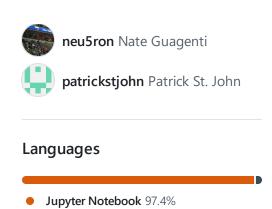




Place for resources used during the Mordor Detection hackathon event featuring APT29 ATT&CK evals datasets.

Agenda

Time	Topic	Session	Туре
10:00 - 10:10	Greet the community	General	Live Team Event
10:10 - 10:20	Getting started and Guidelines	General	Live Team Event
10:20 - 10:40	APT29 Environment & Datasets Overview	General	Live Team Event
10:40 - 11:30	Open infrastructure for open research!	General	Live Team Event
11:30 - 12:00	Break	Break	Break
12:00 - 12:15	Basic Analysis with Jupyter Notebooks	Collaboration	Regular Teams
12:15 - 12:45	Sigma & Zeek Integration	Collaboration	Regular Teams



Dockerfile 2.6%

12:45 - 13:45	Explore the data either on your own or as a group	Collaboration	Regular Teams
13:45 - 14:00	Break	Break	Break
14:00 - 14:30	Sharing detections! Screen Sharing allowed	Collaboration	Regular Teams
14:30 - 15:30	Exploring the data either on your own or as a group	Collaboration	Regulat Teams
15:30 - 16:00	Sharing detections! Screen Sharing allowed	Collaboration	Regular Teams
16:00 - ?	Who knows?	Collaboration	Regular Teams

Emulation Plans:

 Online: https://1drv.ms/x/s!Al3n8YINIUPUbx1TH8bkLU5UWk0?
 e=LeA51U

• Offline: https://github.com/OTRF/detection-hackathon-apt29/tree/master/emulation-plans

Videos

