# Cyberangriffe auf Industrieanlagen

## Panikmache oder Realität?

Udo Schneider
@udo_schneider
IoT Security Evangelist Europe

# IT: Security ist unterbewertet!

„Die haben doch keine Ahnung von Sicherheit!“

„Immer dies Ausrede ‚Verfügbarkeit‘“

„Nicht mal die Basics werden gemacht!“

„Windows XP? Geht ja gar nicht!“

„Haben die noch nie was von Normen gehört?“

**„Angriffe jederzeit! Wieso tut keiner was?“**

**„Lernen durch Schmerz!“**

# **Produktion:** Security ist überbewertet!

„Die haben doch keine Ahnung von Sicherheit!“

„Patchen in der Produktion? Spinnen die denn?“

„Dann müssen wir die Risikobewertung von vorne machen!“

„Update auf Windows 10? Wir haben noch DOS!“

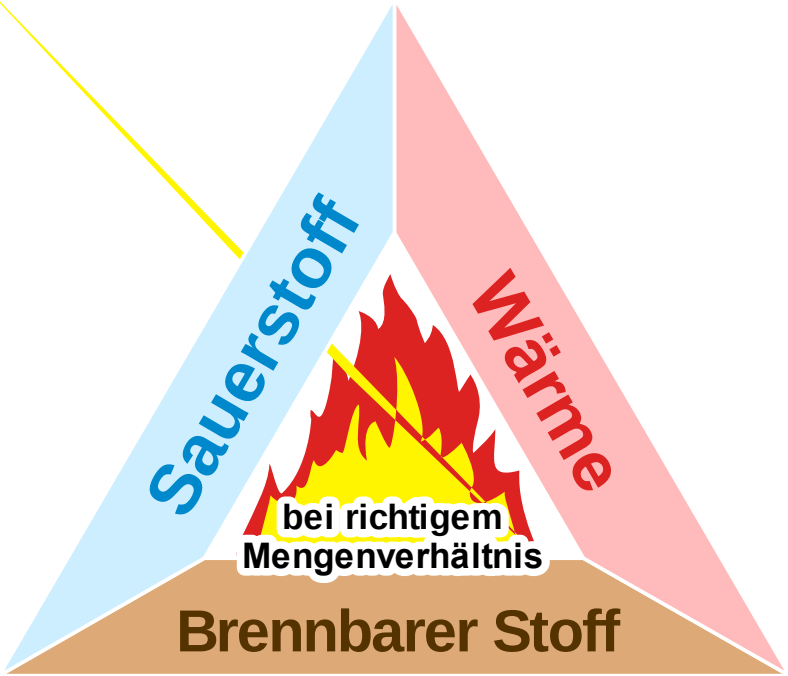
„Haben die noch nie was von Normen gehört?“

**„Wer soll uns schon angreifen…“**

**„Alles nur Panikmache!“**

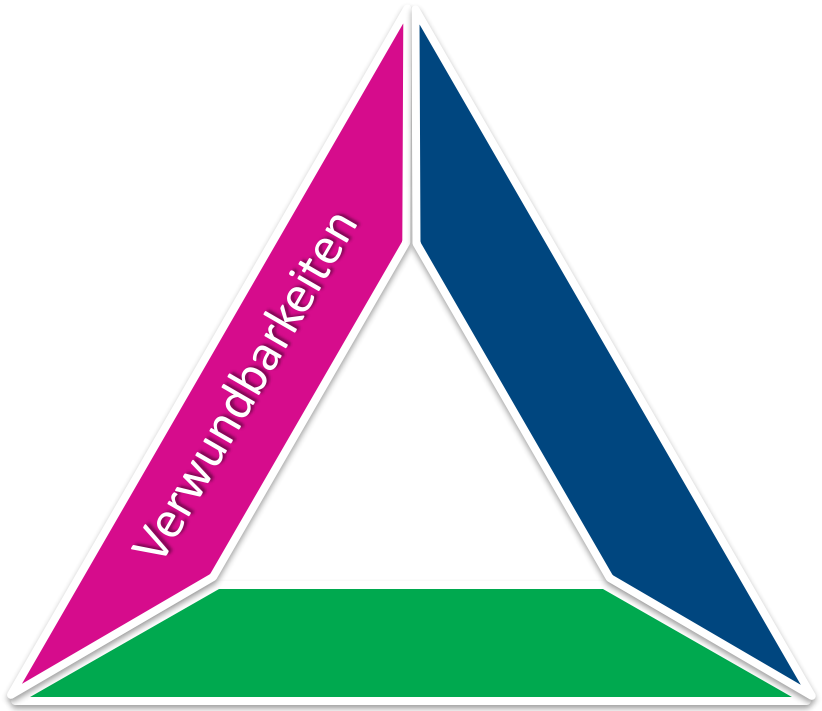
# DON’T PANIC!

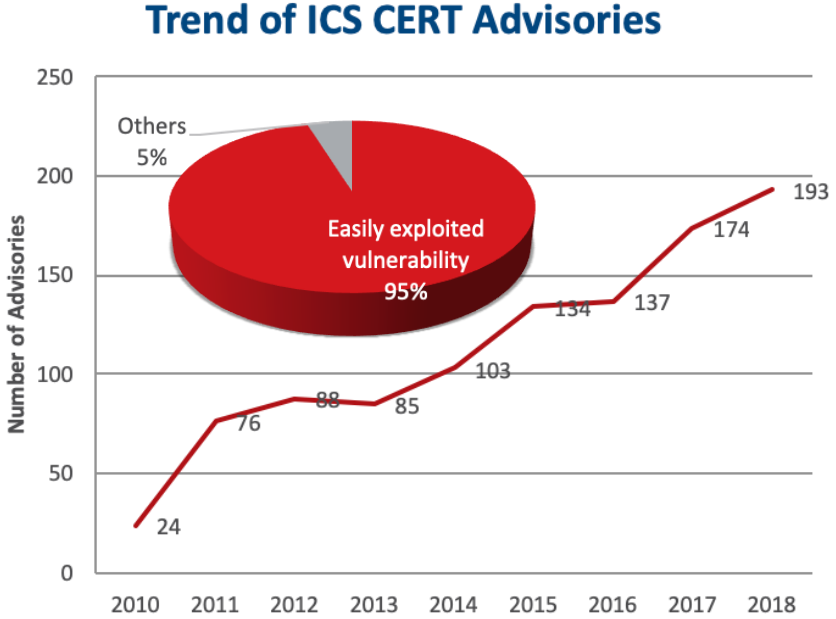
# Feuerdreieck



# (I)IoT Dreieck

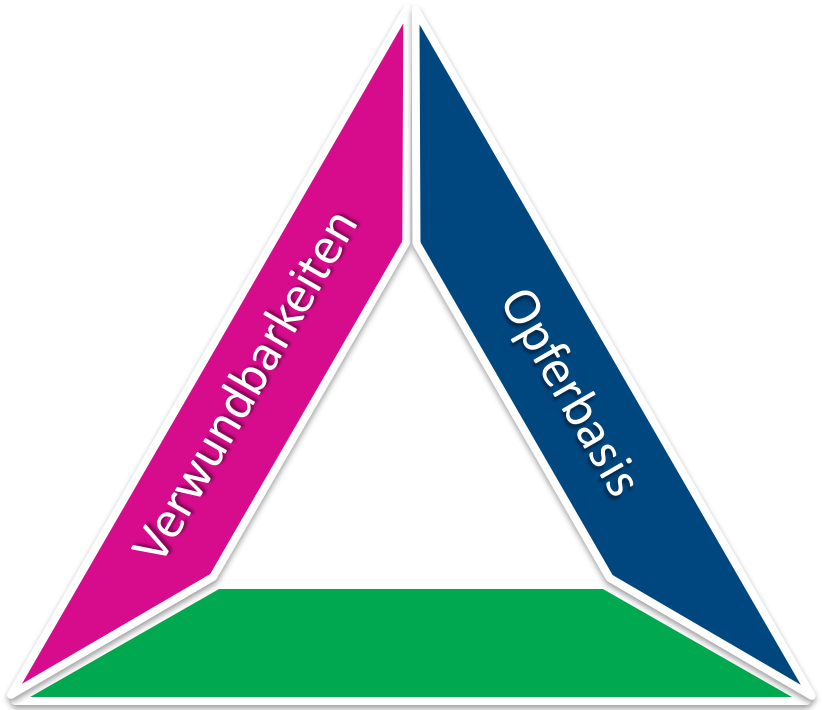
# (I)IoT Dreieck – Verwundbarkeiten



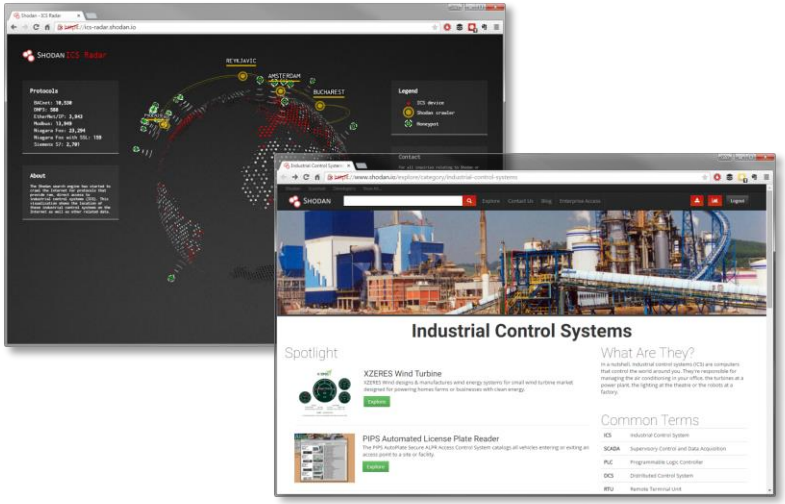




Source: (I)IoT-CERT https://ics-cert.us-cert.gov/

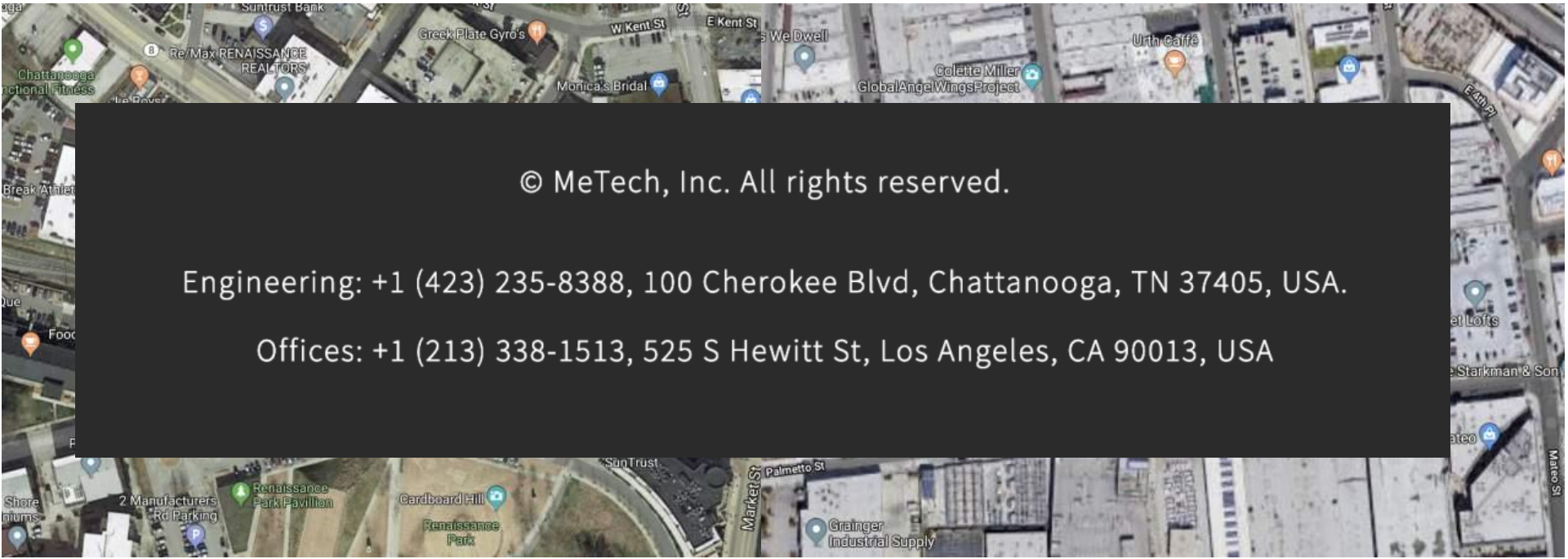
# (I)IoT Dreieck – Opferbasis




- shodan.io, Censys, ZoomEye …



# “Die Firma”






Engineering: +1 (423) 235-8388, 100 Cherokee Blvd, Chattanooga, TN 37405, USA.

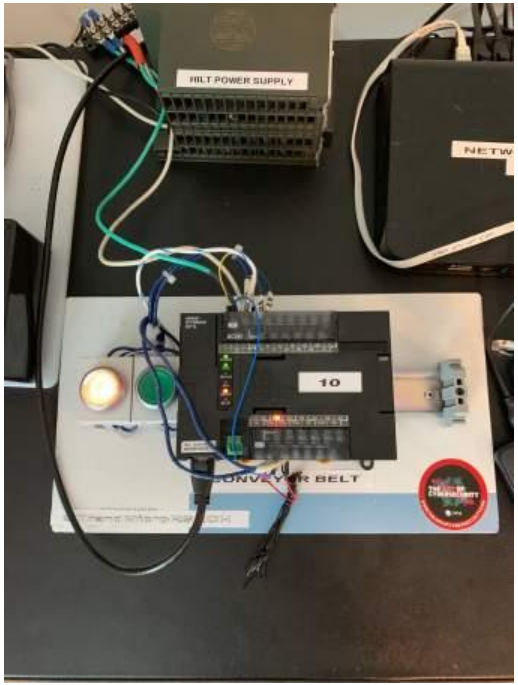
Offices: +1 (213) 338-1513, 525 S Hewitt St, Los Angeles, CA 90013, USA

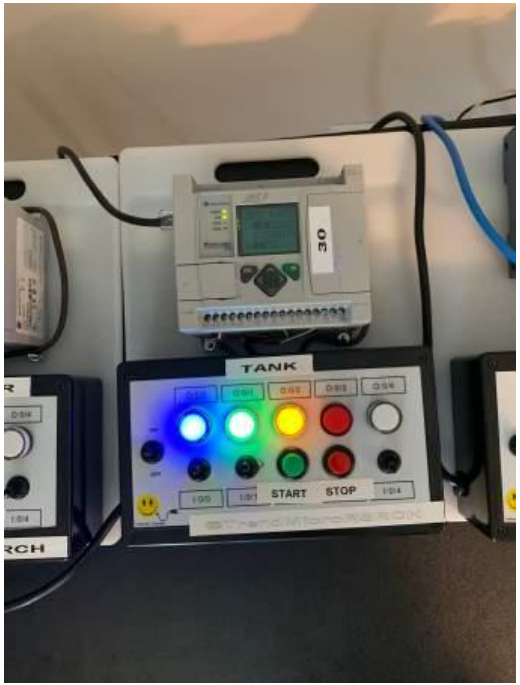

BDC
HAMILTON COUNTY
BUSINESS DEVELOPMENT CENTER

# Mitarbeiter

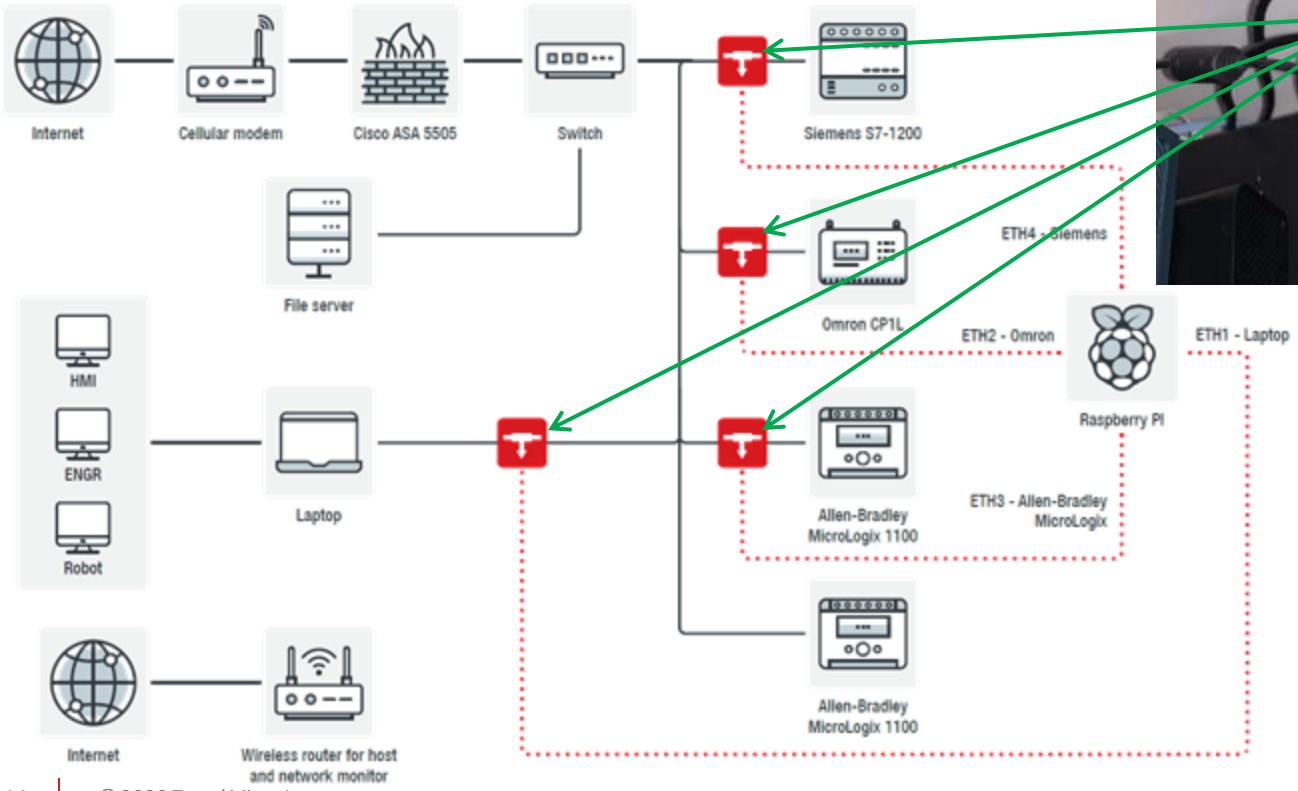

Fake faces generated from https://thispersondoesnotexist.com/

# “Echte” Hardware – SPS, HMI, Digital Twin …

# Systemüberwachung

# Zu gut für einen Honeypot?

**Friday, August 16, 2019 at 3:26:00 PM Eastern Daylight Time**

**Subject:** The most elaborate honeypot.
**Date:** Friday, August 16, 2019 at 3:21:06 PM Eastern Daylight Time
**From:** Dan Tentler
**To:** Stephen Hilt (RD-US), [redacted]
**CC:** [redacted]

Hey everyone!

I wanted to get everyone on the same thread [redacted]

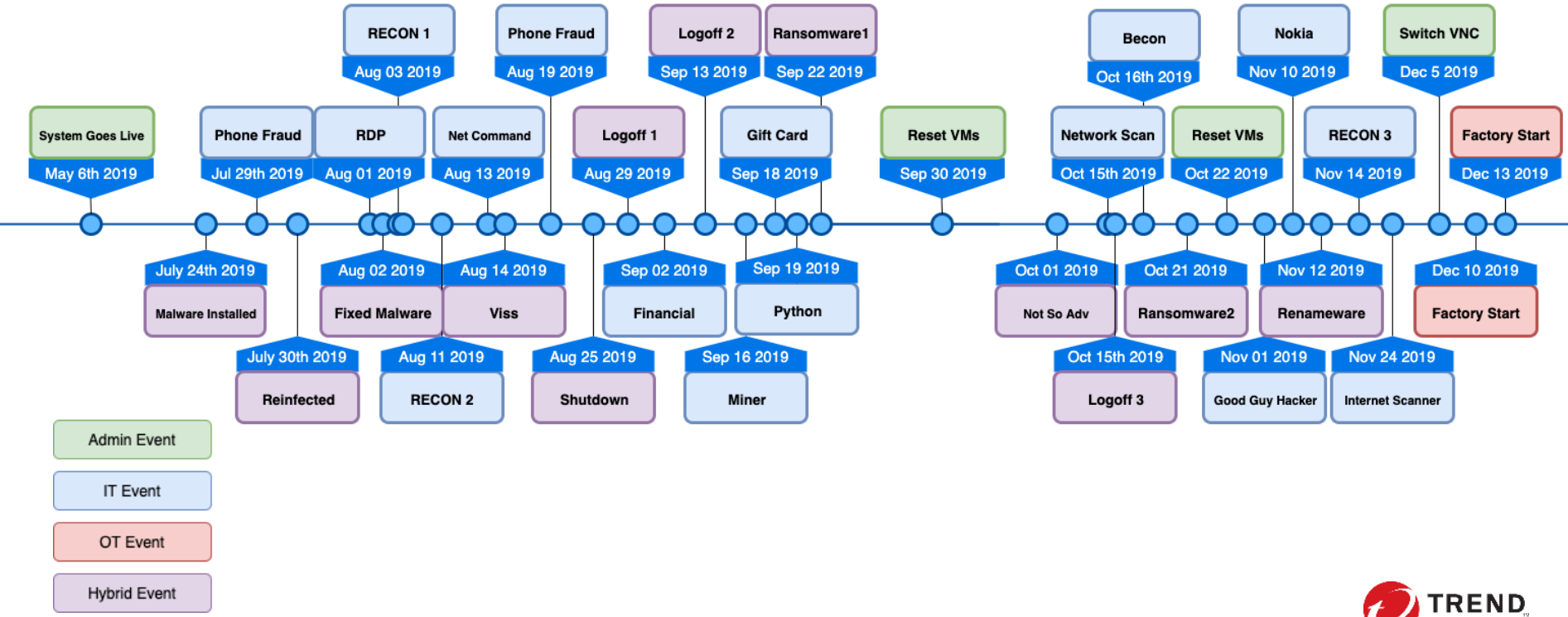
[redacted]

[redacted]stand-down efforts to track down this [redacted]

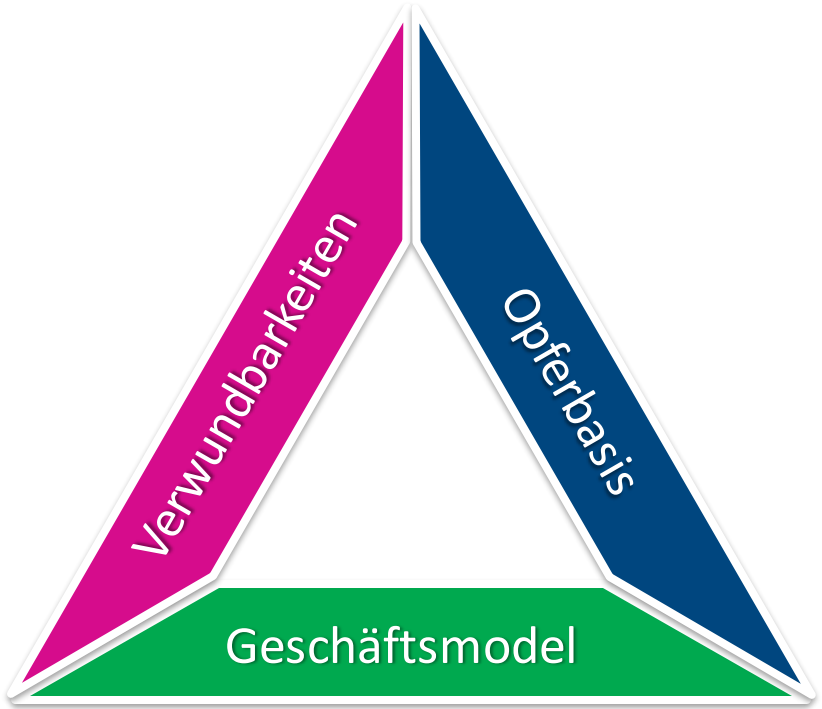
[redacted]

-Dan

# Was ist passiert?



# (I)IoT Dreieck – Geschäftsmodel!!!




- „Historische“ Beispiele:
  - SPAM
  - Ransomware
- IIoT spezifische Angriffe?

# Zusammenfassung

- Keine Panikmache!
  - … aber auch nicht unendlich viel Zeit!
- Zusammenarbeit IT/OT
  - Nur zusammen schaffen wir es!
- Passende IT Security
  - IEC62443
  - IEC TR 63069

# Fake Company, Real Threats

## Logs From a Smart Factory Honeypot


https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/fake-company-real-threats-logs-from-a-smart-factory-honeypot


TREND MICRO
THE ART OF CYBERSECURITY
Trend Micro deployment shifts over time—from on-premises to SaaS-based solutions. **Created with real data by artist Stefanie Posavec.**