Accenture Technology Labs

Innovation is…the unforeseen

High performance. Delivered.

Enhanced Situational Awareness for Advanced Threat Detection and Identification in IIoT (ESTATION)

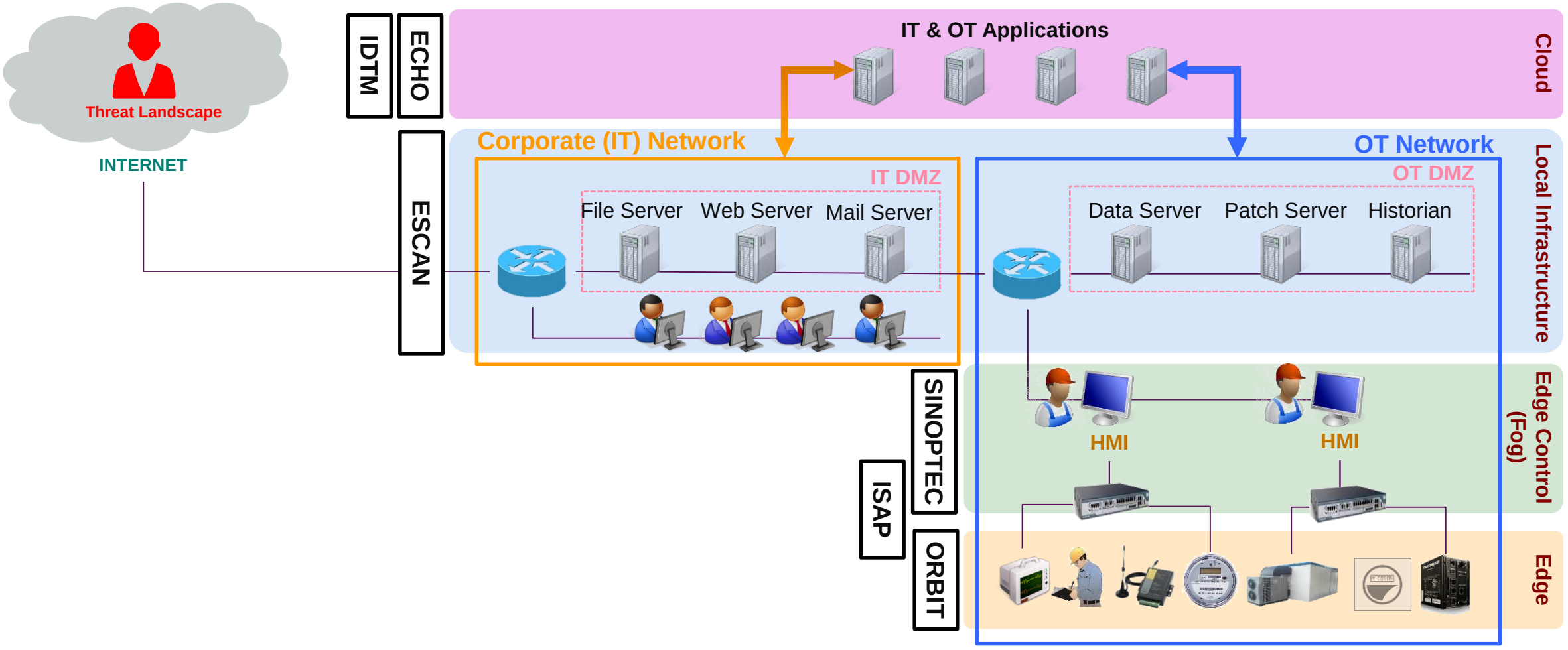
Amin Hassanzadeh, Ph.D.
Accenture Technology Labs

accenture

Strategy | Digital | Technology | Operations

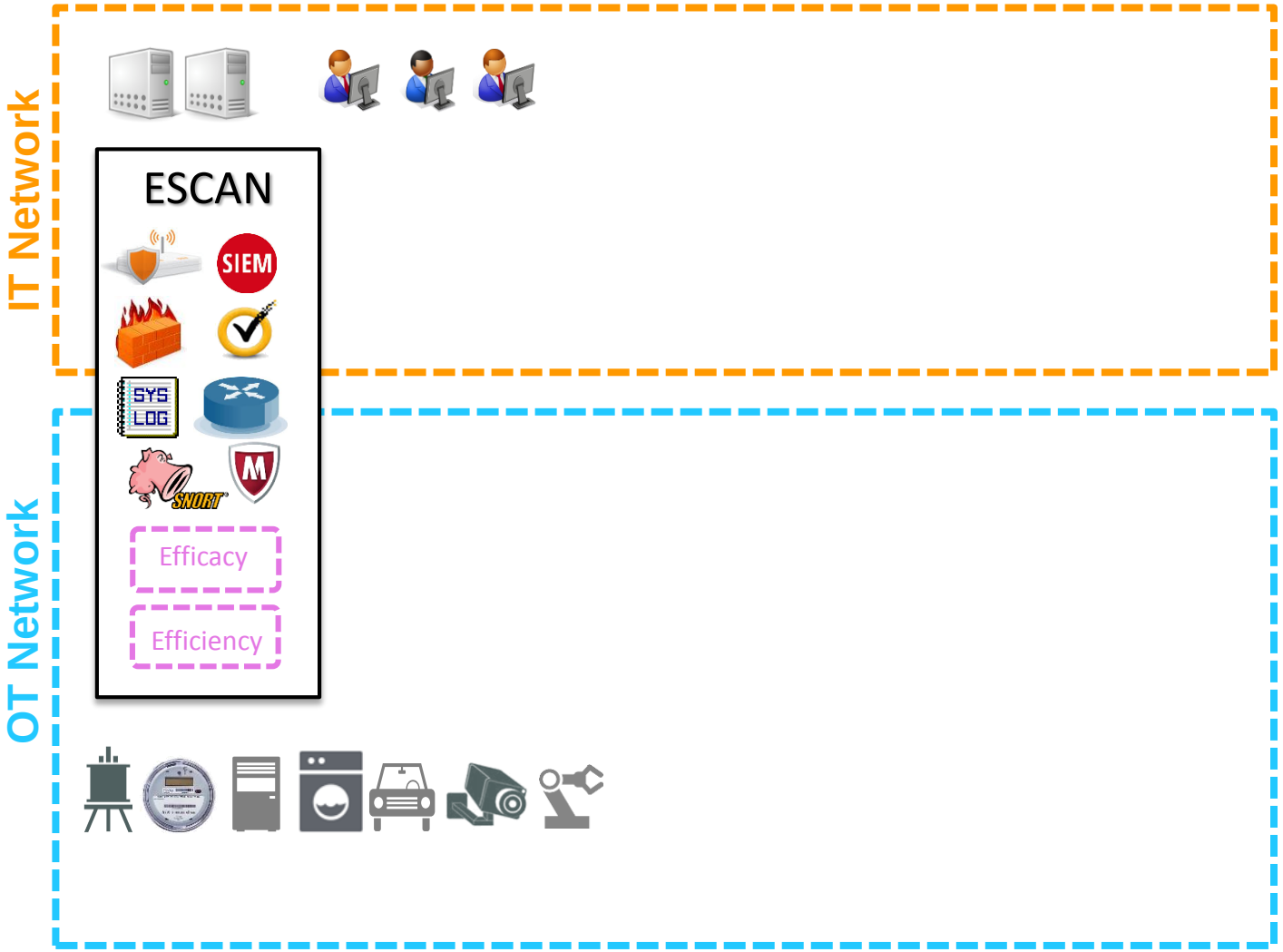
ESTATION: A Holistic, Scalable, and Strategic IIoT Security Framework

To assess, prioritize, implement, and optimize security architecture and capabilities



Architectural View of ESTATION

Effective and Efficient Security Control Assignment in IIoT (ESCAN)



What security capabilities are required?

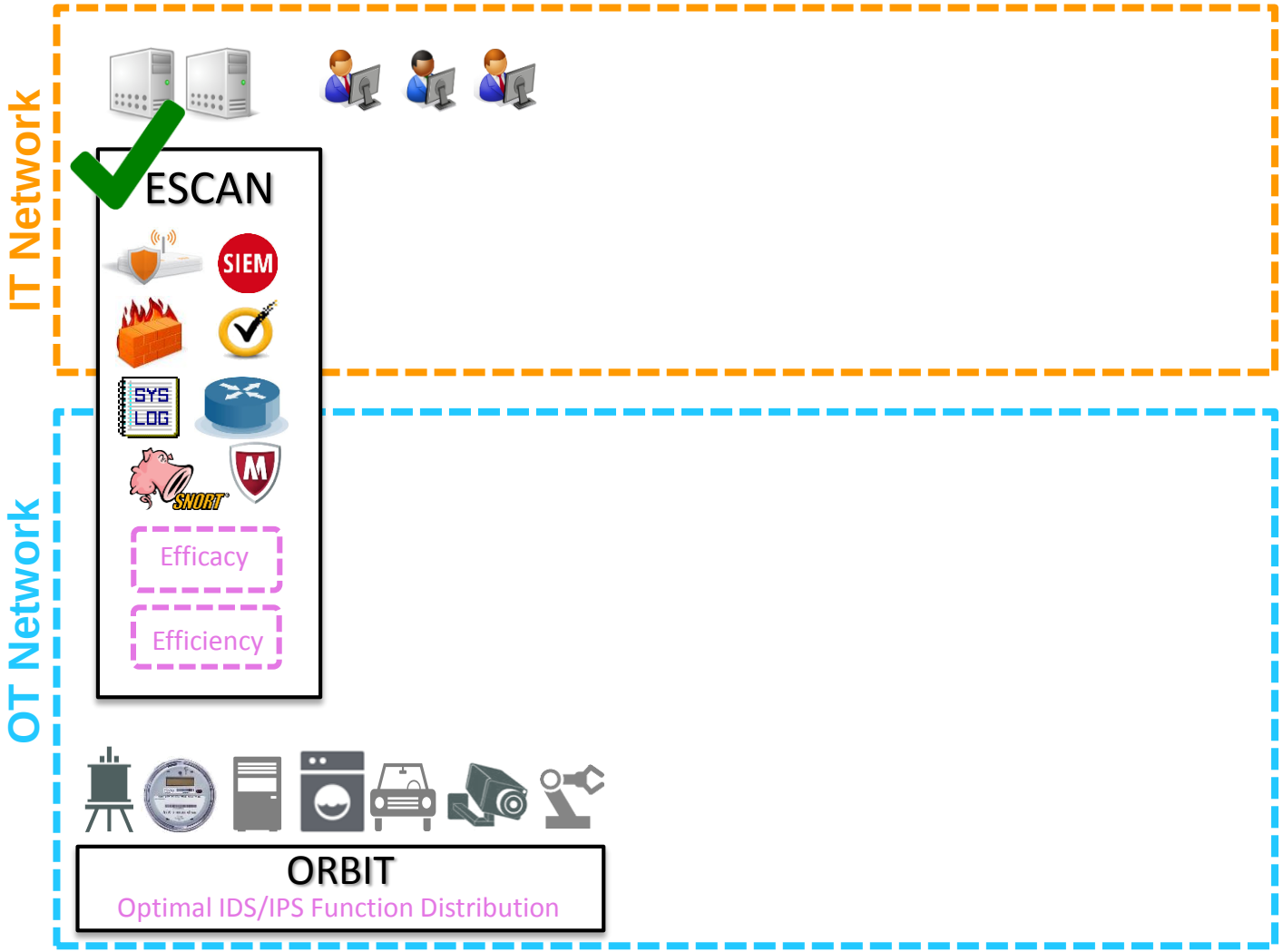
Where do we deploy security capabilities?

How do we deploy security capabilities?

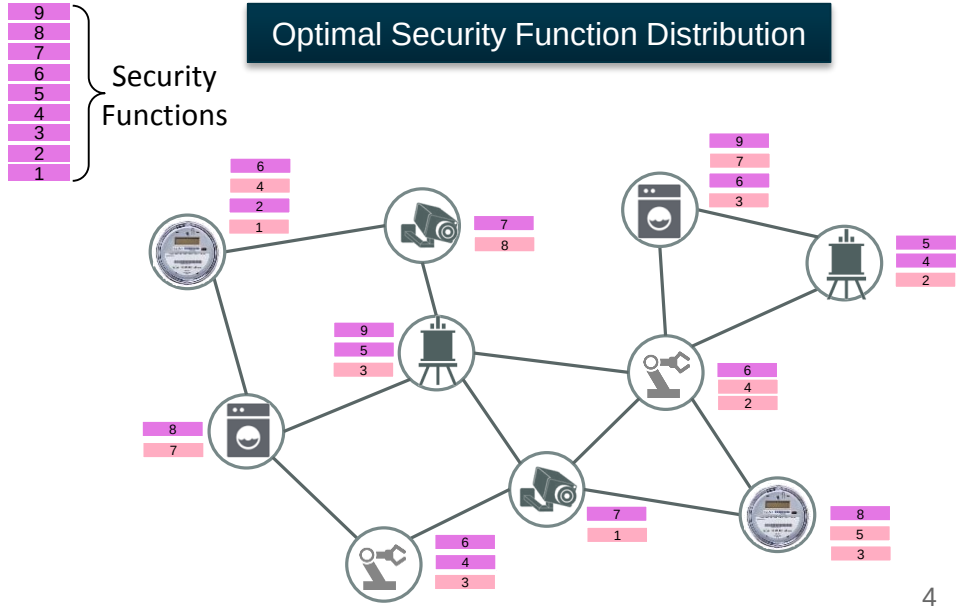
- Enumerating traditional security controls
- IIoT Architecture and functionality
- Publicly available incident analyses
- Conducting a gap analysis to determine the efficacy of security controls

Architectural View of ESTATION

On-the-edge Resource-aware Behavioral Intrusion Tolerance (ORBIT)

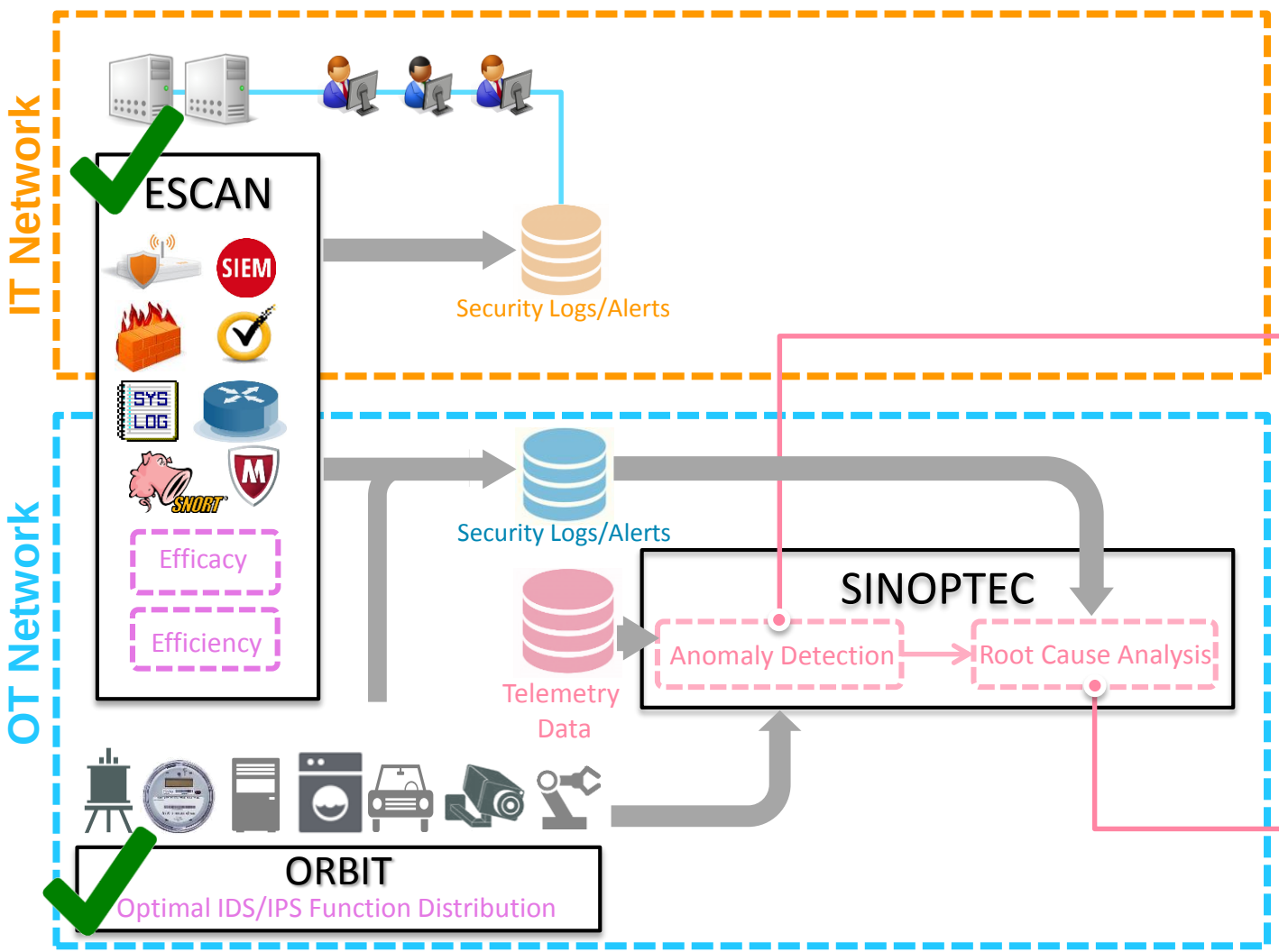


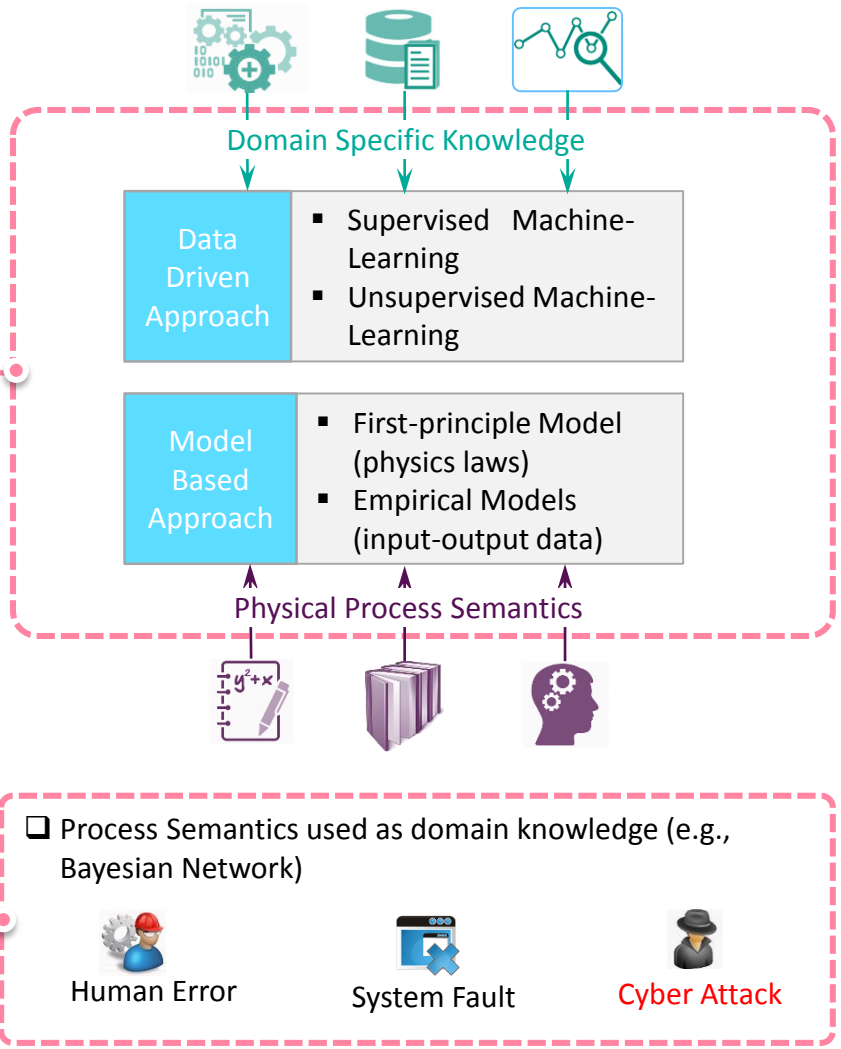
- The vast majority of these things won't be in the cloud, they will be **at the edge** of the network—where the people are
- IIoT will have enormous client-server interactions but it will have even more **interactions among intelligent things** at the edge of the network
- Inefficient data communication to cloud for intrusion detection in large IIoT networks **(communication overhead)**
- **Delayed data processing** in real-time applications



Architectural View of ESTATION

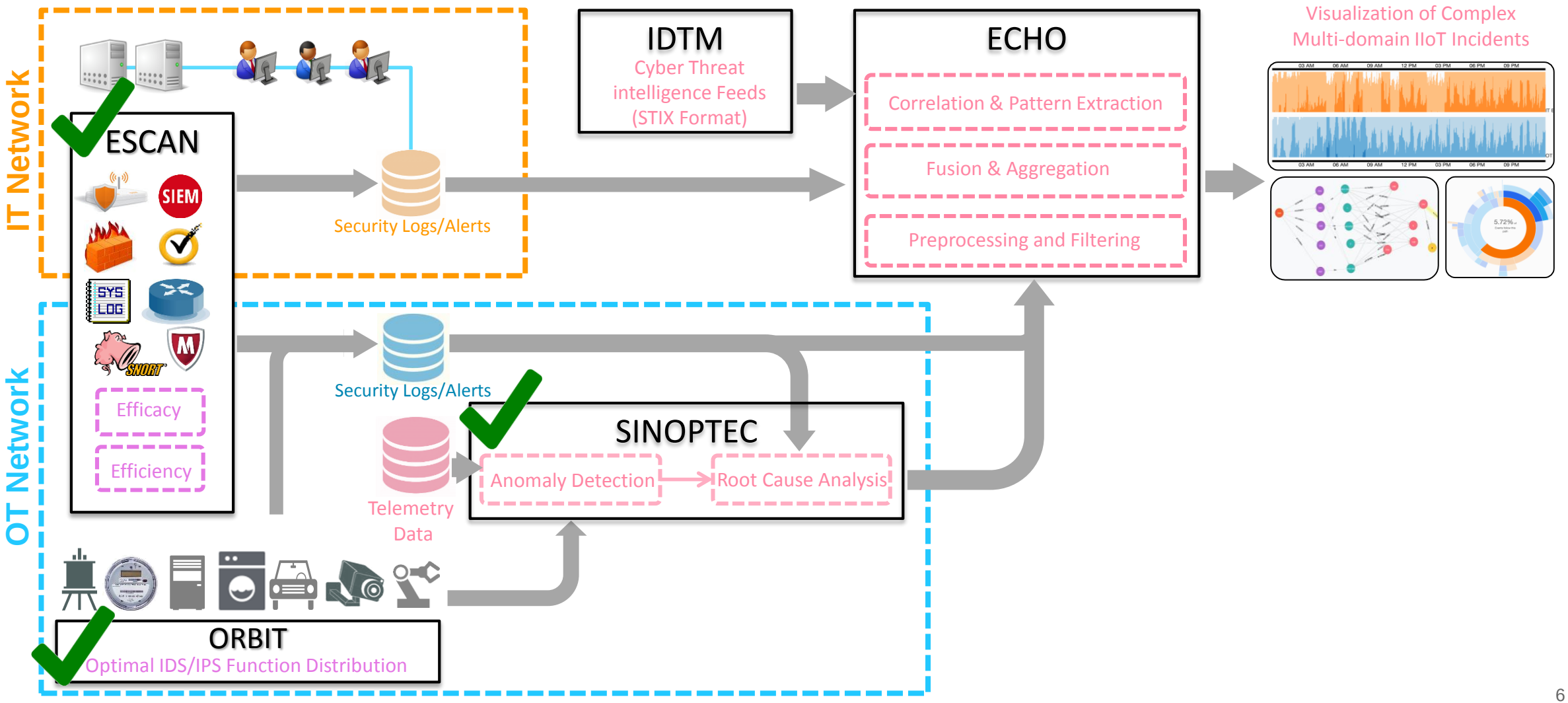
Security Insight through Operational Telemetrics (SINOPTEC)





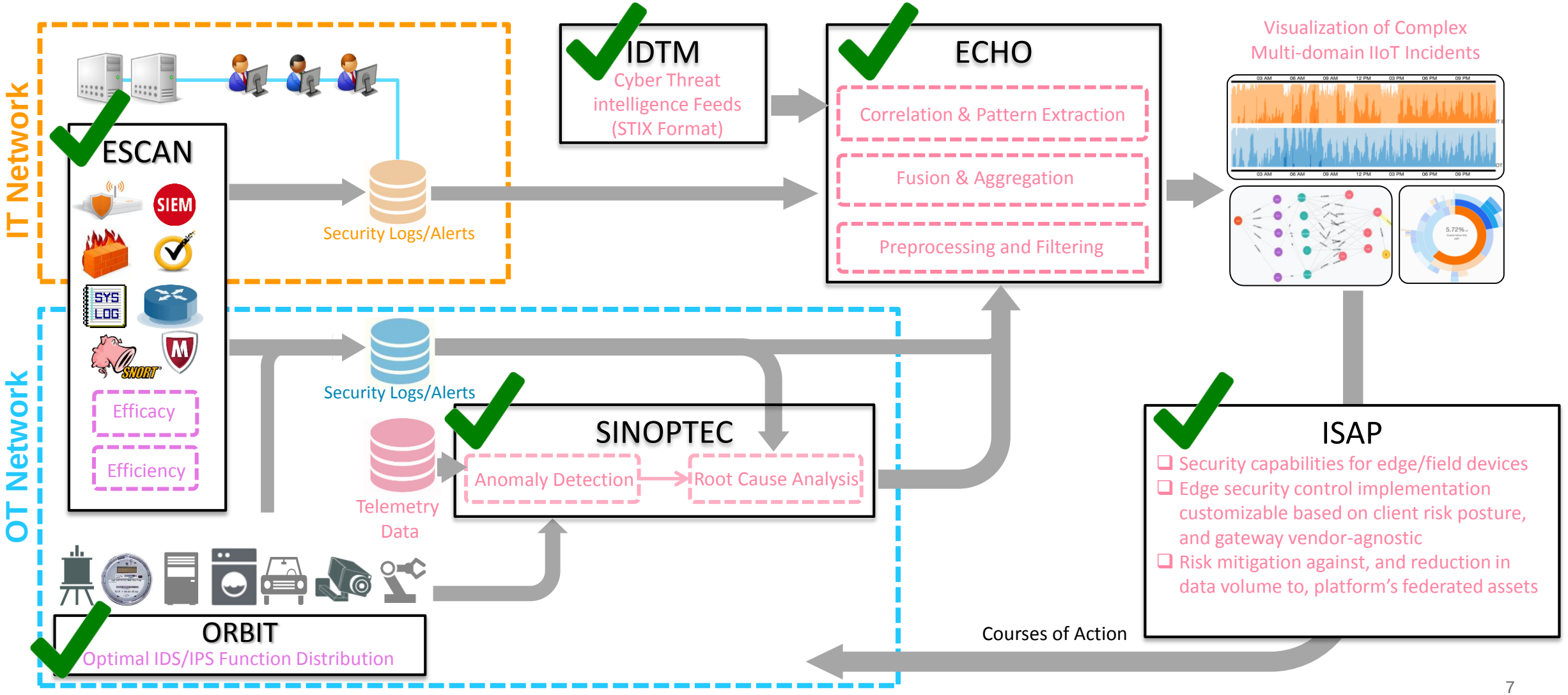
Architectural View of ESTATION

Event Correlation across Heterogeneous Operations (ECHO), Intelligence-Driven Threat Mitigation (IDTM)



Architectural View of ESTATION

Industrial Security Agent Platform (ISAP)



IIoT Security Orchestration

- ❑ Orchestrate complex automated security actions to improve situational awareness and real time mitigation capabilities
- ❑ Coordinate security processes and workflows across disparate security tools through infrastructure orchestration

Accenture Connected Security Solutions (ACCESS)

- ➢ ECHO, IDTM, ISAP/ORBIT
- ➢ Lightning Talk in TCIPG 2015
- ➢ Demo at Hannover Messe 2015

Enhanced Situational Awareness for Advanced Threat Detection and Identification (ESTATION)

- ➢ ECHO, SINOPTEC, ESCAN
- ➢ Submitted to DARPA RADICS BAA, 2016

- ❖ Six Pending Patents
- ❖ One journal and two conference papers accepted