ISSA
Information Systems Security Association

Central Maryland Chapter

Monthly Meeting August 22, 2018

ISSA
Information Systems Security Association

Agenda / Announcements

➢ Welcome to Parsons

➢ 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

<u>Please respect the speakers and other members,</u>

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:
Cybrary, Inc. Clearswift, LogRhythm, Parsons Cyber, Phoenix TS, Tenable Network Security

ISSA
Information Systems Security Association

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

❖ Chuck Dickert, CISSP, CISA, CISM, CAPM – VP Education

❖ Jack Holleran, CISSP, CAP, (ISC)2 Fellow– Treasurer

❖ Steve Chan, CISSP, PMP – VP Membership

❖ Rob Reintges,CISSP - VP Outreach

Central Maryland Chapter Sponsors

CYBRARY

Platinum Sponsor

clearswift

tenable
network security

PHOENIX TS

LogRhythm™
The Security Intelligence Company

PARSONS
CYBER

ISSA
Information Systems Security Association

Fall 2018 CISSP Study Group

Start: September 4, 2018
End: December 11, 2018

Review and Practice Exam

14 Sessions Total
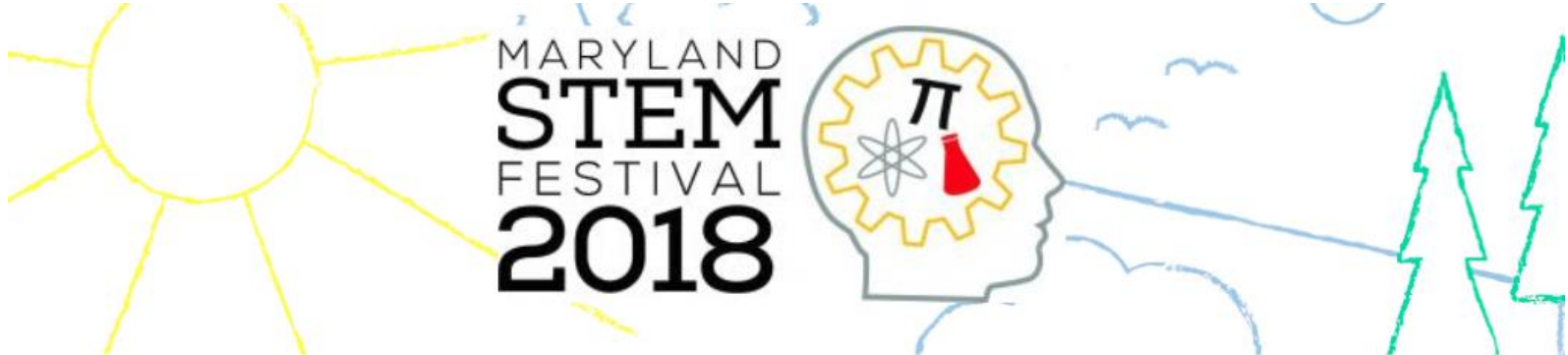
*** Virtual Capture The Flag for High School ***

August 22nd Meeting Location

UMBC
Training Centers

Westridge Corporate Center
6996 Columbia Gateway Drive,
Suite 100
Columbia, MD 21046
Phone: 443-692-6600

New Meeting Location

- Columbia/Ft. Meade Area
- Seat 75 people
- HVAC until 7:30
- AV Equipped
- Internet
- Kitchen

2018 ISSA International Conference

SECURING TOMORROW TODAY

October 17-18 | Georgia World Congress Center | Atlanta, GA

Central Maryland Chapter Sponsors:
Cybrary, Inc. Clearswift, LogRhythm, Parsons Cyber,
Phoenix TS, Tenable Network Security

ISSA 2017-2018 Meetings and Events

Date	Speaker	Organization	Topic
August 22, 2018	Michael A. Tarinellil	Aruba, the HP Enterprise Company	Protecting your data from the insider threat; introducing the Aruba 360 Secure Mobile Fabric
September 26, 2018	Conrad Fernandes	Johns Hopkins - Applied Physics Laboratory (APL)	Security logging and central monitoring of AWS GovCloud accounts

September 26, 2018 Speaker

Conrad Fernandes

Johns Hopkins - Applied Physics Laboratory (APL)

Conrad Fernandes is a long time cyber security engineer and architect, with various security certifications (CISSP, GIAC FA, Certified AWS Solutions Architect and Security Specialist, among others) and has worked extensively with US Defense agencies and the DoD since the early 2000's while at Booz Allen Hamilton. Conrad currently serves as a senior cyber security engineer at the Johns Hopkins Applied Physics Laboratory (APL), where he leads security and governance practices on emerging cloud technologies, including commercial and US GovCloud (e.g., Amazon web services) and Hadoop-based data science platforms from Cloudera and Hortonworks. Conrad recently presented strategies for "Incident Response and Spillage Handling in AWS" at Amazon's Public Sector Summit and re:Invent Conference. Additionally, Conrad has been researching and implementing security and audit logging and monitoring strategies on data science platforms at Johns Hopkins Medical Institute (JHMI) that utilize various emerging services from Hortonworks Data Platform (HDP) distributions and the collection and correlation of security audit events via Splunk. Conrad also enjoys sharing security best-practices and lessons-learned from the experiences with the larger cloud and big-data communities.

September 26, 2018

AWS Security: Central Logging Techniques for Multiple Accounts, and Automating via Cloud Formation Templates

Logging of essential Amazon services, such as Cloudtrail and VPC flow logs, is essential for security and compliance and governance, whether HIPAA, FISMA, PCI and several other regulatory bodies. In this session we will go over the key concepts in detail -- such as setting up a central account for managing and retaining log events, by any number of governed (source) accounts; and the setup for the source accounts to send their respective logs to the centrally managed account. Since working with multiple accounts can become an issue with scaling and consistency and human errors if the setup was done manually, we will go over better methods using cloud formation templates that help tremendously in that regard by automating the setup! Last but not least, we will also cover best practices – including codifying in the templates – that will account for any type of Amazon unclassified account – which includes the commercial regions as well as the GovCloud (US) regions.

August 22, 2018 Speaker

Michael Tarinelli

Aruba, A Hewlett Packard Enterprise company

Michael serves as a Consulting Systems Engineer focusing on cyber security. He spent the first 15 years of his career in the financial services industry working at AlianceBernstein where he led a project to acquire and deliver one of the first secure WLANs in the financial industry. While at AB, Michael led the security engineering group focusing on internal and perimeter security tools before leaving in 2008 to join Panzura, a startup founded by former Aruba engineering folks. Michael then joined Aruba in 2011.

August 22, 2018

Protecting your data from the insider threat; introducing the Aruba 360 Secure Mobile Fabric

Attacks against an organizations valuable and sensible information are getting more and more complex and frequent. Hackers know that the weakest point of attack is the user and exploits that fact by targeted phishing, over the shoulder, and brute force attacks meant to expose a user's credentials. Once they have this, they craft their next steps carefully to evade traditional security mechanisms, masking their maneuvers to appear like normal user traffic. From this session, learn more about this attack vector and Aruba's security solutions and methodology on how to minimize your risk as well as how to apply machine learning and AI to quickly find and remove these threats from your environment.

Central Maryland Chapter Sponsors:
Cybrary, Inc. Clearswift, LogRhythm, Parsons Cyber, Phoenix TS, Tenable Network Security

ISSA Information Systems Security Association