Zeek (Bro) Workshop Europe 2019

Tuesday, April 9, 2019

Workshop presentations - 31/3-004 - IT Amphitheatre (1:00 PM - 3:00 PM)

time	[id] title	presenter
1:00 PM	[1] Opening remarks	HEMMER, Frederic
1:10 PM	[2] Keynote: Finding the balance between academic freedom, operations and security	LUEDERS, Stefan
2:00 PM	[3] How did we get here?	Prof. PAXSON, Vern
2:30 PM	[4] Real time ingestion of MISP threat intel into Zeek coupled with historical SIEM threat hunting	VALSAN, Liviu Dr VALLENTIN, Matthias

Workshop presentations - 31/3-004 - IT Amphitheatre (3:45 PM - 4:45 PM)

time	[id] title	presenter
3:45 PM	[5] Looking Forward: On Supervisors, Packages, and Sandboxes	SOMMER, Robin
4:15 PM	[6] Email security auditing and alert triage with Zeek	Mr WEYMES, Barry

Wednesday, April 10, 2019

Workshop presentations - 31/3-004 - IT Amphitheatre (10:15 AM - 11:45 AM)

time	[id] title	presenter
10:15 AM	[7] Running Zeek on the WAN: Experiences and solutions for large scale flow asymmetry	CAMPBELL, Scott OEHLERT, Sam
10:45 AM	[8] DNSSEC protocol parser - A case study	Ms BANNAT WALA, Fatema
11:15 AM	[9] The new Zeek Configuration Framework	Ms JOHANNA, Amann

Workshop presentations - 31/3-004 - IT Amphitheatre (1:15 PM - 2:45 PM)

time	[id] title	presenter
1:15 PM	[11] Selective Packet Capture at High Speed Rates	Dr ROS-GIRALT, Jordi
1:45 PM	[10] Network Cartography Using Passive Traffic Analysis	VENUTI, Vivien
2:15 PM	[12] A deep dive into the Zeek logging framework	KREIBICH, Christian

Workshop presentations - 31/3-004 - IT Amphitheatre (3:30 PM - 5:00 PM)

time	[id] title	presenter
3:30 PM	[13] DHCP Overhaul	Mr HALL, Seth
4:00 PM	[14] JA3 and Windows hosts	Mr ATKINSON, Jeff
4:30 PM	[15] Using Zeek Endpoint Event Logs when Fishing within a Data Lake	Mr LARSON, Tim

Thursday, April 11, 2019

Workshop presentations - 31/3-004 - IT Amphitheatre (9:00 AM - 10:30 AM)

time	[id] title	presenter
9:00 AM	[16] Without “U” there is no CommUnity: Nurturing and growing an active and contributing community	Ms GRANER, Amber
9:30 AM	[17] Threat hunting @ Mozilla	Mr PURZYNSKI, Michal
10:00 AM	[18] Q&A Session with the Zeek Team	