Kansas City ISSA Newsletter

February 23, 2017
CASB 2.0: 5 Highest-Impact CASB Use Cases
NetSkope
Hereford House

Inside this issue:

The President's Corner

Hello ISSA Kansas City Members!

Hope you all enjoyed this year's first presentation on Data Loss Prevention by James Campbell, InteliSecure. We are working on relevant topics for rest of this year. Please let us know your thoughts on any topics you would like to hear or feedback on past presentations via president@kc.issa.org

Have you looked at the 2016 Annual Research report on ISSA ESG Survey – "Human" issues as the top Cyber Security and Business risk, < PDF LINK >. If you have any articles you would like published in the ISSA KC newsletter please let us know.

The ISSA International web site has a host of resources such as; international conferences, seminars that offer educational programs, and training and valuable networking opportunities.

Also if you are going to InfoSec World April 3-5, 2017, ISSA members get 15% off. The promo code is OS17-ISSA.

Sincerely,
Naeem Babri
President, ISSA Kansas City

Upcoming ISSA-KC Monthly Chapter Meeting Schedule

| February 23, 2017	March 23, 2017	April, 2017
CASB 2.0: 5 Highest-Impact CASB Use Cases *NetSkope* Hereford House	LockPath Lidia's Restaurant	More Information to Come

ISSA KC January 2017 Chapter Meeting Recap

On January 26, 2017 the ISSA-KC Chapter members and other security professionals held a meeting at Brio's Retaurant on the Plaza to network and attend the monthly chapter meeting, on the topic "Data Loss Prevention" presented by James Campbell with InteliSecure. InteliSecure explored the immediate future of data loss prevention, revealing where cyber security innovators are headed and the tools they are using to get there. In this meeting we learned about Data Loss Prevention (DLP) challenges and solutions including: 1). The current state of data loss prevention best practices, 2). Using Identity and Access Management (IAM) as foundational tools to build more proactive cyber security programs, 3). What a proactive cyber security program should look like, leveraging today's security technologies to achieve Predictive Analytics, and 4). The next big step in cybersecurity – Behavioral Analytics It was a great turn out with 35 attendees.

Susan Zimmerman winner of the ISSA KC $50.00 gift card. **Congratulations!**

Commerce Bank Member FDIC
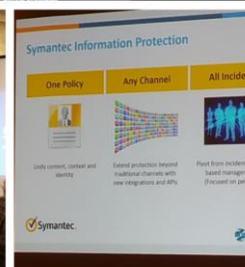
20545 Information Security Analyst III

Job Expectations:
How would you like to work for a great company that offers career growth and values your skills and experience? For over 150 years, Commerce Bank has built a strong reputation as a Super Community" bank and is recognized as an industry leader. In today's growing and competitive financial services industry, we look for creative and innovative solutions to meet the needs of our customers. To achieve our results, we recruit the best and brightest employees who ask, listen and solve to meet our customers' needs!

The Information Security Analyst III is responsible for adhering to Incident Response protocol, administering Information Security systems, assessing information risk, and identifying and remediating vulnerabilities for IT security across the enterprise. The individual will be focused on securing the network perimeter and internal networks through operations of the firewall, virtual private networks (VPNs), intrusion detection system/intrusion prevention system (IDS/IPS), web application firewall (WAF), data loss prevention (DLP) and enterprise anti-virus solutions. The Information Security Analyst III will be well versed in Incident Response protocol and event management.

Primary responsibilities including but not limited to:

- Incident Response and event management, including Incident remediation protocol, lessons learned, and process improvement/efficiency.
- Intrusion prevention, administration of Information Security IPS systems, phishing monitoring and anti-phishing practices.
- Participation in the Internet Monitoring process in addition to Data Loss Prevention.
- Firewall administration, policy configuration and management of web application firewalls.
- VPN configuration and administration.
- Anti-virus anti-malware system maintenance and best practices configuration.
- Remote access maintenance, administration and configuration.
- Internal customer service related to access requests, troubleshooting, and problem resolution.
- Promote awareness of applicable security standards, policy, and best practices across the Bank.
- Participation in the Information Security Operations on-call rotation. This position requires regular, predictable and timely attendance at work to meet department workload demands.

Work Hours: Monday-Friday (8:00am-5:00pm); evening and weekend work required.

Education: Bachelor's Degree, Information Systems, Computer Science, Information Security or related field desired.

The ideal candidate will possess:
- 3-5 years IT security or information security experience with ability to engage with internal customers and management.
- 2+ years' experience conducting incident response remediation and process protocol.
- 2+ years' experience in administering firewall, WAF, and Virtual private network systems/appliances.
- Experience with IPS/IDS, SIEM technologies, Internet Monitoring, and Data Loss Prevention.
- Experience working with threat intelligence and developing proactive best practices.
- Certified Information Systems Security Professional (CISSP), or related certification.
- Project management skills or experience working within Information Security project implementations.
- Working knowledge of Linux and Windows Operating Systems, scripting, and Virtualization experience.
- Strong work ethic, problem solving skills, customer service orientation, and proven dependability and promptness.

- Good communication skills, well developed interpersonal skills, in addition to teamwork and collaboration attributes.
- Creative problem-solving, analytical, and organizational skills.
- The ability to plan, organize, and deliver professional technical documents on time.
- Self-motivation and capability to successfully complete projects and provide support with little supervision.
- Skills in creating documentation and procedures for a variety of technologies.

All inquiries and referrals are confidential. To apply online, visit: https://www.commercebank.com/about/careers/ No 3rd parties or agencies, please. EOE.

How to Secure a Smartphone for the Tweeter-in-Chief

By Anupam Joshi , The Conversation | Contributor Jan. 25, 2017

As President Donald Trump takes office, he has also taken up a new, digital symbol of the presidency. Before, during and since the campaign, he used an Android smartphone to conduct his business and tweet prolifically, directly reaching millions of followers. But when he was inaugurated, Trump surrendered that device and accepted in its place a smartphone that has somehow been made more secure. It is a key move for a man who might now be not only the 45th commander-in-chief but also America's first president with such devotion to Twitter. Many private companies deal with issues like this, in which employees joining the ranks already have a mobile phone they use for their personal life. Should that device be connected to company systems? Or should workers be issued a cumbersome second phone for work-only purposes? There are federal recommendations about that, but few firms are handling data as sensitive as the president's phone might be.

A presidential smartphone is probably the most attractive target imaginable for foreign governments' hackers. Attacking the phone could provide access to the highest secrets of national security, and near-constant real-time information about exactly where the president is, raising the potential for physical threats. Securing a phone like that requires several layers of protection.

Exactly what has been done to protect the president's phone is intentionally left unclear to the public. But as a scholar of mobile security, I know that beyond overall network security measures, there are several technological approaches to securing a smartphone for special use. The most secure, however, is also among the least practical and least likely: ensuring the phone cannot connect to the internet at all. So how might have government cybersecurity specialists locked down Trump's new phone?

Hiding Key Information

One level of protection is what is called "security by obscurity." Many people presumably had Trump's pre-presidential phone number. Now, relatively few people will have his new number. Similarly, his old phone's internal device identifiers, such as its unique 15-digit International Mobile Equipment Identity number, or IMEI, may not have been as carefully guarded as those for his new phone. Keeping that information secret means the first hurdle for potential attackers involves figuring out which phone to attack in the first place.

Another layer of security involves ensuring the device was made by a trusted manufacturer, using trusted components, reducing the risk that the hardware would have any vulnerabilities that an attacker could exploit. Similarly, anyone who worked with or handled the phone at any step would have to be prevented from tampering with it to introduce any weaknesses.

Adding even more security in the physical device itself would be a specialized computer chip to add significant encryption capability for data stored on the phone or transmitted to or from it. Called a "Trusted Platform Module," this hardware element is required by the Defense Department in all new devices handling military information. In addition, it could be used to ensure that any attempts to tamper with the phone, its settings or the operating system installed would be identified immediately. To read more, http://www.usnews.com/news/national-news/articles/2017-01-25/how-to-secure-a-smartphone-for-president-donald-trump-the-tweeter-in-chief

ISSA Journal February 2017

Certification Corner

CISSP Study Group
What is the CISSP®? (Certified Information Systems Security Professional)
The vendor-neutral CISSP certification is the ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their overall information security program to protect organizations from growing sophisticated attacks.
Where: TEKsystems 7421 W. 129th Street, Suite 300 Overland Park, KS 66213
When: 2nd and 4th Mondays of each month, 6-8 PM
Contact: Mark Waugh (waugh.mark.r@gmail.com) 913-636-7900

Thanks,
Director of Education, Larry Dilley
certification@kc.issa.org

Save the Date — March 2017

March 23, 2017 Chapter Meeting
Sponsor: Lockpath
Topic: More Information to Come
Speaker: Sam Abadir has over twenty years of experience helping companies realize value through improving processes, identifying performance metrics, and understanding risk. Early in Sam's career he worked directly with financial institutions and manufacturing companies to help them realize institutional value. As a Sr Manager at Deloitte he focused on improving processes and increasing value for Global 2000 companies. In the past five years, Sam has worked with software companies like LockPath to build the tools that help companies create and manage value in a structured and efficient manner.

Webinars/Conferences

Webinars & Conferences

Webinars are an easy way to stay informed on trending industry developments from the convenience of your own office. In everything from mobile technology to compliance. Webinars and conferences provide insight into topics affecting our industry and your business.

2017 Kansas City Secure World - Overland Park Convention Center – May 3, 2017

SecureWorld conferences provide more content and facilitate more professional connections than any other event in the cybersecurity industry. Through their network of industry experts, thought leaders, practitioners, and solution providers, they collaborate to produce leading-edge, relevant content and educational opportunities.

Register Now

ISSA Kansas City Chapter Membership

2017 Fellows Cycle is Now Open

The Fellow Program recognizes sustained membership and contributions to the profession. 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 next cycle will open 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 for the 2017 Cycle will be recognized at the 2017 ISSA International Conference. Submissions received after the deadline will not be considered.

Familiarize yourself with the Fellow Program, and the **submission guidelines**. If you have questions, contact **The Fellow Manager** or call 866 349 5818 (US toll free) extension 4082.

Become a Senior Member
Any member can achieve Senior Member status, the first step in the Fellow Program. What are the criteria?

- 5 years of ISSA membership
- 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

   Application forms:

- **Submit your application for Senior Member**
- **Submit an endorsement on behalf of a Senior Member candidate**

Fellow and 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 consult the **Fellow Program Guidelines** and use the current forms to ensure you comply with all requirements.

Fellow Qualifications

- 8 years of association membership
- 12 person-years of relevant professional experience
- 3 years of volunteer leadership in the association
- 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 developing and teaching courses
- All Fellow applications require a nomination to qualify
- For your convenience, please feel free to use this **Fellow Application Check-list** to confirm eligibility and completion of application

   Application forms:

- **Submit your application for Fellow**

- **Submit a nomination on behalf of a Fellow candidate**
- **Submit a letter of recommendation on behalf of a Fellow candidate**

Distinguished Fellow Qualifications

- 12 years association membership
- 16 person-years of relevant professional experience
- 5 years of sustained volunteer leadership in the association
- 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
- For your convenience, please feel free to use this **Distinguished Fellow Application Check-list** to confirm eligibility and completion of application

 Application forms:

- **Submit your application for Distinguished Fellow**
- **Submit a nomination on behalf of a Distinguished Fellow candidate**
- **Submit a letter of recommendation on behalf of a Distinguished Fellow candidate**

Please send an email if you have any questions about the ISSA membership and benefits.

Thanks,
Membership Director, membership@kc.issa.org

ISSA-Kansas City February Chapter Event

On February 23, 2017 the ISSA-KC Chapter members, and other security professionals will hold a meeting at Hereford House Restaurant in Town Center Plaza to network and attend the monthly chapter meeting, with presentation topic.

Speaker Bio:
Chad Ray has had roles at technology manufactures for 20 years, as a Network & Security Solutions Architect and Mobile Security Specialist across organizations such as Cisco, Alteon, and Bay Networks. Chad has 18+ years of network and security theoretical and applied technical knowledge in a diverse set of technologies including distribution, stimulus, and encapsulation protocols, WiFi methods and controls, and several security technologies.

Speaker Bio:
Kameron Klein has been actively working in Information Security for more than 18 years. He has consulted for large financial institutions such as Discover Financial and JP Morgan Chase, Large Service Providers as well as many local and national organizations. Additionally, he has worked for several Technology manufacturers including TippingPoint/HP, Palo Alto Networks and currently works for Netskope, Inc.

Company Description
Netskope is the leader in cloud security. Using patented technology, Netskope's cloud-scale security platform provides context-aware governance of all cloud usage in the enterprise in real time, whether accessed from the corporate network, remote, or from a mobile device. This means that security professionals can understand risky activities, protect sensitive data, stop online threats, and respond to incidents in a way that fits how people work today. With granular security policies, the most advanced cloud DLP, and unmatched breadth of workflows, Netskope is trusted by the largest companies in the world. Netskope — security evolved. To learn more, visit www.netskope.com

Topic Summary: CASB 2.0: 5 Highest-Impact CASB Use Cases
Abstract: Cloud application and data security is a top priority for many enterprises. Whether securing data in the Office 365 suite, ensuring compliance in ServiceNow, verifying activities within DevOPS or getting control over shadow IT, information security leaders are exploring how Cloud Access Security Brokers can make an impact in their organizations. Join Kameron Klein, Sr. Systems Engineer and Chad Ray, RSM at Netskope, for a session on which use cases are challenging enterprises today and how a next generation CASB can solve for them.

Attendees will learn:
• Industry-specific data that's foundational to any cloud security business case;
• The five highest-impact CASB 2.0 use cases from our customers, demonstrated from the perspective of users and security professionals; and
• How those use cases translate to "must-have" requirements for any CASB evaluation

Agenda:
11:30 AM - 12:00 PM Greeting and registration
12:00 PM - 1:00 PM - Meeting & Presentation
1:00 PM - 1:30 PM - Questions, Answers & Networking

Location: Hereford House, Town Center Plaza, 5001 Town Center Drive, Leawood, KS 66211

Menu:
Choice of one: Beef, Chicken, or Salmon,
Salad, Potato, Vegetable, Drink

Soft drinks, Iced Tea, Coffee

* *Vegetarian option available, please note at registration**.
* *Menu subject to change. **

Price:
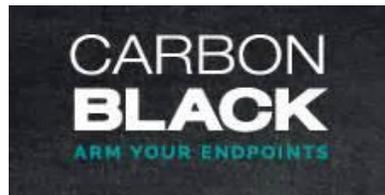$20.00 for ISSA Members,
$30.00 for Guests/Non-Members

Maximum Reservation: 35
Credit(s): 1 CPE credit

We look forward to seeing you at the event. If you have any questions about the event or how to register, please email our RSVP email, or contact the venue for directions.

*** Register ***

The Information Systems Security Association (ISSA) is an international organization providing educational forums, publications and peer interaction opportunities that enhance the knowledge, skills and professionalism. The primary goal of ISSA is to promote management practices that will ensure availability, integrity and confidentiality of organizational resources.

novacoast

OPTIV

IBM

radware

AOS

CARBON BLACK
ARM YOUR ENDPOINTS

InteliSecure

Integrity
SECURITY | RISK | COMPLIANCE

VARONIS

tenable
network security

CISCO
OpenDNS

viawest

SonicWALL | One Identity

DELL

President
Naeem Babri
president@kc.issa.org

Vice President
Cheryl Cooper
mailto:vp@kc.issa.org

Director of Social Media
Melissa Salazar
socialmedia@kc.issa.org

Secretary of Board
Rochelle Boyd
secretary@kc.issa.org

Newsletter Chief Editor
Cheryl Cooper
newsletter@kc.issa.org

Treasurer
Gary Kretzer
treasurer@kc.issa.org

Director of Membership
Wei Cheng
membership@kc.issa.org

Director of Education
Larry Dilley
certification@kc.issa.org

Director of Programs
Carmen Banks
programs@kc.issa.org

Webmaster
Thomas Badgett
webmaster@kc.issa.org

Director of Events
Dan Boethe
events@kc.issa.org

Past Presidents
Bob Reese
Tom Stripling
Jeff Blackwood
Michelle Moloney