

# SECURING THE FUTURE

Cyber Resilience Strategies for  
Emerging Technologies

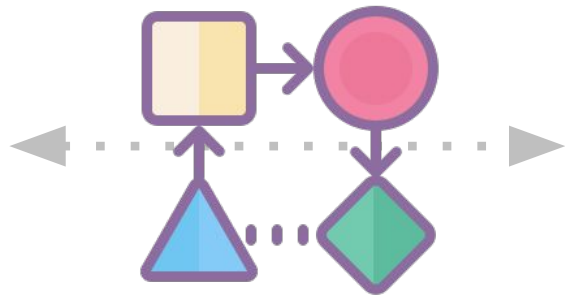
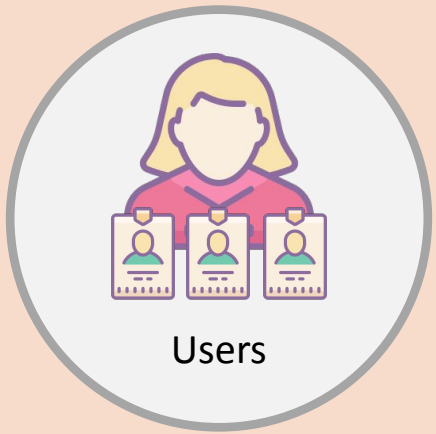
Rik Ferguson  
VP Security Intelligence  
[@rik\\_ferguson](#)



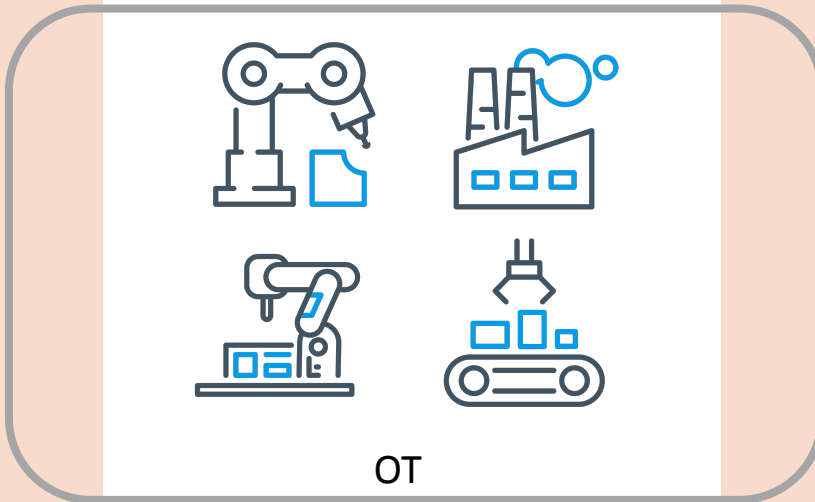
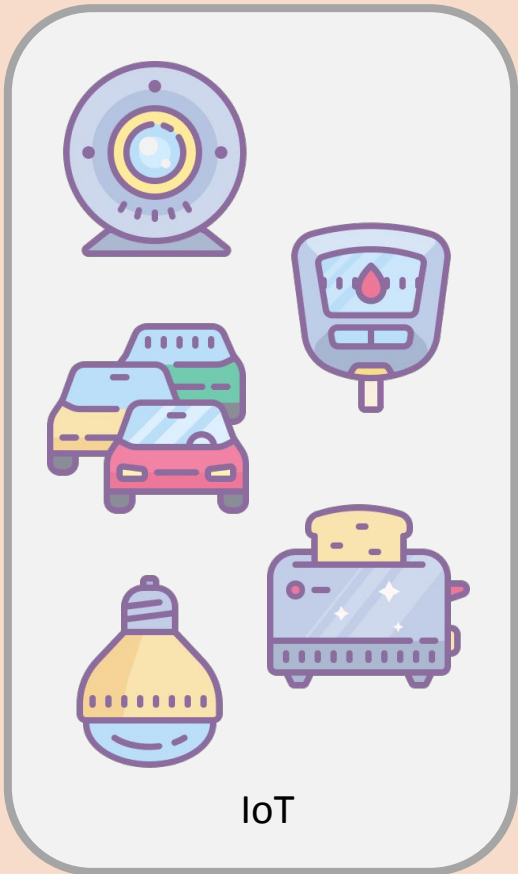
# Drivers of Change







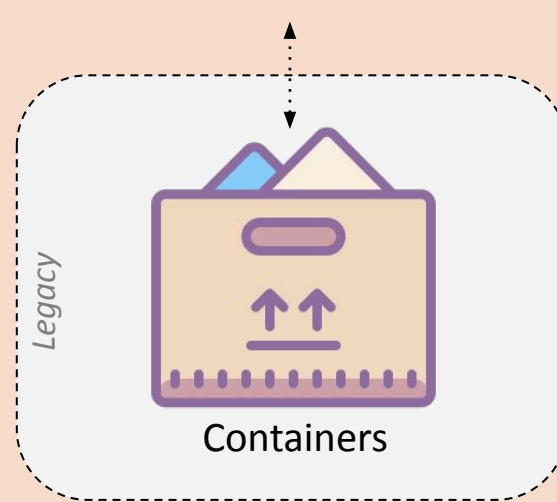
Business Process



Serverless



AI / ML



Mountain of Data

# Changing Threat Model with IoT

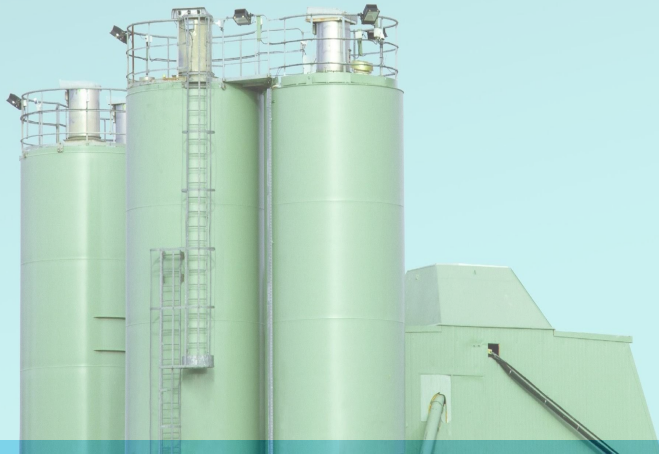


Image: Engadget

# OT Security Challenges

## ICS/OT vulnerabilities

- 2,010 ICS/OT vulnerability advisories in 2023.
- 27% of advisories had no patch, of those 18% had no mitigation either!



## Operational technology

- Rarely managed by integrated security teams.
- Limited to zero visibility of assets.



## Industrial Control Systems

- Not designed for connectivity.
- Insecure by design.
- Supply chain weakness.



# The riskiest devices in 2024



	IT	IoT	OT	IoMT
1	Router	Network Attached Storage (NAS)	Uninterruptible Power Supply (UPS)	Medical Information System
2	Wireless Access Point	VoIP	Distributed Control System (DCS)	Electrocardiograph
3	Server	IP Camera	Programmable Logic Controller (PLC)	DICOM Workstation
4	Computer	Network Video Recorder (NVR)	Robotics	Picture archiving and communication system (PACS)
5	Hypervisor	Printer	Building Management System (BMS)	Medication Dispensing System

# Riskiest IT devices



#	Device
1	Router
2	Wireless Access Point
3	Server
4	Computer
5	Hypervisor



## ▶ Two main groups

- **Endpoints** – computers, servers and hypervisors
- **Network infrastructure** – routers, wireless access points

## ▶ Network infrastructure surpassed endpoints

- Often exposed online and have dangerous open ports
- Targeted by APTs and cybercriminals
- Several exploits observed since 2022 targeted security appliances from major security vendors

## ▶ Endpoints remain risky

- Entry points for phishing
- Unpatched systems and applications
- Hypervisors are an often unmanaged type of server targeted by ransomware



# Riskiest IoT devices



#	Device
1	Network Attached Storage (NAS)
2	VoIP
3	IP Camera
4	Network Video Recorder (NVR)
5	Printer



## ▶ Usual suspects: IP cameras, printers and VoIP

- Most commonly exposed online
- Historically targeted by APTs. Examples:
  - Chinese attacks on Indian grid – 2022
  - Russian attacks on corporate printers and VoIP
- Typically misconfigured with exposed services and default credentials
- NAS has become a new standard target for ransomware, more than half a dozen families in the past couple of years

## ▶ New entry: NVR

- Sit alongside IP cameras on the network and have similar vulnerabilities

# Riskiest OT devices



#	Device
1	Uninterruptible Power Supply (UPS)
2	Distributed Control System (DCS)
3	Programmable Logic Controller (PLC)
4	Robotics
5	Building Management System (BMS)



- ▶ **UPSs present in many data centers and other facilities with default credentials**
- ▶ **Critical, insecure-by-design, and often targeted PLCs and DCSs**
  - See OT:ICEFALL for critical vulnerabilities
  - See hacktivist report Dec/2022 for examples of attacks
- ▶ **Building management systems** are everywhere and have also been targeted by sophisticated attackers
- ▶ **Robotics**
  - Use of robots quickly increasing in with “smart factories” – 4 million robots worldwide in 2023
  - Often legacy security issues similar to other OT

# Riskiest IoMT devices



#	Device
1	Medical Information System
2	Electrocardiograph
3	DICOM Workstation
4	Picture archiving and communication system (PACS)
5	Medication Dispensing System



- ▶ **Medical information systems** store and manage critical patient data
- ▶ **DICOM and PACS** used in medical imaging and often exposed online
- ▶ **Medication dispensing** have decades-old vulnerabilities and is the sixth most vulnerable device type overall in our study (not just in IoMT)

# XIoT Attacks

CISCO IOS-XE Critical Vulnerability



Municipal Water Authority of Aliquippa

# ESG

Barracuda  
Email Security Gateway


# Consequences of war

**GhostSec** @ghost\_s3curity

We, #GhostSec declare that we were infact responsible for the "mysterious" emergency shutdown.

We now state that the ICS attack was successfully executed with 0 casualties in the actual explosion due to our proper timing while preforming our attacks.

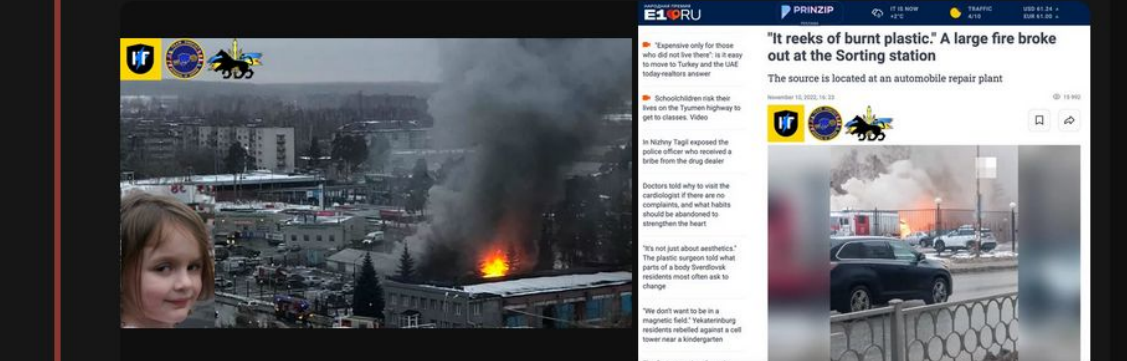
[mirror.co.uk/news/world-new...](https://mirror.co.uk/news/world-new...)



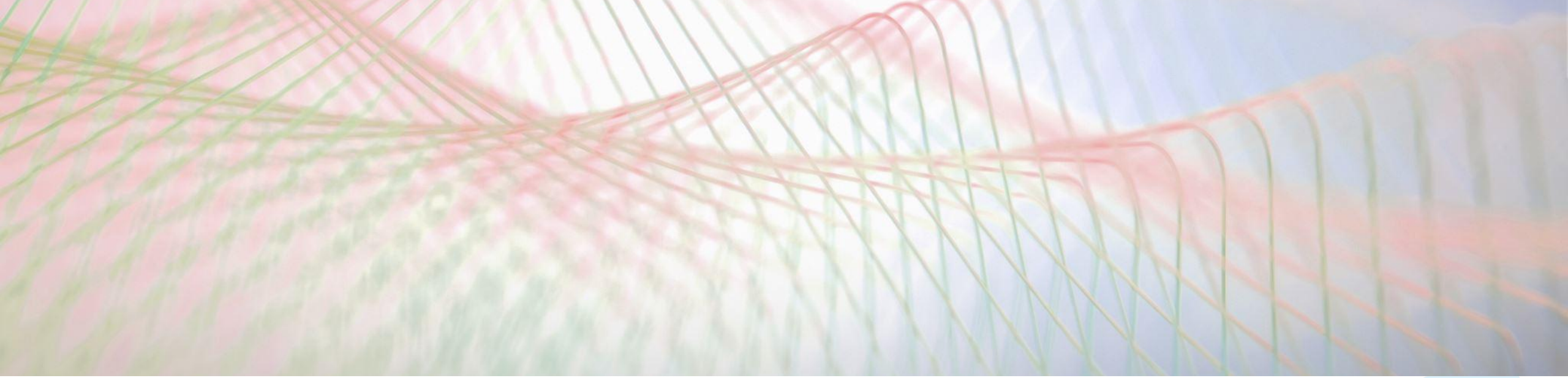
1:14 AM · Jul 20, 2022 · Twitter for Android

**Thraxman** @ThraxmanOneFist Nov 13

We attacked their #SCADA/#ICS, demolishing 8 expensive Schneider M258s #PLC, w/2400 channels & 16 DOF each for complex machines. This led to a fire that erased an entire workshop building, and took 13 trucks to extinguish! According to locals the first 3 arrived without water 😂 2/



0:01 19.4K views

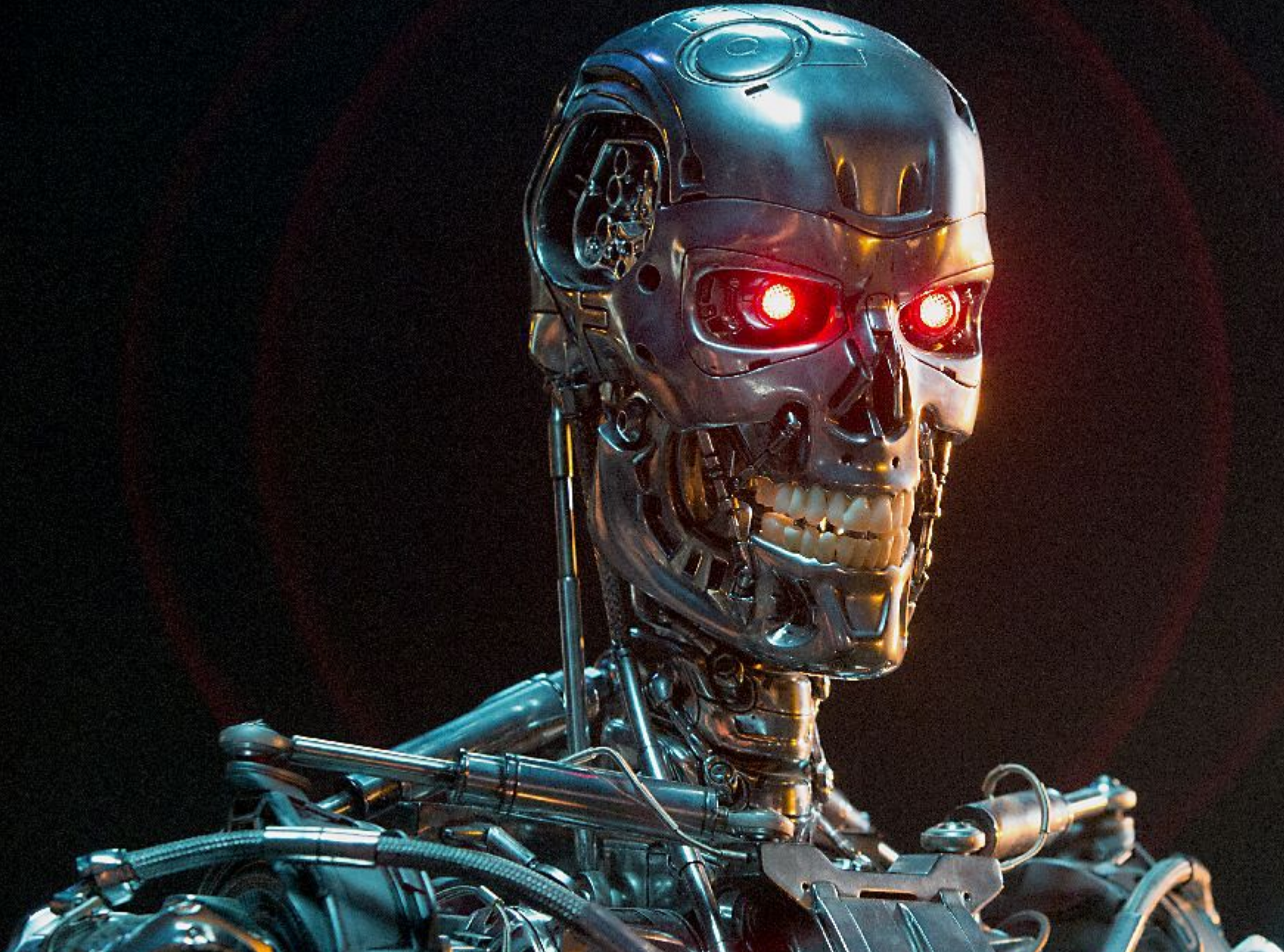


## Areas of concern

- ▶ Volatile & Software-defined networks
- ▶ M2M/MIoT (new subscriber type) (IAM?)
- ▶ Vast amounts of data
- ▶ Steep learning curve
- ▶ Exponentially greater attack surface
- ▶ Legacy technology & architecture integration
- ▶ Skills gap & security politics









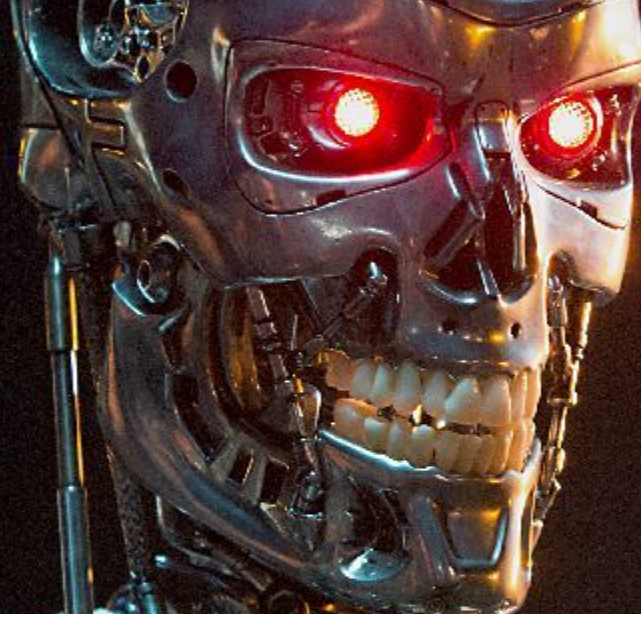


**The greatest challenge facing humanity  
over the next decade is the ability to tell  
fact from fiction and reality from fantasy**









## Areas of concern

- ▶ Faster more effective attacks
- ▶ Context-aware malicious code
- ▶ Adaptive impersonation of systems and people
- ▶ Inability to know what is real

# Let's put that together



# Key Takeaways



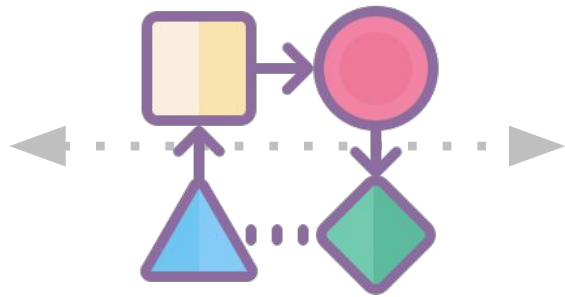
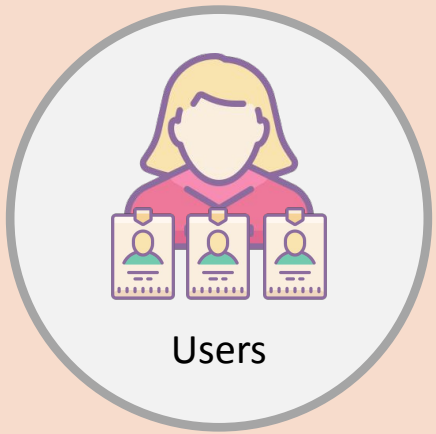
**Attack surface increasing:** IoT, OT, network infrastructure, virtualization servers, security appliances, medical devices, ...



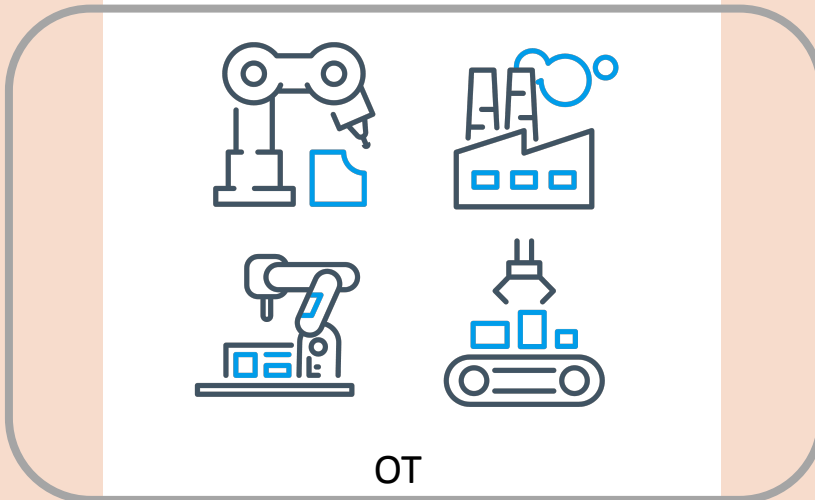
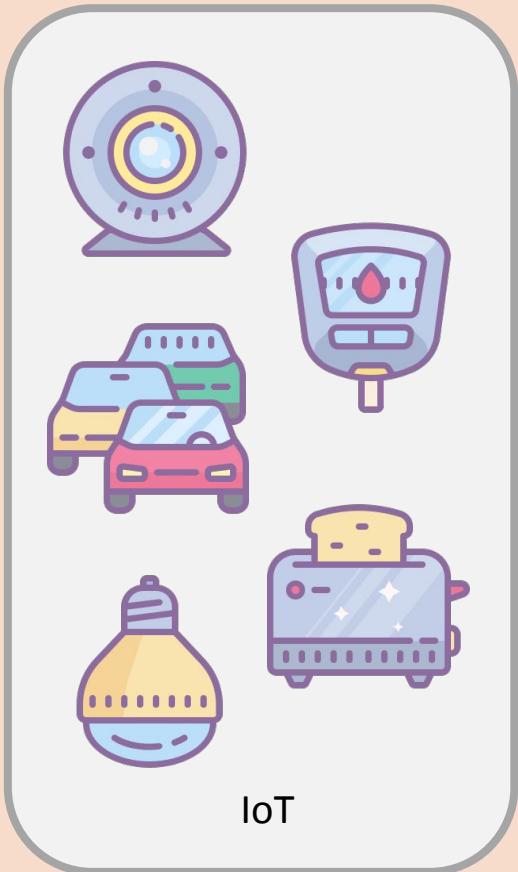
Cybercrime, hacktivists and state-sponsored actors are all leveraging this increased attack surface



**Risk mitigation should prioritize the increased attack surface**



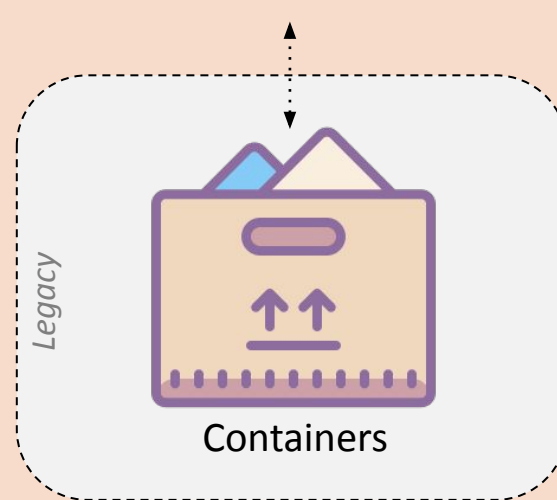
Business Process



Serverless



AI / ML



Mountain of Data



# Cybersecurity Reality



# Cybersecurity, the Department of No?

Know your threat

Know your e

Know your

Know yo

Know



Thank you.





See it. Secure it. Assure it.

