ISSA
Information Systems Security Association
Greater Kansas City Chapter

Volume 63, Issue 5 The Newsletter of the Greater Kansas City ISSA Chapter May 2019

The President's Corner

Inside This Issue

Happy May !

Hope you enjoyed last month's presentation on Insider Risk by Krina Snider. This month we will have a presentation on eCommerce security. Did you know ISSA has scholarships for cybersecurity students at the undergraduate and graduate levels? Check this details.

Information Systems Security Association Int is pleased to announce the dates and location of this year's ISSA International Summit! Join us in Irving/Dallas, Texas - October 1-2, 2019!

If you are interested in serving on the ISSA KC board as a member or committee member, please reach out to me at president@kc.issa.org.

Sincerely,
Naeem Babri
President, ISSA-Greater Kansas City Chapter

Upcoming Events

Chapter Meeting
May 23th 2019
eCommerce Security

Chapter Meeting
June 27, 2019
MITRE ATT&CK framework

Connect With Us
kc.issa.org

Twitter
KansasCityISSA

Facebook @kcissa

LinkedIn

Chapter News

ISSA Journal : May 2019

Feature articles include:

- Choosing Tokenization or Encryption
- Trends in Security Executive Leadership and the Rise of the vCISO
- The Mathematics behind RSA Encryption
- NIST Cryptographic Algorithm and Module Validation Programs: Validating New Encryption Schemes

Members: please click on the following Journal issue links for access: Computer: Bluetoad - PDF; Mobile: ePub - Mob

Not a member? Read this month's feature article - The Future of IT Risk Management Will Be Quantified - at no charge or Join Now and gain full access to the *ISSA Journal*.

Last month's Chapter Meeting at Lidia's (Krina, Naeem and Gary)

At InfoSec Community Showcase (Jeff)

Webinars & Conferences

Kansas City CyberSecurity Conference - "Cybersecurity is no longer just an IT problem"

Date: Wednesday May 22nd, 2019
Place: Kansas City Marriott Downtown
Time: 8AM-6PM

ISSA KC would like to invite our members with a complimentary pass
8 CPE CREDITS
Please use the promo code **ISSA** to register for a full day pass.

https://futureconevents.com/events/kansas-city-mo/

Gain the latest knowledge you need to enable applications while keeping your computing environment secure from advanced Cyber Threats. Demo the newest technology and interact with the world's security leaders and gain other pressing topics of interest to the information security community.

KEYNOTE SPEAKER: John Dickson Principal at Denim Group, Ltd
Topic: "Security in a World of Digital Transformation"

John Dickson is an internationally recognized security leader, entrepreneur and Principal at Denim Group, Ltd. He has nearly 20 years' hands-on experience in intrusion detection, network security and application security in the commercial, public and military sectors. As a Denim Group Principal, he helps executives and Chief Security Officers (CSO's) of Fortune 500 companies and government organizations launch and expand their critical application security initiatives. Dickson is a popular Speaker on security at industry venues including RSA Conference, the SANS Institute, the Open Web Application Security Project (OWASP). A Distinguished Fellow of the International Systems Security Association, he has been a Certified Information Systems Security Professional (CISSP) since 1998.

4:00 – 4:45 CISO /THOUGHT LEADER PANEL SESSION/ *Cocktails included*
(Dark Web, Insider Threat, Cyber Resilience)

Closing Remarks /Cocktail Reception/ Prize Drawings (Must be in attendance): 4:30 - 6:00 p.m.

Agenda: ***Click here for the complete agenda***

This event is being documented for a CISO series by Cybercrime Magazine.
A collaboration of CISO interviews are being conducted at each event.

Once again, if you would like to register use **ISSA** for your complimentary VIP pass:

https://futureconevents.com/register/

INTERFACE-Kansas City

Jul 18th, 2019

8:30 am – 4:30pm

Overland Park Convention Center
Ballrooms A-C
6000 College Boulevard
Overland Park, KS 66211

Register

https://f2fevents.com/evite/kcm19-issa-kansas-city/

Upcoming Chapter Event

May 23, 2019 the ISSA KC Chapter Meeting

Topic: eCommerce Security

Topic Summary:
Presentation around the History of Online Credit Card Skimmers, and our research around the Magecart exploits.

Speaker Bio:
Brad Liggett, After dialing into his first BBS in 1993, Brad has immersed himself in technology at every turn. After spending several years as a data network and voice engineer for Everest Connections (now Consolidated Communications), Brad has focused on helping companies adopt best practices when it comes to all aspects of technology. With over 20 years of industry experience, Brad currently assists companies with continuously defending their ever-changing attack surface as a solution. Protecting companies, brand, people, and data is at the core of his role with RiskIQ.

Location:
BRIO Tuscan Grille
502 Nichols Rd, Kansas City, MO 64112

Agenda:
11:30AM -12:00PM - Registration and Check In
12:00 PM -1:00 PM - Lunch // Speaker's Presentation
1:00 PM - 1:30 - Networking

Price:
$25 members| $30 guests

CPE's: 1 Credits *Please note actual CPE hours granted are dependent upon duration of the speaker's presentation and may differ from advertised number of CPE hours.

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 **

Next Month: June 27, 2019 the ISSA KC Chapter Meeting

Topic: MITRE ATT&CK

Presentation Topic
The MITRE ATT&CK framework is a very effective tool for "adversary emulation", cataloging how adversaries behave, what they're trying to do, and the techniques used to accomplish their means. Moreover, the framework aims to provide a common language and vocabulary for practitioners, vendors, and all parties working to understand common threat actors and techniques.

In November 2018, MITRE evaluated a subset of techniques in an open-test environment, working with vendors to analyze their detection capabilities against these common techniques. With the results of this first evaluation now published, many are trying to make sense of results to understand the efficacy of different solutions in the marketplace today.

In this event, we'll boil down the complexity of the MITRE ATT&CK framework so your organization can understand:
- How to adapt the framework to your company's environment and needs in order to get the most utility out of it
- What different detection categories mean and how to interpret results of ATT&CK Framework evaluations
- How Cybereason allows customers to search and understand their environment based on the ATT&CK Framework

Speaker Bio
John Morton is a Senior Sales Engineer at Cybereason. Having been on both sides of the fence, now as a solutions provider and previously as a practitioner for the US Navy & Federal government, John is a veteran in merging day-to-day cybersecurity efforts – always protecting the enterprise and a keen knack for actively hunting for the threat.

cybereason

Location:
Hereford House
5001 Town Center Dr, Leawood, KS 66211

Agenda:
11:30AM -12:00PM - Registration and Check In
12:00 PM -1:00 PM - Lunch /Speaker's Presentation

Price:
$25 members| $30 guests

Membership

Please contact membership@kc.issa.org for question or concern when applying to be an ISSA Senior Member or ISSA Fellow

Senior Member, Fellow, and Distinguished Fellow applications are available. Please read and apply here:

https://www.issa.org/page/FellowProgram

Best Regards,
Director of Membership
Wei Cheng

Job Posting

Security Specialist - Governance

The Security Specialist position requires an individual who has an IT and controls related background with general security knowledge. The security specialist will be tasked with a range of responsibilities to include interaction with several departments throughout the organization to coordinate compliance and project related activities.

Key Responsibilities

- Maintains awareness of security directives, orders, standards, plans and procedures.
- Ensures security operating manuals and procedural documents stay current when regulations change.
- Assists with the efforts involving work plans, schedules, project estimates, resource plans and status reports within time, budget and specification constraints.
- Maintains all policy, procedure and associated governance documentation related to organization specific security compliance methodologies.
- Assists with risk assessment and third party audit documentation and remediation tracking.
- Interfaces regularly with staff from various departments communicating security issues, obtaining additional information as needed, and providing status of remediation to security management
- Performs third party vendor security reviews and document concerns
- Assists Security team with internal process improvement initiatives including establishing workflows and automation of manual processes

Job Link

Security & Privacy: Articles and News

Feature Articles

Microsoft: Consider Dropping Password Expiration Policies

By Trend Micro

Microsoft is changing their baseline for password-expiration policies in Windows. The proposal is a move from the previous policy that requires users to change their login passwords periodically.

In the company's new security configuration baseline draft for Windows 10 v1903 and Windows Server v1903, periodic password requests (i.e., changing login passwords at pre-set time intervals or the recommended 60-day password expiration policy) will be removed from their baseline. Microsoft says recent research calls into question the long-standing password expiration policies. They encourage additional protections for stronger authentication and cite better alternatives such as enforcing banned-password lists.

Aaron Margosis, a principal consultant for Microsoft, explains that previous security practices led to weaker security due to new passwords typically being based on old ones. Often, users compelled to regularly change passwords only made small and predictable changes to existing passwords, or even forget new ones.

*** Continued

GandCrab attackers exploit recently patched Confluence vulnerability

By - Lucian Constantin

A group of attackers are actively exploiting a critical vulnerability in Atlassian's Confluence collaboration software to infect servers with the GandCrab ransomware. Confluence is a Java-based web application that provides a shared wiki-type workspace for enterprise employees and is used by tens of thousands of companies worldwide. The vulnerability, tracked as CVE-2019-3396, is in the software's Widget Connector that allows users to embed content from YouTube, Twitter and other websites into web pages.

Attackers can exploit the flaw to inject a rogue template and achieve remote code execution on the server. According to Atlassian's advisory, published March 20, all versions of Confluence Server and Confluence Data Center before versions 6.6.12, 6.12.3, 6.13.3 and 6.14.2 are affected.

According to a new report from security firm Alert Logic, proof-of-concept exploit code for the vulnerability was released publicly on April 10 and malicious hackers wasted no time adopting it in attacks. "Within a week of the first exploit code appearing within our data lake we saw the first set of breached customers," the Alert Logic researchers said.

*** Continued

Mentor Program: ISSA Greater Kansas City

The program is designed to formalize relationships between senior professional individuals in the chapter (Mentors) and the various levels of security professionals seeking entry or moving through the different phases of this profession (Mentees). There are many different types of mentoring partnerships; peer to peer, adult to adolescent, apprentice to master, cross generational, and mentoring within a company or a few. It depends on what type of mentoring relationship you're seeking.

Mentor/Mentee application: Mentor Application :: Mentee Application

Feature Articles - continued

Continued News from Article Page

Security Top Concern as Mobile Providers Think 5G

By Kelly Sheridan

Mobile service providers think the future of 5G networks will drive revenue opportunities and new use cases driven by the Internet of Things (IoT) — however, security must be improved for 5G to fulfill its potential.

Sixty-seven percent of mobile providers will deploy their first commercial 5G networks within 18 months, another 21% within the next two years. Most (94%) expect increases in network traffic growth, connected devices, and mission-critical IoT use cases to drive security and reliability concerns. A majority (79%) say 5G is a factor in current security investments.

The insights come from "Securing the Future of a Smart World," a new report based on a survey conducted by the Business Performance Innovation (BPI) Network and commissioned by A10 Networks. As a whole, mobile providers recognize new applications (such as self-driving cars, smart cities, and remote patient observation) will heighten the need for safe and secure network connections.

"When we look at what happened when 4G networks came in, there was a lot of disruption to the industry," says Paul Nicholson, director of product marketing for A10, who anticipates the rise of 5G networks will cause greater disruption than 4G networks did in the past. "Security issues normally come when there's a disruption in the technology," he explains.

Researchers found the top drivers for 5G include smart cities (60%), industrial automation and smart manufacturing (48%), high-speed connectivity (39%), fixed wireless (37%), and connected vehicles (35%). As 5G continues to grow, so too will use cases and devices relying on it, he adds. A connected car, for example, has to be reliable in a split second — there's little room for error.

While mobile providers think 5G networks will drive opportunity, it will also increase risk. 5G will bring more traffic and connected devices, many of which will be mission-critical. Network security is very important (72%) or important (26%) to most respondents asked about 5G.

Sixty-three percent view advanced distributed denial-of-service (DDoS) protection as the most important security tool built into 5G. Nearly 80% have or will upgrade to Gi/SGi firewalls; 73% have or will upgrade to a GTP firewall. Progress is slow going: Only 11% have upgraded their Gi firewalls and 13% have upgraded GTP firewalls, resulting from the complexity of control and management planes in 5G.

*** Continued

Sponsors

Board of Directors

President
Naeem Babri

Secretary of Board
Rochelle Boyd

Treasurer
Gary Kretzer

Director of Membership
Wai Cheng

Director of Education
Nicole Windholz

Director of Programs
Chris Mcleod

Webmaster
Thomas Badgett

CISSP Study Group,
Mark Waugh
issakc-study@kc.issa.org

Past Presidents
Bob Reese
Tom Stripling
Jeff Blackwood
Michelle Moloney

Our Sponsors

viawest
CARBON BLACK
CYBERARK
Integrity
proofpoint.
CRITICALSTART
okta
Zerto IT RESILIENCE
Symantec.
FORCEPOINT POWERED BY Raytheon
McAfee
SECURONIX
vmware
KENNA Security