Zeek (Bro) Workshop Europe 2019

Report of Contributions

https://indico.cern.ch/e/bro-workshop-europe-2019

Contribution ID: **1** Type: **not specified**

Opening remarks

Tuesday, April 9, 2019 1:00 PM (10 minutes)

Presenter: HEMMER, Frederic (CERN)

Session Classification: Workshop presentations

Contribution ID: **2** Type: **not specified**

Keynote: Finding the balance between academic freedom, operations and security

Tuesday, April 9, 2019 1:10 PM (50 minutes)

Presenter: LUEDERS, Stefan (CERN)

Session Classification: Workshop presentations

Contribution ID: **3** Type: **not specified**

How did we get here?

Tuesday, April 9, 2019 2:00 PM (30 minutes)

Presenter: Prof. PAXSON, Vern (UC Berkeley / Corelight / ICSI)

Session Classification: Workshop presentations

Contribution ID: **4** Type: **not specified**

Real time ingestion of MISP threat intel into Zeek coupled with historical SIEM threat hunting

Tuesday, April 9, 2019 2:30 PM (30 minutes)

Presenters: VALSAN, Liviu (CERN); Dr VALLENTIN, Matthias (Tenzir)

Session Classification: Workshop presentations

Contribution ID: **5** Type: **not specified**

Looking Forward: On Supervisors, Packages, and Sandboxes

Tuesday, April 9, 2019 3:45 PM (30 minutes)

Presenter: SOMMER, Robin (Corelight / ICSI / LBNL)

Session Classification: Workshop presentations

Contribution ID: **6** Type: **not specified**

Email security auditing and alert triage with Zeek

Tuesday, April 9, 2019 4:15 PM (30 minutes)

Presenter: Mr WEYMES, Barry

Session Classification: Workshop presentations

Contribution ID: **7** Type: **not specified**

Running Zeek on the WAN: Experiences and solutions for large scale flow asymmetry

Wednesday, April 10, 2019 10:15 AM (30 minutes)

Presenters: CAMPBELL, Scott (Unknown); OEHLERT, Sam

Session Classification: Workshop presentations

Contribution ID: **8** Type: **not specified**

DNSSEC protocol parser - A case study

Wednesday, April 10, 2019 10:45 AM (30 minutes)

Presenter: Ms BANNAT WALA, Fatema (University of Delaware)

Session Classification: Workshop presentations

Contribution ID: **9** Type: **not specified**

The new Zeek Configuration Framework

Wednesday, April 10, 2019 11:15 AM (30 minutes)

Presenter: Ms JOHANNA, Amann (ICSI/Corelight/LBL)

Session Classification: Workshop presentations

Contribution ID: **10** Type: **not specified**

Network Cartography Using Passive Traffic Analysis

Wednesday, April 10, 2019 1:45 PM (30 minutes)

Presenter: VENUTI, Vivien

Session Classification: Workshop presentations

Contribution ID: **11** Type: **not specified**

Selective Packet Capture at High Speed Rates

Wednesday, April 10, 2019 1:15 PM (30 minutes)

Presenter: Dr ROS-GIRALT, Jordi

Session Classification: Workshop presentations

Contribution ID: **12** Type: **not specified**

A deep dive into the Zeek logging framework

Wednesday, April 10, 2019 2:15 PM (30 minutes)

Presenter: KREIBICH, Christian (Corelight)

Session Classification: Workshop presentations

Contribution ID: **13** Type: **not specified**

DHCP Overhaul

Wednesday, April 10, 2019 3:30 PM (30 minutes)

Presenter: Mr HALL, Seth (Corelight)

Session Classification: Workshop presentations

Contribution ID: **14** Type: **not specified**

JA3 and Windows hosts

Wednesday, April 10, 2019 4:00 PM (30 minutes)

Presenter: Mr ATKINSON, Jeff (Verizon Media)

Session Classification: Workshop presentations

Contribution ID: **15** Type: **not specified**

Using Zeek Endpoint Event Logs when Fishing within a Data Lake

Wednesday, April 10, 2019 4:30 PM (30 minutes)

Presenter: Mr LARSON, Tim

Session Classification: Workshop presentations

Contribution ID: **16** Type: **not specified**

Without “U” there is no CommUnity: Nurturing and growing an active and contributing community

Thursday, April 11, 2019 9:00 AM (30 minutes)

Presenter: Ms GRANER, Amber (Corelight)

Session Classification: Workshop presentations

Contribution ID: **17** Type: **not specified**

Threat hunting @ Mozilla

Thursday, April 11, 2019 9:30 AM (30 minutes)

Presenter: Mr PURZYNSKI, Michal (Mozilla Corporation)

Session Classification: Workshop presentations

Contribution ID: **18** Type: **not specified**

Q&A Session with the Zeek Team

Thursday, April 11, 2019 10:00 AM (30 minutes)

Session Classification: Workshop presentations

Contribution ID: **19** Type: **not specified**

Workshop Wrap up

Session Classification: Workshop presentations