

Integrated Project Cyber security of energy systems for the digital-energy transition

AI-based techniques and tools for cybersecurity energy ranges



- Monitoring and detection cyber attack based on AI techniques
 - Preventive measures not applicable
 - Preventive measures not updatable
 - Challenges of Quantum revolution
- OT systems and protocols specific
 - Monitoring
 - AI techniques
- Attack process oriented
 - Intercept cyber kill chain
- Regulation
 - Monitoring, incident detection and response



CER (Critical Entities Resilience)

Proactive Protection

Continuous Monitoring: 24/7 surveillance to detect and respond quickly to threats.

Attack Prevention: Identifying and neutralizing threats before they can cause damage.

Rapid Incident Response

Incident Management: Structured procedures to effectively respond to attacks.

Reduced Recovery Time: Minimizing impact and downtime.

Threat Intelligence

Threat Analysis: Collecting and analyzing data to better understand emerging threats.

Constant Updates: Up-to-date information to adapt to new attack techniques.

Compliance and Regulation

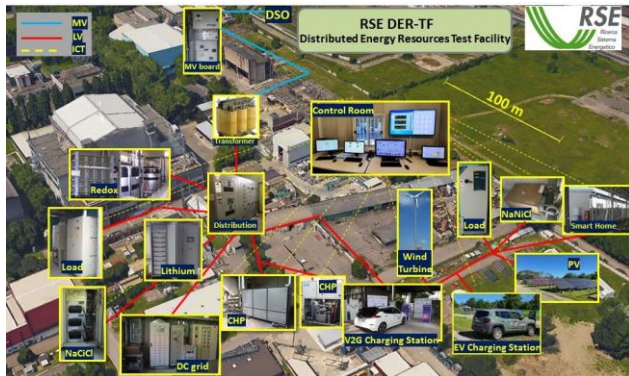
Regulatory Compliance: Ensuring adherence to security laws and regulations.

Audits and Reporting: Documentation and reporting to demonstrate compliance.

Continuous Improvement

Learning and Adapting: Continuously improving defense strategies based on new information.





Real-time interception of the communication flow

Traffic interpretation according to specific protocols

**Selection of significant indicators and events
Information extraction**

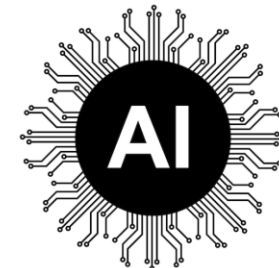
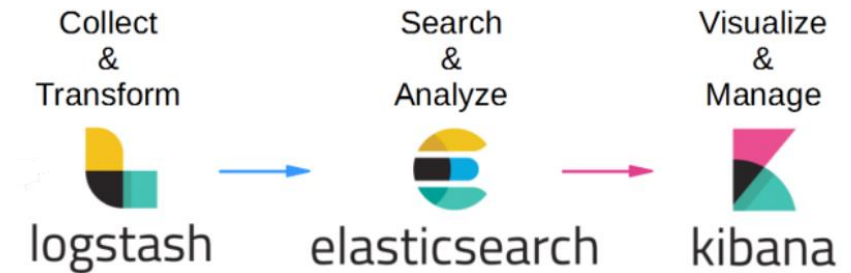
Data storage and indexing

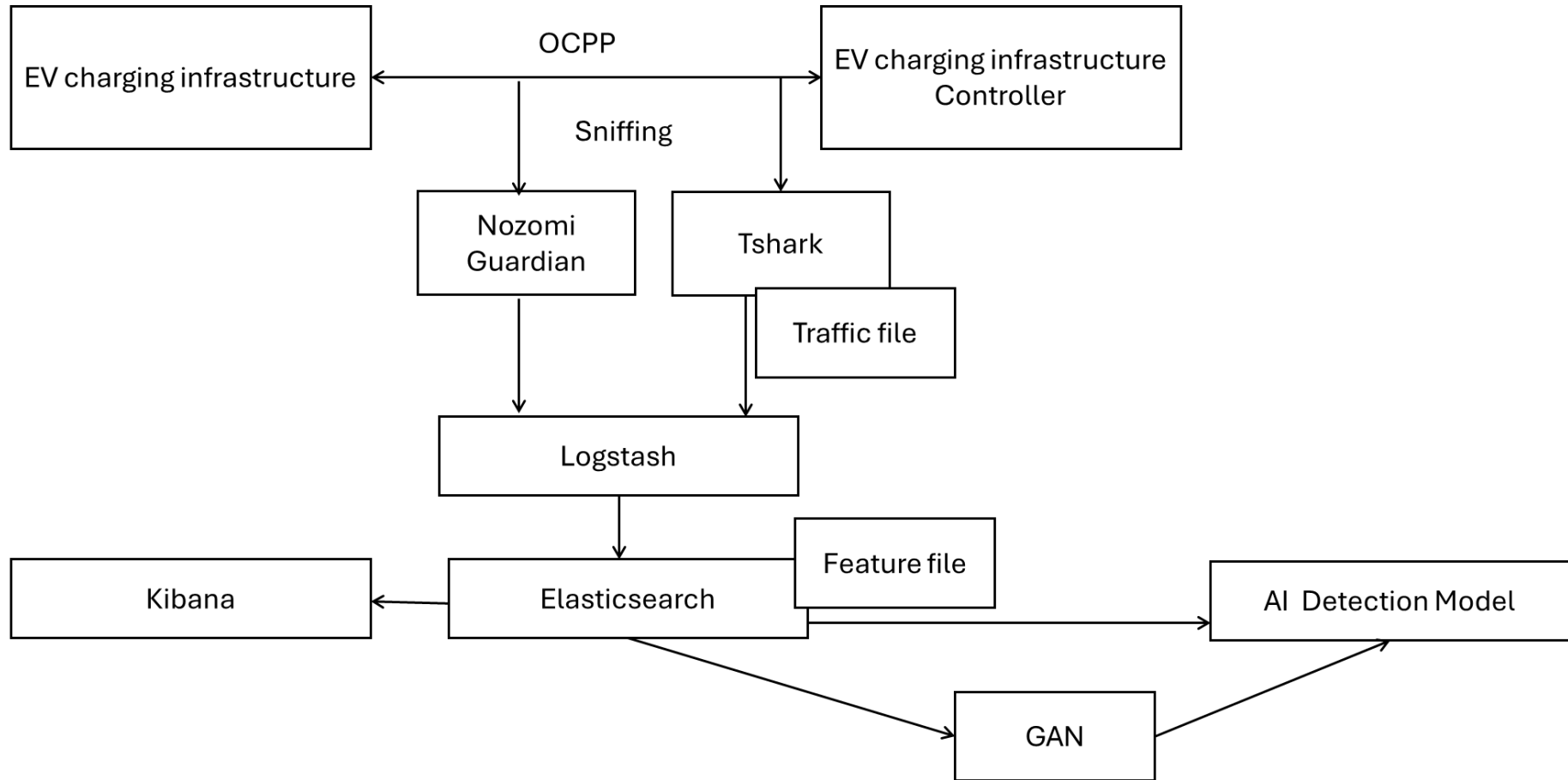
Visualization through graphical interfaces

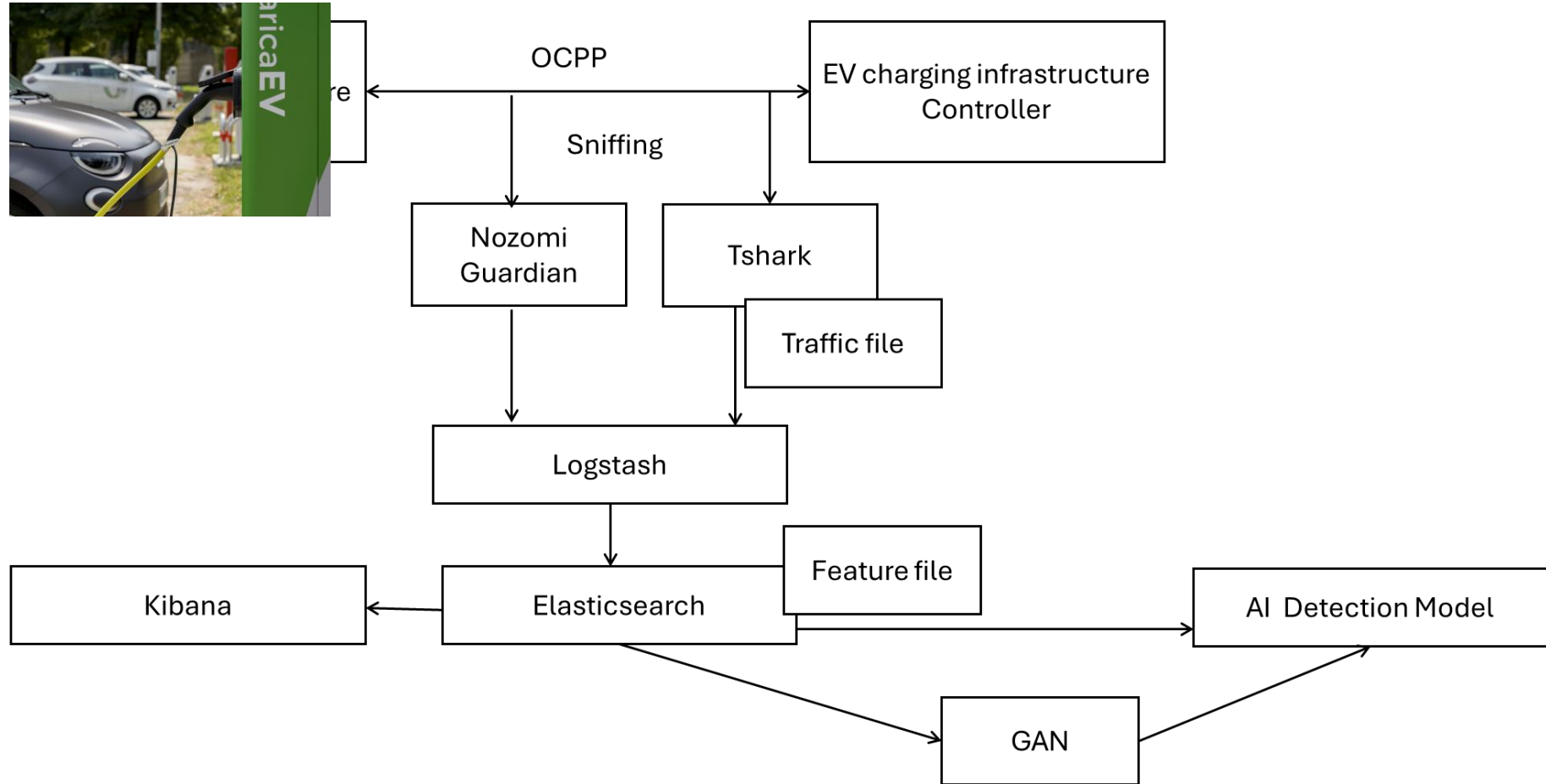
Transmission of information to analysis modules

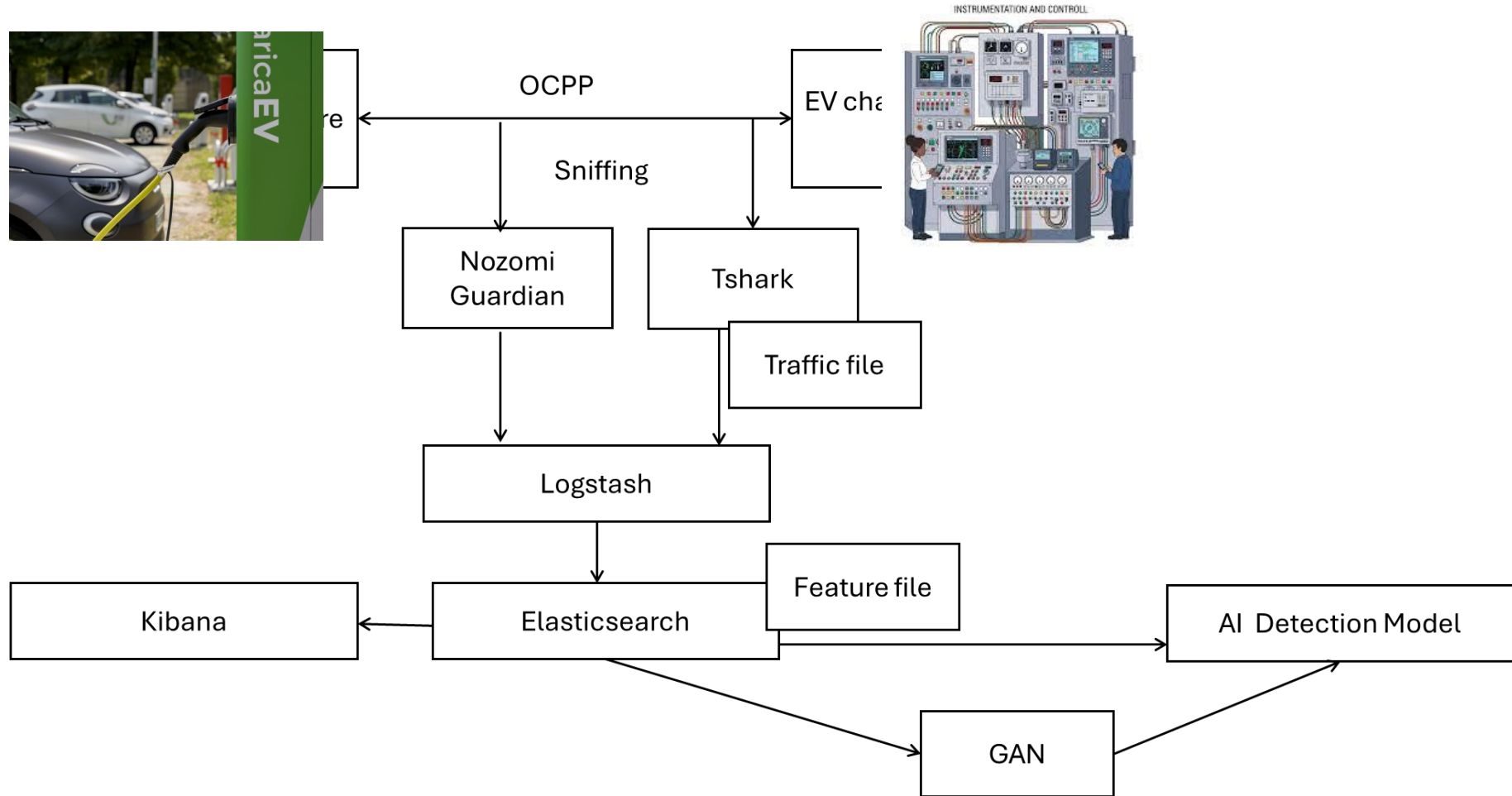
Analysis using AI-based tools

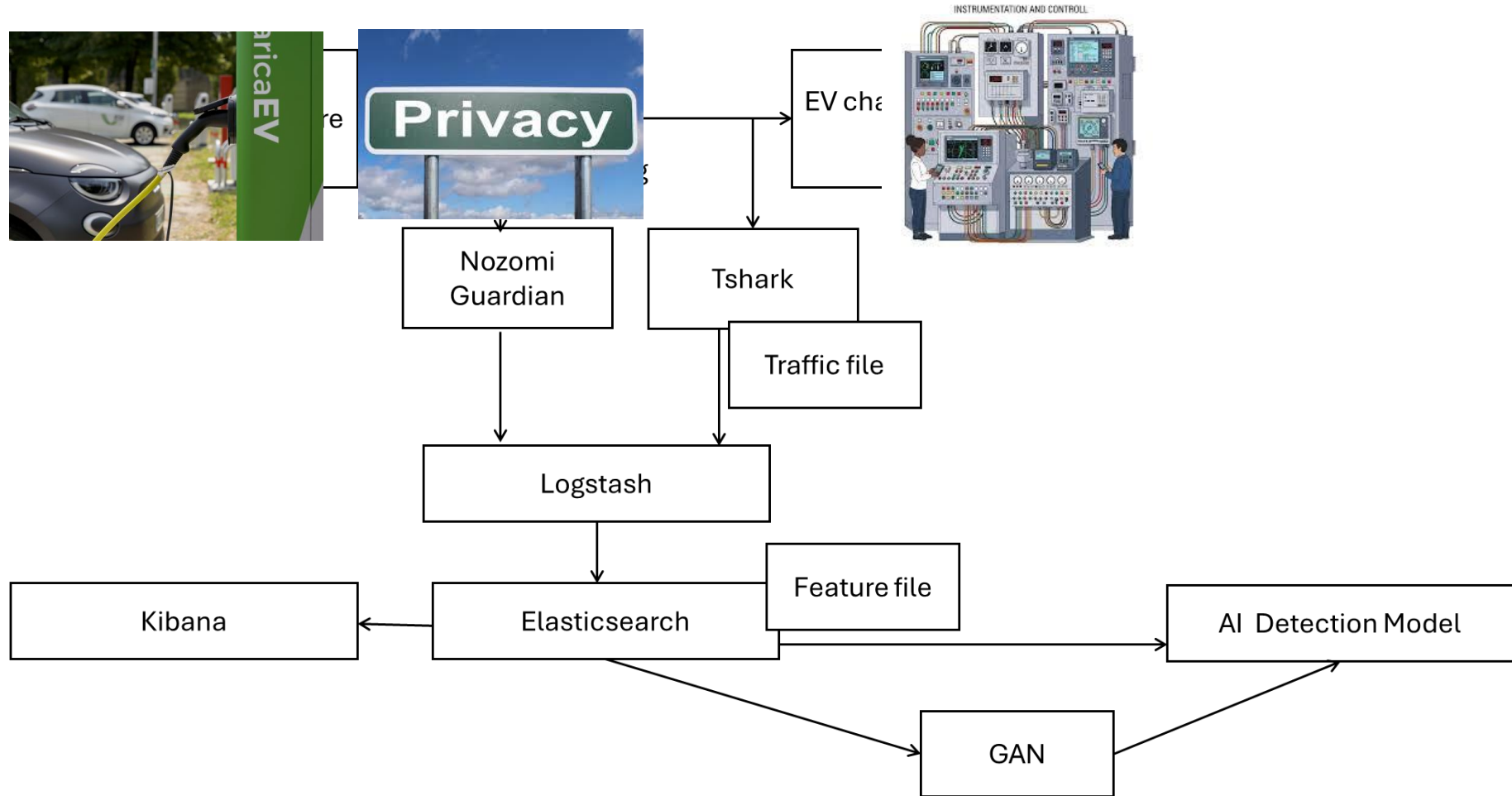
Reporting of any detected malicious actions

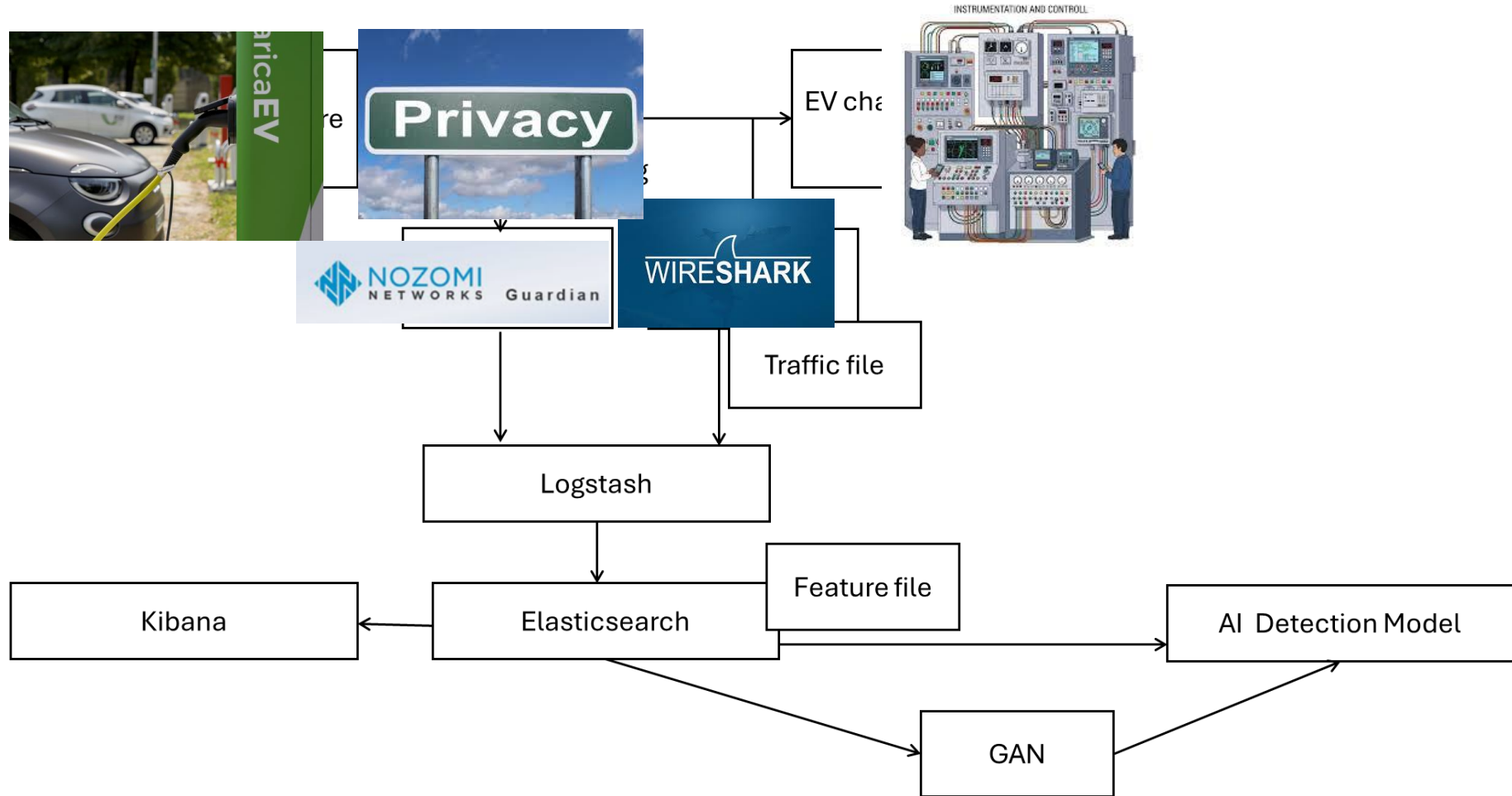


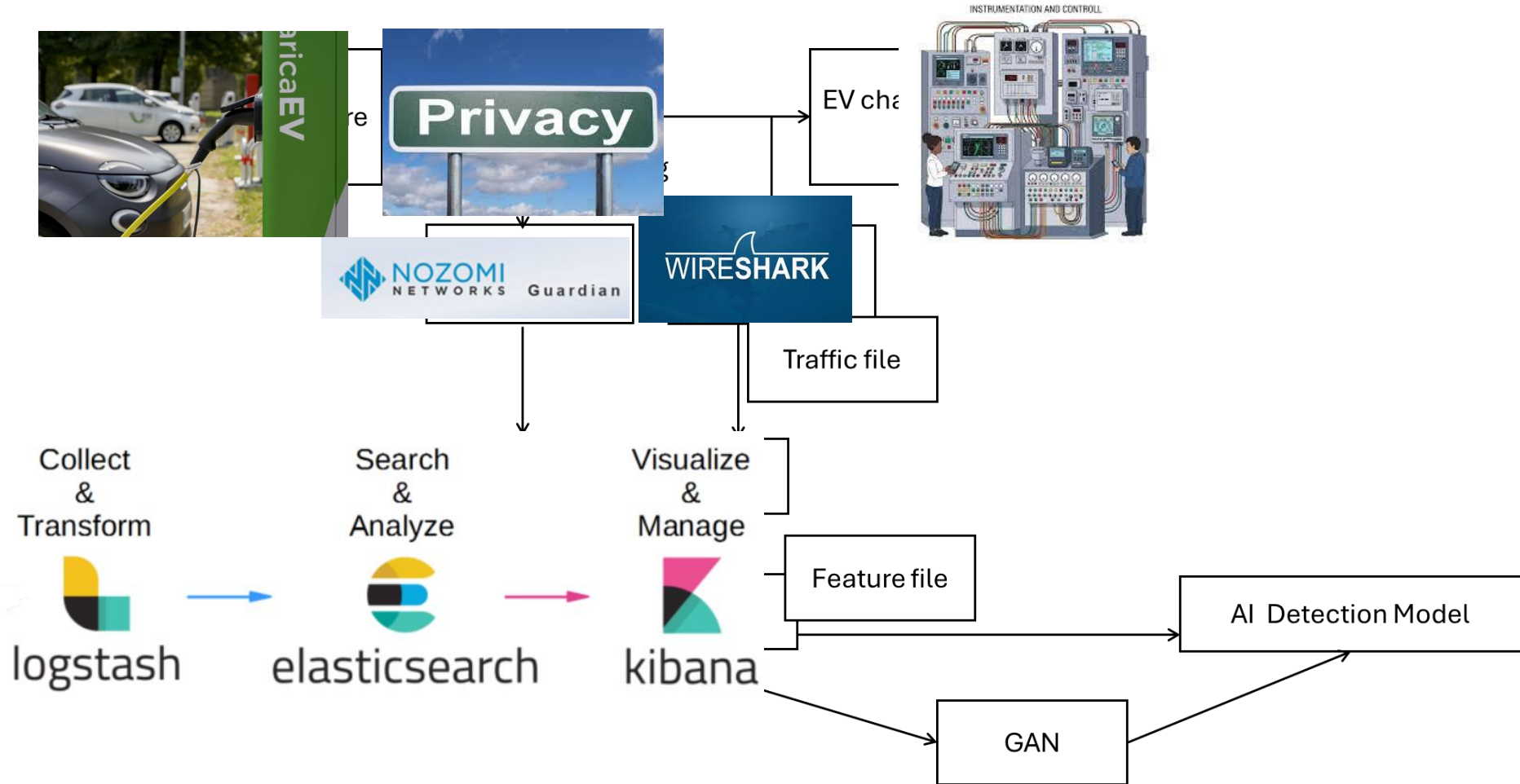


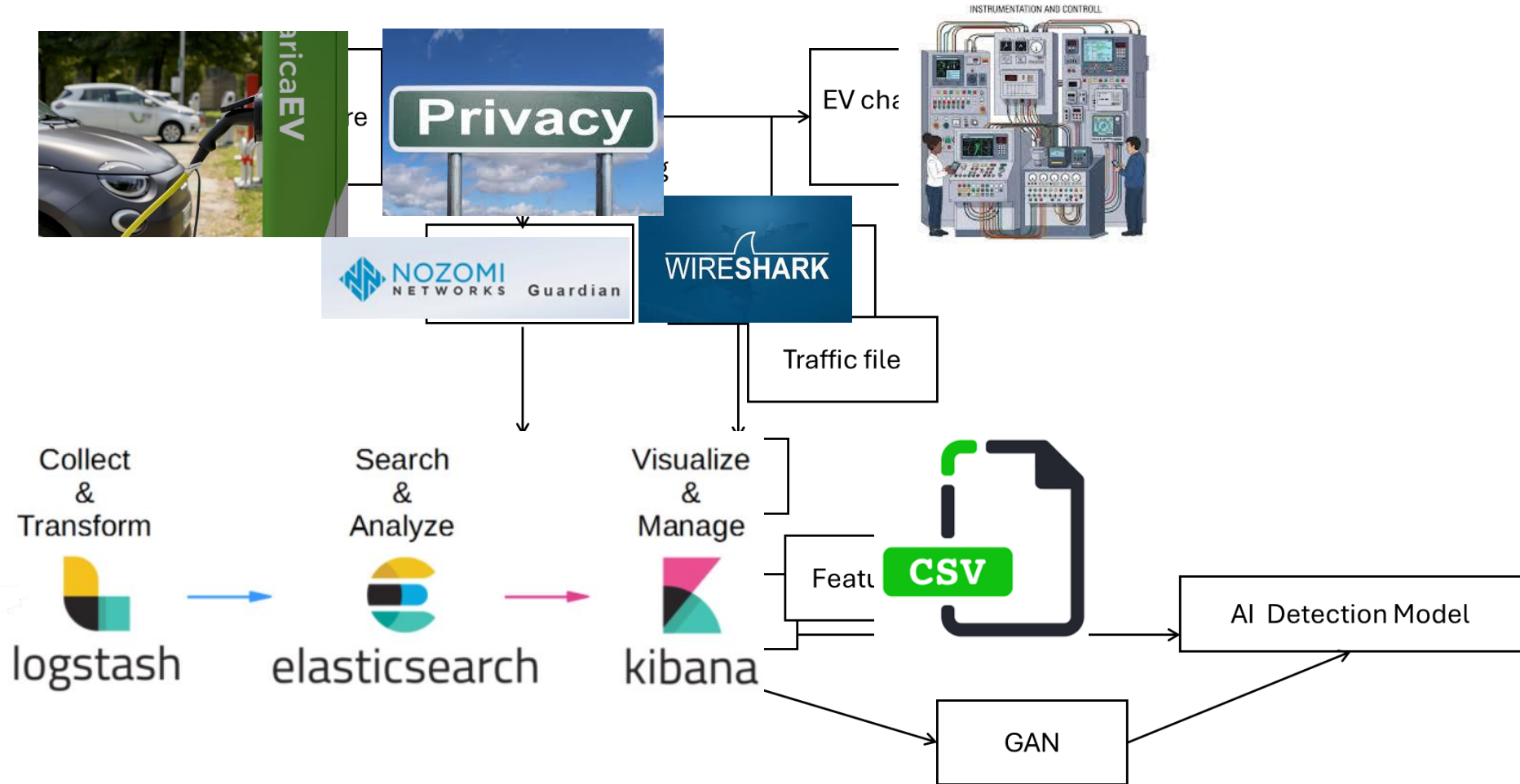


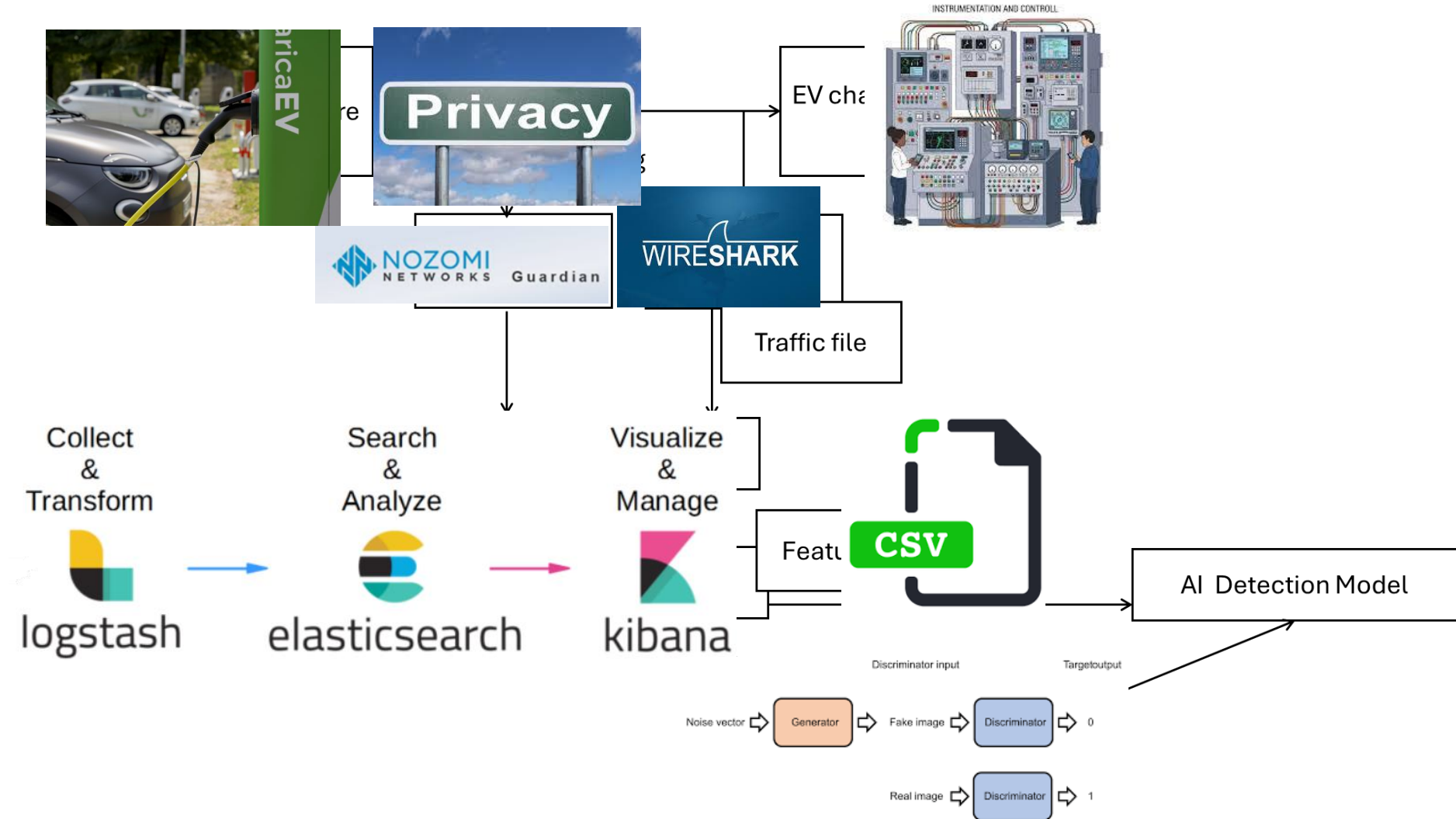


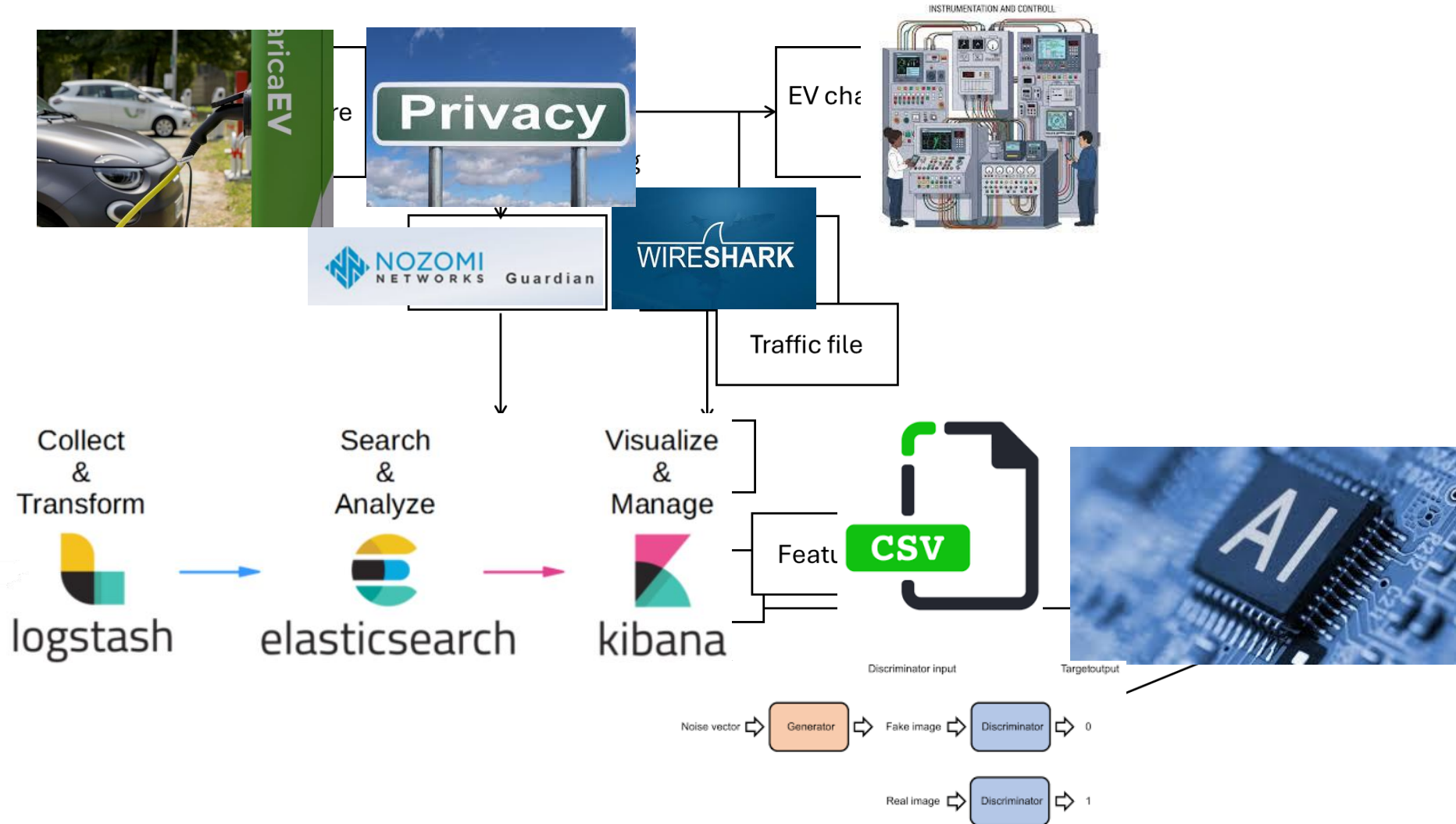


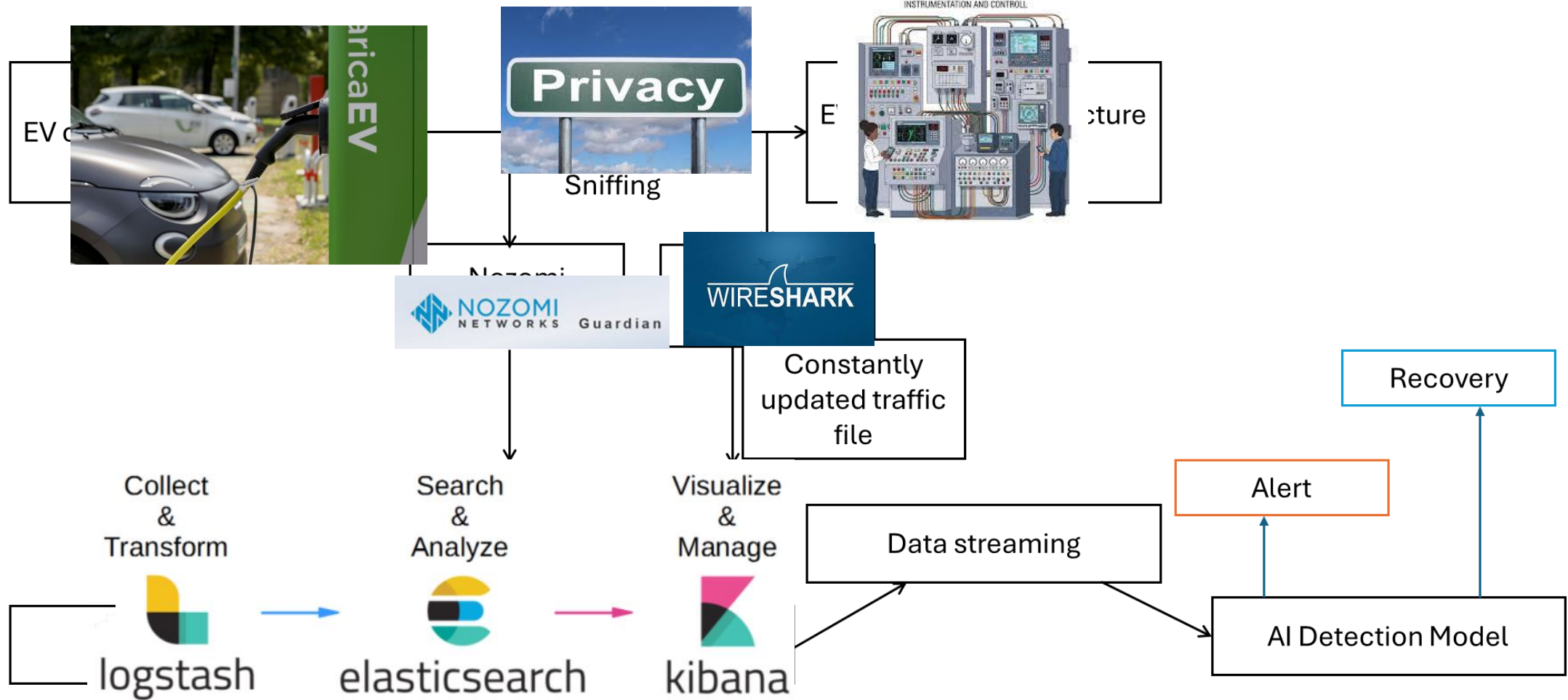


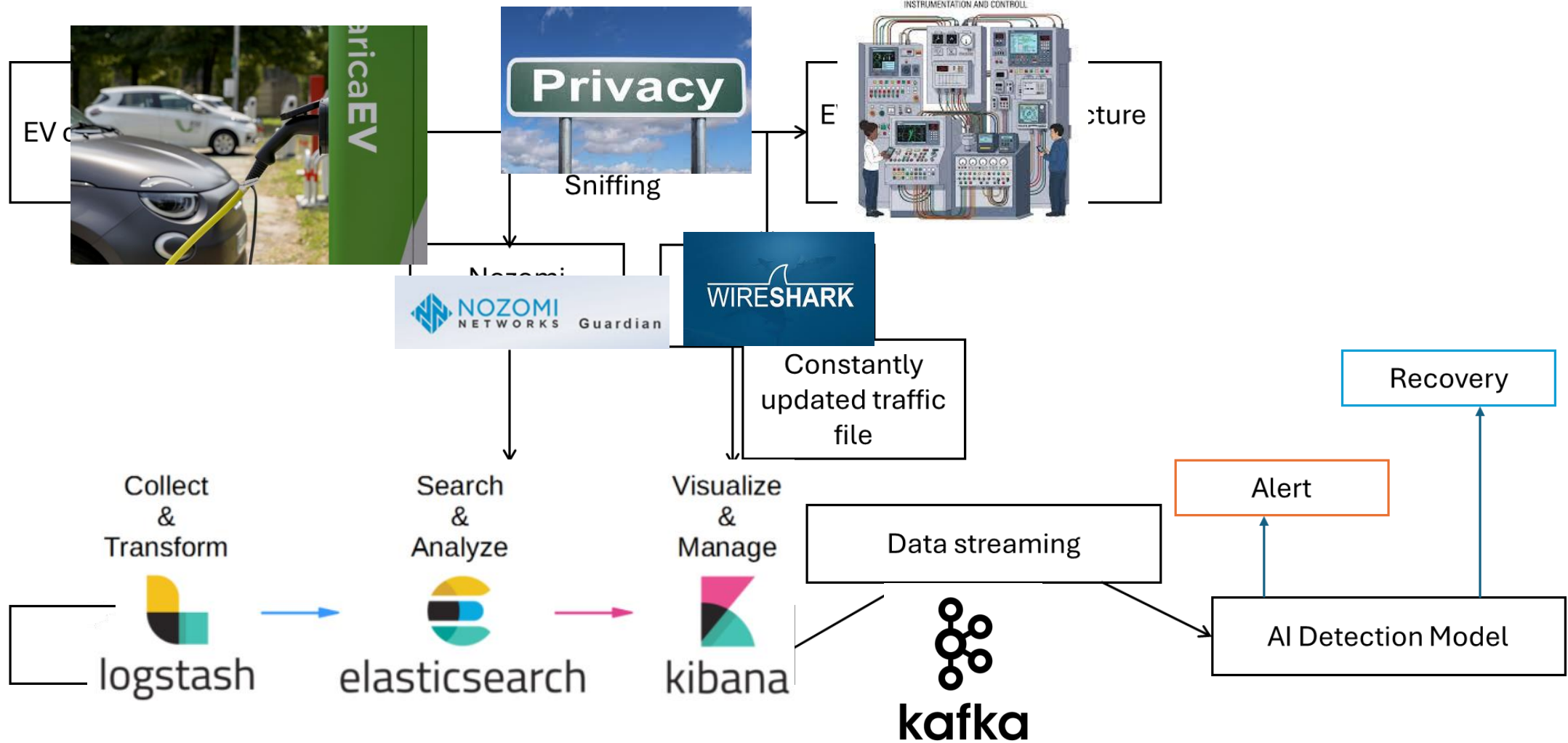


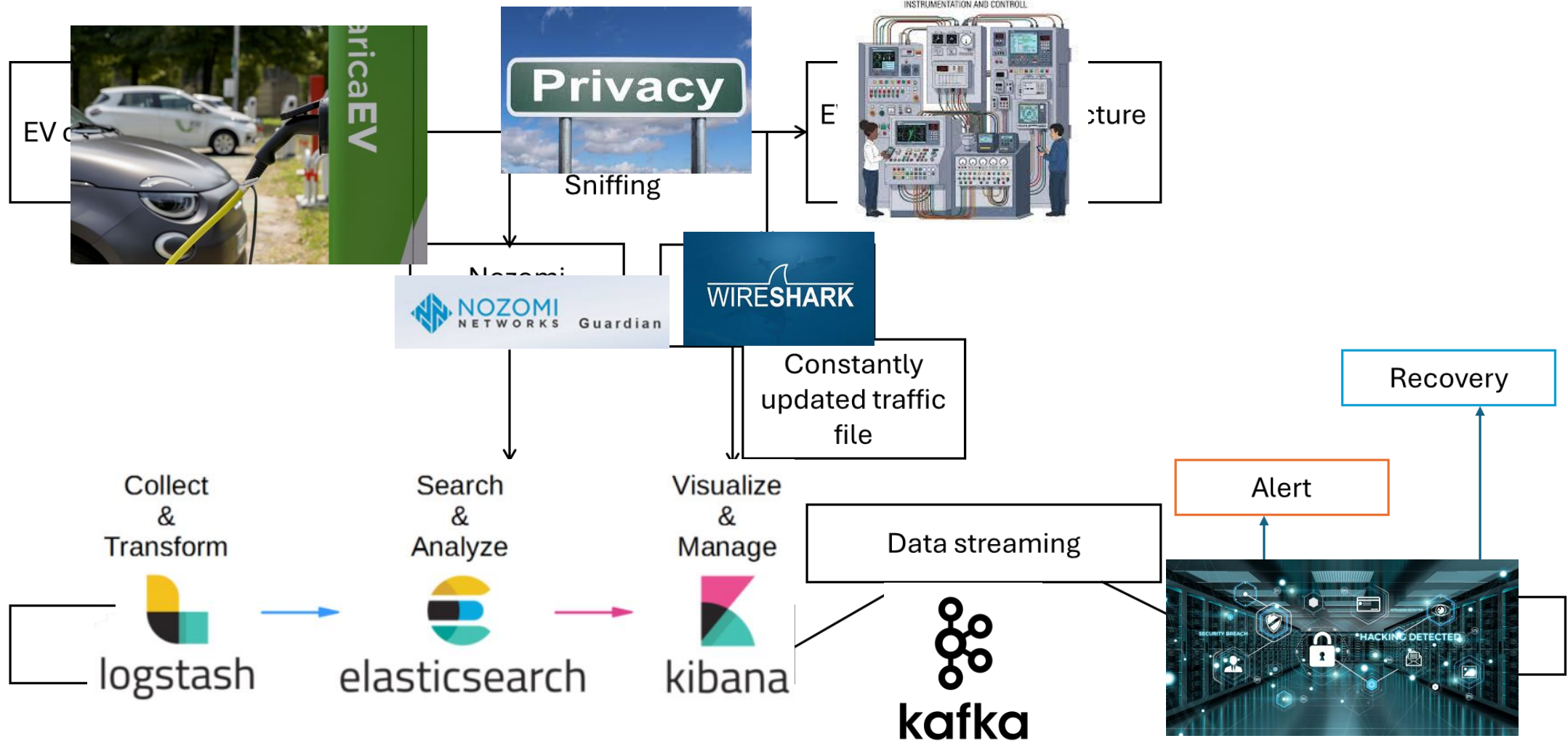


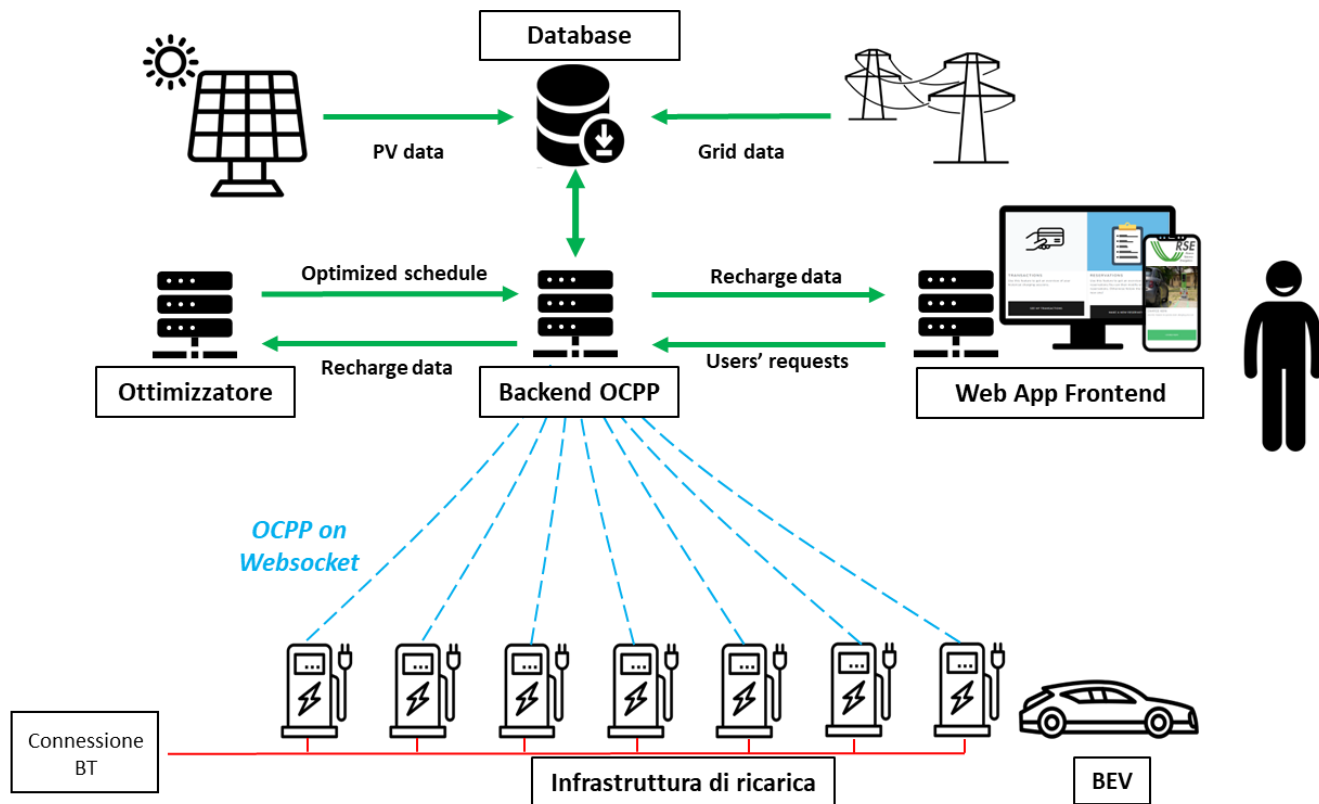








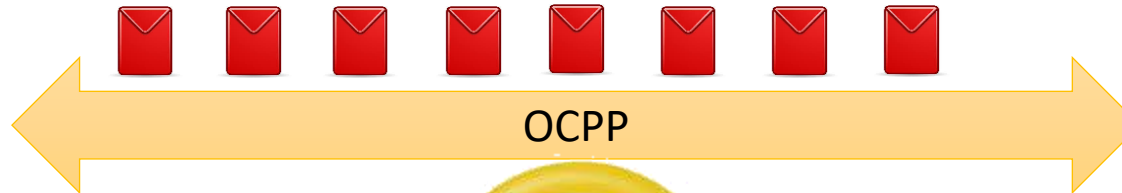




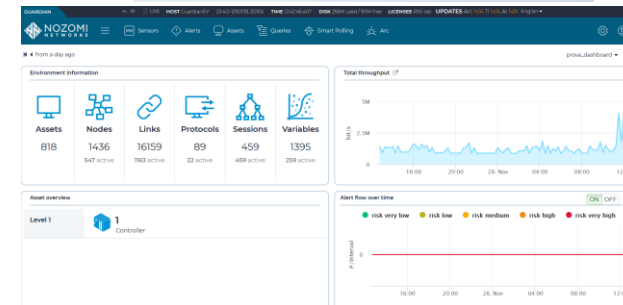
- Charging Point – Controller Communications
- OCPP Protocol (Open Charge Point Protocol)
- TCP/Websocket
- 1.6j version -> no cybersec ☹️
- JSON

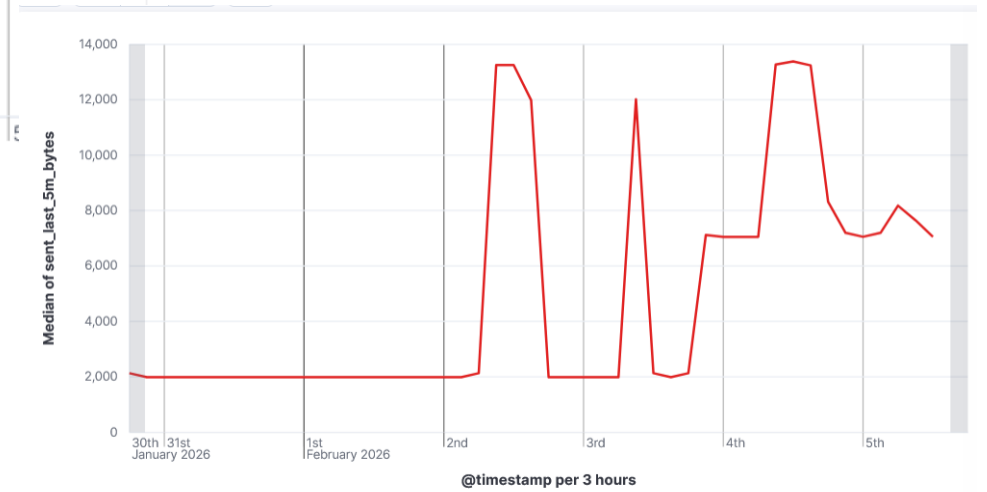
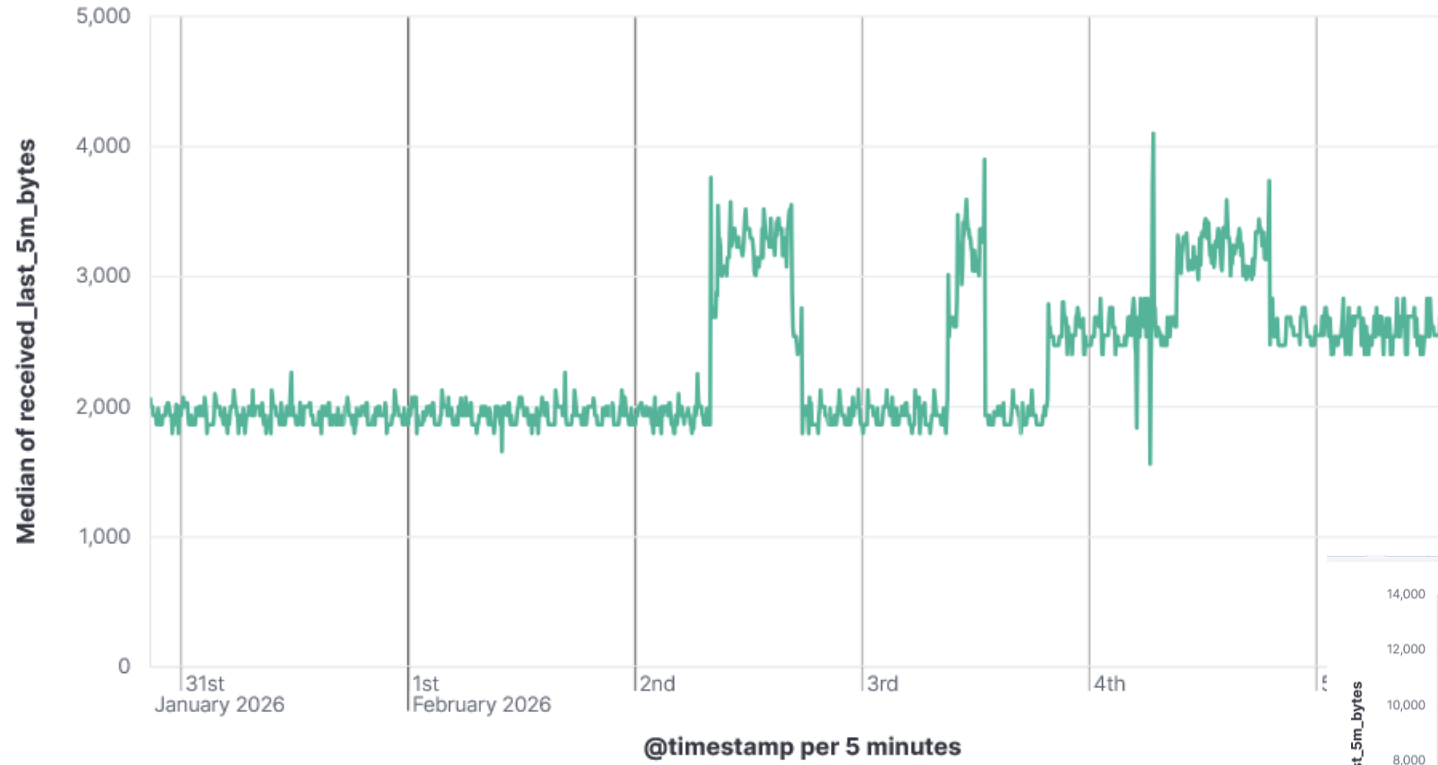


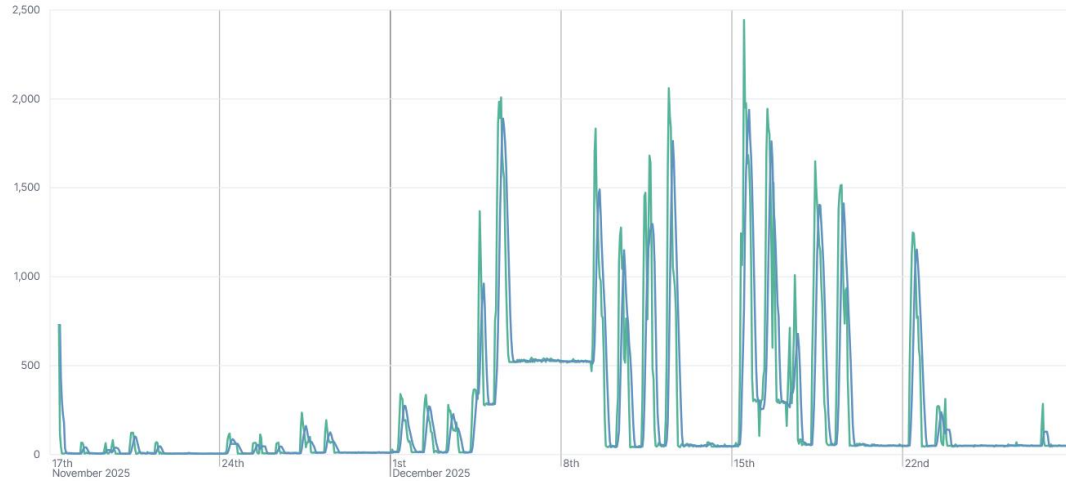
1781	2026-01-29	15:54:27,241209	172.25.98...	172.25.102...	OCPP	273	WebSocket	Text	[FIN]	[MASKED]
1783	2026-01-29	15:54:27,249657	172.25.10...	172.25.98...	OCPP	190	WebSocket	Text	[FIN]	
1881	2026-01-29	15:54:35,680583	172.25.98...	172.25.102...	OCPP	341	WebSocket	Text	[FIN]	[MASKED]
1897	2026-01-29	15:54:35,759078	172.25.10...	172.25.98...	OCPP	178	WebSocket	Text	[FIN]	
1901	2026-01-29	15:54:35,788564	172.25.98...	172.25.102...	OCPP	341	WebSocket	Text	[FIN]	[MASKED]
1907	2026-01-29	15:54:35,794670	172.25.10...	172.25.98...	OCPP	178	WebSocket	Text	[FIN]	
1917	2026-01-29	15:54:35,908690	172.25.98...	172.25.102...	OCPP	341	WebSocket	Text	[FIN]	[MASKED]
1921	2026-01-29	15:54:35,915455	172.25.10...	172.25.98...	OCPP	178	WebSocket	Text	[FIN]	
1929	2026-01-29	15:54:35,980670	172.25.98...	172.25.102...	OCPP	341	WebSocket	Text	[FIN]	[MASKED]
1935	2026-01-29	15:54:35,991295	172.25.10...	172.25.98...	OCPP	178	WebSocket	Text	[FIN]	
1939	2026-01-29	15:54:36,020654	172.25.98...	172.25.102...	OCPP	341	WebSocket	Text	[FIN]	[MASKED]
1943	2026-01-29	15:54:36,035573	172.25.10...	172.25.98...	OCPP	178	WebSocket	Text	[FIN]	
1953	2026-01-29	15:54:36,160629	172.25.98...	172.25.102...	OCPP	341	WebSocket	Text	[FIN]	[MASKED]



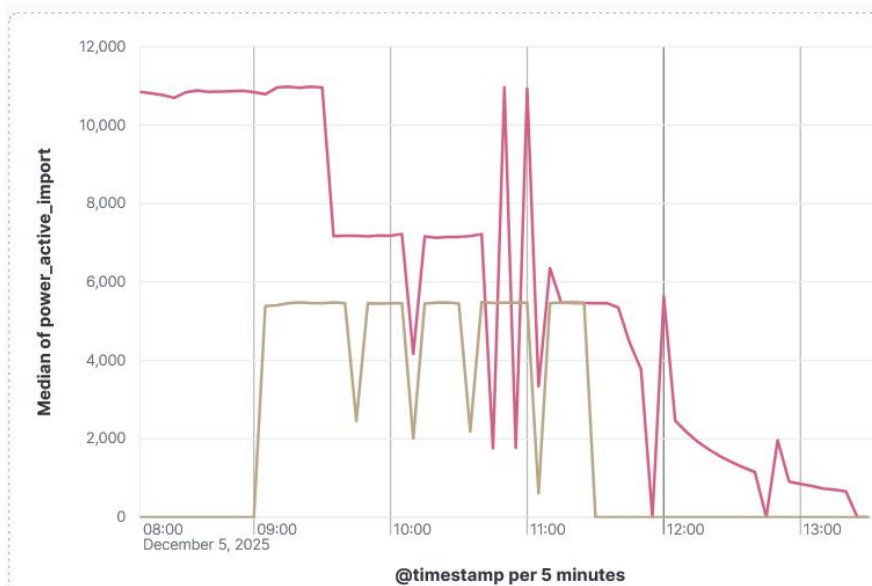
```
> WebSocket
  > OCPP Protocol Payload
    Message Type: 2 (2=Request, 3=Response, 4=Error)
    Message ID: 67eee430-fd22-11f0-99f1-09f302e77d67
    Message Name: BootNotification
  > Payload (JSON): Payload
```





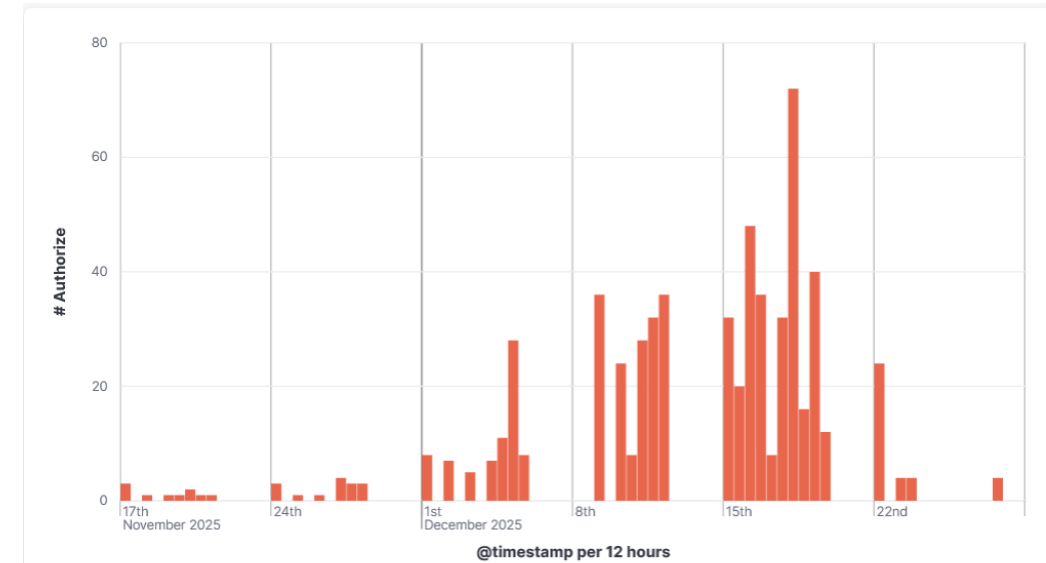


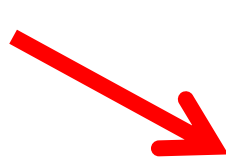
OCPP Commands



Active power import

OCPP «Auth» Command





Collect
&
Transform



logstash



Search
&
Analyze



elasticsearch



Visualize
&
Manage

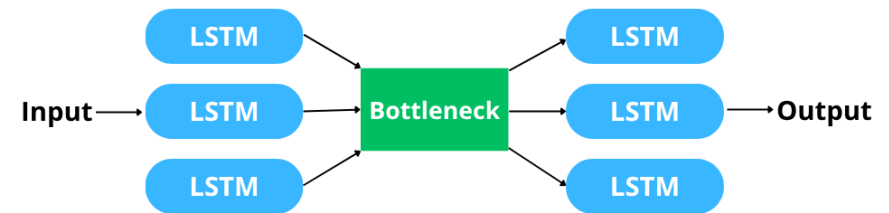


kibana

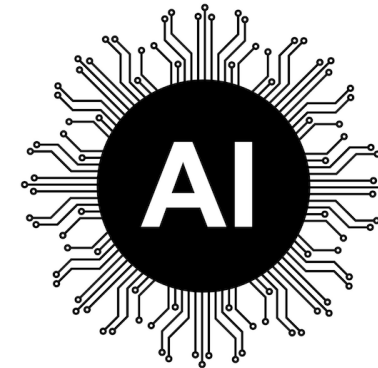


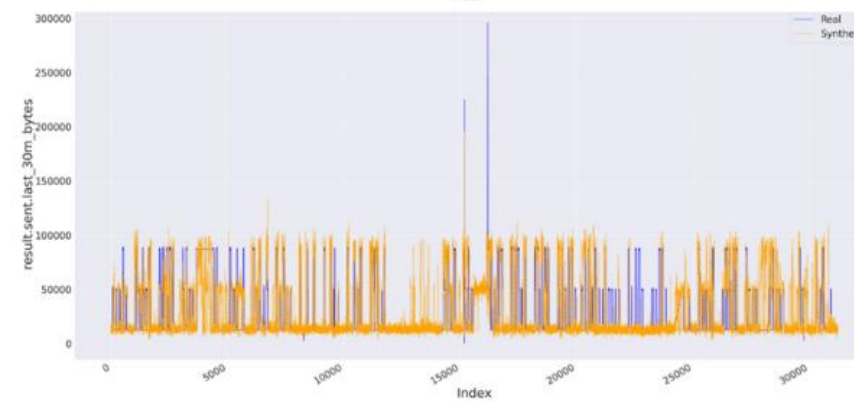
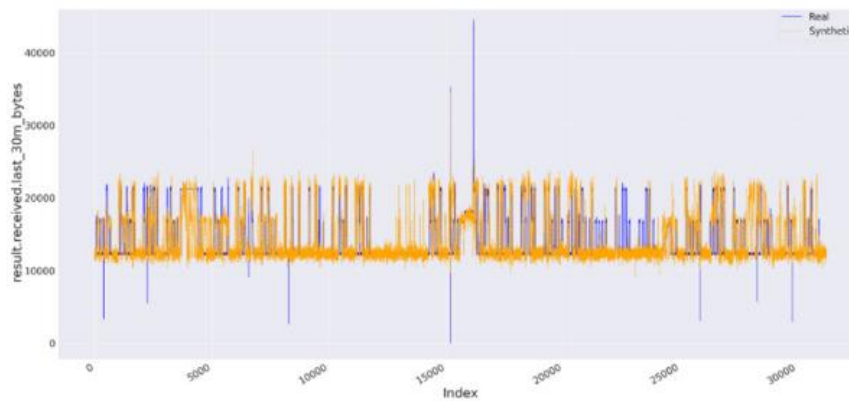
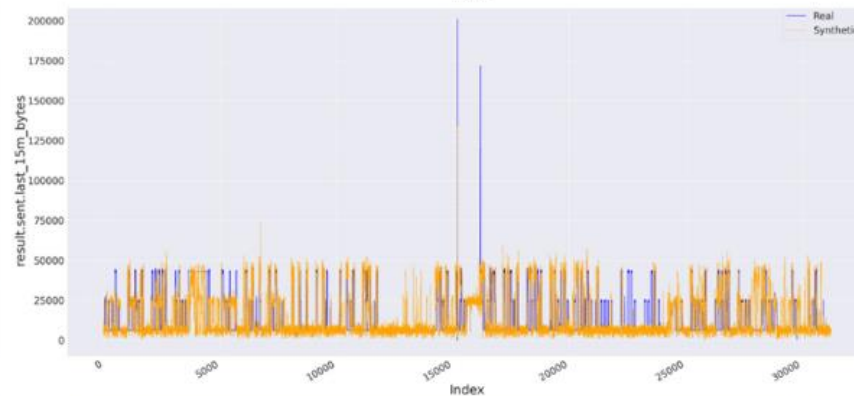
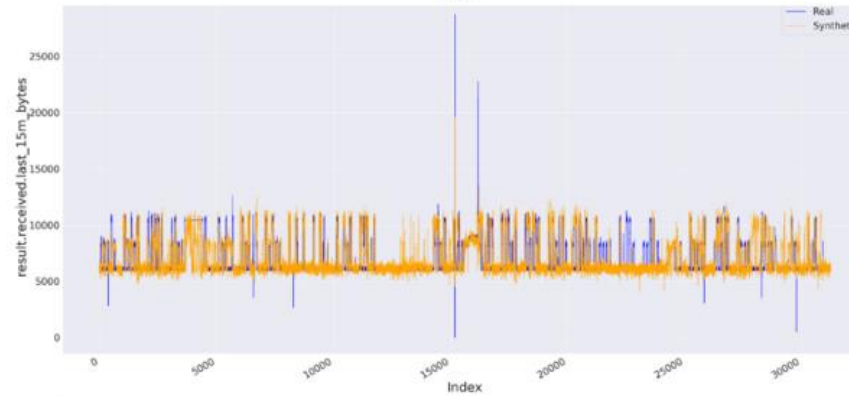
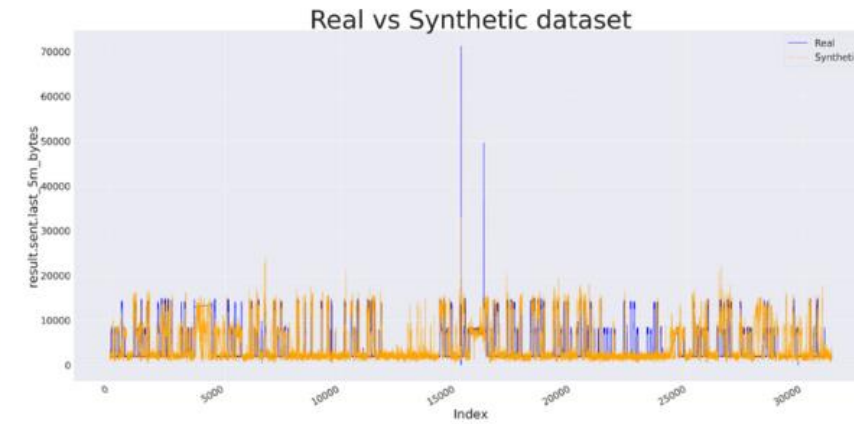
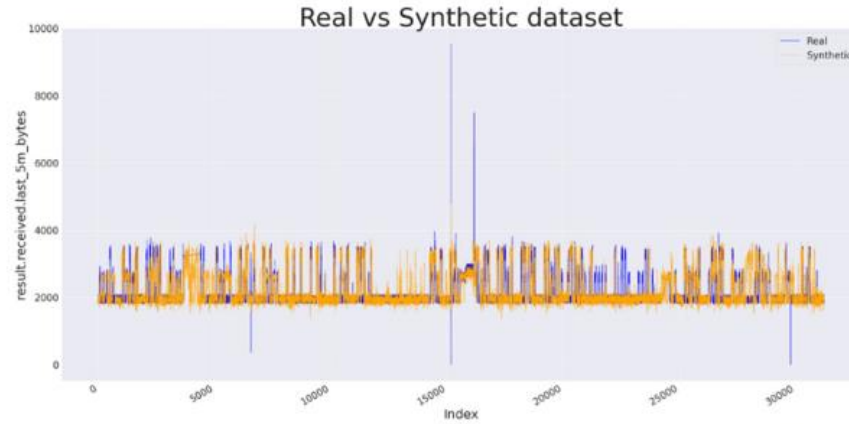
kafka

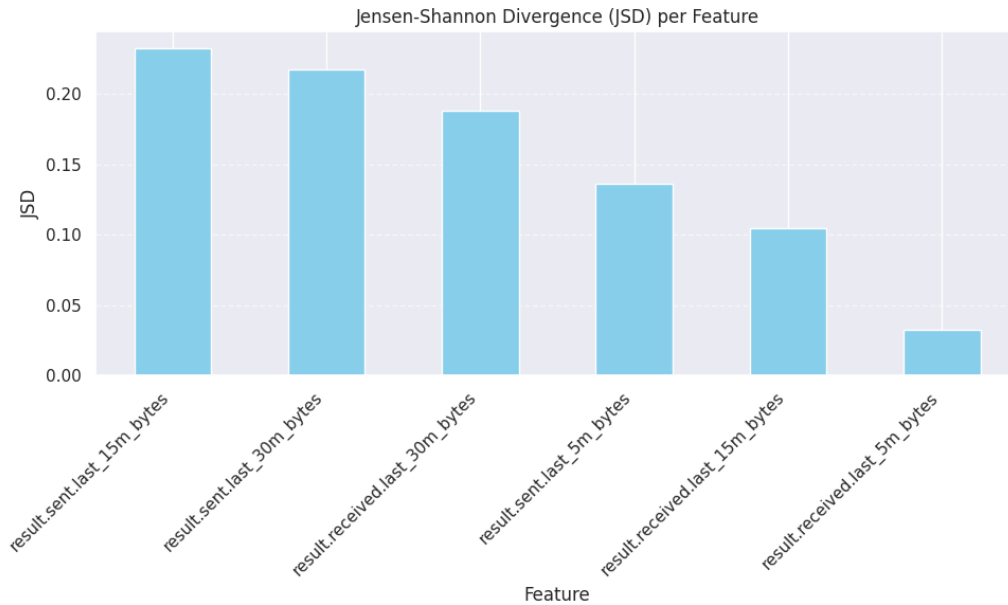
LSTM Autoencoder



- *Generative Adversarial Networks (GAN)*
- *Wasserstein GAN (W-GAN)*
- *Structure:*
 - *Generator: generates realistic sequences starting from random noise.*
 - *Discriminator: attempts to distinguish between real sequences and synthetic ones generated by the generator.*
- *Data augmentation*

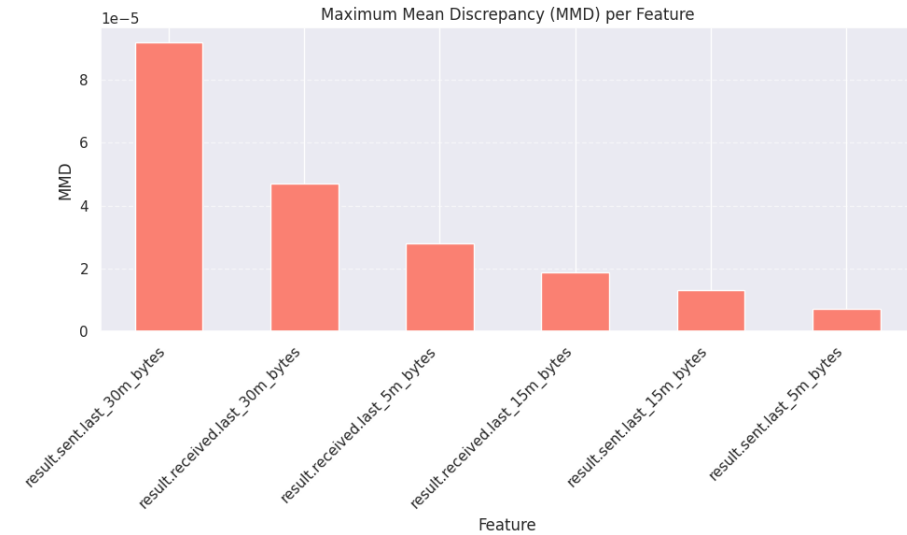






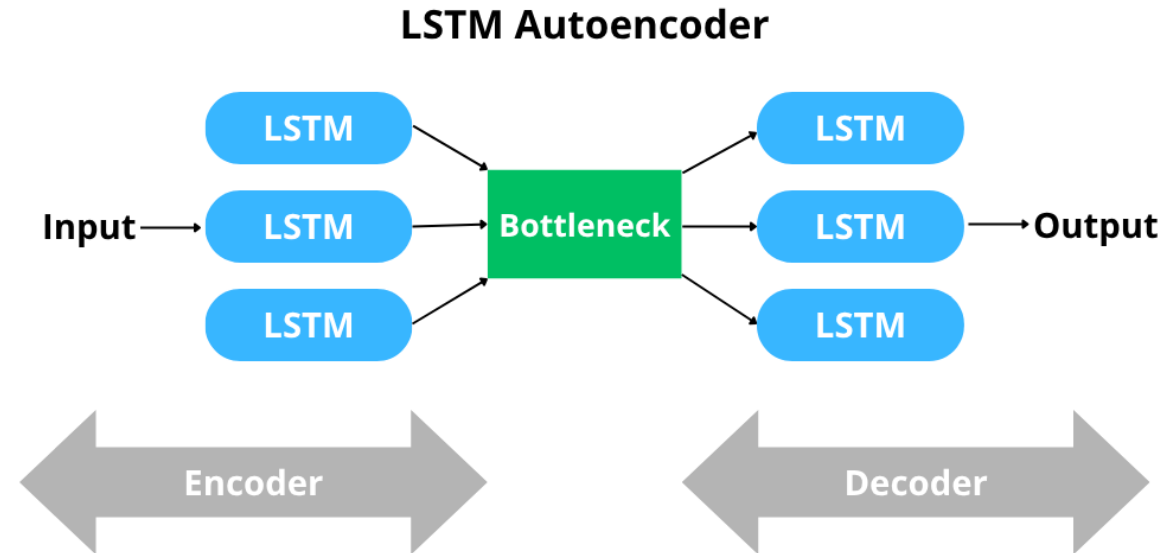
Jensen-Shannon Divergence (JSD)

- Measures divergence between real and synthetic data distributions
 - Lower values indicate higher similarity

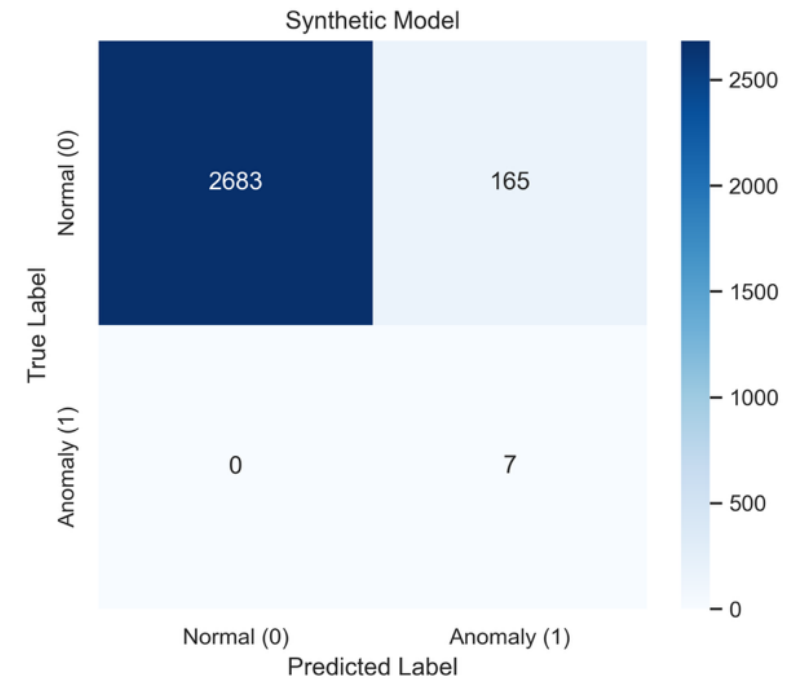
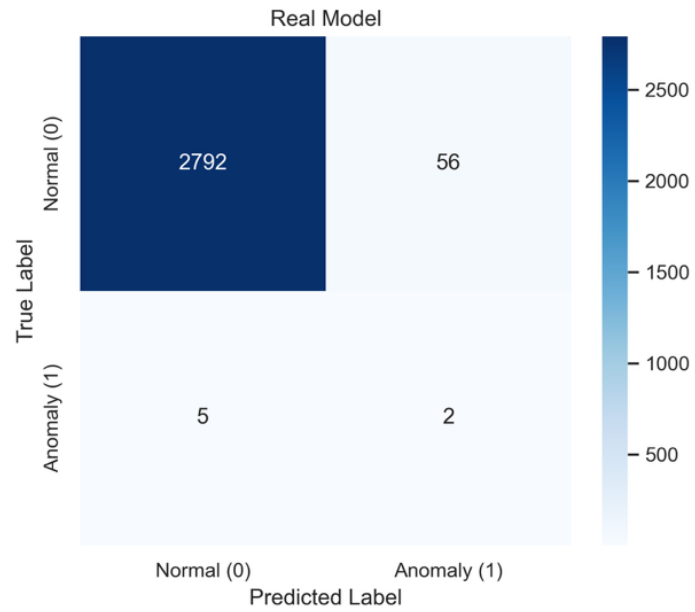


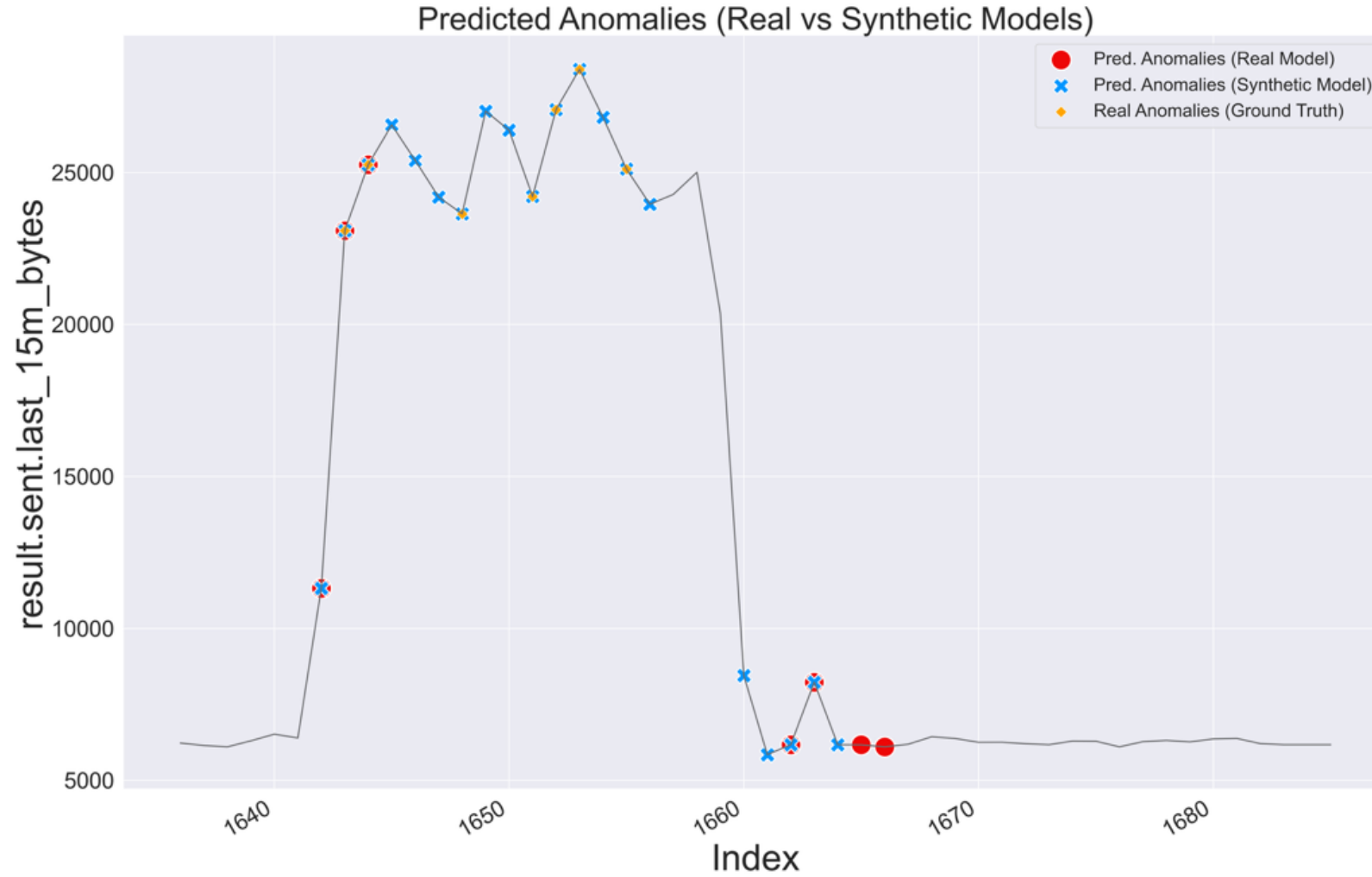
Maximum Mean Discrepancy (MMD)

- Non-parametric distance between sampled distributions
 - Lower values indicate higher similarity



- Real vs Synthetic Dataset
- Loss Function -> Mean Squared Error (MSE)
- Difference between the input and reconstructed sequences.
- By minimizing this loss, the autoencoder learns the normal data patterns





- **AI-based approaches** represent a **strategic solution** to **enhance** the **cybersecurity** of energy infrastructures, particularly EV charging systems
- A **modular anomaly detection platform**, combined with **realistic attack scenarios** and **synthetic data generation** (W-GAN), effectively addresses key challenges such as dataset scarcity and threat complexity
- **Benefits** for operators and society include:
 - Increased infrastructure **resilience**
 - Faster **incident response**
 - Improved **decision support** through advanced analytics
- Future directions
 - **Consolidation of results** through Proof of Concept validation and experimental datasets
 - Systematic analysis of **vulnerability combinations** and **attack chains**
 - Simulation of **composite attacks** using automated, containerized environments
 - Generation of **hybrid datasets** (legitimate + malicious traffic) with contextual labels
 - **Advanced feature engineering** across network and application layers (e.g., XMPP, OCPP, MMS)
 - Definition of a rigorous **experimental pipeline** to ensure robustness, generalization, and reduced false positives



Overall, these activities pave the way for more **reliable AI/ML detection models**, deeper understanding of attacker behavior, and more **effective countermeasures**, ultimately strengthening the **resilience of critical energy infrastructures**.

Thank you for the attention

Roberta Terruggia, Alberto Maldarella
roberta.terruggia@rse-web.it

