15 February 2018

From Malware Analysis to Suricata Signatures – How to Defend your Networks (1:10-1:50 pm ET)

Mark your calendars and come join your friends in the CAE community for a Tech Talk. We are a warm group that shares technical knowledge. CAE Tech Talks are free and conducted live in real-time over the Internet so no travel is required. You can attend from just about anywhere (office, home, etc.) Capitol Technology University (CTU) hosts the presentations using their online delivery platform (Adobe Connect) which employs slides, VOIP, and chat for live interaction. Just log in as "Guest" and enjoy the presentation(s).

Below is a description of the presentation(s) and logistics of attendance:

Date: Thursday, 15 February 2018

Time: 1:10-1:50 pm ET

Location: https://capitol.adobeconnect.com/cae_tech_talk/

Just log in as "Guest" and enter your name. No password required.

Title/Topic: From Malware Analysis to Suricata Signatures – How to Defend your Networks

Audience Skill Level: Intermediate

Presenter(s): Dr. Josh Stroschein – Dakota State University

Description:

The use of an IDS/IPS is crucial in providing not only visibility into your networks, but also to help protect your organizations resources. In this talk, we will discuss how you can leverage malware analysis to

create Suricata signatures. This presentation will provide you with tips, insights and resources to get started using Suricata and writing your own signatures right away!

Suricata is a free and open source, mature, fast and robust network threat detection engine. The Suricata engine is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline pcap processing. Suricata inspects the network traffic using a powerful and extensive rules and signature language, and has powerful Lua scripting support for detection of complex threats.

CAE Tech Talks are also recorded

Recordings of live presentations are posted to the website below:

https://capitol.instructure.com/courses/510/external_tools/66

Pdf versions of the presentations are posted to the website below:

https://capitol.instructure.com/courses/510/files

Contact

CAE Tech Talk events are advertised thru email and posted to the news and calendar section of the CAE community website: www.caecommunity.org

For questions on CAE Tech Talk, please send email to CAETechTalk@nsa.gov