ISSA
Information Systems Security Association
Greater Kansas City Chapter

Volume 63, Issue 6 The Newsletter of the Greater Kansas City ISSA Chapter June 2019

The President's Corner

Inside This Issue

Happy June!

Hope you enjoyed last month's presentation. 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.

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!

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

Upcoming Events

Chapter Meeting
June 27, 2019
MITRE ATT&CK framework

Chapter Meeting
July 25th
12 Ways to Hack 2FA

Connect With Us
kc.issa.org

Twitter
KansasCityISSA

Facebook @kcissa

LinkedIn

Chapter News

ISSA Journal : June 2019

Feature articles include:

- 2019 International Election Candidate Profiles.
- Smart Cities & Privacy
- Privacy Preserving Blockchains
- Privacy Concerns of Smartphone Technology
- The Python Programming Language: GUI

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*.

Webinars & Conferences

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

June 27, 2019 the ISSA KC Chapter Meeting

Topic: MITRE ATT&CK

Topic Summary:
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

**** REGISTER ****

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.

July 25th Meeting:

Topic: 12 Ways to Hack 2FA

Topic Summary:
Everyone knows that multi-factor authentication (MFA) is more secure than a simple login name and password, but too many people think that MFA is a perfect, unhackable solution. It isn't! I can send you a regular phish email and completely take control of your account even if you use a super-dooper MFA token or smartphone app. Attend this webinar and learn the 12+ ways hackers can and do get around your favorite MFA solution. The webinar will include a (pre-filmed) hacking demo by KnowBe4's Chief Hacking Officer, Kevin Mitnick, and real-life successful examples of every attack type. It will end by telling you how to better defend your MFA solution so that you get maximum benefit and security.

Speaker Bio
Roger A. Grimes, Data-Driven Defense Evangelist for KnowBe4, Inc., is a 30-year computer security consultant, instructor, holder of dozens of computer certifications, and author of 10 books and over 1,000 magazine articles on computer security. He has spoken at many of the world's biggest computer security conferences, been in *Newsweek*™ magazine, appeared on television, been interviewed for NPR's *All Things Considered*™, and been a guest on dozens of radio shows and podcasts. He has worked at some of the world's largest computer security companies, including Foundstone, McAfee, and Microsoft. He has consulted for hundreds of companies, from the largest to the smallest, around the world. He specializes in host and network security, identity management, anti-malware, hackers, honeypots, Public Key Infrastructure, cloud security, cryptography, policy, and technical writing. His certifications have included CPA, CISSP, CISA, CISM, CEH, MSCE: Security, Security+, and yada-yada others, and he has been an instructor for many of them. His writings and presentations are often known for their real-world, contrarian views. He has been the weekly security columnist for *InfoWorld* and *CSO* magazines since 2005.

LinkedIn: https://www.linkedin.com/in/rogeragrimes/

Twitter: @rogeragrimes

CSOOnline: https://www.csoonline.com/author/Roger-A.-Grimes/

Author's other books on Amazon: https://www.amazon.com/Roger-A.-Grimes/e/B001IQUMT4/

KnowBe4
Human error. Conquered.

Location:
Lidia's Restaurant
101 W 22nd St, Kansas City, MO 64108

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

Security & Privacy: Articles and News

Feature Articles

5G Security Challenges: A Vendor's POV

By Tara Seals

How will 5G vendors deal with the issues of security? Nokia's head of end-to-end security solutions discusses during the GSMA Mobile 360 conference.

How are vendors preparing themselves for the onslaught of 5G networks from a security standpoint? When it comes to 5G there are a slew of use cases being utilized at the bleeding edge – from smart factories to IoT – but these are also opening up security risks.

At the GSMA Mobile 360 Security for 5G conference last week in the Netherlands., Threatpost talked to Nils Ahrlich, head of end-to-end security solutions at Nokia, about security measures that OEMs and vendors are taking.

*** Continued

5G Networks Spark Concerns For Enterprise Risks - by Sara Seals

As 5G deployments continue to increase, what are the top security risks for enterprises? We discuss with an expert

MITRE ATT&CK Framework Effective in Defending CNI

By - Dan Raywood

Speaking at Infosecurity Europe 2019 on 'Effective Steps to Reduce Third Party Risk,' Scott W. Coleman, director of product management at Owl Cyber Defense, said that the average number of connections to a facility is 583. "Most are legitimate, but how many are appropriate" he asked.

He said that there are "vendors and companies and entities who need access to your plant, enterprise or base" and while many have a good reason to have access, you need to be sure that they are not presenting a risk that you don't need.

Coleman recommended determining what you need to protect, which connectors and disaster recovery systems you need to protect, and which vendor service level agreements you need to maintain "but be subversive on what needs to have access."

He encouraged companies to focus on the following when evaluating a third party: which products and services require access; which companies have a higher level of personnel turnover; who have been involved in breaches themselves "as a lot of the time, a company has a third party connecting" so depending on their level of cybersecurity.

during GSMA's Mobile360 conference.
THE HAGUE, Netherlands – The rise of 5G networks – and subsequent security risks – was the centerpiece issue discussed during the GSMA's Mobile360 conference on 5G security this past week.

While researchers warn that 5G security issues could literally be a matter of life or death for certain applications, the new technology is also triggering another type of concern: the risks that 5G networks potentially pose for enterprise organizations.

*** Continued

Looking at strategies for mitigation, Coleman asked if many people will know who the 583 people are, and what access they have if you have a good handle on what they are doing? "Understand and measure what they are doing as it is hard to protect against them," he 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

Premera Blue Cross reaches proposed $72M settlement with 2014 breach victims

by Bradley Barth

Health insurance company Premera Blue Cross has agreed to a $72 million proposed settlement that would resolve a contentious class-action lawsuit stemming from a 2014 data breach affecting roughly 10.6 million people.

Pending court approval and barring further appeals, the deal would require Premera to pay $42 million to fund comprehensive remedial measures and injunctive relief in the form of information security program improvements and business practice changes over the next three years, according to a motion filed on May 30 in Oregon District Court.

To that end, Premera has committed to "encrypting, archiving, and maintaining protected environments for data; requiring two-factor authentication for remote access for all personnel and vendors; performing various audits and testing exercises, and collecting and maintaining logs of covered information systems; operating a Cyber Security Operations Center; employing a Chief Information Security Officer; requiring Information Security training for its associates, etc." according to the motion.

*** 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