Cyber Security Advisory Board meeting - ENTA project

21 November 2022| Online

Biswajit Nandy, Solana Networks

ITEA 4

ITEA 4 is the Eureka Cluster on software innovation

Encrypted Network Traffic Analysis

ENTA project

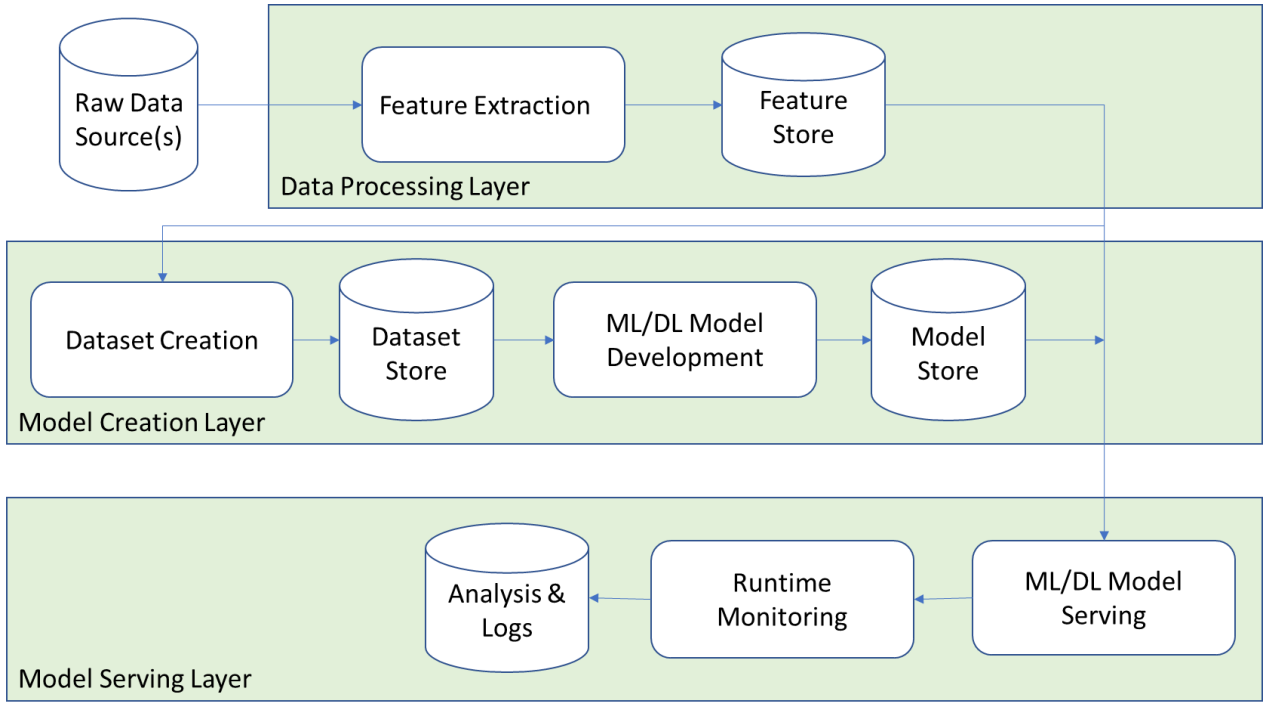
- More than 80% of internet traffic is encrypted and it is growing
- Various sectors are impacted due to lack of visibility into encrypted traffic:
  - SOC – unable to detect malware, data exfiltration using encrypted channels, rogue IoTs as attack surface
  - IT department – unable to enforce policy, quality of service
  - LEAs – difficult to perform forensics
  - Router/Switch and Firewall vendors – need to know traffic types, applications
  - Military – Less accurate network situational awareness
- ENTA project:
  1. Develop an AI based encrypted network traffic analysis platform to create ML/DL based product quality solutions
  2. Usecase1 – Detect/classify encrypted applications and traffic classes
  3. Usecase2 – Discover and detect rogue IoT devices
- Use temporal and spatial traffic characteristics to derive to solutions – i.e., without having to inspect traffic payload

There are many other Use cases that can leverage ENTA platform:
-- Detection of malware hiding in encrypted traffic
-- Data exfiltration using covert channel
-- C&C Botnet detection

ITEA 4 | Σ

Project summary

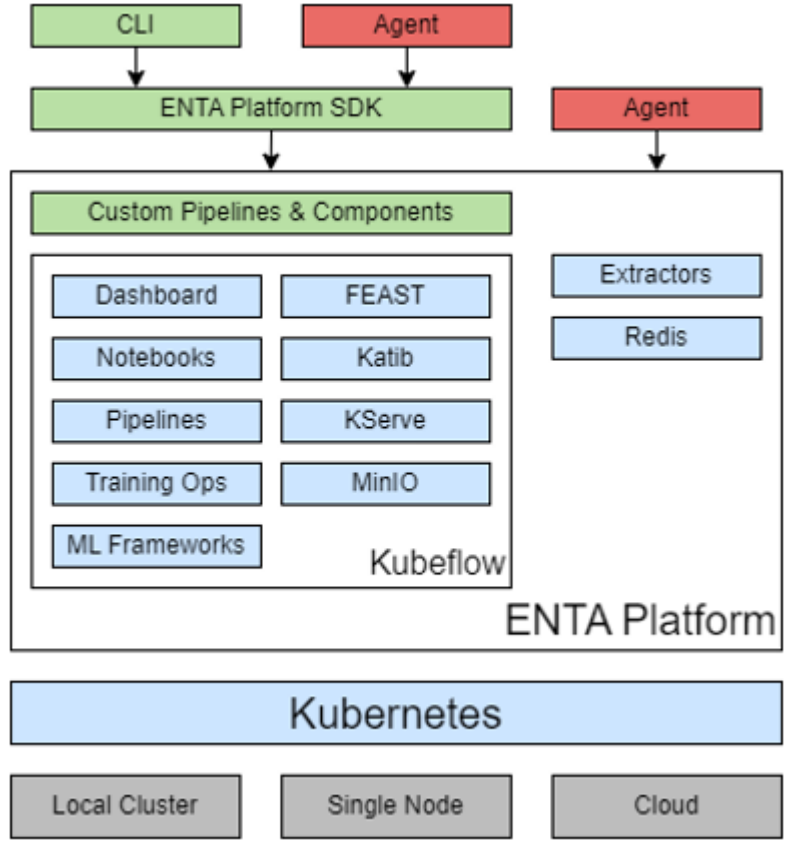
- AI platform for network data
  - Provides (>100) network features
  - Ability to experiment with ML/DL pipeline
  - Export models for runtime environment
  - Ability to develop production quality ML/DL models
  - Enables to share data, experiment with various models and validate results
- UseCase1: Application detection
  - Encrypted applications (Netflix, YouTube etc.)
  - Traffic classes (Streaming, Chat, VoIP etc.)
  - Certain User actions (clicking on certain button)
- UseCase2: Discover & detect rogue IoT
  - Discover presence of IoTs devices on a network (potential attack surface)
  - Detect rogue IoT



ENTA Platform: Functional Block Diagram

Recent Progress

- Project started on 31st January, 2022
- Various early documents are complete:
  - SotA, Exploratory data analysis, ENTA platform architecture
- Labeled dataset generation is in progress:
  - Encrypted applications (IMA: WhatsApp, Messenger, Telegram, Teams, Discord, Signal)
  - Testbeds are created for IoT data collection
- ENTA Platform architecture defined, detail design completed and software being developed
- Dissemination: Website, workshop & conference presentations and publications



ENTA Platform: Architecture Diagram

Project partners and data

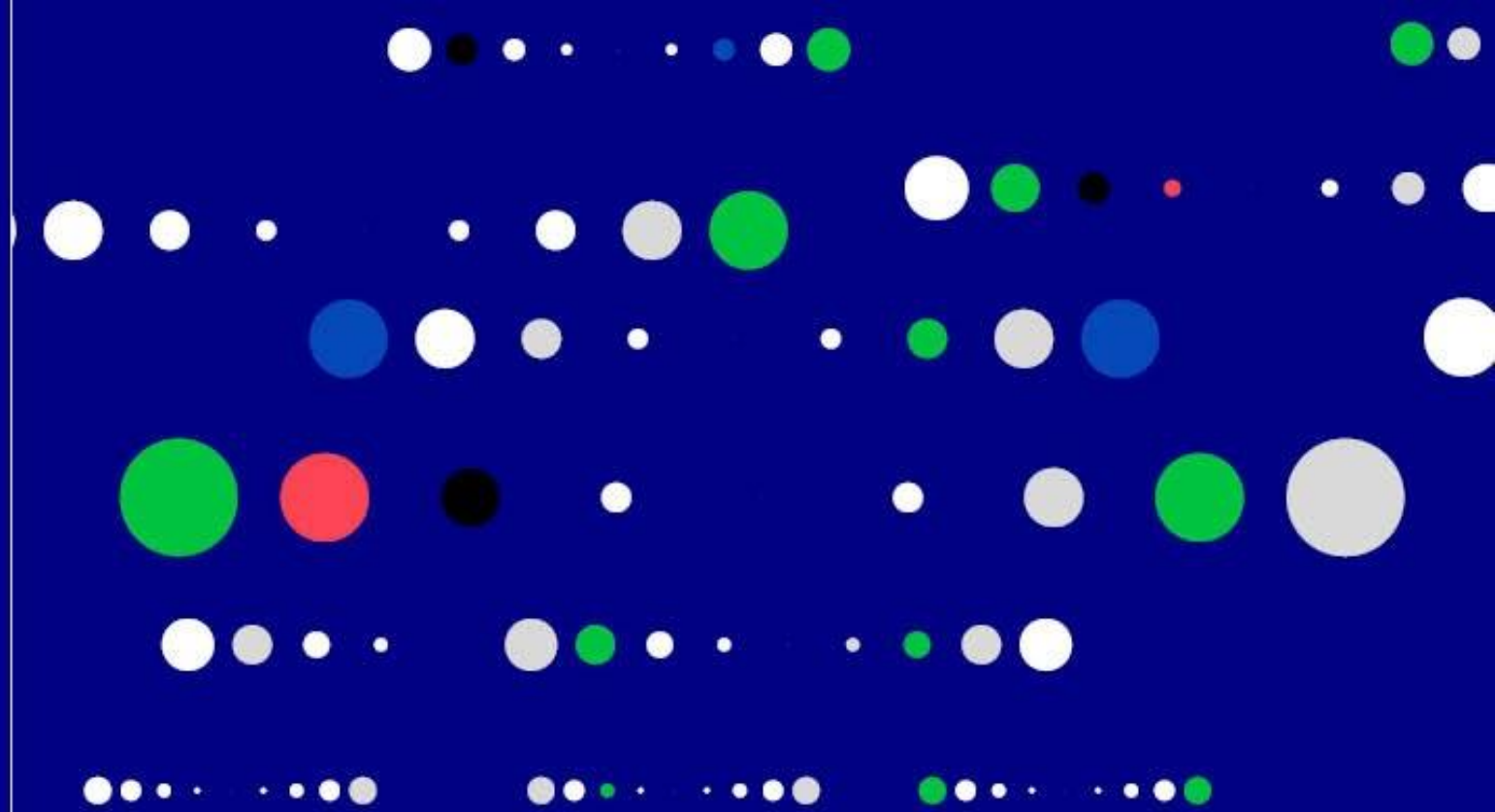
ENTA project

	Organisation	Technical contact	Country
1	BEIA GmbH	George Suciu	AUT
2	Centre for Factories of the Future Ltd	Lakhvir Singh	GBR
3	Dalhousie University	Nur Zincir-Heywood	CAN
4	Metodos y Tecnologia	Luis Redondo Lopez	ESP
5	Ruag AG	Stefan Burschka	CHE
6	Solana Networks	Biswajit Nandy	CAN

- Start date: 31 Jan 2022
- End date: 30 Jan 2025
- Project leader: Solana Networks (Canada)
- Website: https://itea4.org/project/enta.html
  https://project-enta.com/

Contact Details:

Biswajit Nandy
Solana Networks (Canada)
bnandy@solananetworks.com
Phone: +1 613-799-1230



ITEA 4

https://itea4.org

ITEA is the Eureka Cluster on software innovation

eureka

https://www.eurekanetwork.org

Thank you