

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



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**.

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

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

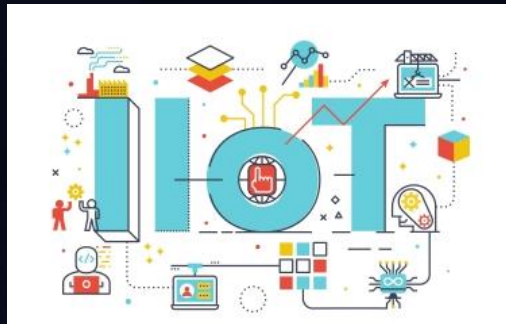
What about the digitalization of industry?



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



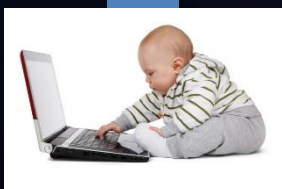
Threat level would be Moderate-to-High, as of current actors are more in the dormant state, but investing big money in such attacks.

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

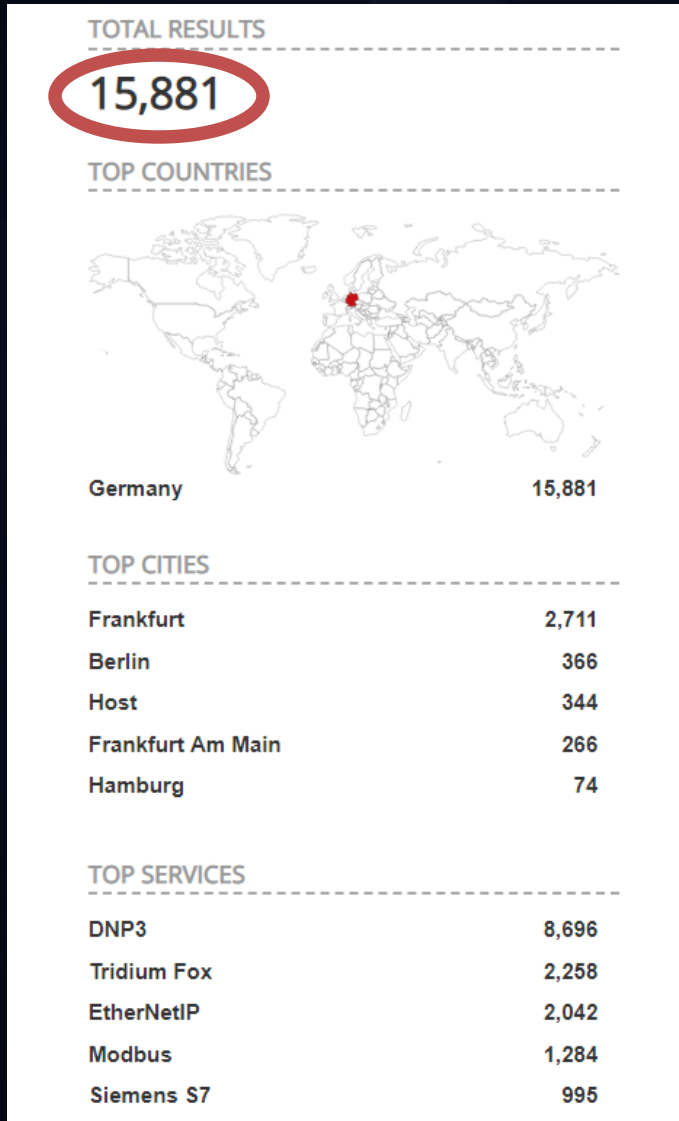
... all correlated with the careless direct connectivity of industrial devices to Internet and an increasing open source toolset.

Costs

Scale of Impact



FACTS AND FIGURES – OPEN SOURCE INTELLIGENCE



*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**.*

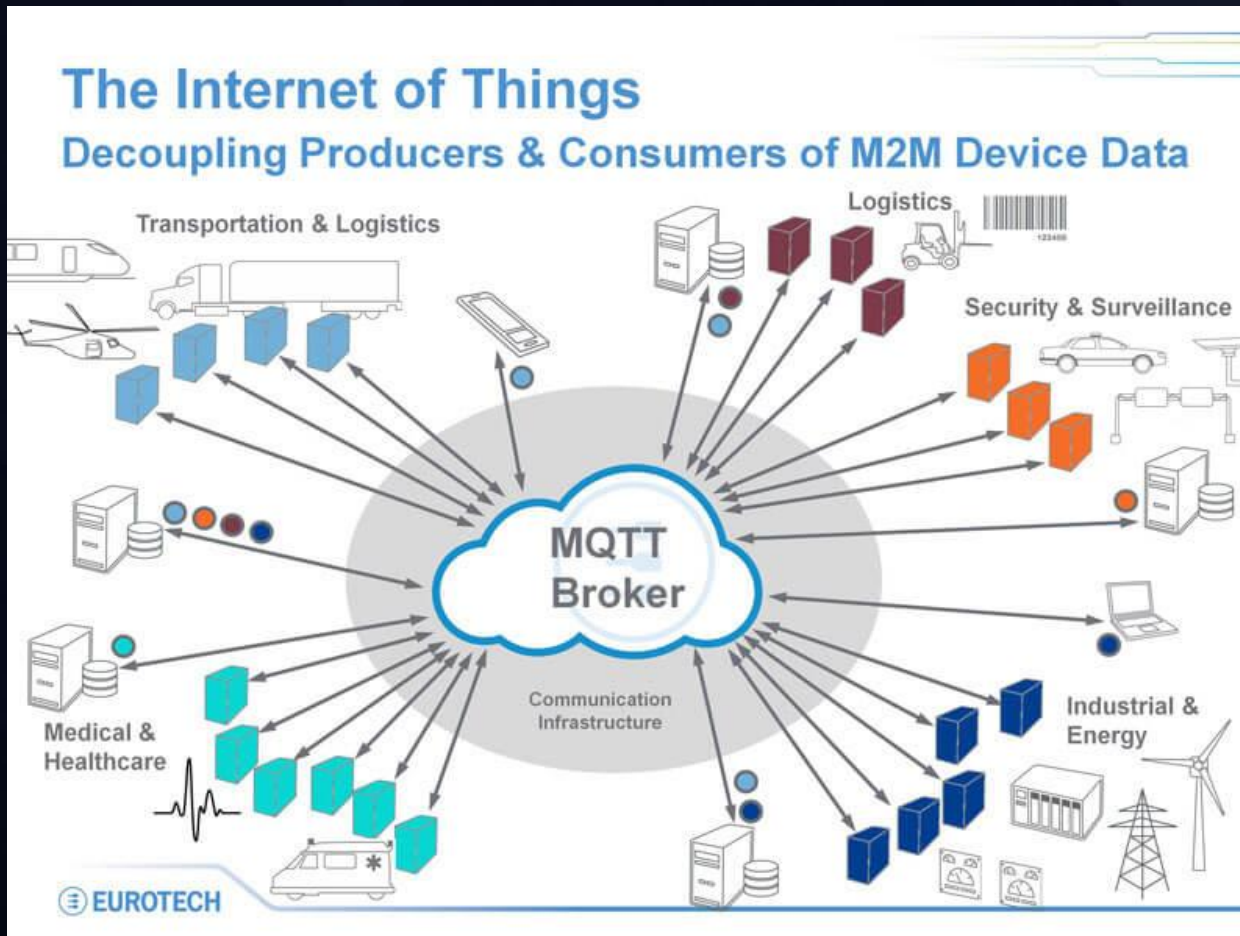
*Tridium is **the latest buzz** word in the **Building Automation** Industry. There are three driving factors behind the adoption of Tridium:*

- *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**.*



WHAT ABOUT US, THE NORMAL PEOPLE?



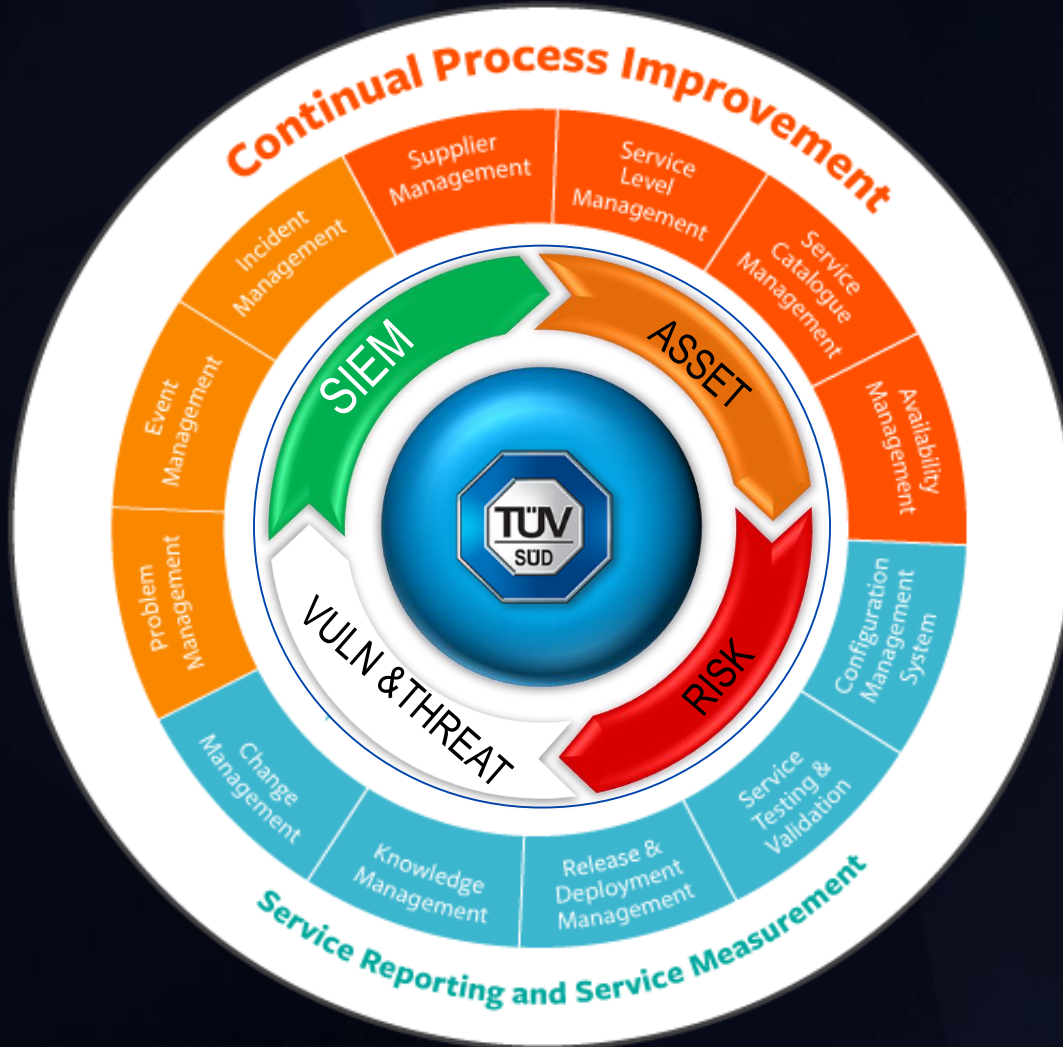
- Fact: more and more “things” get connected to Internet.
- A widespread protocol is MQTT, designed as lightweight, resilient and **insecure** protocol.
- Most of the devices come without long term support (firmware updates) and are produced outside NATO area.
- Limited local storage space, central management, 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

```
smarththings/Kitchen | Motion | Fibaro ZW5/temperature/state: 20.4
$SYS/broker/load/connections/15min: 0.44
smarththings/Kitchen | Heat | 1/switch/state: off
smarththings/BTN | Virtual | Test/button/state: pushed
$SYS/broker/publish/messages/dropped: 0
smarththings/2-Wave Metering Switch/switch/state: on
smarththings/MS | Landing | Fibaro ZW5/illuminance/state: 596
$SYS/broker/load/sockets/5min: 0.43
$SYS/broker/load/messages/sent/15min: 15.91
smarththings/Garden Room | Heat/energy/state: 1.0
smarththings/Extractor Fan/switch/state: off
$SYS/broker/retained messages/count: 116
$SYS/broker/publish/bytes/sent: 57453
smarththings/2-Wave Metering Switch/power/state: 0.00
$SYS/broker/load/messages/received/15min: 18.18
smarththings/Garden Room | Heat/power/state: 0.00
smarththings/Guest Home/switch/state: off
smarththings/Wifi access point plug/energy/state: 1.0
$SYS/broker/clients/active: 4
smarththings/Ensuite Sensor/humidity/state: 62
$SYS/broker/version: mosquito version 1.4.15
smarththings/Garden Room | Fibaro ZW5/temperature/state: 20.8
$SYS/broker/clients/expired: 0
$SYS/broker/load/messages/sent/5min: 15.08
smarththings/Kitchen | Heat | 1/power/state: 0.00
$SYS/broker/bytes/received: 1061250
smarththings/Garden Room | Multi | Fibaro ZW5/illuminance/state: 254
$SYS/broker/messages/sent: 15310
smarththings/BTN | Alarm override | Xiaomi/battery/state: 100
smarththings/O/C | Garage | Samsung/acceleration/state: inactive
smarththings/MS | Landing | Fibaro ZW5/temperature/state: 20.1
$SYS/broker/load/bytes/sent/15min: 330.36
smarththings/MS | Landing | Fibaro ZW5/motion/state: active
smarththings/Wifi access point plug/switch/state: off
$SYS/broker/load/publish/sent/1min: 4.82
smarththings/Kitchen Heat/power/state: 398.9
$SYS/broker/load/bytes/sent/5min: 262.09
smarththings/VS | Alarm | Intruder/switch/state: off
smarththings/Sarah Home/switch/state: on
$SYS/broker/clients/maximum: 6
smarththings/MS | Hallway | Samsung/temperature/state: 19
smarththings/O/C | Garage | Samsung/contact/state: closed
$SYS/broker/uptime: 59962 seconds
$SYS/broker/load/bytes/received/15min: 1832.04
smarththings/O/C | Garage | Samsung/battery/state: 1
smarththings/MS | Living Room | Fibaro ZW5/temperature/state: 19.1
smarththings/MS | Living Room | Fibaro ZW5/motion/state: inactive
$SYS/broker/publish/bytes/sent: 367899
smarththings/MS | Living Room | Fibaro ZW5/illuminance/state: 25
smarththings/MS | Hallway | Samsung/motion/state: active
smarththings/MS | Living Room | Fibaro ZW5/battery/state: 81
$SYS/broker/load/bytes/received/5min: 1832.86
smarththings/O/C | Garage | Samsung/threeAxis/state: -46,79,-993
smarththings/Kitchen | Multi | Fibaro ZW5/temperature/state: 20.1
smarththings/Ensuite Sensor/temperature/state: 23.7
smarththings/Kitchen | Multi | Fibaro ZW5/motion/state: inactive
smarththings/Kitchen | Motion | Fibaro ZW5/illuminance/state: 101
smarththings/Set | Away/switch/state: off
smarththings/Kitchen | Motion | Fibaro ZW5/motion/state: inactive
```

```
$SYS/broker/messages/sent: 102072
tele/front_balcony/LWT: Offline
$SYS/broker/load/bytes/sent/15min: 662.89
state/Balcony Room/POWER: OFF
iot-2/type/mt/id/99344dfb-2a29-4a6e-ab98-d12c222b2
"d" : {
  "topics" : [
    {
      "compression" : "",
      "nickname" : "SiemensPLC",
      "topic" : "SiemensPLC"
    },
    {
      "compression" : "",
      "nickname" : "CO2",
      "topic" : "sensor"
    },
    {
      "compression" : "",
      "nickname" : "Solar",
      "topic" : "solar"
    },
    {
      "compression" : "",
      "nickname" : "solar_radiation",
      "topic" : "solar_radiation"
    },
    {
      "compression" : "",
      "nickname" : "Watt1",
      "topic" : "Watt1"
    },
    {
      "compression" : "",
      "nickname" : "Watt2",
      "topic" : "Watt2"
    },
    {
      "compression" : "",
      "nickname" : "Watt3",
      "topic" : "Watt3"
    }
  ],
  "ts" : "2017-10-15T08:31:29.795994"
  $SYS/broker/load/connections/5min: 4.33
  stat/office main/POWER: OFF
  $SYS/broker/load/publish/sent/1min: 90.77
  stat/front_door/POWER: OFF
73,"lon":153. 662673,"acc":5,"p":101.42103576660156,"vel":23,"vac":6,"lat":-27.
": "m","tst":1530859952,"alt":6,"_type": "location","tid": "S"}
37.14
/_level":31,"longitude":153 "latitude":-27. "altitude":51.20000076293945,"gps_a
",
battery_level":94,"longitude":153 ,"latitude":-27. altitude":53,"gps_accuracy":22
1,"tid": "1","acc":10,"batt":72,"conn": "m","lat":-27. 'lon":153 ,"t": "c","tst":1
1":153.0 129374,"acc":65,"p":101.86373138427734,"vac":10,"inregions":["Home","Home"],"la
38,"alt":5,"_type": "location","tid": "1i"}
18.88
```


“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

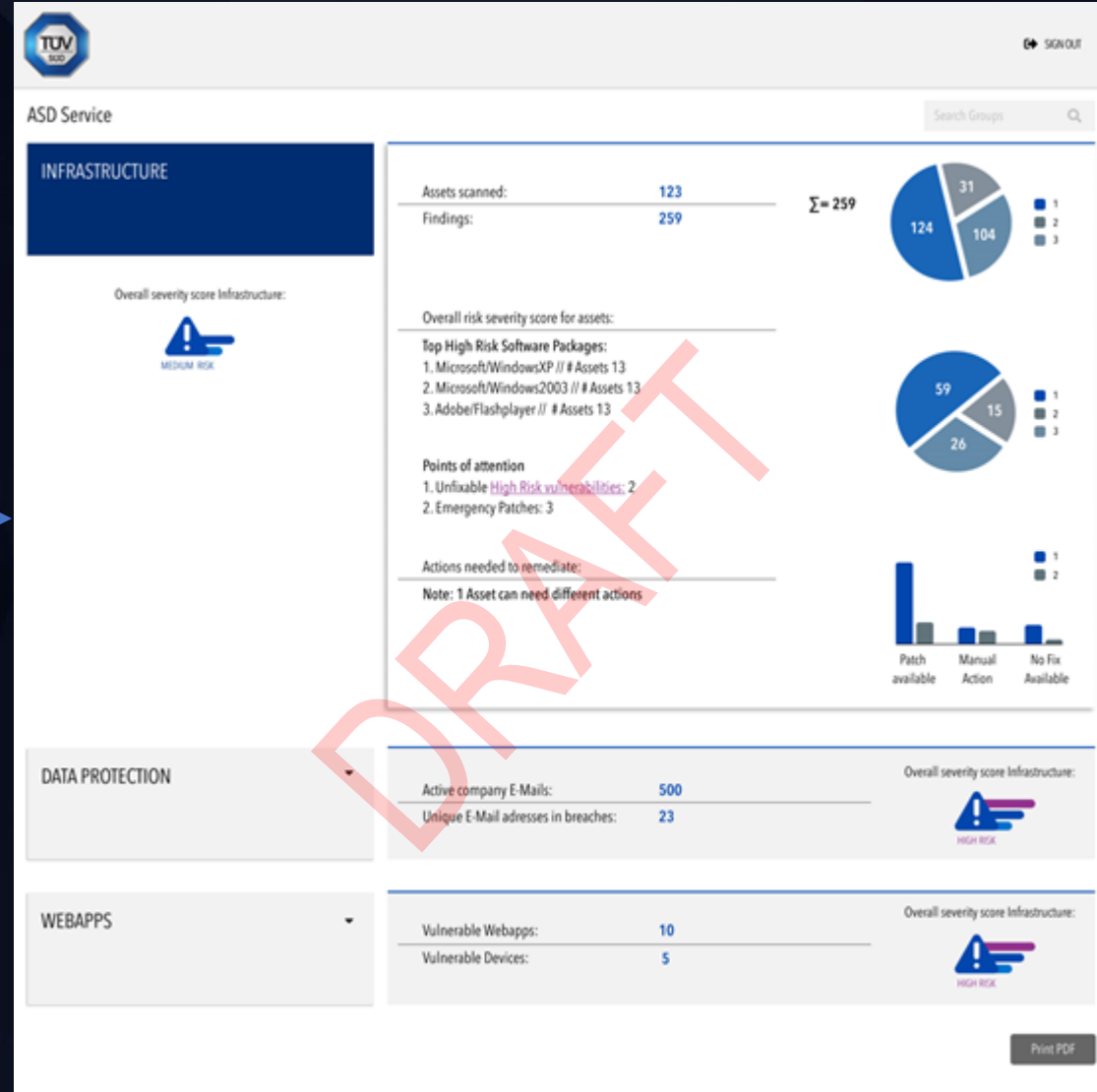
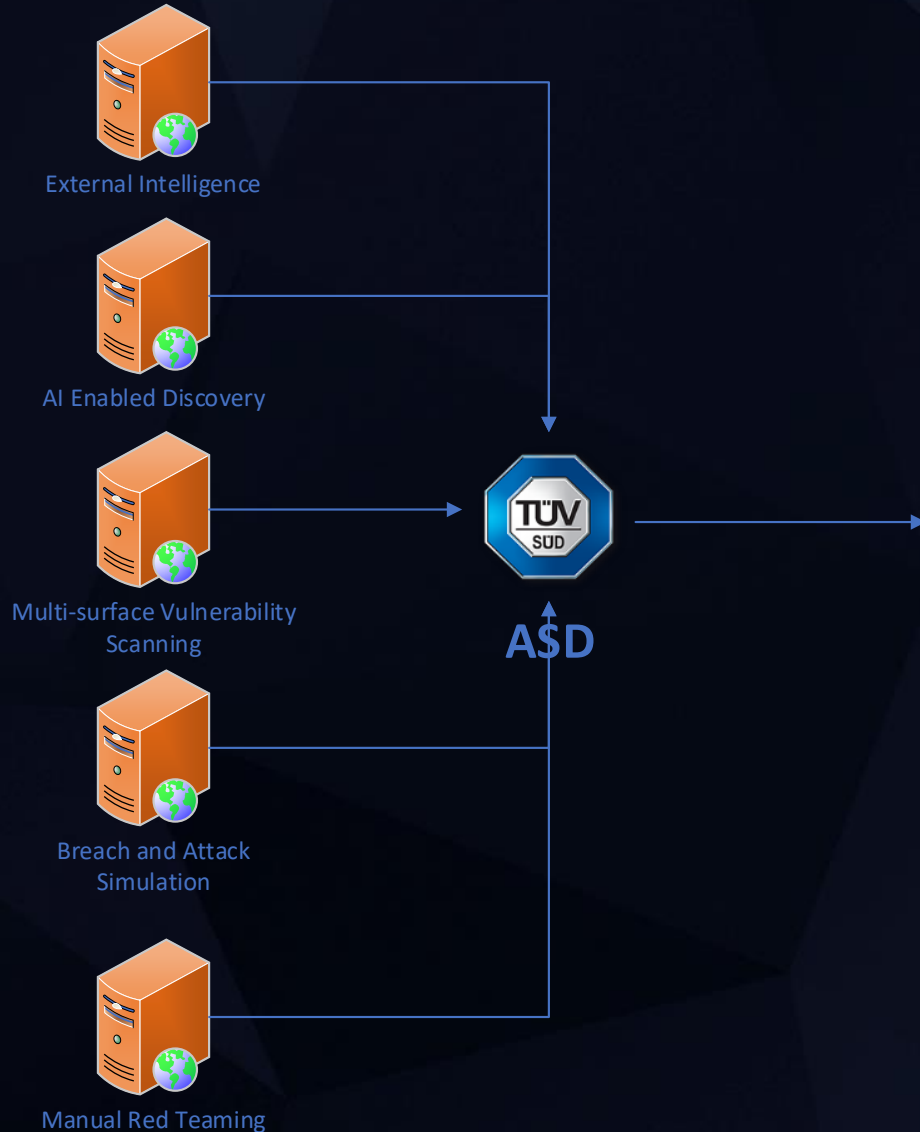
Proposed Benefits:

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!