Zeek (Bro) Workshop Europe 2019

Tuesday 9 April 2019

Workshop presentations - 31/3-004 - IT Amphitheatre (13:00 - 15:00)

time	[id] title	presenter
13:00	[1] Opening remarks	HEMMER, Frederic
13:10	[2] Keynote: Finding the balance between academic freedom, operations and security	LUEDERS, Stefan
14:00	[3] How did we get here?	Prof. PAXSON, Vern
14:30	[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 (15:45 - 16:45)

time	[id] title	presenter
15:45	[5] Looking Forward: On Supervisors, Packages, and Sandboxes	SOMMER, Robin
16:15	[6] Email security auditing and alert triage with Zeek	Mr WEYMES, Barry

Wednesday 10 April 2019

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

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

Workshop presentations - 31/3-004 - IT Amphitheatre (13:15 - 14:45)

time	[id] title	presenter
13:15	[11] Selective Packet Capture at High Speed Rates	Dr ROS-GIRALT, Jordi
13:45	[10] Network Cartography Using Passive Traffic Analysis	VENUTI, Vivien
14:15	[12] A deep dive into the Zeek logging framework	KREIBICH, Christian

Workshop presentations - 31/3-004 - IT Amphitheatre (15:30 - 17:00)

time	[id] title	presenter
15:30	[13] DHCP Overhaul	Mr HALL, Seth
16:00	[14] JA3 and Windows hosts	Mr ATKINSON, Jeff
16:30	[15] Using Zeek Endpoint Event Logs when Fishing within a Data Lake	Mr LARSON, Tim

Thursday 11 April 2019

Workshop presentations - 31/3-004 - IT Amphitheatre (09:00 - 10:30)

time	[id] title	presenter
09:00	[16] Without “U” there is no CommUnity: Nurturing and growing an active and contributing community	Ms GRANER, Amber
09:30	[17] Threat hunting @ Mozilla	Mr PURZYNSKI, Michal
10:00	[18] Q&A Session with the Zeek Team	