologies to catch them. However, the architecture has not. So even if the obstacle course may be harder, it is still an obstacle course...

As companies layer new products and technologies, they now find themselves with 40+ security products and vendors in 40+ silos. And because these products aren’t integrated, each layer in the architecture creates its own logs and events, generating a massive amount of data and a massive management challenge. Where does all this data go? How can you keep up with this data overload? Recent ESG research finds that 42 percent of security professionals say their organization ignores a significant number of security alerts due to the volume and more than 30 percent say they ignore more than half! In most cases, it is the security operators within the Security Operations Center (SOC) that find themselves drowning in this data as they undertake the onerous task of manually correlating logs and events for investigations and other activities.

In search of a solution

In an attempt to overcome the data overload challenge, SIEMs emerged as a way to store all this data and aggregate and correlate logs and events. This has worked to an extent; however, even SIEMs have limitations – some technological and some economical. On the technology front, SIEMs can be complex and, with today’s volumes of data, can face scale challenges. On the economic front, it can be costly for a company to store everything in the SIEM and thus they pick and choose what to include and what to exclude.

The SIEM has been the tool of choice for SOCs and it has certainly helped, but the volume of data is so great that security operators still can’t keep up. They are now looking at ways to mine through the SIEM data to find threats and breaches. One use case is to apply threat data from an outside feed – commercial, industry, government, open source, etc. – directly to the SIEM. Using data on threats found “in the wild,” the goal is to see what indicators of compromise (IoCs) may be ‘hidden’ in the vast amounts of data. In theory, applying threat feeds directly to the SIEM should work and provide some relief, but in reality this approach creates new and additional challenges for multiple reasons:

1. Lack of Context. SIEMs can only apply limited (if any) context to logs and events. Context comes from correlating events and associated indicators from inside your environment with external data on indicators, adversaries and their methods.

2. False Positives. Without context it is impossible to determine the “who, what, where, when, why and how” of an attack, in order to assess the relevance to your environment. As a result, SIEMs generate frequent false positives. Security operators end up wasting valuable resources and time chasing problems that don’t matter.

3. Questionable Relevance. Threat intelligence feeds only offer “global” risk scores based on the provider’s research and visibility, not within the context of their company’s specific environment. Security operators using these global scores find themselves chasing ghosts.

4. No Prioritization. Prioritization based on company-specific parameters is imperative for faster decision making that improves security posture. Intelligence priority must be calculated across many separate sources (both external and internal) and updated as more data and context comes into the system.

5. SIEM Architecture Limitations. As previously mentioned, SIEMs themselves are already overwhelmed by the vast volumes of logs and events defense-in-depth generates. Adding millions and millions of additional data does not scale in an affordable way. In addition, SIEMs were built as a reactive technology to gather logs and events that previously occurred. Aggregating threat data and intelligence to correlate, contextualize and prioritize in a proactive manner is not a SIEM’s primary design.

Read the rest here:
http://www.securityweek.com/defense-depth-has-failed-us-now-what
5 reasons your company can't hire a cybersecurity professional, and what you can do to fix it

By Alison DeNisco, TechRepublic, March 29, 2017

The shortage in skilled cybersecurity professionals is only growing worse, with the projected talent gap reaching 1.8 million jobs by 2022.

"It's definitely a seller's market," said Forrester analyst Jeff Pollard. "If you have security skills, there are plenty of opportunities available for you. If you have an interest in security and perhaps have a nontraditional background but are willing to learn, opportunities are certainly open from that perspective as well."

However, the shortage has left many companies stuck:
A recent report from ISACA found that 55% of organizations reported that open cyber positions take at least three months to fill, while 32% said they take six months or more. And, 27% of US companies said they are unable to fill cybersecurity positions at all.

Here are five common reasons companies struggle to find cybersecurity professionals, and solutions to help you better recruit and retain them.

1. Demanding too many skills
   It's no secret that the US suffers from a shortage of people trained in cybersecurity. However, companies often exacerbate the shortage by demanding that cyber job applicants have mastered a large number of highly-specialized practices, as well as soft skills like project management and communication.

   "It can be difficult to find employees who possess all of the skills, experience, and intangibles the job requires," said Keri Christman, manager of talent and culture for Rook Security. "This skills gap is compounded by the fact that the industry and threat landscape change and evolve so quickly that it can be difficult even for talented professionals to keep pace with new skills and demands. It's without question a challenge for job seekers."

   A good course of action is to prioritize which specialized skills are most important, and hire for those positions, according to Pollard. Then, to fill gaps in your security structure, you can hire a service provider or vendor partner.

   "They help augment the skills gaps you have on your team," Pollard said. "Security has traditionally fought every battle, and tried to hire for every skill. You have to get smarter about how you staff your team and what you are going to have internally versus what you'll go external for."

2. Poor compensation
   Cybersecurity specialists generally make more money than others working in IT. However, for general security practitioners, pay has remained stagnant, Pollard said.

   "Whenever I talk to an organization that says 'We're struggling to find security talent,' I tell them to add an ellipsis to that sentence, and add '...at the rates I'm willing to pay for that talent,'" he said.

   As mentioned above, companies are often looking for people with highly specialized skillsets who will work for a low cost, which is not practical, Pollard said. "They're trying to hire someone that can do incident response, malware analysis, firewall management, and design cryptographic algorithms, and are paying that person what they would pay a firewall engineer," he said. "You're not going to find that person."

   "There are a lot of openings in the security profession, but the dream list of qualifications they want is either not realistic, or definitely not realistic for the pay grade," Pollard said.

   As important as security is, no company has an unlimited budget, said James Stanger, senior director of products at CompTIA. "Costs—including salaries, software, hardware, training and certification—are all considered very, very carefully," he said. Companies need to be selective about the skills they truly need on staff, and willing to pay competitive rates for those skills, Pollard added.

3. Overlooking talent
   Current employees, recent graduates, veterans, and women are all untapped cybersecurity resources, Pollard said. Companies struggling to find cyber employees should consider cross-training current staff members, particularly those already in IT, he added. For example, your web app developer could become a web security assessment resource. Job rotation programs, in which people try out different security roles for a set amount of time, can help identify talent, Pollard said.

   Women comprise only 11% of the cybersecurity workforce, according to recent research from the Center for Cyber Safety and Education and (ISC)². "Companies should reexamine their cyber recruiting practices and ensure that women are included in the interview process," said Suzanne Hall, managing director in PricewaterhouseCoopers' cybersecurity practice. "Once on board, pair new hires with strong female role models and mentors within their organizations to build relationships and provide personal and professional support."

   Working with local universities to create internships and jobs for students and recent graduates is another way to build up your talent pool, said Rob Clyde, a member of the ISACA board of directors. "A lot of times people only want to hire those with experience, but it is worth exploring how you can bring people into the organization and the field that are straight out of school and help them gain the necessary experience so they will be great employees," Clyde said.

   Read the rest here: http://www.techrepublic.com/article/5-reasons-your-company-cant-hire-a-cybersecurity-professional-and-what-you-can-do-to-fix-it/
The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Covert Electronic Video Camera

“The Qwonn line introduces its newest camera product, the Q-FOB. The Q-FOB is built to imitate the look and structure of an electronic vehicle key. This key camera includes such features as a USB rechargeable battery, a built-in time stamp, 90 minutes of video recording time and two GB of memory! The new Q-FOB is the newest product from a line of state of the art covert cameras from Qwonn.”

No, I’m not going to tell you how to get one. Just be aware that some organizations are already prohibiting automobile fobs. And we thought they were just being paranoid!