WASTC 2020 Faculty Development Weeks

Interactive Threat Hunting

Dates: Fully Online, June 15-19, 2020
Times: 8:30 am - 11 am and 1pm - 3 pm each day, office hours TBD

Workshop Description:
This session will provide an overview of the tools and techniques commonly used for detecting threats to an enterprise infrastructure. Implement strategies for documenting and reporting detected events based on industry standard compliance frameworks. We will use the Security Onion distribution. Tools include Elasticsearch, Logstash, Kibana (ELK/Elastic Stack), Wazuh, Snort, Zeek, Wireshark, and TCP Dump.

From the instructor:

The full class overview (I will be picking a subset of the labs out to cover each of these topics in the 1 week class):

Full Interactive Threat Hunting class description (Note: It is currently named "Intrusion Detection" at our college)

The NIST Nice mappings for the class we used for CAE-2Y:
Mapping Class to CAE-2Y [NIST Nice]
Scripting for Cybersecurity for Powershell:

Instructor: Michael Masino is the Information Security Program Director at Madison Area Technical College. Michael has developed numerous courses in Information Technology and Cyber Security. He developed several of the labs that will be used in this workshop. Michael holds several industry certifications including: GIAC Certified UNIX Security Administrator (GCUX) GIAC Certified UNIX Security Administrator (GCUX) GIAC Python Coder (GPYC) GIAC Penetration Tester (GPEN) GIAC Certified Intrusion Analyst (GCIA) GIAC Certified Forensic Analyst (GCFA) GIAC Advisory Board

Sponsored by:

CSSIA
National Resource Center for Systems Security and Information Assurance