E-ISAC CRISP
CYBERSECURITY
RISK INFORMATION SHARING PROGRAM

CRISP Spring Workshop

Gaining Insight with Zeek

May 10 – 11, 2022

Presented by:
Critical Path Security and E-ISAC's
Cybersecurity Risk Information Sharing Program (CRISP)
crisp@eisac.com

Hosted by:
Pacific Northwest National Laboratory (PNNL)
crisp@pnnl.gov

TLP: AMBER – Limited disclosure, restricted to participants organizations

Agenda

Event Location: Discovery Hall at PNNL
650 Horn Rapids Road
Richland, WA 99354

Format: In-person (registered attendees only); remote dial-in not available

Day 1 | Tuesday, May 10

Time (Pacific)	Topic and Presenter	Room
8:00 – 9:45 am	**Gaining Insight with Zeek – Part 1** Patrick Kelley (Critical Path Security)	**Horizon A, B & C**
9:45 – 10:00 am	**BREAK**	
10:00 am – 12:00 pm	**Gaining Insight with Zeek – Part 1 (Resumed)** Patrick Kelley (Critical Path Security)	**Horizon A, B & C**
12:00 – 1:00 pm	**Working Lunch for Participants** – provided by PNNL CRISP Team Introductions by E-ISAC, PNNL, and DOE	**Horizon A, B & C**

Day 2 | Wednesday, May 11

Time (Pacific)	Topic and Presenter	Room
8:00 – 9:45 am	**Gaining Insight with Zeek – Part 2** Patrick Kelley (Critical Path Security)	**Horizon A, B & C**
9:45 – 10:00 am	**BREAK**	
10:00 am – 12:00 pm	**Gaining Insight with Zeek – Part 2 (Resumed)** Patrick Kelley (Critical Path Security)	**Horizon A, B & C**
12:00 – 1:00 pm	**Working Lunch for Participants** – provided by PNNL Q&A Session with Frank Honkus (E-ISAC), Jeffrey Mauth (PNNL), Michael Toecker (DOE CESER)	**Horizon A, B & C**

Course Syllabus

Instructor: Patrick Kelley

Course Web: https://www.criticalpathsecurity.com

Course Description

Zeek is a great open-source tool that allows you to monitor your network and analyze events within it. This course will teach you about this tool, and how to configure and use it within your network to suit your needs.

What Students will Learn

Zeek is network event-based monitoring and analysis tool used by many organizations around the world. It enables users to see the traffic going through their networks and respond to it in several different ways. This course will teach the user how to configure, use, and customize this tool to discover attackers on the network, perform in-depth forensic investigations, and resolve network issues. In this course, Gaining Insight with Zeek Training, the student will learn how to install and configure Zeek, how to use it, how it functions, and where to place it on the network. First, the student will learn about Zeek, deployment types, placement, and functionality. Next, the student will learn how to install popular Zeek packages and threat intelligence, followed by understanding the Zeek outputs. Finally, the student will explore the language Zeek uses and how they can use it to help your environment, along with customizing and deploying Zeek scripts. When the student is finished with this course, they will have an in-depth understanding of Zeek and be able to use it effectively to defend their networks.

Course Objectives

At the end of this course students should know:

- How Zeek works and what are the proper use cases
- The Zeek deployment types and proper placement on the network
- How to install Zeek on Ubuntu Linux
- How to install popular Zeek packages
- How to review protocol logs and Zeek outputs
- How to leverage Zeek Threat Intelligence Feeds
- How to understand Zeek scripts and how to customize them

Course Materials

A laptop will be required for this course. It is recommended that the laptop have 8GB of RAM and VirtualBox installed. Though instruction will be provided on how to properly install Zeek, for sake of time and brevity, VirtualBox images will be provided of Ubuntu with Zeek installed, along with an image with test traffic to replay for analysis. At the conclusion of the training, a PowerPoint presentation will be provided to students. It is recommended that students be prepared to take notes.

Course Format

This course will be provided in two (2) four-hour sessions. This will provide the student with the opportunity to clear any potential challenges with installation and traffic replay between the individual sessions. As each student might provide sensitive information regarding their own internal networks, this course will not be recorded. A recorded version of the course, without user questions will be provided at a later date.

Course Training Room Policies

Students are expected to adhere to the following:

- Students should be on-time and ready to begin at the assigned class time.
- Cell phones and mobile devices should be turned off.
- Only respectful classroom discussions, comments, and questions relevant to the current topic will be allowed.
- No video or audio taping of classes is allowed.

TLP: AMBER – Limited disclosure, restricted to participants organizations

Biographies

Course Instructor

Patrick Kelley, Chief Technical Officer
Critical Path Security

Patrick is an experienced security researcher and public speaker with 25 years of industry experience. With his knowledge of information security and how it applies to a wide array of industry verticals, he works as the chief technology officer for Critical Path Security.

Patrick and the Critical Path Security team use their breadth of experience and depth of knowledge to solve security problems that are unique to their clients' organization, as well as those that typically plague the corporate and energy landscape. His clients span numerous industries, including retail, manufacturing, healthcare, defense, national power grid, financial services, and ultra-high net worth individuals.

He is frequently interviewed and quoted by Forbes, Fortune, Motley Fool, NBC News, The Guardian, and speaks at numerous conferences around the world each year.

Electricity Information Sharing and Analysis Center (E-ISAC)

Frank Honkus, Associate Director of Intelligence Programs and CRISP Program Manager

Frank Honkus supports the cybersecurity of electric utilities members of CRISP through ensuring growth of the program and refinement of technical capabilities, reporting, and information sharing. Prior to joining the E-ISAC, Frank supported the Department of Energy's Office of Intelligence and Counterintelligence analyzing CRISP data for anomalous and malicious cyber activity. He was the red team lead and wrote the foundational mitigation and recovery sections for the Joint Base Architecture for Security Industrial Control Systems (J-BASICS) Joint Test, and supported the United States Cyber Command focusing on cyber threats to operations technology systems. He received his Masters in Public and International Affairs (MPIA) with a major in Security and Intelligence from the University of Pittsburgh's Graduate School of Public and International Affairs, and received a dual major in History and Political Science from the University of Pittsburgh.

Colin Stuver, CRISP Program Specialist

Colin Stuver is a Program Specialist for CRISP at the E-ISAC, joining in 2018. In his role, Colin serves as one of the primary points of contact for all financial, contractual, and programmatic matters related to CRISP, as well as fostering valuable relationships with new and existing participating utilities and government partners. Prior to joining the E-ISAC, Colin served as a project manager and research analyst for the world's fastest-growing commercial real estate firm at Avison Young.

Irene Tzinis, CRISP Program Analyst

Electricity Information Sharing and Analysis Center (E-ISAC)

Irene Tzinis joined the E-ISAC in April 2021 to help provide outreach and strategic engagement for the CRISP program. Prior to the E-ISAC, Irene was with ASRC Federal for eleven years as a senior communications specialist supporting NASA's Space Communications and Navigation program office at NASA Headquarters in Washington, DC. Irene also served two years with ASRC Federal at NASA's Goddard Space Flight Center in Greenbelt, MD as a technology transfer specialist. She is the recipient of numerous NASA awards, including the 2019 Space Flight Awareness Honoree award. She received her Masters in Public and International Affairs from the University of Pittsburgh's Graduate School of Public and International Affairs and her Bachelors in International Studies with minors in Political Science and German from Millersville University.

Pacific Northwest National Laboratory (PNNL)

Jeffery Mauth, Senior Project Manager

Jeffery Mauth is a Senior Project Manager at the Pacific Northwest National Laboratory, joining the Lab in 1994. Starting in 1998, Jeff has worked closely with DOE-IM, and the DOE-IN to establish and operate the wide area network security monitoring capability for the Department of Energy. In 2009, working with DOE-OE, he established and continues to manage the Cyber Risk Security Information Sharing Program (CRISP) for the energy sector to continuously enhance the security of the energy sector. Prior to his work in network security monitoring, Jeff served as the PNNL Senior Network Engineer, deploying and managing high performance network architectures and high-performance wide area networking. Jeff has 31 years of experience, with the last 20 years focusing on wide area networking security monitoring, cyber intelligence, big data processing and analytics, and high-performance networking.

Bryce Kaspar, Lead Cyber Security Analyst

Bryce is a Lead Cyber Security Analyst at Pacific Northwest National Laboratory (PNNL) where he works in cyber intelligence information sharing. He leads a team of cyber analysts that support programs that provide private sector partners in critical infrastructure with threat intelligence products, briefings on intelligence products, and contribute to wide area situational awareness analytic development. Mr. Kaspar has been with PNNL for 20 years in a wide variety of systems administration, software development, and cyber security related projects across a wide breadth of computing environments.

U.S. Department of Energy (DOE)

Michael Toecker, Program Manager for CRISP

Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

At the Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response (CESER), Michael is the program manager for the Cybersecurity Risk Information Sharing Program (CRISP) and a subject matter expert in cyber security for energy operational technology systems. Michael brings an understanding of the electric power sector, technical expertise in cyber security for energy, and an operational focus to DOE CESER activities.

Prior to DOE, Michael collected broad expertise in the cyber security of energy sector control systems and risk management for energy. He has spent 16 years working in electric power and control system security, first at a Big 5 power engineering firm, then at the power generation arm of a major utility. Michael has worked for the control system security firm Digital Bond on vulnerability research, penetration testing, and various ICS security research projects. Michael left Digital Bond to build an energy sector focused consultancy in 2014 to explore important electric power resilience and security issues as a consulting engineer, and worked as the liaison between DOE and DARPA for the series of RADICS exercises between 2018 and 2020. He left private practice in January of 2021 to join DOE CESER to contribute to solutions to cybersecurity issues of national focus.