CISUC

Centre for Informatics and Systems
of the University of Coimbra

The ATENA
Intrusion and Anomaly Detection System

POSEIDON Workshop on Privacy, Data Protection and Digital Identity
Department of Informatics Engineering of the University of Coimbra
July 11, 2019

Tiago Cruz - tjcruz@dei.uc.pt

ATENA

CISUC

Centre for Informatics and Systems
of the University of Coimbra

Presentation outline

- Introduction: the sad state of IACS security
- ATENA challenges and goals
- Cyber Analysis and Detection in ATENA
- Security probes and detection techniques
- Leveraging SDN/NFV in the IADS
- Forensics and compliance auditing capabilities
- The (big) problem nobody thought about
  (aka *Privacy and data security: the next frontier*)
- Conclusions

CISUC

Centre for Informatics and Systems
of the University of Coimbra

Our problem

- Our modern living standards would be impossible to achieve without automation technologies.
- **Industrial Automation and Control Systems** (IACS) (and particularly SCADA systems) are often in charge of managing and controlling the delivery of several **Essential Services**.
- Naturally, they constitute a desirable target for Advanced Persistent Threats and any other individual/organization committed to disrupt our daily lives.

We went from this…

Nuclear Plant Overview

njection Tank

Motor Clutch

PowerFlex

OFFLINE

Turbine

Generator

BWR Reactor

Cooling Towers

Feedwater Pump

OFFLINE

jection Pump

RUNNING

Condenser

Circulating Water Pump

OFFLINE

Nuclear Plant Over

...to this

Wednesday, May 23, 2012 3:09:29 PM

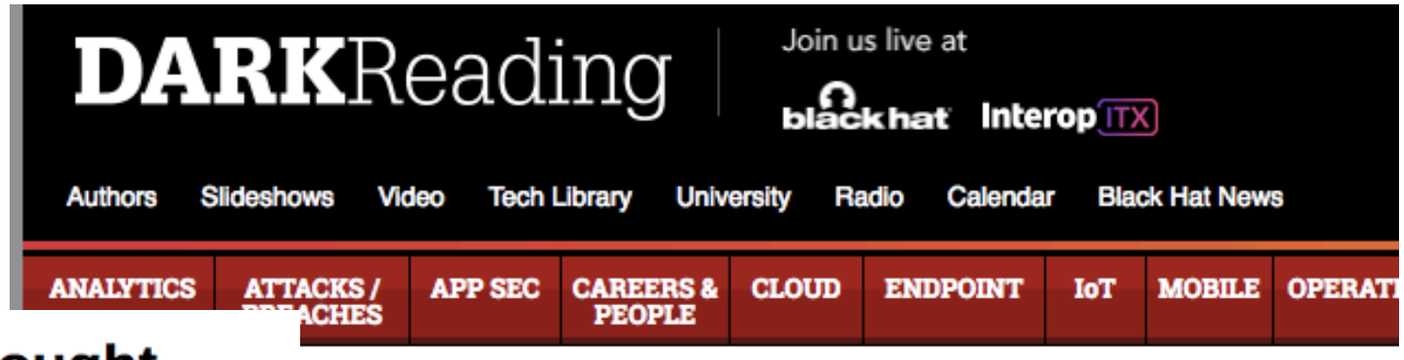
CONTROLS

plete.

downtownTank.PNG ... | Inbox (3) - david.c.th... | Nuclear Plant Cont... | My Drive - Google Dr...

And, yes, it got worse

The unholy marriage between IoT and IACS…



Smart grid security WORSE than we thought

OSGP's DIY MAC is a JOKE

11 May 2015 at 02:03, Richard Chirgwin

Don't try crypto at home, kids: the Open Smart Grid Protocol project rolled its own crypto and ended up with something horribly insecure.

Smart Meter Hack Shuts Off The Lights

European researchers will reveal major security weaknesses in smart meters that could allow an attacker to order a power blackout.

A widely deployed smart meter device can be programmed to cause a power blackout or commit power usage fraud.

Researchers Javier Vazquez Vidal and Alberto Garcia Illera will reveal this month at Black Hat Europe in Amsterdam how they reverse engineered smart meters and found blatant security weaknesses that allowed them to commandeer the devices to shut down power or perform electricity usage fraud over the power line communications network. The researchers aren't disclosing the specific smart meter manufacturer at this time -- they haven't yet disclosed anything to the vendor in question, either. They have hinted heavily that it's a brand installed broadly in Spain.

ATENA

The challenges of protecting a modern IACS

- Modern IACS tend to be dispersed over large geographic areas, with increasingly small areas of coverage as we progress towards its periphery – **capillarity**.
- This **distributed nature** makes it difficult not only to understand the nature of incidents, but also to assess their progression and threat profile.
- Detecting those threats is something that is becoming increasingly difficult
- This requires **orchestrated and collaborative distributed detection** and evaluation capabilities well beyond the reach of a single entity.

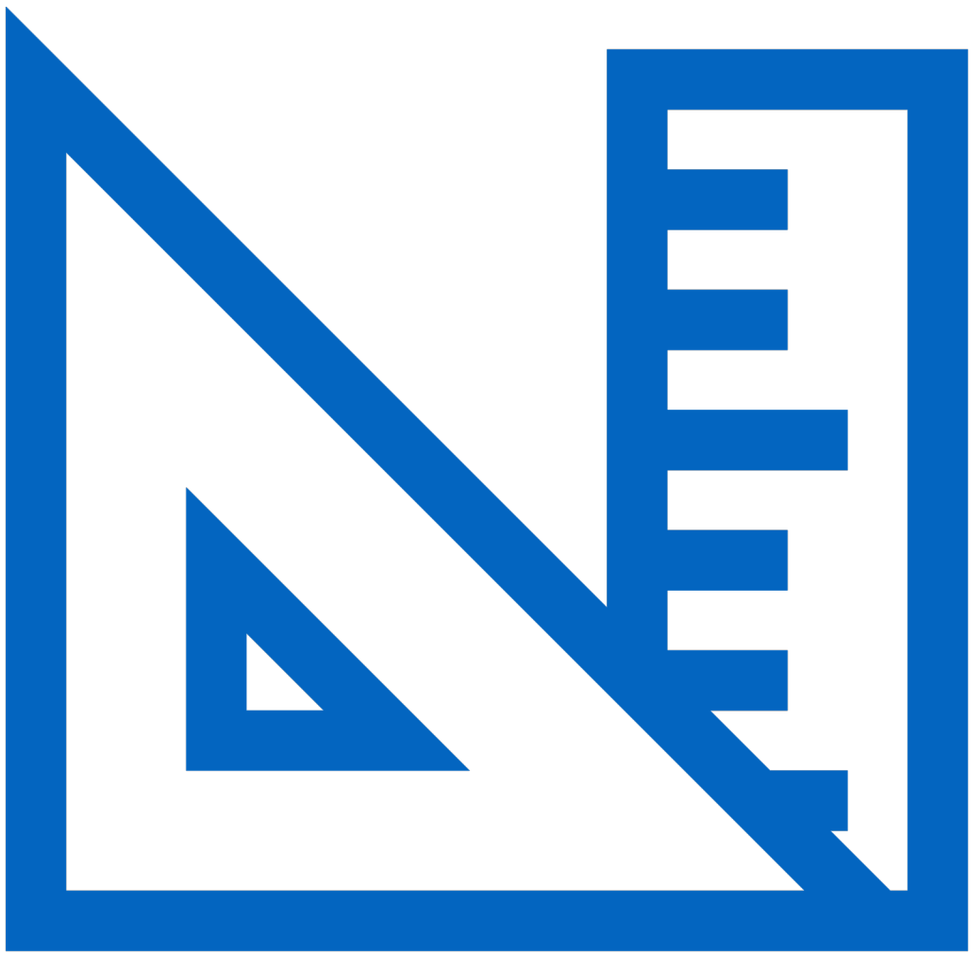
ATENA IADS: challenges and goals

ATENA

Moving beyond conventional approaches – our challenges

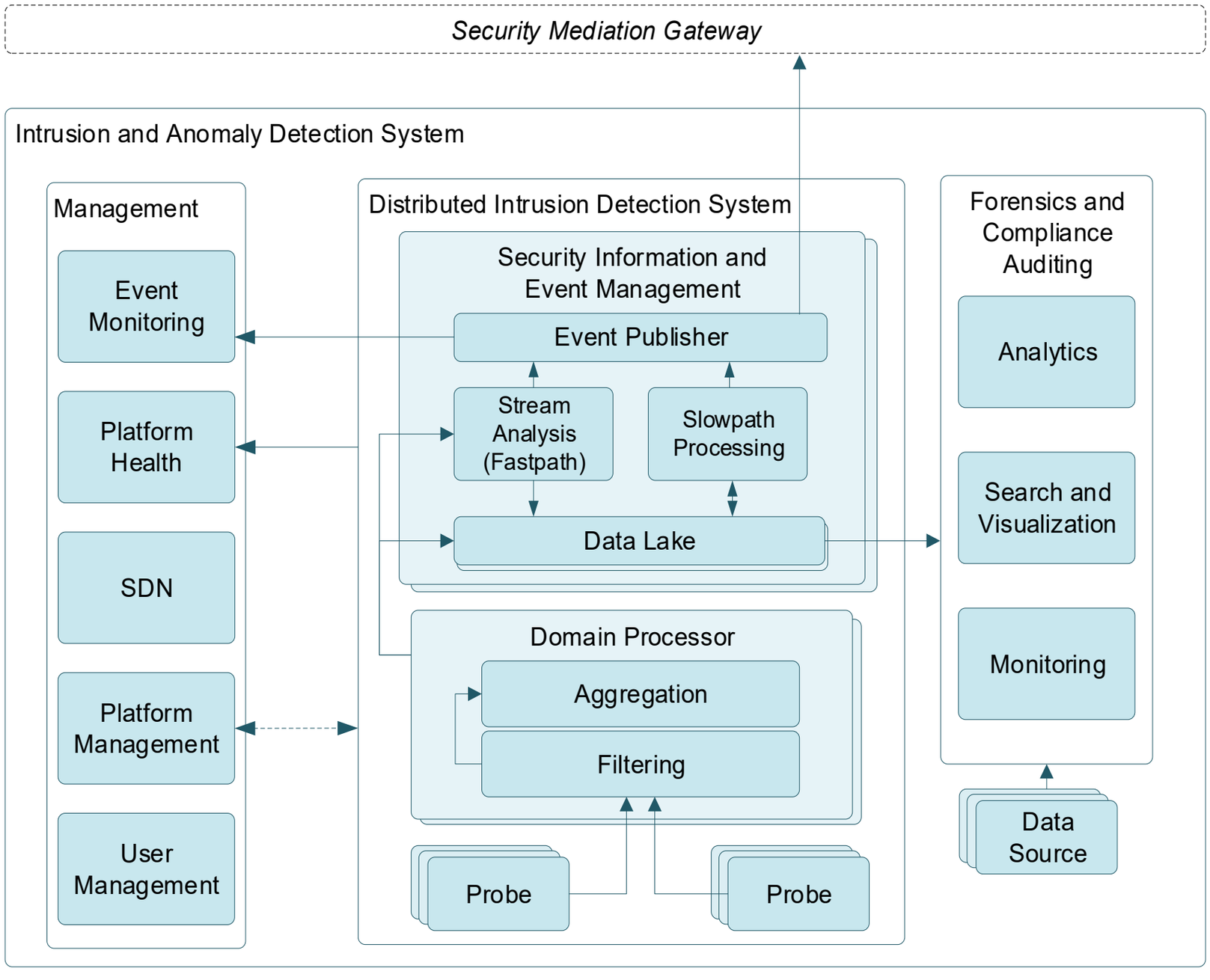
- Evolve the existing Security Information and Event Management (SIEM) systems model
- Big Data Approach for event and alarm handling (Big data SIEM)
- Introduction of Software Defined Networking (SDN)/ Network Function Virtualization (NFV)
- Introduction of forensics and compliance auditing mechanisms
- New probes / attacks
- Event correlation + Anomaly detection locally and globally
- Machine learning at I/O level (Shadow Security Unit)

The ATENA IADS architecture: design and implementation strategy

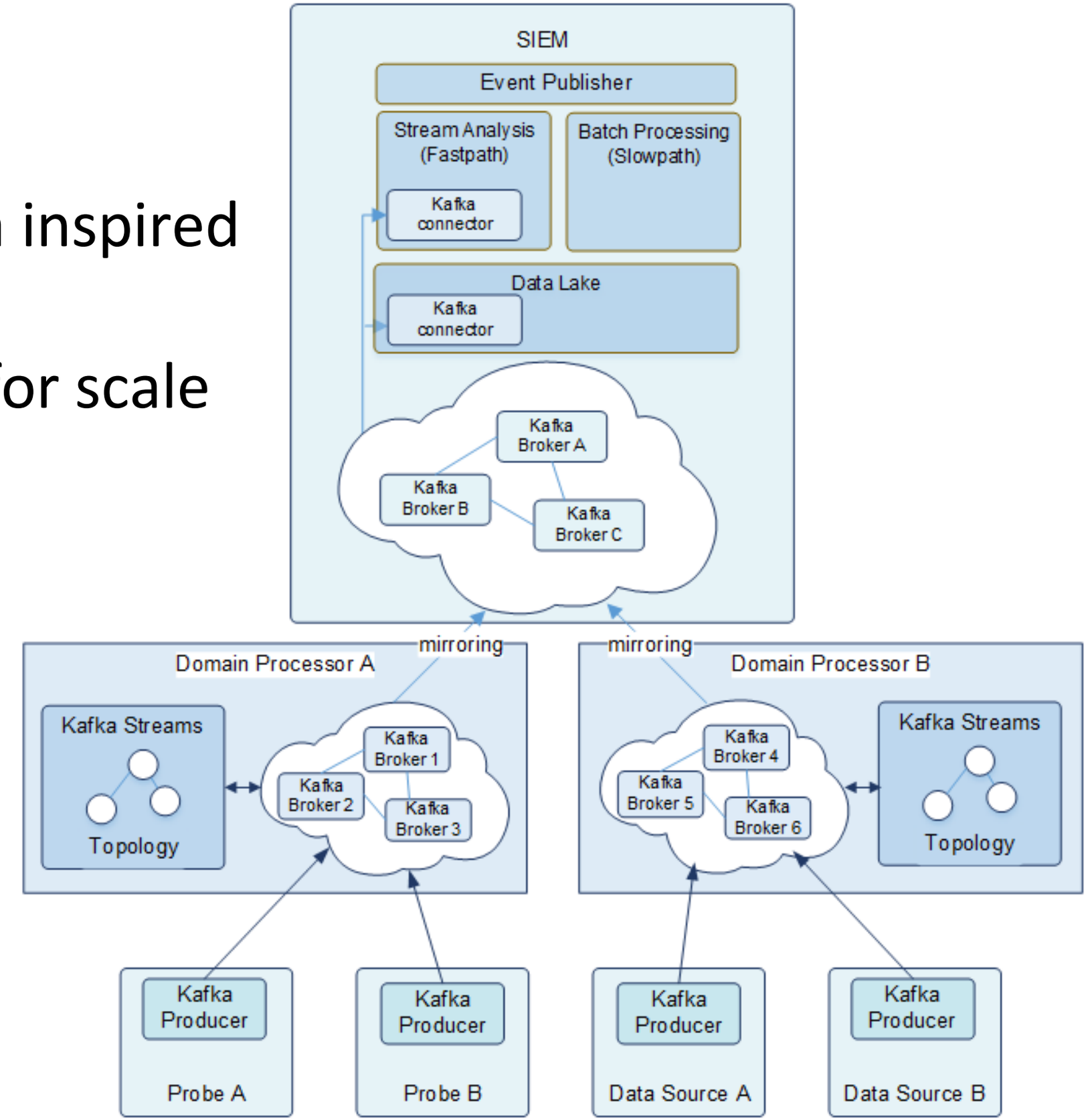


ATENA

ATENA IADS Subsystem Architecture



A Big-Data inspired approach, designed for scale



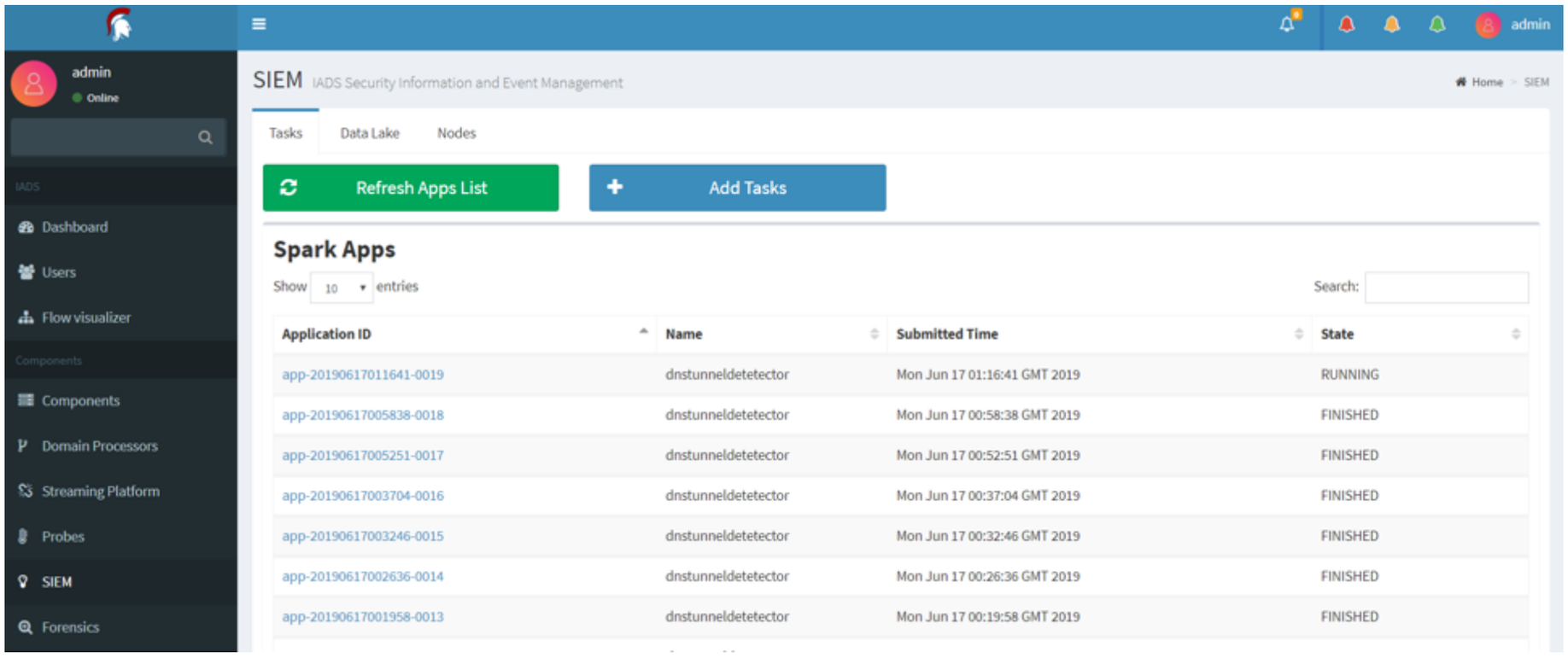
Core computing layer

Edge computing layer

ATENA

The ATENA IADS: born open

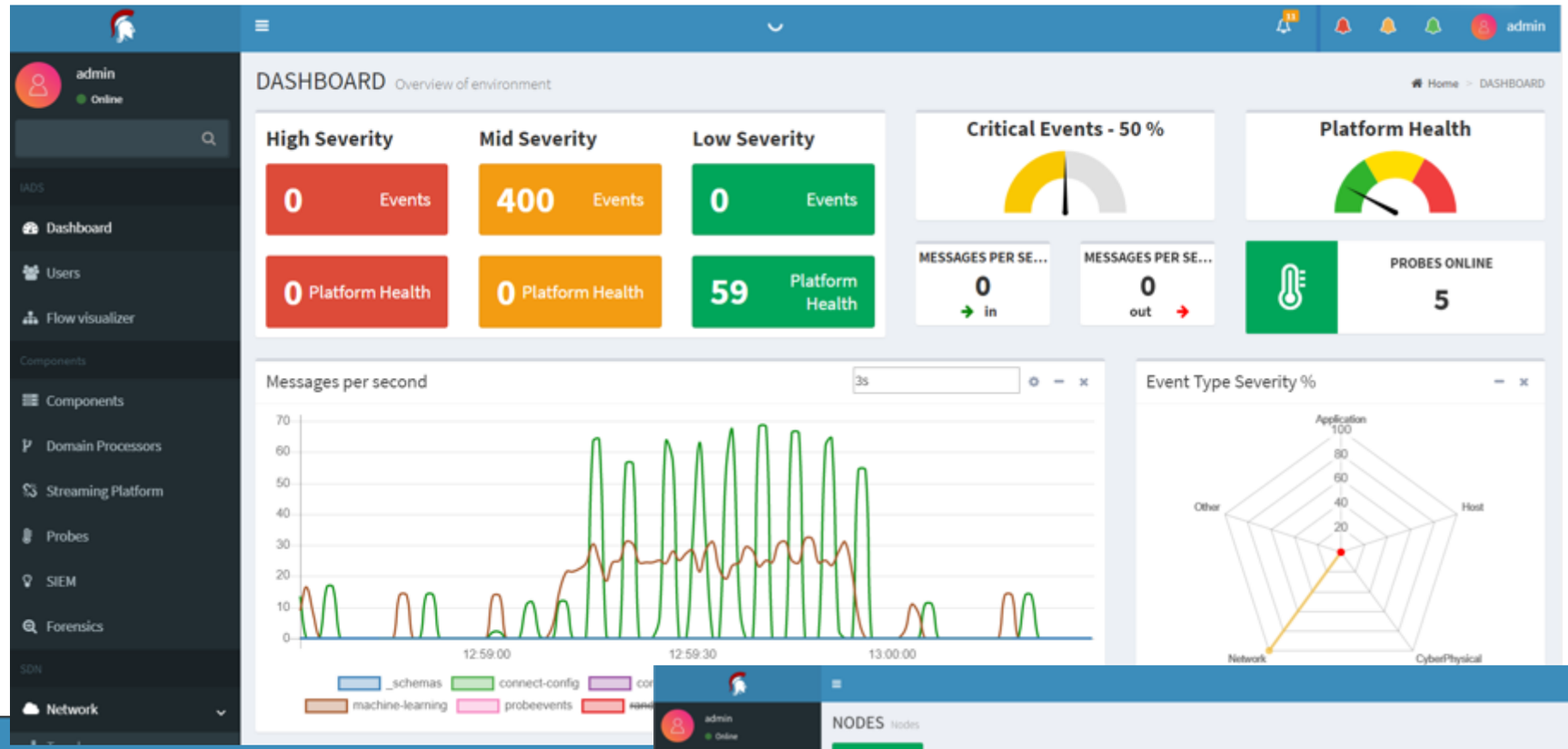
The IADS was designed from the ground up to be open: the event data model, as well as the encoding formats and API endpoints are open and documented

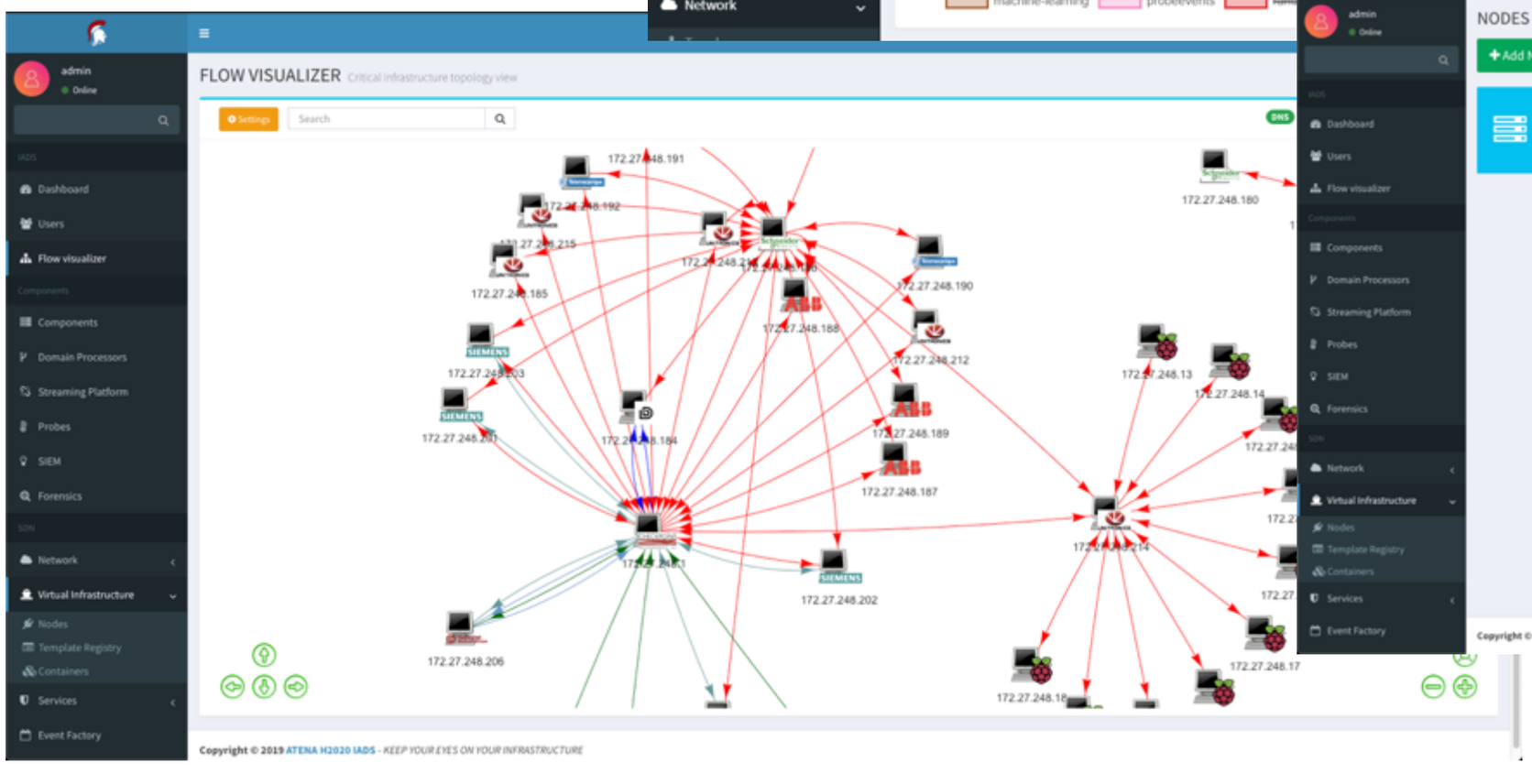


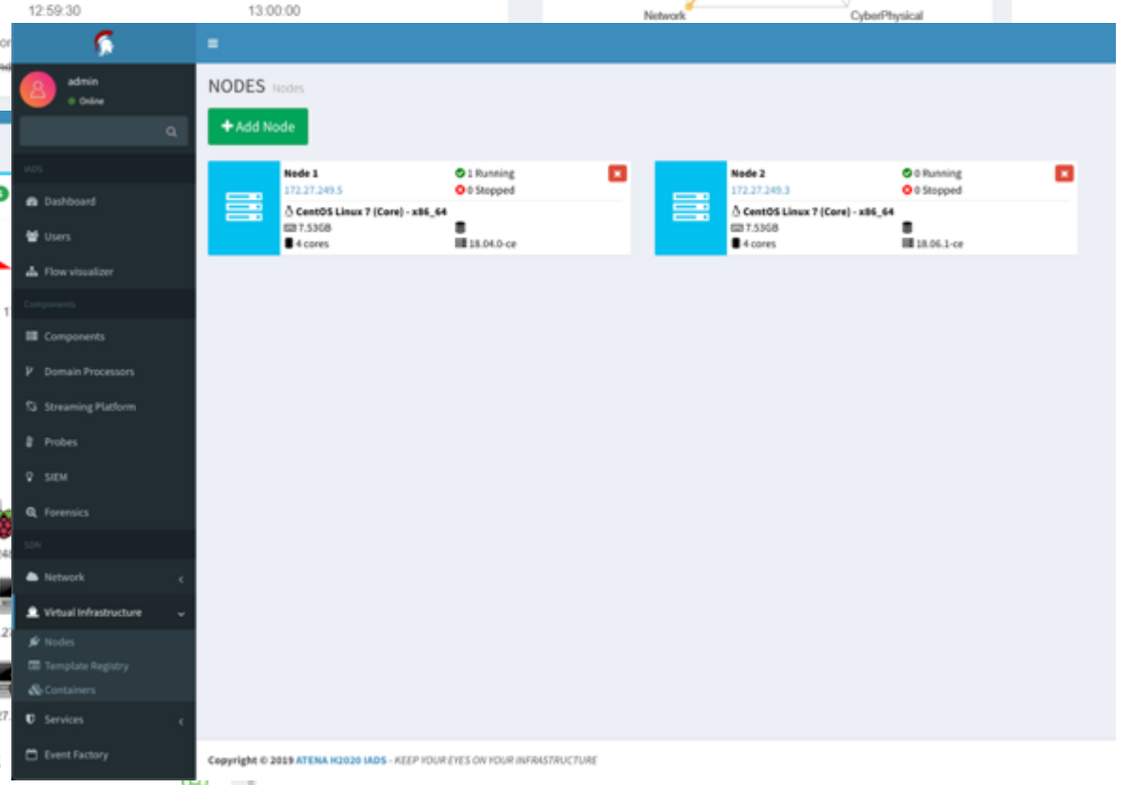
In fact, a third party can develop and provide a turnkey solution for the ATENA IADS, providing new capabilities ranging from new probes to anomaly detection algorithm implementations.

IADS Web UI

Dashboard, Management and Intelligence

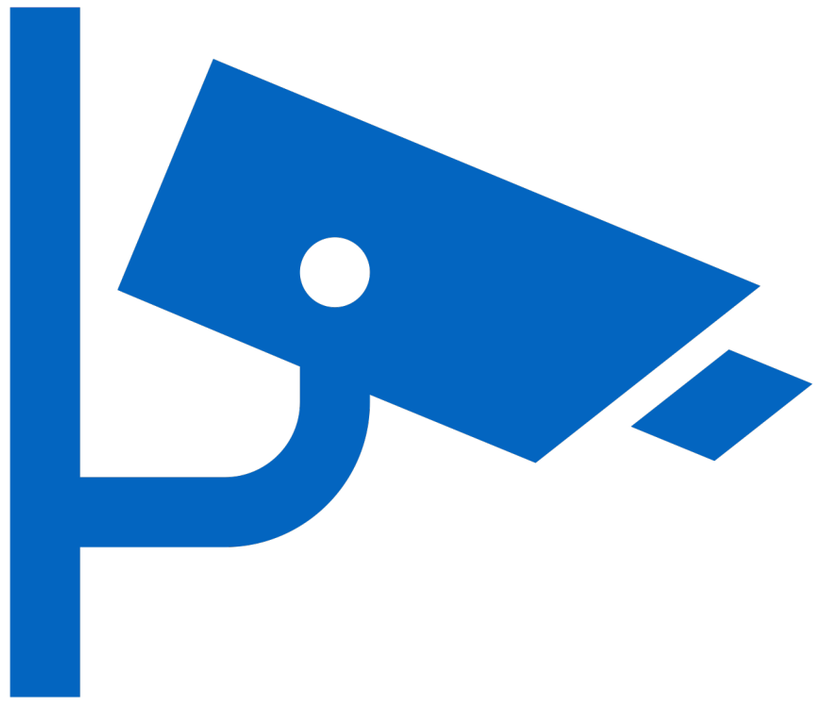






ATENA

Security probes and detection techniques



ATENA

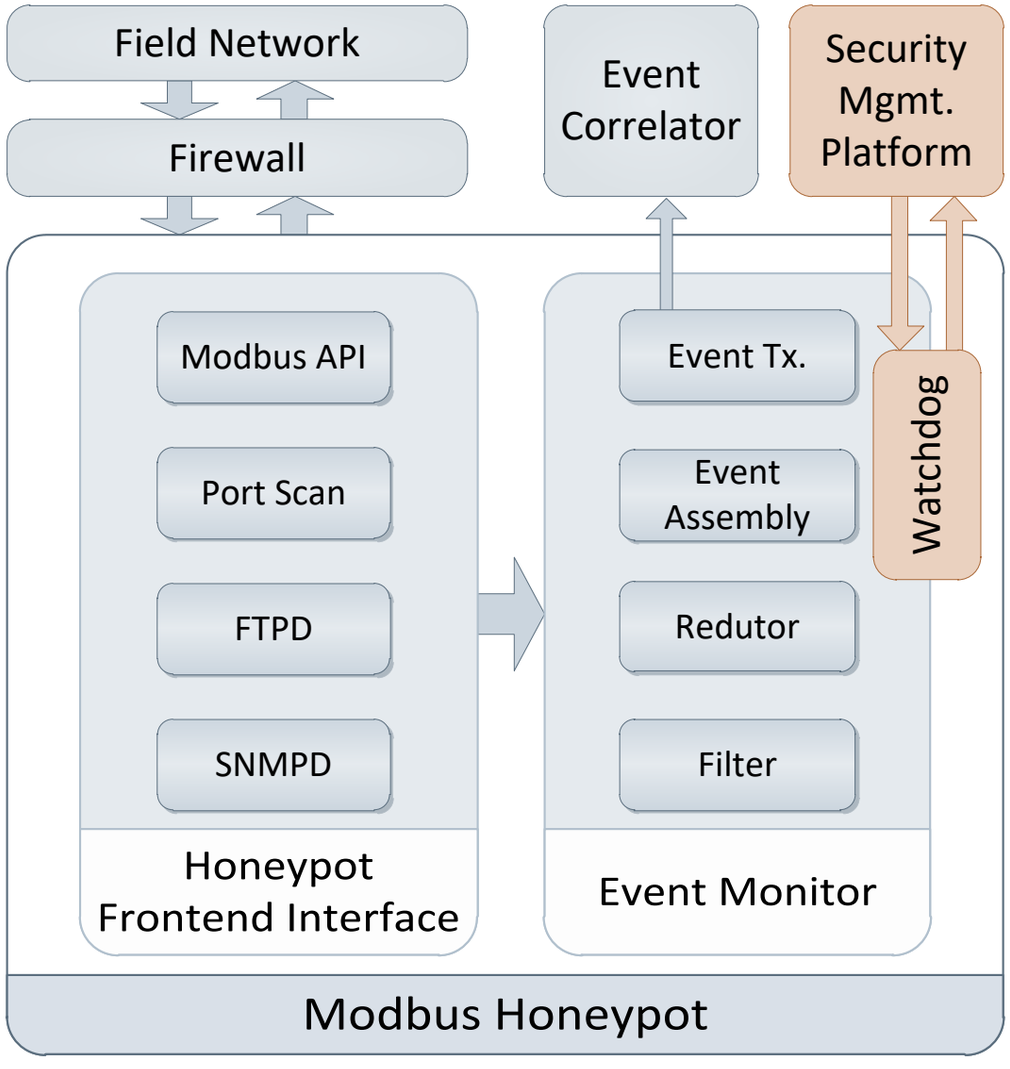
IADS probes and detection techniques

- The ATENA IADS integrated both already existing components and new probes
- Adaptation and integration of already existing components (Snort, OSSEC, among others) was achieved by means of generic coupling agents, which provide IADS event and management integration mechanisms (abstracting data sources and models using the YAML format).
- Research upon new detection techniques was also undertaken, ranging from adversarial techniques to cyber-physical anomaly detection models.

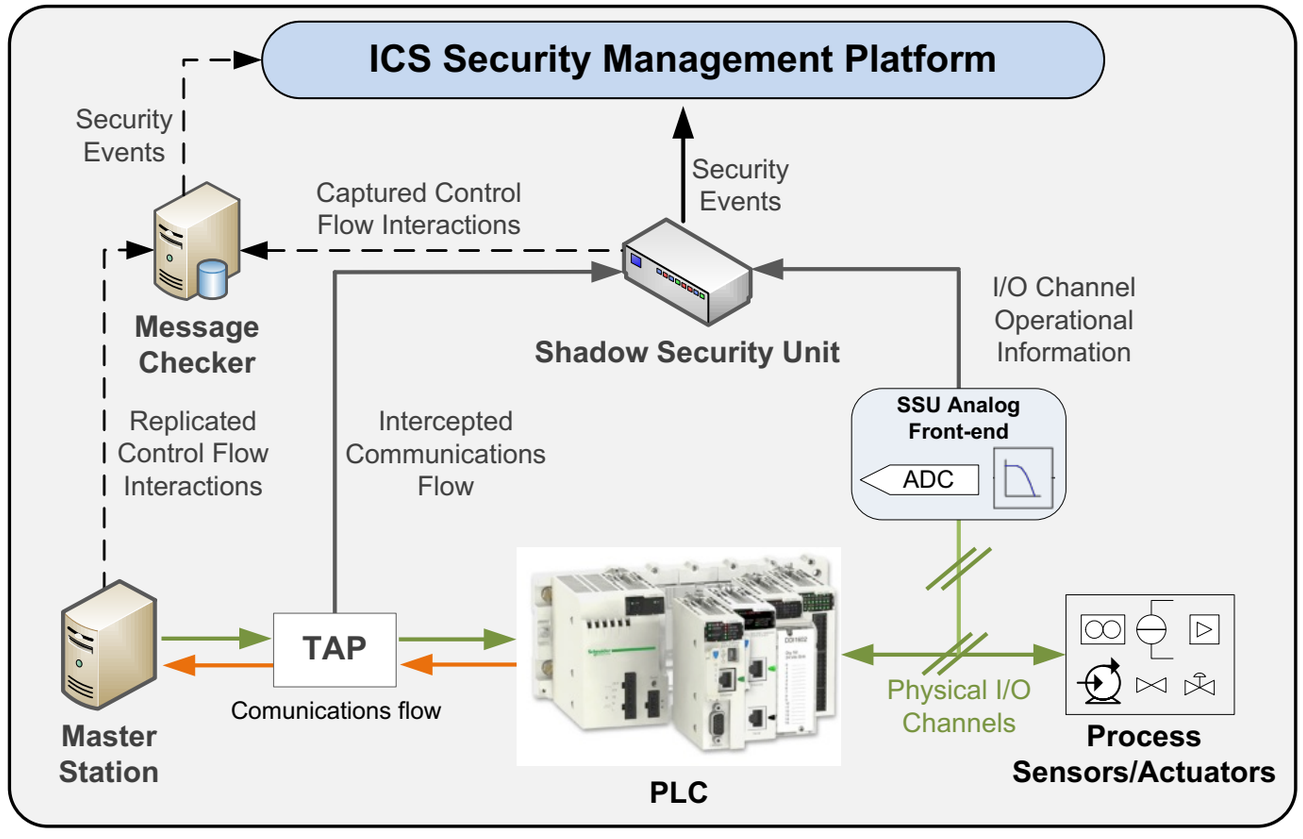
IADS security probes

- Examples of probes developed in the scope of the ATENA IADS:
  - **Shadow Security Unit (SSU)**
  - **SCADA Honeypot**
  - **Environmental Monitoring Unit (EMU)**
  - **SDN security agent**
  - **Software, multi-AV and configuration checker**
  - **Smart Home IDS**
  - **….and, of course, the virtual probes**

Specialized Security Probes:
the SCADA Honeypot and the Shadow Security Unit



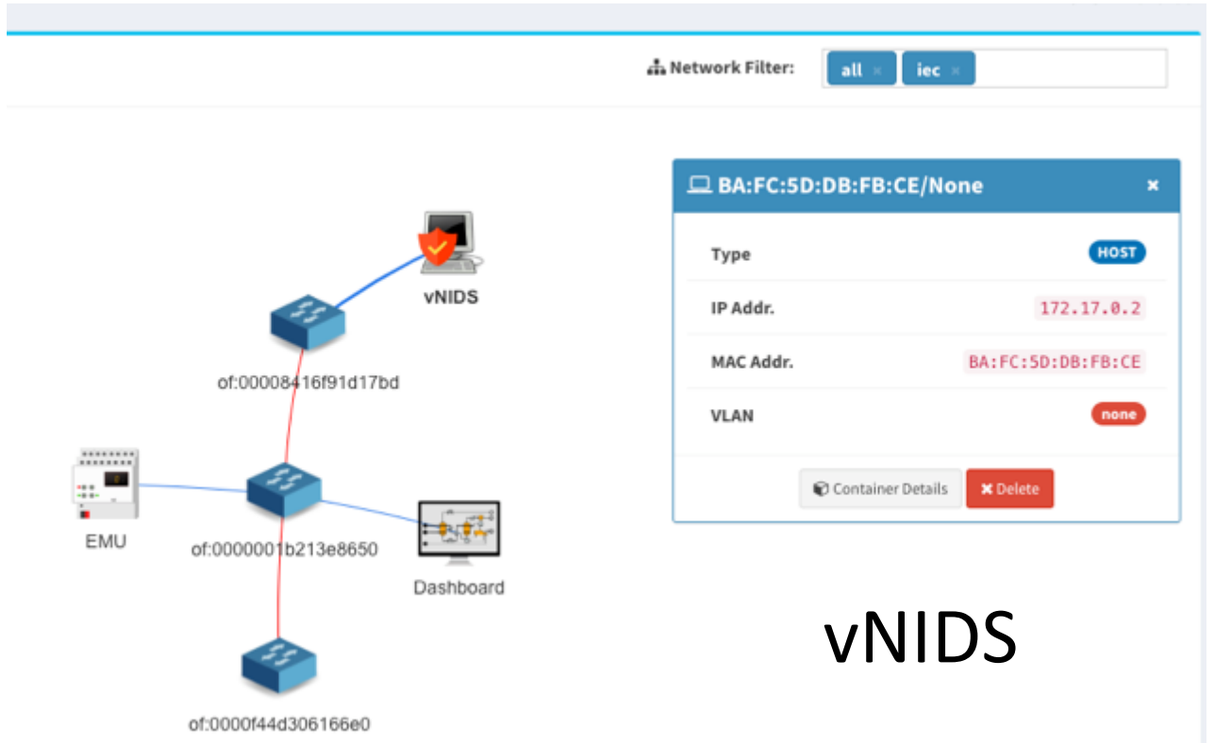
SCADA Honeypot



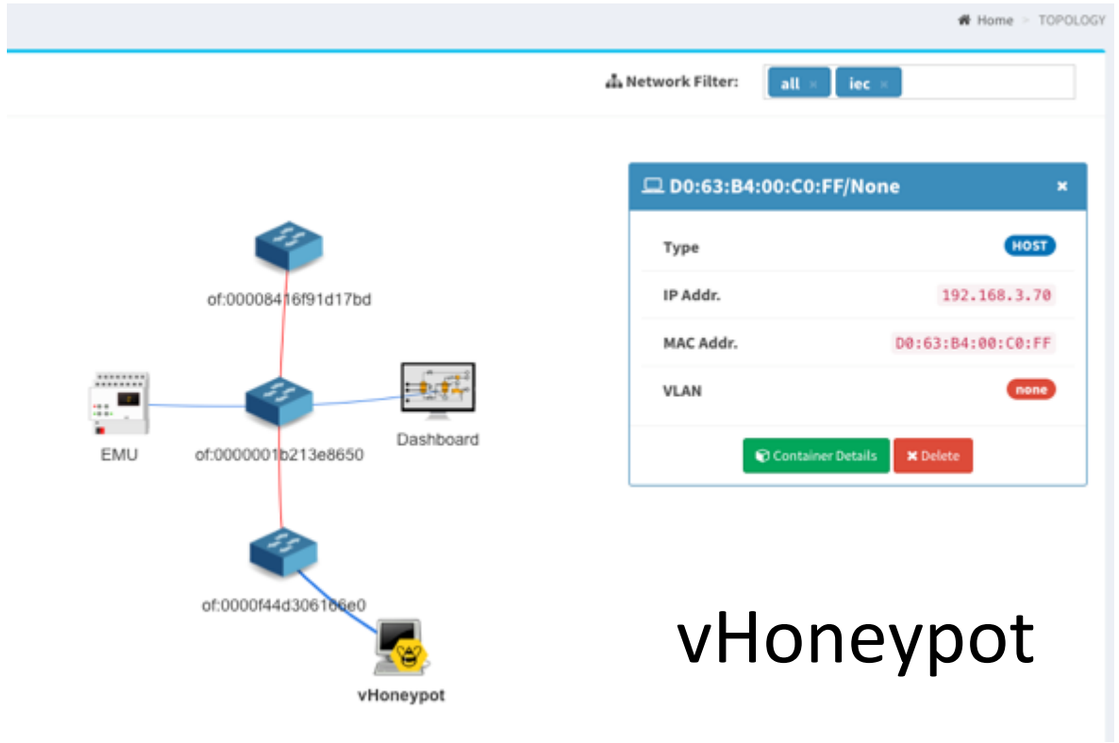
ATENA

Leveraging SDN/NFV in the IADS

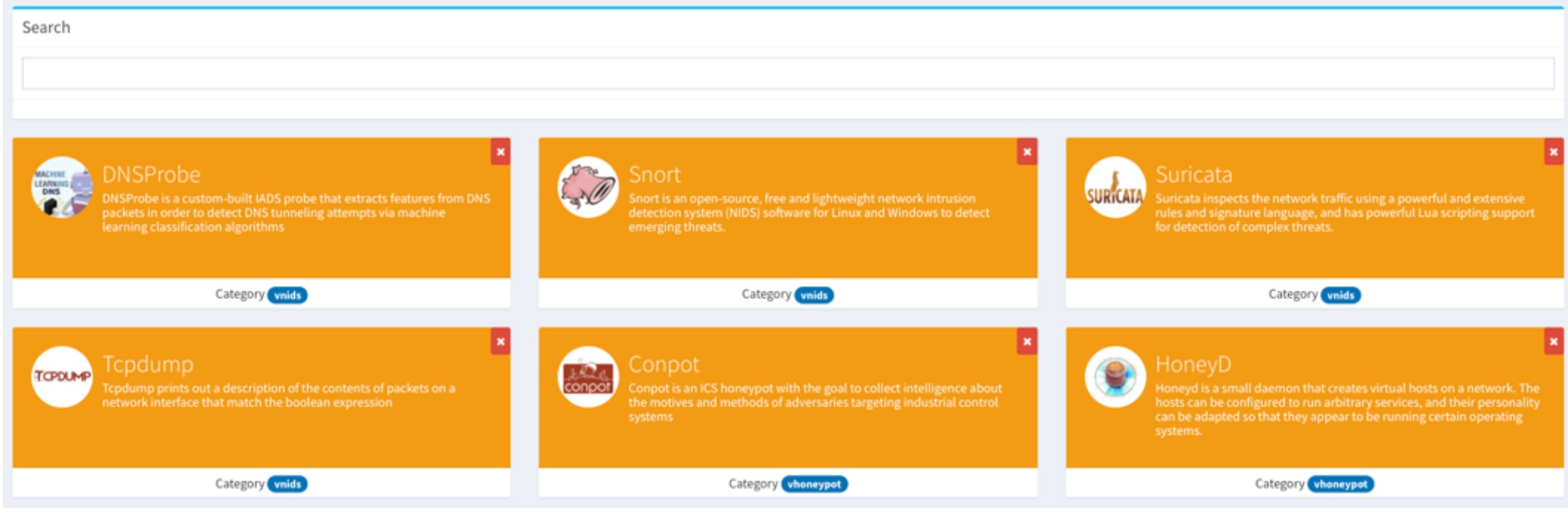
SDN and NFV-enabled virtual probes (*vProbes*)



vNIDS



vHoneypot

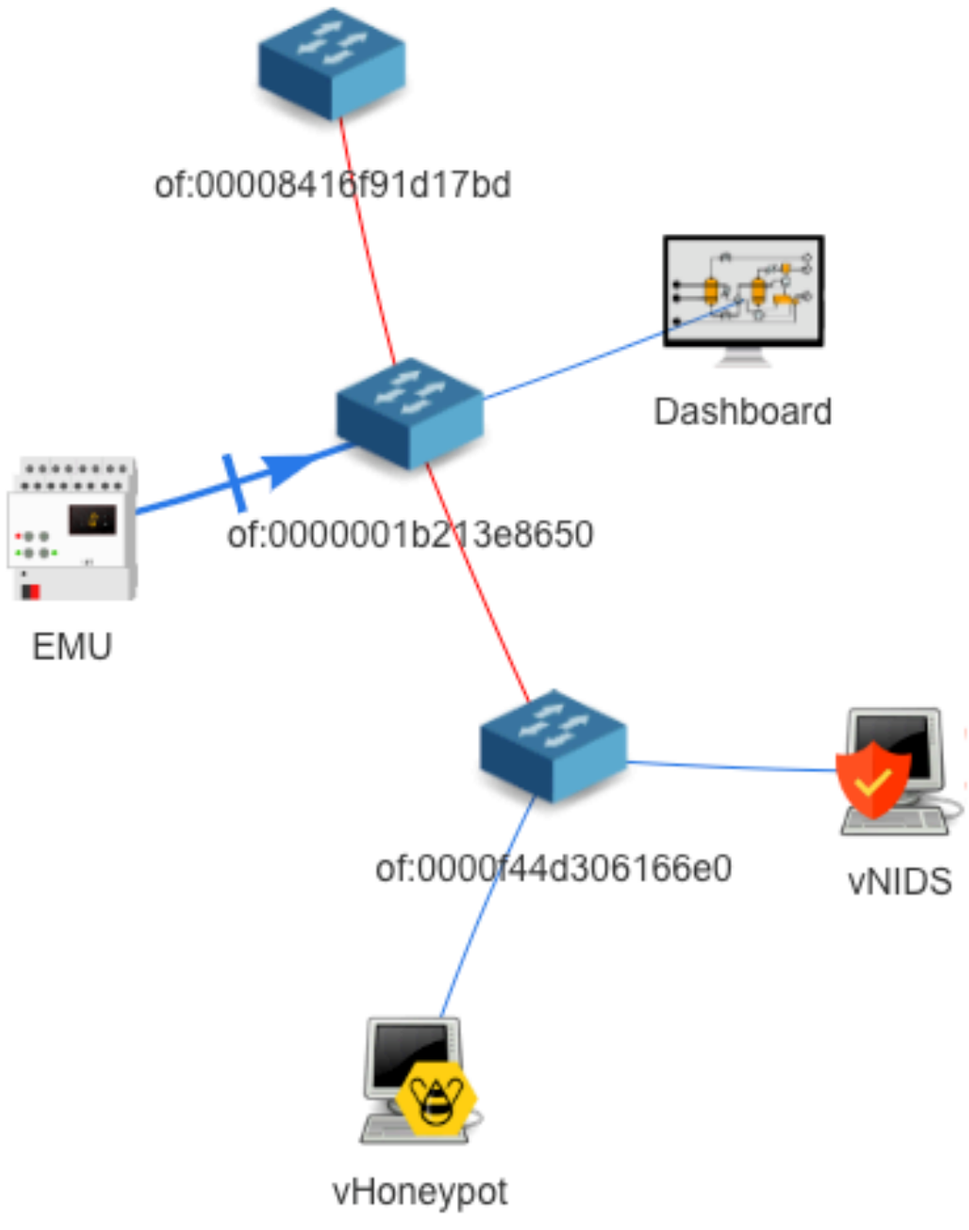


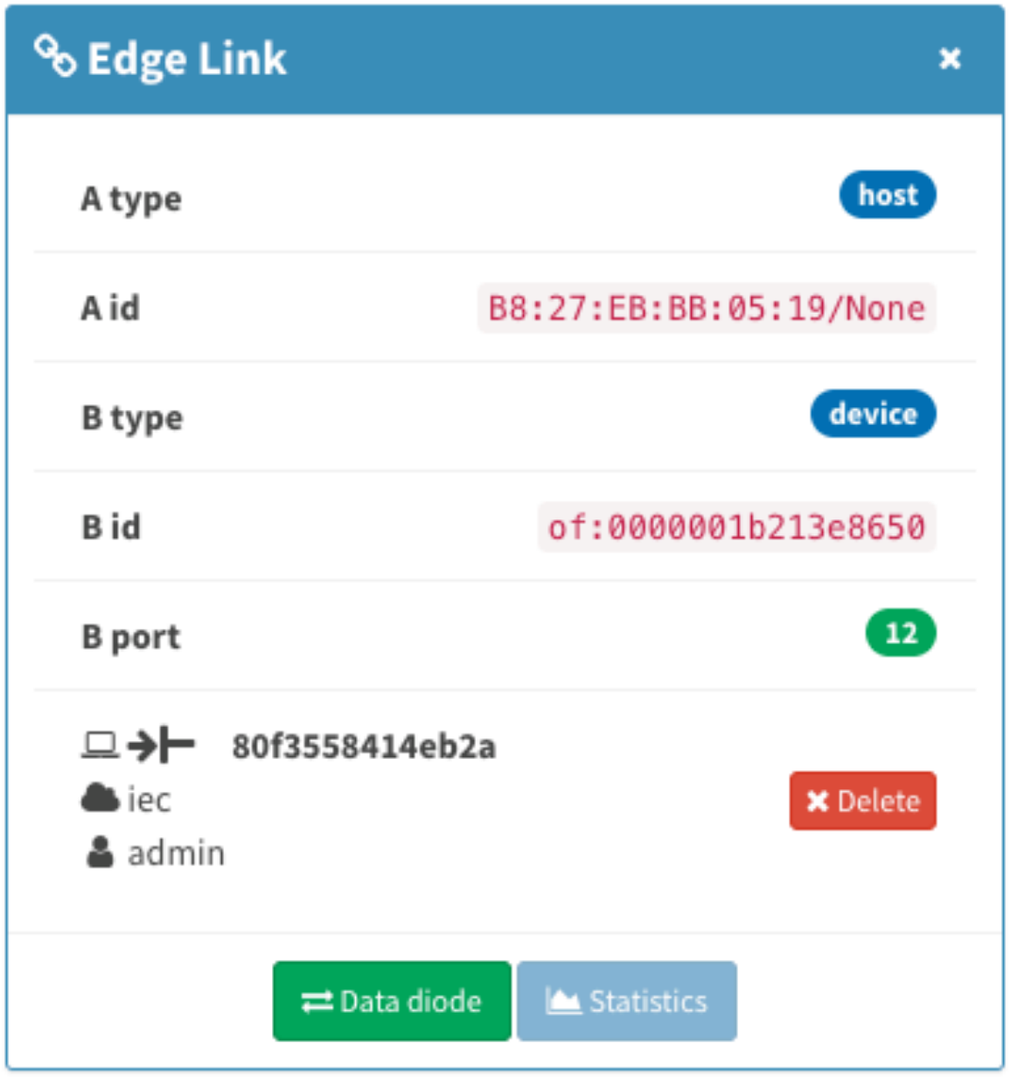
vProbe catalog

ATENA

SDN and NFV-enabled Service Support

Virtual Data Diode





Forensics and compliance auditing

ATENA

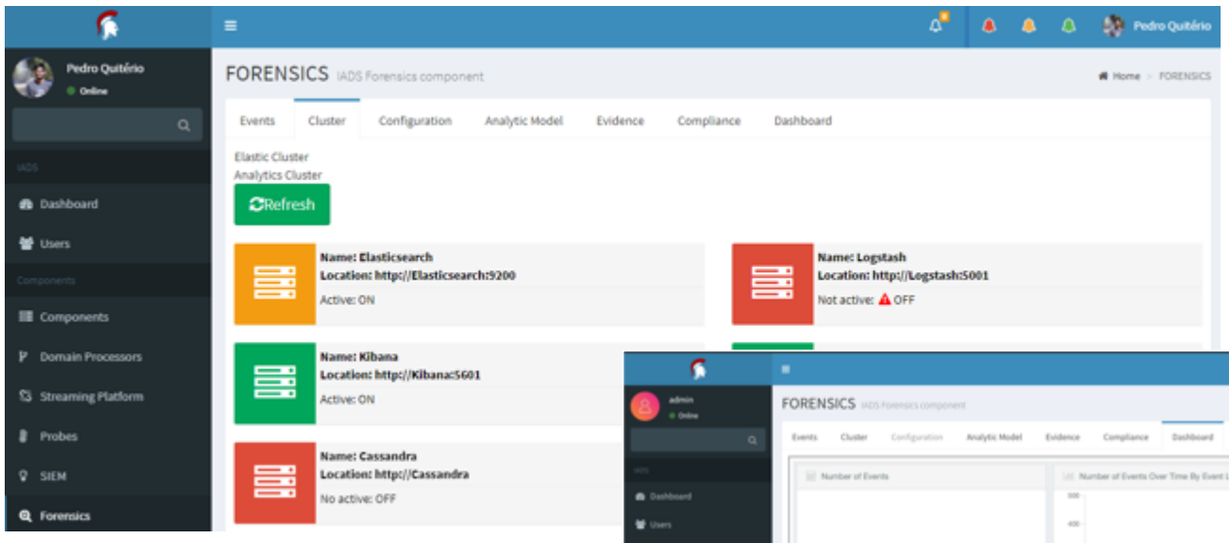
Forensics and Compliance Auditing (FCA)

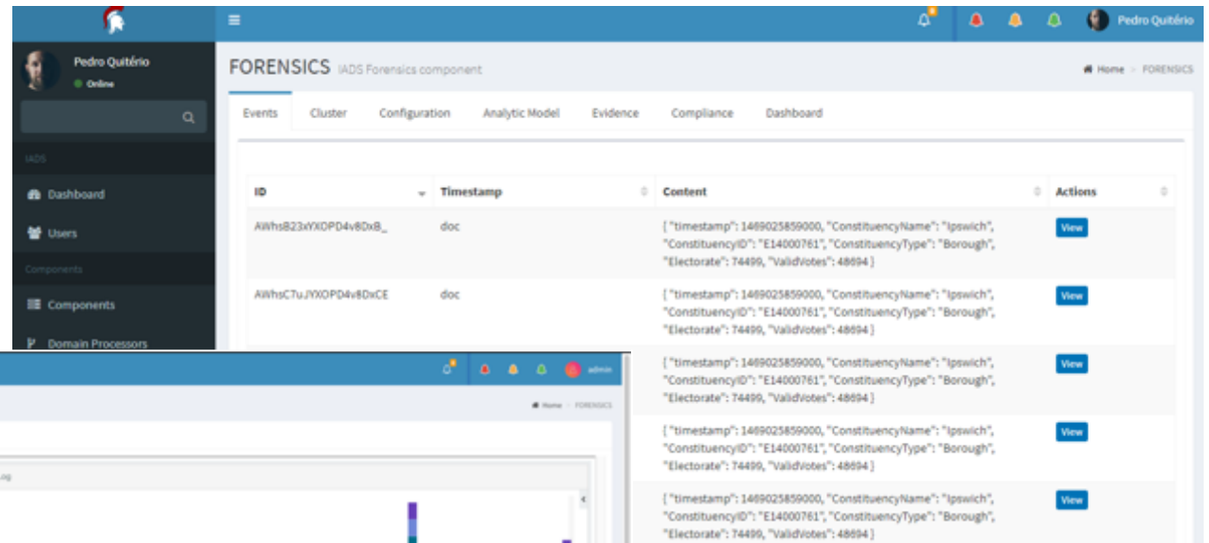
- The FCA subsystem constitutes a big Data **black-box** infrastructure to support **forensics** analysis of events, but also a Data Frame for **log analytics**.

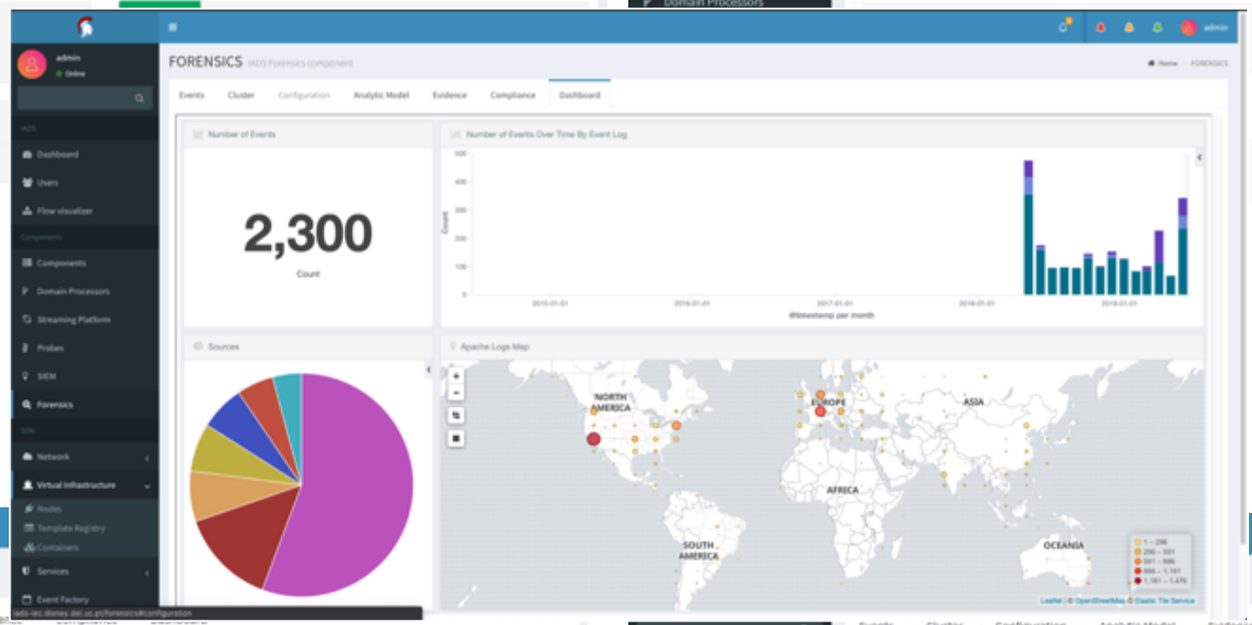
- It supports **data log pre-processing** and **interfacing** with registered Computer Security Incident Response Team (**CSIRT**), providing pertinent and reliable data **samples** for forensic and root cause analysis in case of security incidents.

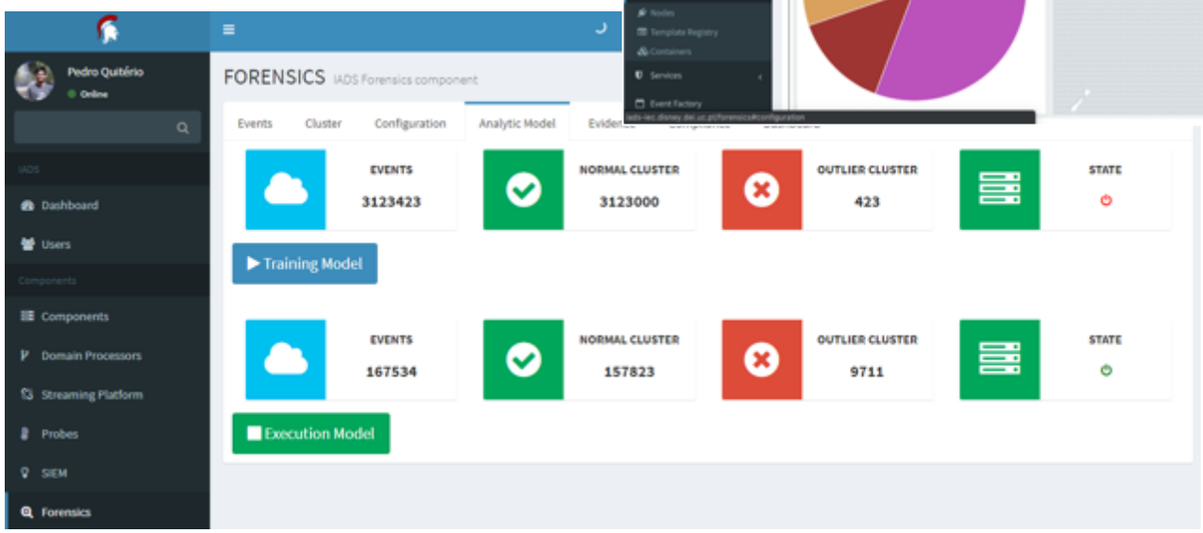
- It provides support for the **continuous auditing** of third-parties (subcontractors, supply chain, equipment providers) and internal personnel activity for **trust** and **compliance processes**, service quality **assessment** and detection of cyber **policy violations**.

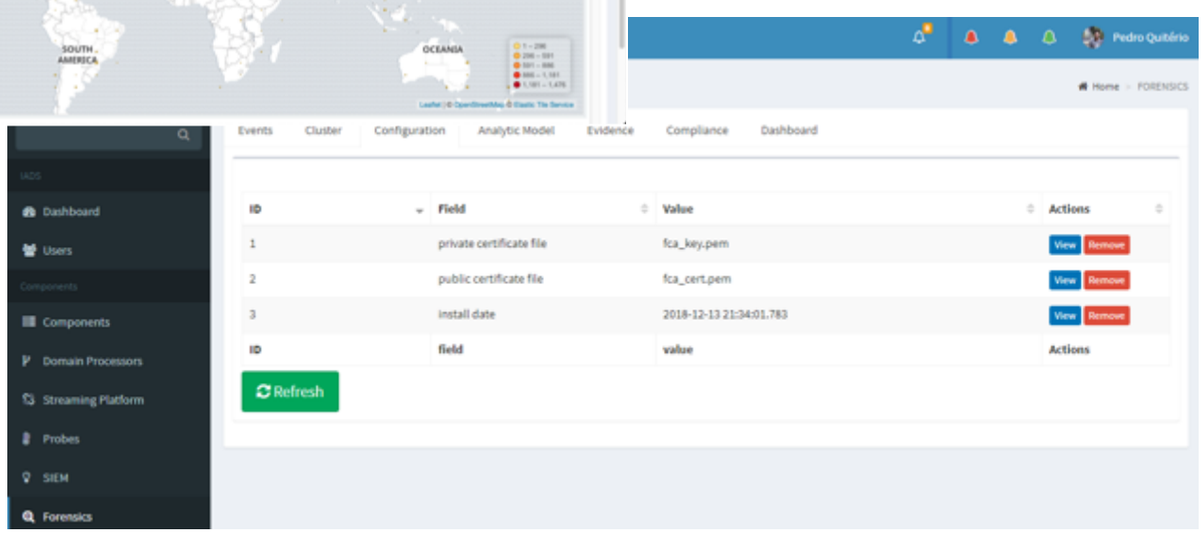
FCA subsystem interfaces









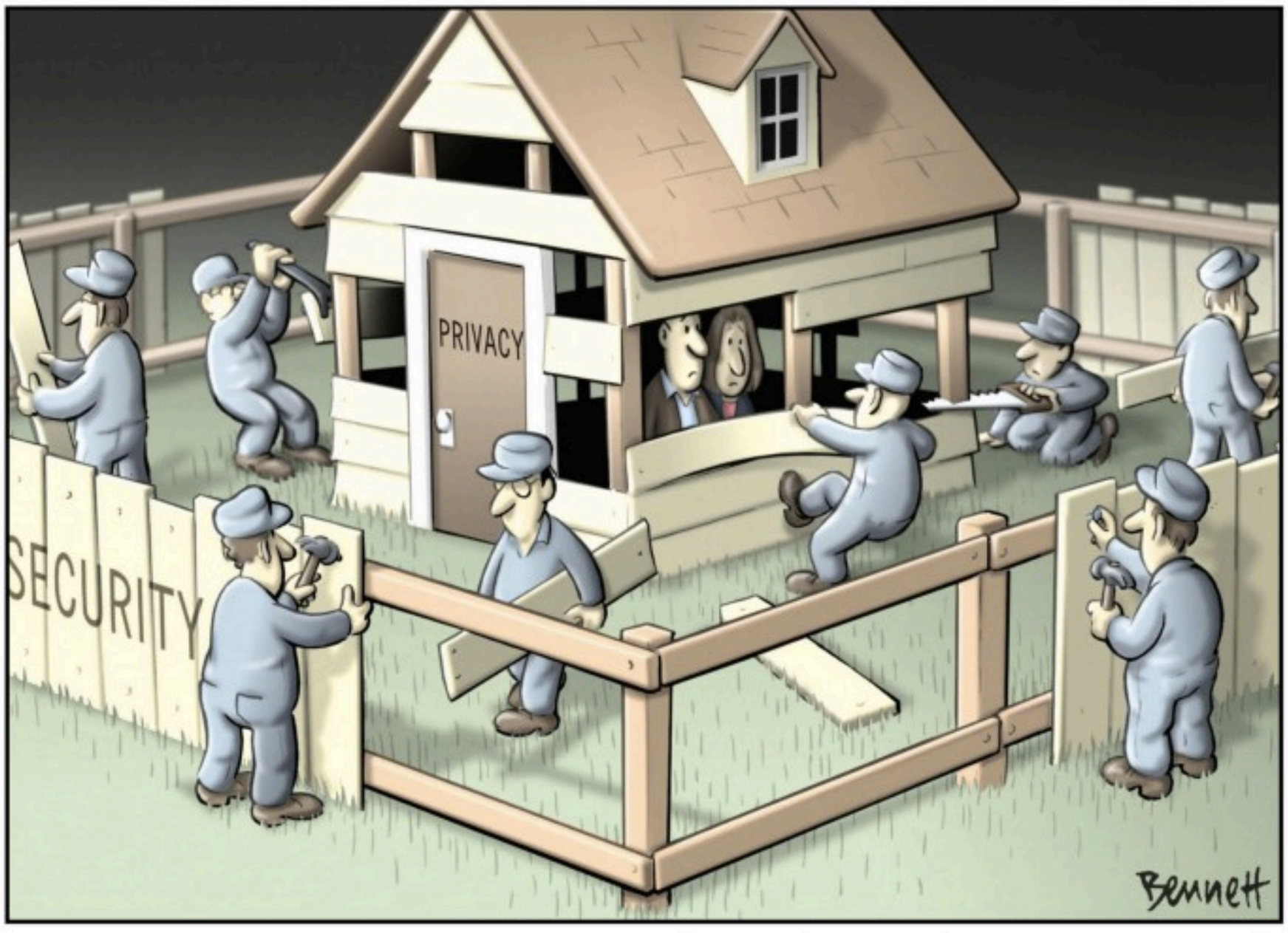


ATENA

Privacy and data security: the next frontier

ATENA

It’s all about trade-offs



Did we really forget this ?

Not quite…

- For instance, the FCA subsystem was built with data protection in mind, both for integrity and attribution purposes
- For instance, all evidence extracted from the FCA blackbox is signed and encrypted, to protect against tampering
- The FCA was designed to provide (semi-)automated supply-chain conformity assessment checks (encouraging compliance with **ISO 27000 standards** but also helping implement **ISO 28000 supply chain management services**)

But…

Detecting Activities of Daily Living with Smart Meters

Jana Clement, Joern Ploennigs, and Klaus Kabitzsch

2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)

Enabling Edge Intelligence for Activity Recognition in Smart Homes

Year: 2018, Volume: 1, Page

DOI Bookmark:

Peek-a-Boo: I see your smart home activities, even encrypted!

technologies

Abbas Acar*, Hossein Fereidooni†, Tigist Abera†, Amit Kumar Sikder*, Markus Miettinen†, Hidayet Aksu*, Mauro Conti‡, Ahmad-Reza Sadeghi†, and A. Selcuk Uluagac*

MDPI

Article

A Stochastic Memory Model for ADL Detection in Human Households †

Jana Clement * and Klaus Kabitzsch

Department of Computer Science, University of Technology Dresden, 01062 Dresden, Germany; klaus.kabitzsch@tu-dresden.de

* Correspondence: jana.clement@tu-dresden.de; Tel.: +49-351-4633-8375

† This paper is an extended version of our paper published in the 10th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA), Island of Rhodes, Greece, 21–23 June 2017.

Received: 16 October 2017; Accepted: 24 November 2017; Published: 30 November 2017

A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic

Noah Apthorpe
Computer Science Dept.
Princeton University
apthorpe@cs.princeton.edu

Dillon Reisman
Computer Science Dept.
Princeton University
dreisman@princeton.edu

Nick Feamster
Computer Science Dept.
Princeton University
feamster@cs.princeton.edu

ATENA

The next frontier

To provide a fair balance between protection and privacy

What we need to do:

- Make sure users know what the service operators are doing (which information is collected and persisted, for how long and for which purposes) – the GDPR can really be helpful here, but **you cannot create awareness by decree**
- Provide users with the means to access (and manage) their profile data
- Carefully evaluate trade-offs (HAN security poses a lot of questions)

The next frontier

To provide a fair balance between protection and privacy

What we need to do:

- Carefully control and monitor the supply chain (for multitenant environments this is crucial)
- Improve the evidence collection mechanism, enforcing anonymity as much as possible (whenever possible);
- Data provided for training and modeling must purposes must be anonymized
- Effective analytics do not necessarily imply intrusive data collection

Conclusions and next developments

The ATENA IADS departs from the conventional ICT-centric IDS paradigm to offer a complete solution to deal with ICS cyber-security, oriented towards Industrial IoT scenarios.

The IADS was designed to scale and be flexible, while providing consolidated management and orchestration features. Besides its cibersecurity capabilities, the IADS is also a valuable instrument to foster ISO 27000 and 28000 compliance.

But once IIoT becomes pervasive, a significant effort will be required to protect users' privacy, while providing eficient cibersecurity capabilitites

While most of the existing solutions do not take such issues into consideration, it's only a question of time until someone realizes that the "next best security solution ever" cannot be deployed simply because it goes against privacy and data protection regulations.

Any Questions?

And thank you for your attention

Acknowledgements

Picture from slide 4 – source:
https://upload.wikimedia.org/wikipedia/commons/8/8d/NS_Savannah_control_room_MD1.jpg

Pictures from slide 6 – source:
https://www.theregister.co.uk/2015/05/11/smart_grid_security_worse_than_we_thought/
https://www.darkreading.com/perimeter/smart-meter-hack-shuts-off-the-lights/d/d-id/1316242

Image from slide 26 – source:
http://www.lossofprivacy.com/index.php/2010/12/privacy-vs-security/