Improved Industrial Security using TÜV Attack Surface Detection

Stefan Laudat
TÜV SÜD Sec-IT GmbH

Mehr Wert.
Mehr Vertrauen.

Add value.
Inspire trust.

Risk, The Eternal Equation

ASSET

VULNERABILITY

THREAT

ASSETS

Hey, that has to be the industrial equipment, like robots or so, right?

Makes sense! What about the people and teams around them?

What about the digitalization of industry?

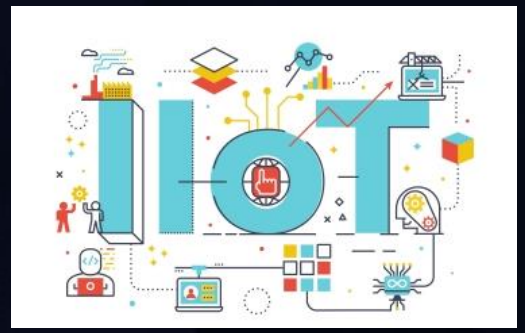
Pretty close. Let's think about what ties them together. Dedicated networks, sometimes exposed to internet..

Their suppliers, their partners, the suppliers of suppliers…

Actually, that's the beginning of it… The race of productivity, new and better technologies, increased complexity and so little time to test… however the biggest asset at risk is human lives.

VULNERABILITIES

- High Inherent Level
- Weak Access Control Systems
- Designed mostly for Functionality
- Projected, deployed and tested by subject matter engineers

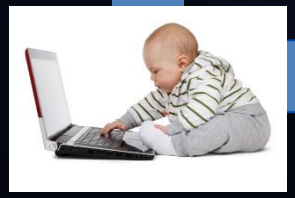


- Complex Off-Boundary Connectivity
- Proprietary Protocols
- High Speed, Low (No?) Authentication

- Mostly Industry Experts
- Low Regulatory Framework
- Insufficient IT Security Awareness

- Complex Supply Network
- Lack of In-Depth Transparency
- “Chain of Trust”

THREAT ACTORS



Costs

Scale of Impact

Threat level would be Moderate-to-High, as of current actors are more in the dormant state, but investing big money in such attacks.

However, due to increasing geopolitical tensions and accelerated industry automation and digitalization and usage of insecure protocols, the scale of impact will increase…

… all correlated with the careless direct connectivity of industrial devices to Internet and an increasing open source toolset.

FACTS AND FIGURES – OPEN SOURCE INTELLIGENCE

TOTAL RESULTS

15,881

TOP COUNTRIES

Germany	15,881

TOP CITIES

Frankfurt	2,711
Berlin	366
Host	344
Frankfurt Am Main	266
Hamburg	74

TOP SERVICES

DNP3	8,696
Tridium Fox	2,258
EtherNetIP	2,042
Modbus	1,284
Siemens S7	995

DNP3 *(Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.*

Tridium is the latest buzz word in the Building Automation Industry. There are three driving factors behind the adoption of Tridium:

- *A large amount of third-party integration drivers*
- *A distributor model that provides open availability of the product*
- *A SDK that allows developers to customize their own integrations*

Possible conclusion: an adversary state would have statistically a good chance for a cyber attack that can impact human lives.

TOTAL RESULTS

418,653

TOP COUNTRIES

United States	418,653

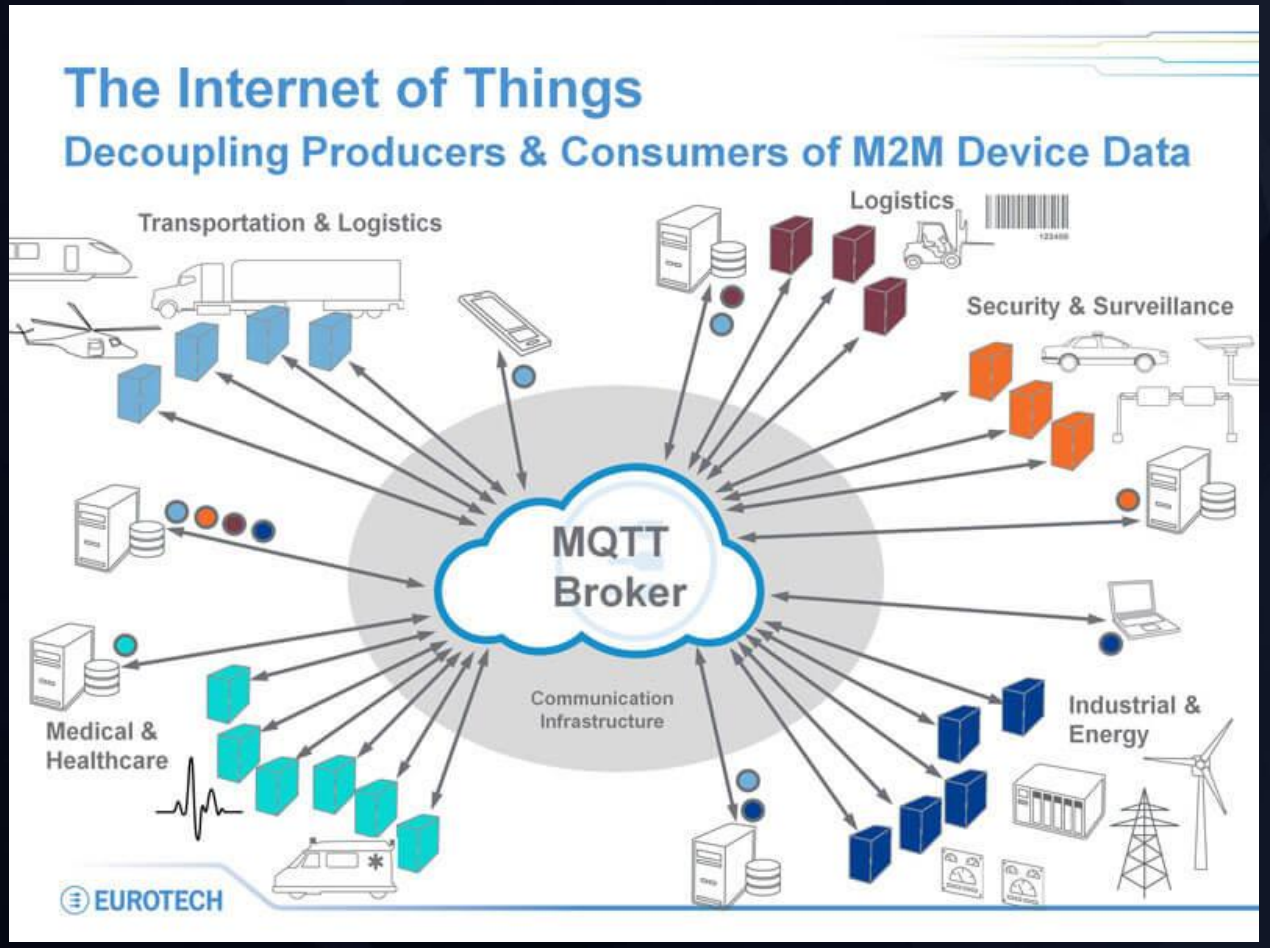
TOP CITIES

New York	9,397
Los Angeles	7,956
San Jose	5,240
Dallas	2,640
Washington	1,873

TOP SERVICES

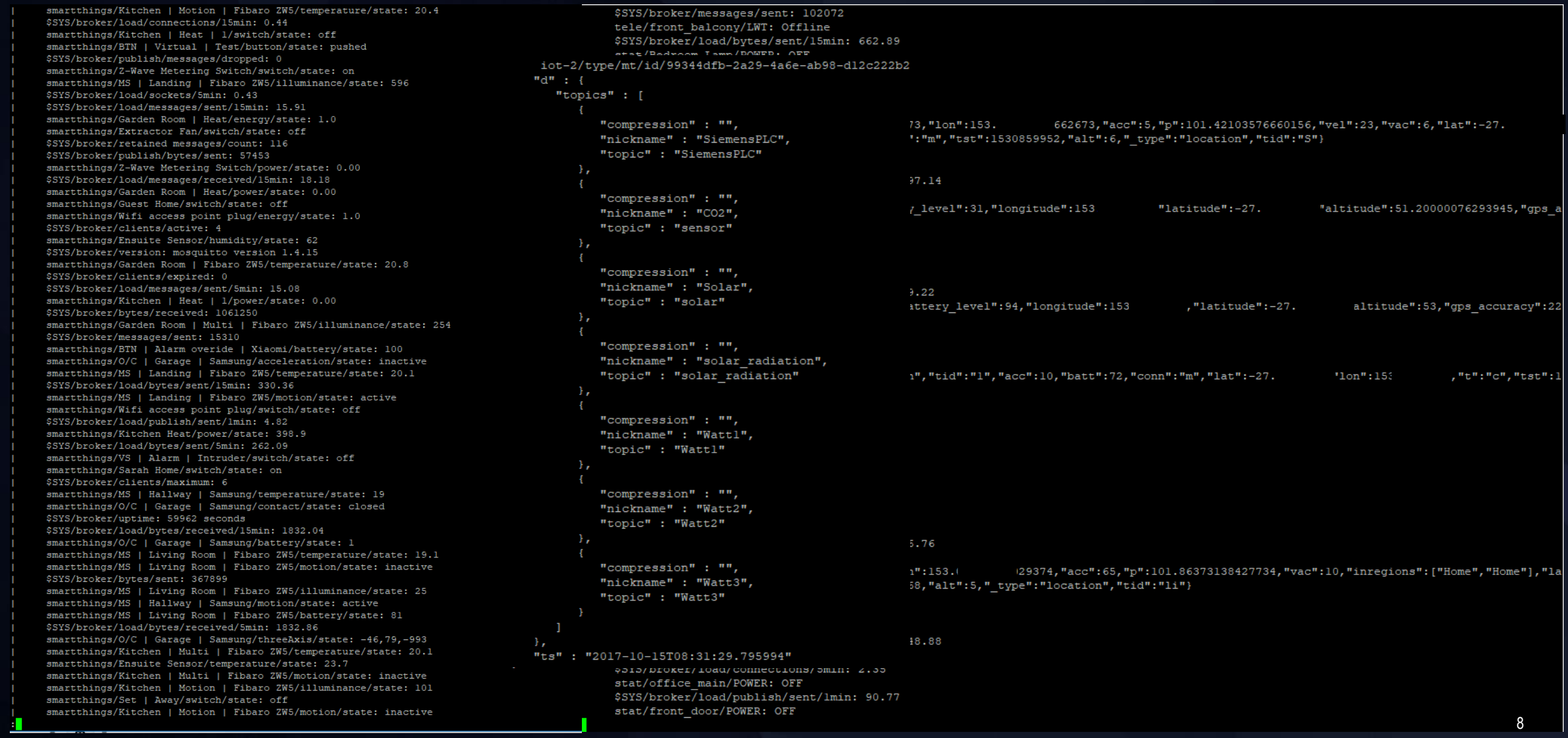
DNP3	352,168
Tridium Fox	30,545
EtherNetIP	14,605
BACnet	10,120
Tridium Fox + SSL	3,851

WHAT ABOUT US, THE NORMAL PEOPLE?

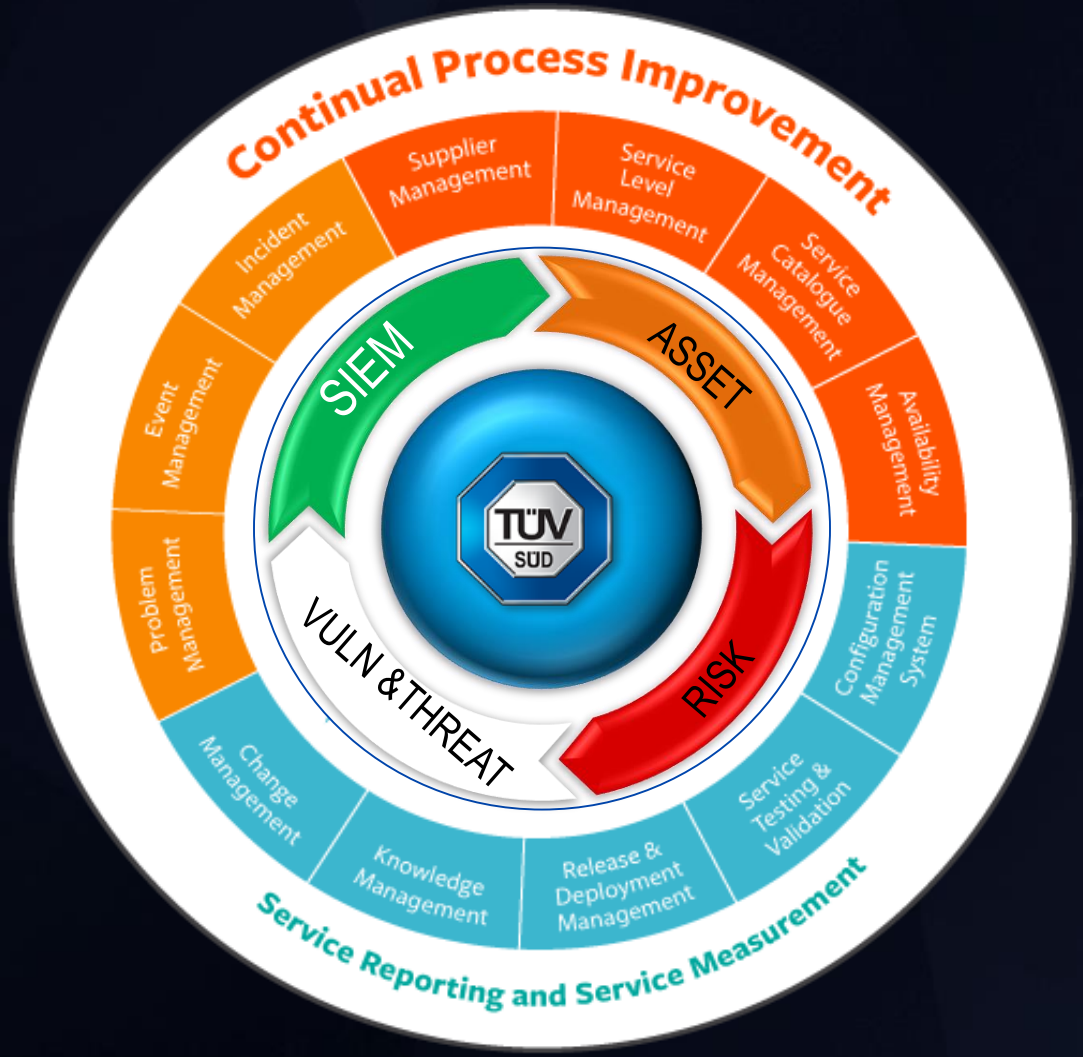


- Fact: more and more “things” get connected to Internet.
- A widespread protocol is MQTT, designed as lightweight, resilient and insecure protocol.
- Most of the devices come without long term support (firmware updates) and are produced outside NATO area.
- Limited local storage space, central management, programming knowledge and competitive pressure leave these devices orphaned.
- Toolchain and libraries used for IoT are inherently prone to security flaws (e.g. OpenSSL)
- Emergency access ports (e.g. JTAG) allow local tampering.

OVER 5 MILLION IOT GATEWAYS ON INTERNET



“If you want Peace, Prepare for War”



Enter ASD – Attack Surface Detection (Work in Progress):

- Digital footprint of an entity
- Automated and manual Red Teaming
- Device fingerprinting based on AI
- OSINT based digital reputation
- Intelligence Led Penetration Testing
- Critical asset identification
- Top management risk reports
- Customers: Industry or Government

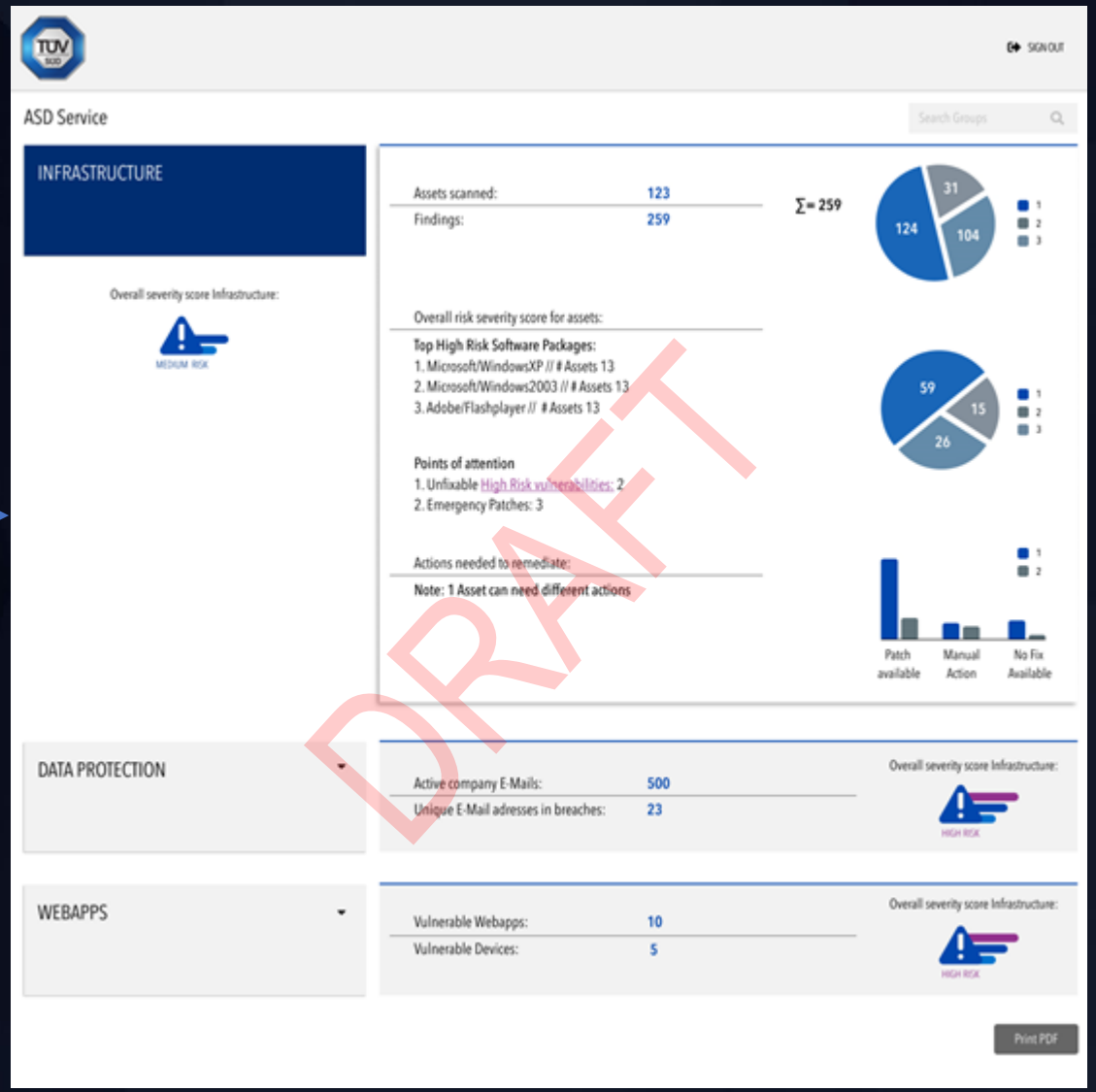
Proposed Benefits:

Increased OT/IT Efficiency: Align OT with IT and reuse customer internal processes combined with best practices (ITIL, CObIT).

Complete Risk Awareness: Best-of-breed tools and intelligence orchestrated with AI/ML to outline web, infrastructure, cloud or social engineering weaknesses.

Impartial Reports: Easy to understand updated metrics and indicators, intelligence and forecasting, targeted at customers or third parties (e.g. insurers, regulators etc).

ASD as a Trusted Service



Thank You
for Your Attention!