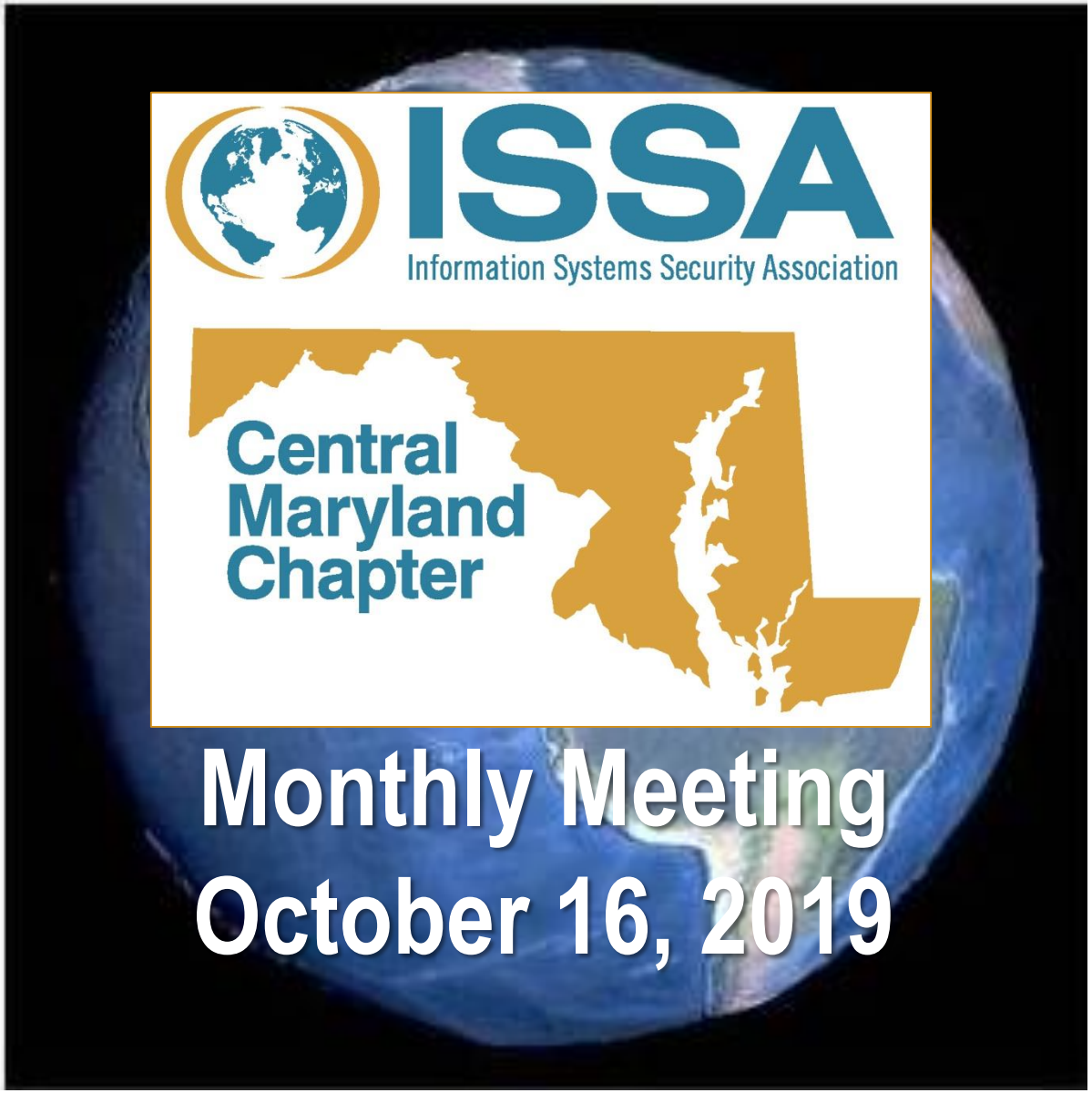

Central Maryland Chapter Sponsors:
Zscaler, Clearswift, LogRhythm, Parsons Cyber,
Phoenix TS, Tenable Network Security

ISSA
Information Systems Security Association

ISSA Information Systems Security Association
Central Maryland Chapter

Please respect the speakers and other members,

Silence or turn off cell phones and electronic devices,

No video or audio recordings.

Questions are welcome; please keep them on-topic and brief. Further discussion should be taken off-line with the presenters so as to allow them the courtesy of being able to finish their presentations within the allotted time without being rushed.

Sidebar discussions should be constrained. If you must discuss something, allow your fellow members (and the presenter) the courtesy of doing so outside or on break.

Central Maryland Chapter Sponsors:
Zscaler, Clearswift, LogRhythm, Parsons Cyber, Phoenix TS, Tenable Network Security

ISSA Information Systems Security Association

Agenda / Announcements

- Welcome to The National Electronics Museum
- Any guests or new members in attendance?
- $(ISC)^2$ CPE Submissions – Individual Responsibility
- CISSP Chapter Badges / Shirts and Jackets with ISSA-Central MD Logo
- CISSP & Study Group
- Future Meeting schedule

ISSA Information Systems Security Association
Central Maryland Chapter

Board of Directors

- Bill Smith, Jr., CISSP, GSNA, CEH, GPEN, GCFA, GCFE - President
- Sidney Spunt, CISSP - VP Operations
- Zac Lechner, CISSP, CEH, MBA – Secretary
- Carol Klessig, CISSP - VP Professional Development
- Kevin Newman, CISSP, GCIH – VP Education
- Christina Holleran – Treasurer
- Steve Chan, CISSP, PMP – VP Membership
- Keith Bull, CISSP - VP Outreach

Central Maryland Chapter Sponsors:
Zscaler, Clearswift, LogRhythm, Parsons Cyber, Phoenix TS, Tenable Network Security

ISSA Information Systems Security Association

ISSA Information Systems Security Association
Central Maryland Chapter

Central Maryland Chapter Sponsors

zscaler™
Platinum Sponsor

clearswift

tenable network security

PHOENIX TS

LogRhythm™
The Security Intelligence Company

PARSONS
CYBER

Central Maryland Chapter Sponsors:
Zscaler, Clearswift, LogRhythm, Parsons Cyber,
Phoenix TS, Tenable Network Security

ISSA Information Systems Security Association

ISSA Information Systems Security Association
Central Maryland Chapter

2020-1 CISSP Study Group

CISSP®

Start: February 18, 2020
End: May 19, 2010
UMBC Training Center

Review and Practice Exam

14 Sessions Total

Central Maryland Chapter Sponsors:
Zscaler, Clearswift, LogRhythm, Parsons Cyber,
Phoenix TS, Tenable Network Security

ISSA Information Systems Security Association

ISSA Information Systems Security Association
Central Maryland Chapter

ISSA Central MD Chapter
October Monthly Meeting

Sponsored by: Jazz Networks & LogRhythm

Jazz Networks

LogRhythm
The Security Intelligence Company

Wednesday, October 16, 2019
5:00 PM to 7:00 PM

National Electronics Museum
1745 West Nursery Rd, Linthicum MD 21090

2019 Central Maryland Chapter of ISSA Board of Directors Elections

Election Held at 20 November Meeting

Secretary

- Vacant
- Record and keep minutes of meetings
- Maintain the official records of the Chapter.
- Transmit and respond to all correspondence of the Chapter,
- Make official records available to members upon request.

Vice President of Professional Development:

- Vacant
- Recommend, initiate, and oversee programs for professional development to include monthly meetings, security conferences / seminars, and interaction with peer organizations
- Work with the VP of Outreach to schedule any speakers identified by that officer
- Evaluate and organize any career development events.

Treasurer:

- Vacant
- Receive membership dues
- Keep an accurate account of all treasury receipts, expenditures, and deposits as well as other monies or articles of value belonging to the Chapter

Vice President of Operations:

- Incumbent - Sidney Spunt
- Attend to the duties of the President in his / her absence
- Attend to any other duties as the President may require

If interested and would like to know more, please email the secretary at secretary@issa-centralmd.org

ISSA Information Systems Security Association
Central Maryland Chapter

ISSA Dark Web Tour Workshop
November 8 @ 1:00 pm - 3:00 pm

Join the ISSA Central Maryland Chapter and IntSights for an afternoon of knowledge transfer on Dark Web and Threat Intelligence. This workshop will include a *live* Dark Web Tour. What was once a figment of the imagination, the Dark Web has evolved into an Amazon-ish shopping destination where nation-states, hackers, and even the most unsophisticated cyber criminals can purchase and barter for malware, crime ware-as-a-service, VIP emails and passwords, credit card numbers, bank accounts and more.

Objectives covered:

- How threat intelligence platforms collect threat intelligence from the clear, deep and dark web to deliver contextual and tailored digital risk protection against emerging threats
- How to automate threat intelligence to automate proactive defense
- How crypto currency is being used extensively to monetize criminal activity
- Which nation-states are expanding their Dark Web presence in an effort to keep up with national defenses
- Why organizations of all sizes need to understand what is lurking on the Dark Web in order to properly protect against external and internal threats
- This presentation is open to members and security professionals. This presentation is not intended for security vendors.

Central Maryland Chapter Sponsors:
Zscaler, Clearswift, LogRhythm, Parsons Cyber, Phoenix TS, Tenable

ISSA Information Systems Security Association

ISSA Information Systems Security Association Central Maryland Chapter

Crash Course in PowerShell

December 14 @ 8:30 am - 4:30 pm
UMBC Training Center

This course will give you the basics of PowerShell. You will learn the PowerShell syntax, as well as various other topics (examples: how to repeat tasks, how to iterate through a list of objects, and the various things you can do with PowerShell objects). You will also learn how to discover new cmdlets, modules, and functions. You will gain hands-on experience by practicing what the instructor is teaching, and demos of production scripts and tools. The target audience for this course are individuals who are new to scripting and individuals who are new to PowerShell.

ISSA Information Systems Security Association

Central Maryland ISSA Chapter
Information Security Conference

SAVE THE DATE!!

Looking for Speakers and Sponsor

January 29, 2020

8:30-4:00 pm

USRA, 7178 Columbia Gateway Drive, Columbia, Md

Cost: $100, $90 for ISSA Members

More details soon!!

Central Maryland Chapter Sponsors:

Zscaler, Clearswift, LogRhythm, Parsons Cyber, Phoenix TS, Tenable

Central Maryland ISSA Chapter
Maryland STEM Festival
October 11th – November 10th

MARYLAND STEM FESTIVAL 2019

Chapter-Bronze Sponsor

Central Maryland Chapter Sponsors:
Zscaler, Clearswift, LogRhythm, Parsons Cyber, Phoenix TS, Tenable

ISSA Information Systems Security Association

MARYLAND STEM FESTIVAL 2019

2nd State-Wide Virtual HS Cybersecurity Competition

Test your cyber knowledge against High School students across the state! Teams will consist of 4 students. Bring your laptop. Prizes for the winners!!!

November 2, 2019
12:00-4:00 PM
All Over Maryland

http://marylandstemfestival.org/

ISSA 2017-2018 Meetings and Events

Date	Speaker	Organization	Topic
October 16, 2019	Charles Finfrock Darren Cathey	Tesla LogRhythm	Taking a holistic approach to an insider threat program Security Operations Maturity Model (SOMM)
November 20, 2019	Michael Long II	Mitre ATT&CK Team	Threat Informed Defense with MITRE ATT&CK™
December 18, 2019	Razvan Miutescu	Whiteford, Taylor & Preston LLP	Risk Mitigation Strategies for Cybersecurity Service Providers

ISSA Information Systems Security Association
Central Maryland Chapter

November 20, 2019 Speaker #1

Michael C. Long II

Senior Cyber Adversarial Engineer, The MITRE Corporation

Michael Long is a Senior Cyber Adversarial Engineer with the MITRE Corporation and a former U.S. Army Cyber Operations Specialist. Michael has over 10 years of experience in information security disciplines including adversary threat emulation, red teaming, threat hunting, and digital forensics and incident response. Michael Long has a proven track record of service in the public interest. Michael served on countless cyber operations for organizations including the Army Cyber Protection Brigade and Army Cyber Command, the results of which he regularly briefed to commanding generals, strategic executives, and congressional staffers. With MITRE, Michael continues to apply his technical expertise to improve the cybersecurity of our nations most sensitive and critical networks. Michael has a Masters Degree in Information Security Engineering from SANS Technology Institute and holds many information security certifications including the prestigious GIAC Security Expert certification (GSE).

ISSA Information Systems Security Association

ISSA Information Systems Security Association
Central Maryland Chapter

November 20, 2019

Threat Informed Defense with MITRE ATT&CK™

The MITRE ATT&CK framework has become a widely used knowledge base and model for real cyber adversary behavior. In use across governments, private sector, and security solutions providers, ATT&CK helps to focus defenses against known threats, provides an effective tool for measuring security improvements, and drives innovation.

The session will cover the history of ATT&CK and what drove its creation at MITRE, the philosophy behind how ATT&CK is maintained, and several use cases for how it can be applied including behavioral analytic development, defensive gap analysis, and adversary emulation.

Central Maryland Chapter Sponsors:
Zscaler, Clearswift, LogRhythm, Parsons Cyber, Phoenix TS, Tenable Network Security

ISSA Information Systems Security Association

ISSA Information Systems Security Association
Central Maryland Chapter

October 16, 2019 Speaker #1

Charles Finfrock, Senior Threat Investigator, Tesla

Charles Finfrock is a Senior Threat Investigator in Tesla's Security Intelligence Department, the team responsible for protecting Tesla's Intellectual Property and confidential business information from internal and external threats. Prior to joining Tesla, Charles spent 18 years as an operations officer in the Central Intelligence Agency. Charles is also the head of Insider Threat at the Washington DC based, Cyber Intelligent Partners, a training and education company focused on helping companies develop programs to counter cyber threats, regional threats, and insider threats.

ISSA Information Systems Security Association

ISSA Information Systems Security Association Central Maryland Chapter

October 16, 2019

Taking a holistic approach to an insider threat program

This presentation will provide insider threat mitigation strategies for every phase of the employment life cycle, including pre-employment screening; ongoing insider threat and security training; leveraging tools like Jazz Networks for user activity monitoring, and finally what to watch out for when an employee is leaving the organization. We will share anecdotes from public and private sector service experience, highlighting vulnerable areas of the employee life cycle where an insider can become an active threat. We will also provide a brief demonstration of the Jazz Networks insider threat and detection platform.

ISSA Information Systems Security Association

October 16, 2019 Speaker #2

Darren Cathey, Sr. Systems Engineer, LogRhythm

Darren Cathey has several decades of experience in programming, operating systems, and applications security. His multi-functional experience in engineering, marketing and sales lends itself well to supporting both SMB and Enterprise customers in the Mid-Atlantic territory as a Sr. Systems Engineer. Past experience includes positions with HP, Wind River Systems, Arxan, Vormetric and Varonis.

ISSA Information Systems Security Association
Central Maryland Chapter

October 16, 2019

Security Operations Maturity Model (SOMM)

SOMM explores how to assess and evolve the principle programs of the security operations center (SOC): threat monitoring, threat hunting, threat investigation, and incident response. LogRhythm developed the Threat Lifecycle Management (TLM) framework to help organizations ideally align technology, people, and process in support of these programs. The TLM framework defines the critical security operations technological capabilities and workflow processes that are vital to realize an efficient and effective SOC. LogRhythm's SOMM helps organizations measure the effectiveness of their security operations, and to mature their security operations capabilities. Using our TLM framework, the SOMM provides a practical guide for organizations that wish to optimally reduce their mean time to detect (MTTD) and mean time to respond (MTTR) — thereby dramatically improving their resilience to cyberthreats.

ISSA Information Systems Security Association