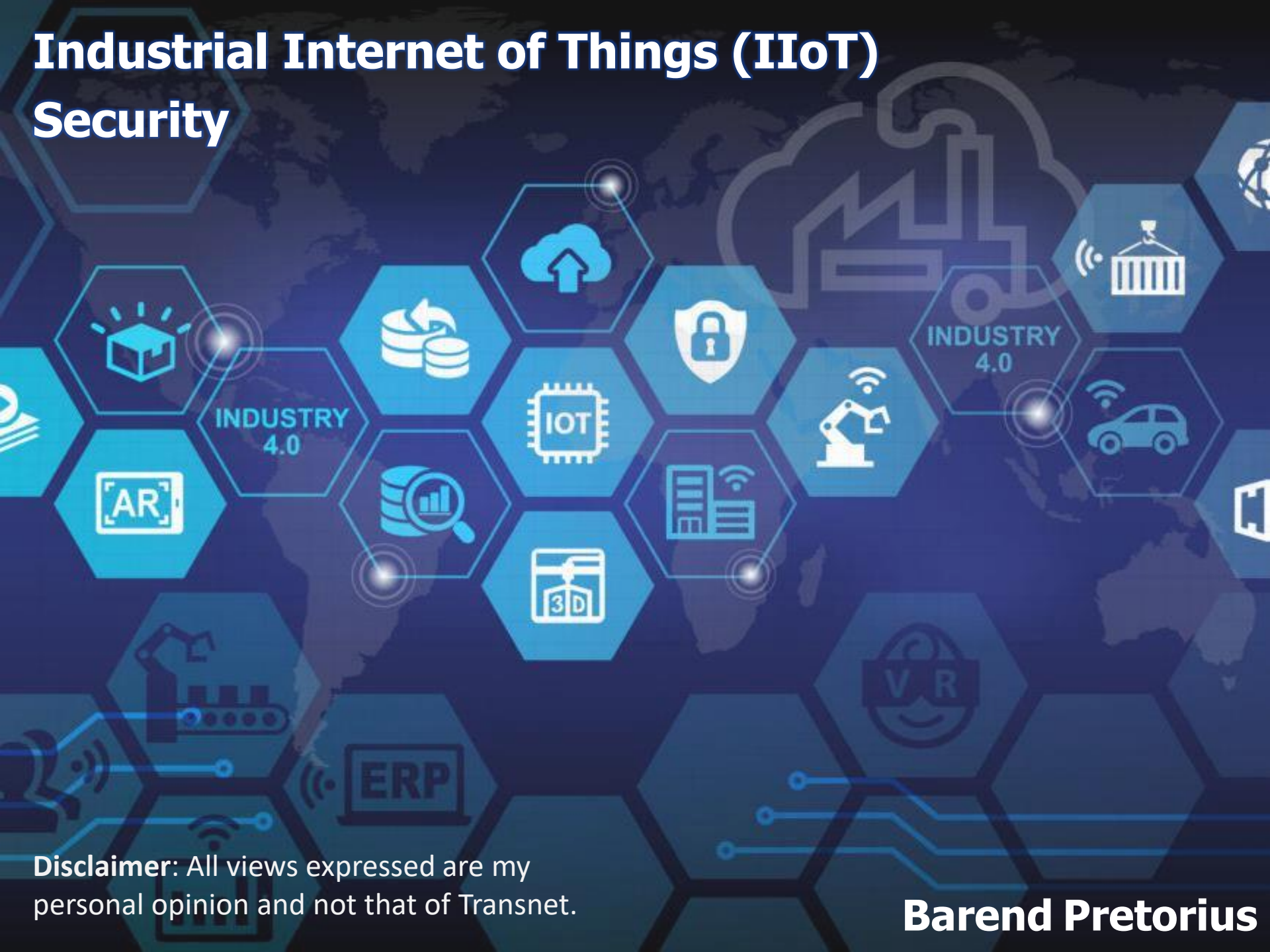
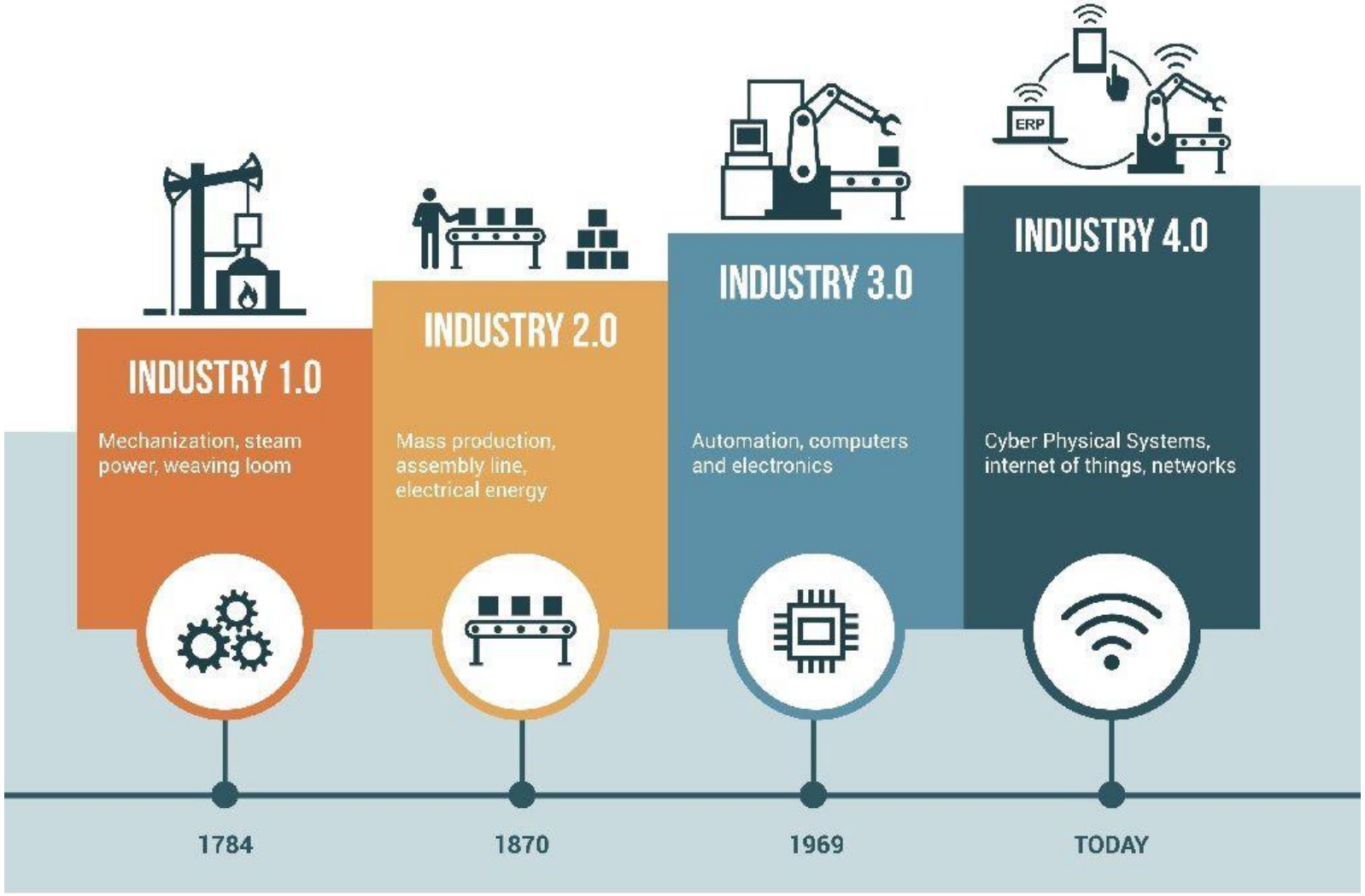
Industrial Internet of Things (IIoT) Security



Disclaimer: All views expressed are my personal opinion and not that of Transnet.

Barend Pretorius

4th Industrial Revolution



Source: Soracom.io

Introduction

"Internet of things (IoT) devices will outnumber the world's population this year for the first time."

- Gartner (2017)

Gartner predicts 20 billion device next year (2020)

Things


iBaby


© Edmunds Inc.


11:01


THOMSON
SMART TV
Home
03:26 pm
hotstar
NETFLIX
YouTube
Radioline
TED


REDMOND

More and more Things

What is IIoT?

- The Industrial Internet of Things (IIoT) is the integration of complex machinery with networked sensors and software.
- The machines are connected and talking to each other, and communicating back to centralized control systems.
- The IIoT is a network of intelligent computers, devices, and objects that collect and share huge amounts of data.

IoT reference model

Levels

7 **Collaboration & Processes**
(Involving People & Business Processes)

6 **Application**
(Reporting, Analytics, Control)

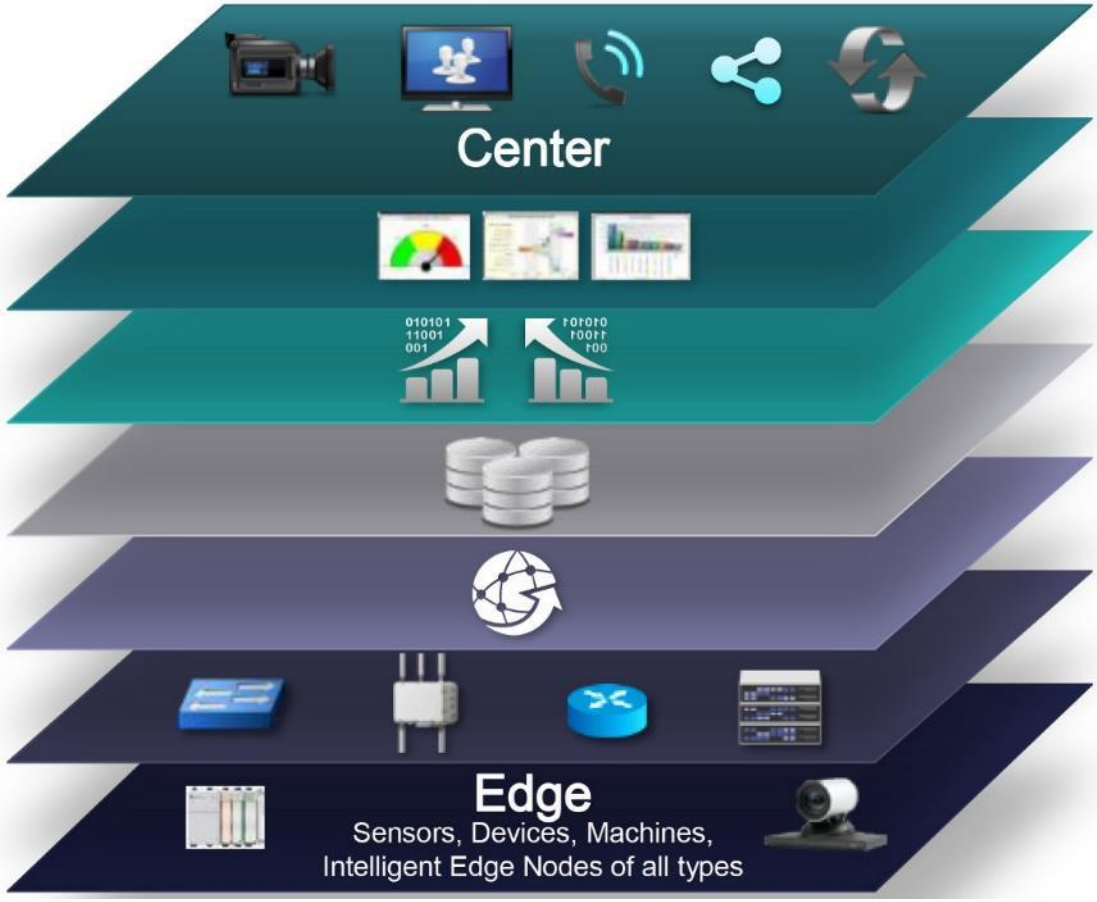
5 **Data Abstraction**
(Aggregation & Access)

4 **Data Accumulation**
(Storage)

3 **Edge Computing**
(Data Element Analysis & Transformation)

2 **Connectivity**
(Communication & Processing Units)

1 **Physical Devices & Controllers**
(The "Things" in IoT)



Source: www.iotwf.com/resources

IIoT uses by Industry

HOME
- Smart Temperature Control
- Optimized Energy Use

INDUSTRIAL
- Machine-to-Machine Communication
- Quality Control

AUTOMOTIVE
- Vehicle Auto-Diagnosis
- Optimized Traffic Flow
- Smart Parking

AGRICULTURE
- Offspring Care
- Crop Management
- Soil Analysis

MILITARY
- Situational Awareness
- Threat Analysis

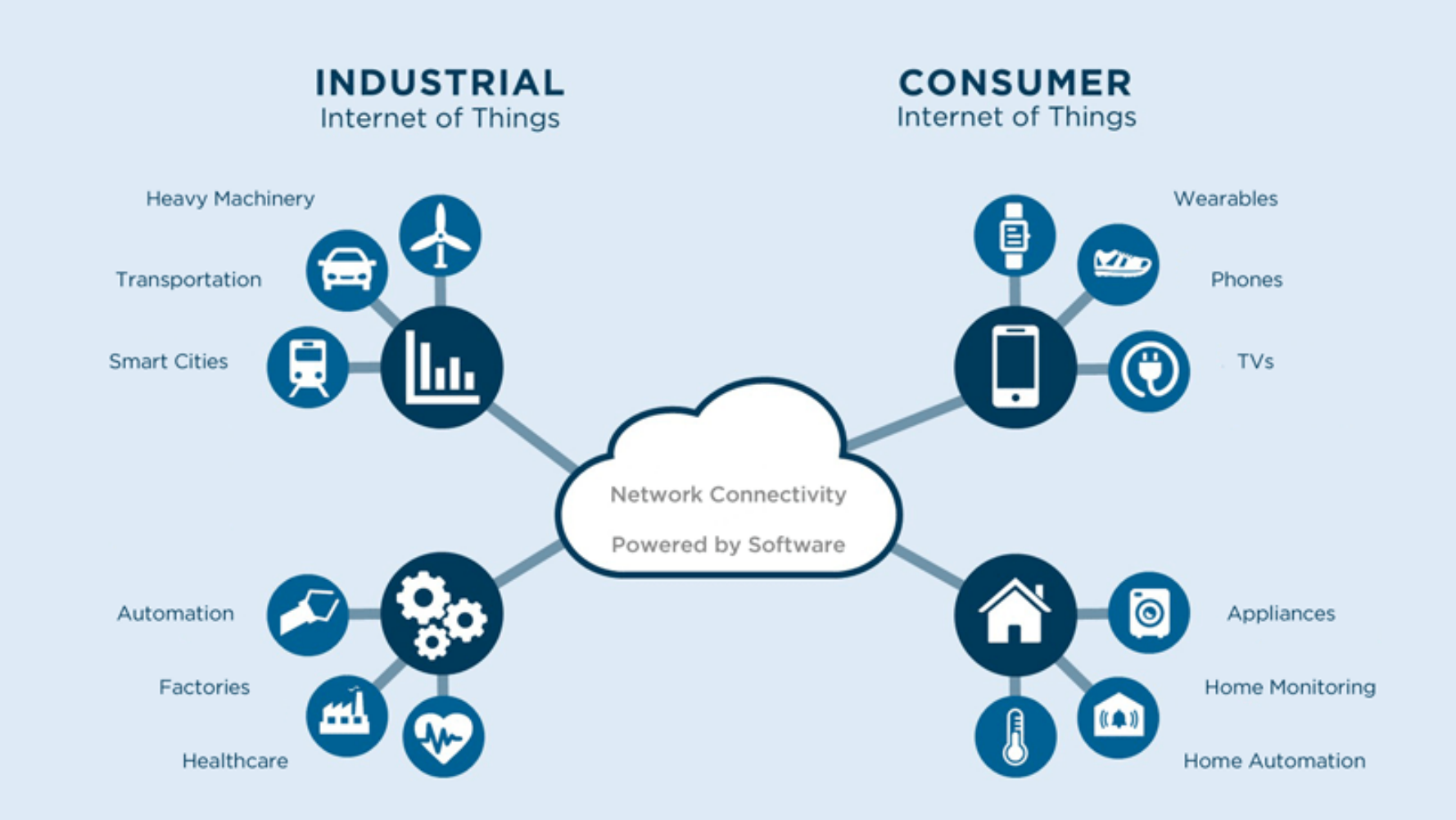
MEDICAL
- Optimized Patient Care
- Wearable Fitness Devices
- Quality Data Reporting

ENVIRONMENTAL
- Forest Fire Detection
- Species Tracking
- Weather Prediction

RETAIL
- Theft Protection
- Inventory Control
- Focused Marketing

Source: www.bignerdranch.com

IoT vs IIoT

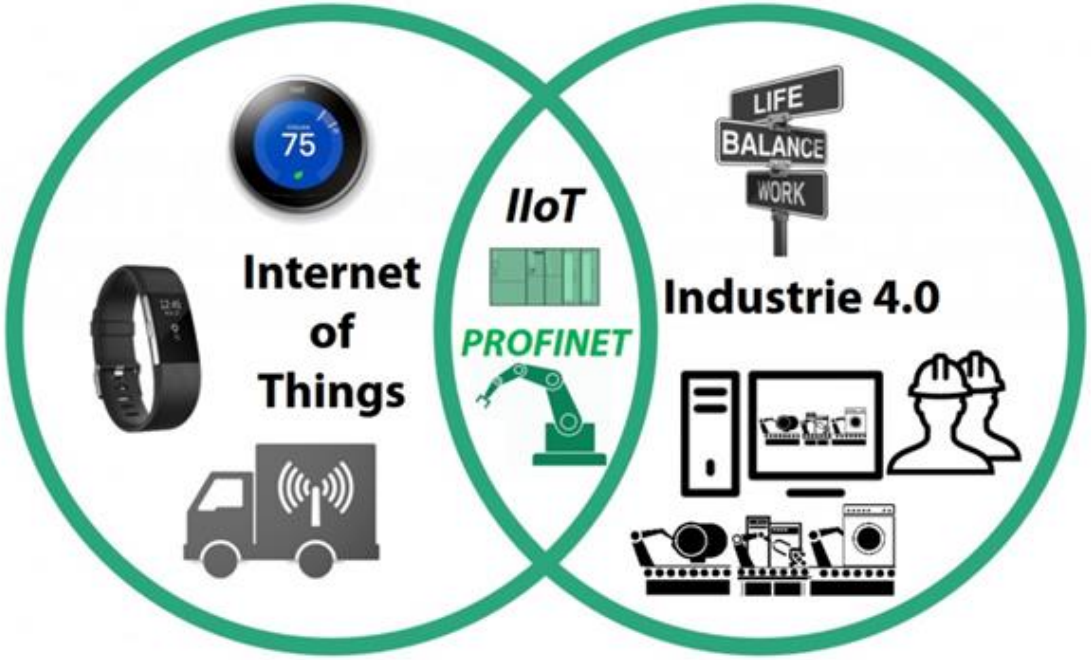


Source: intellinium.io

IoT vs IIoT cont'd

IoT	IIoT
Revolution	Evolution
Things	Data
Ad hoc connectivity	Structured connectivity
Important – but not critical	Mission critical • Analytics (ML/AI) • **Security** • Data integrity • Response times
User serviced	User + OEM + Vendor serviced
New • Devices • Standards	Existing • Devices • Standards
Proprietary Solutions	Defined Standards

IoT vs IIoT cont'd



Source: Henning (2017)

IT vs IIoT


IT
IIoT
+
Importance
–
Confidentiality
Integrity
Availability
–
Importance
+

NETSCOUT Threat Intelligence Report
– Powered by ATLAS

DAWN OF THE TERRORBIT ERA

Findings from Second Half 2018

THE TERRORBIT ERA

We saw the growth of internet-scale campaigns that use a vast array of devices related solely by internet connectivity to strike strategic targets.

INCREASED SOPHISTICATION

INCREASED SOPHISTICATION AND EFFICIENCY at monetizing malicious attacks. **MODULAR, PERSISTENT CRIMEWARE** that provides a better ROI than a simple smash-and-grab method.

MIRAI

REMAINS THE KING OF IoT MALWARE

TORii + VPNFILTER

ARE TWO NEW BREEDS OF ADVANCED IoT BOTS

IoT DEVICES

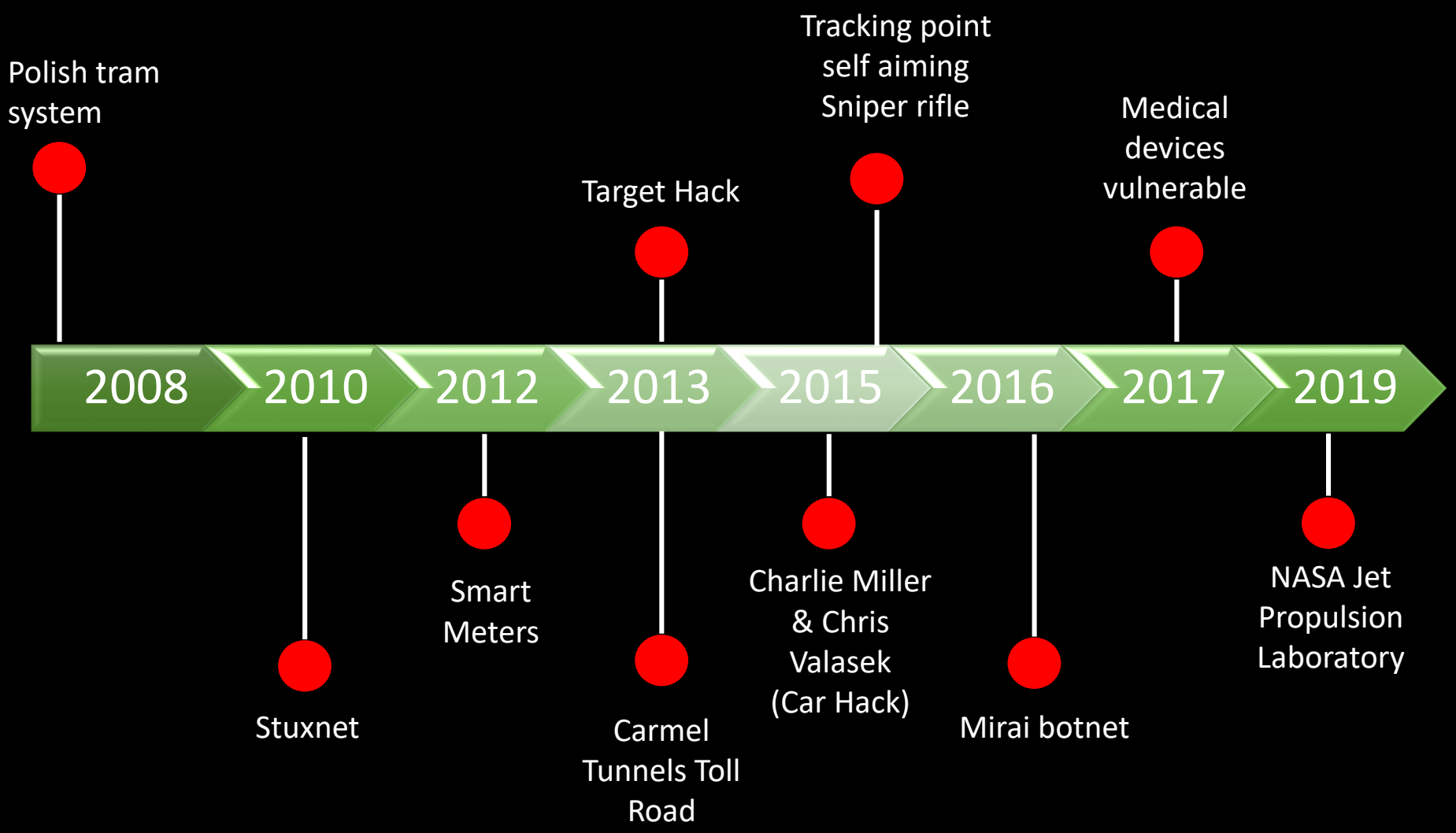
Once plugged into the internet, IoT devices are attacked within

5 MINUTES

and targeted by specific exploits in

24 HOURS

Notable Incidents



Other Incidents

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

April 16, 2018 | Wang Wei

BBC Menu

NEWS

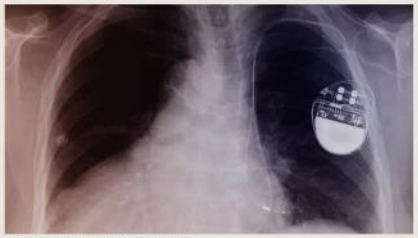
Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment &

Technology

Fridge sends spam emails as attack hits smart gadgets

17 January 2014 | Technology

Hackers can now get into pacemakers



[Photo: Lucien Monfils/Wikimedia Commons]

About Us | Contact Us | Go to ESET.COM | eset

welivesecurity

Security news, views and insight from the ESET experts

All Posts | Latest Research | How To | Videos | Papers | Our Experts

'Major' Smart TV vulnerability could allow mass wireless attacks

BY ROB WAUGH POSTED 9 JUN 2014 - 02:33PM

CYBERCRIME | 0 | TAGS SMART TV VULNERABILITY

Security Community Blog

Brian Witten

Hospitals Breached via Medical Devices?

By: Brian Witten | SYMANTEC EMPLOYEE

Created 24 Jun 2015

0 Comments | Share

TECH | December 21, 2018 | Updated: Decem

Wi-Fi baby monitor hacked: Parents up to voice threatening to kidnap th child

By Rebecca Joseph | National Online Journalist, Breaking News, Global News

Comments 6 | Facebook 21.4k | Twitter | LinkedIn | Email

WATCH: Texas family experiences scare after baby monitor hacl

Security

Yes, you can remotely hack factory, building site cranes. Wait, what?

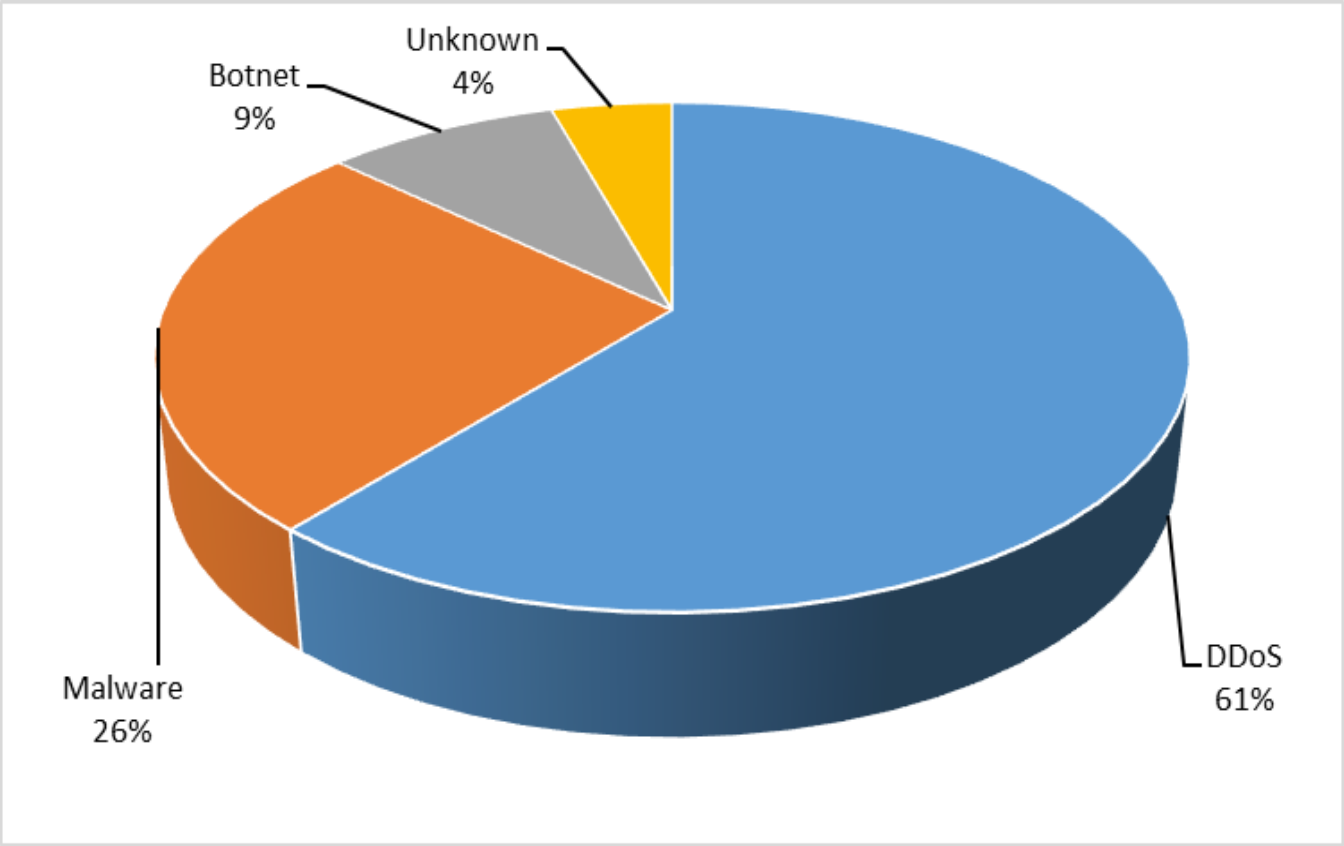
Authentication is simply AWOL for remote RF control equipment, says Trend Micro

By Gareth Corfield 15 Jan 2019 at 16:36 | 46 | SHARE

Exclusive: Hackers Take Control Of Giant Construction Cranes

Thomas Brewster Forbes Staff
Cybersecurity
I cover crime, privacy and security in digital and physical forms.

Top IoT threats

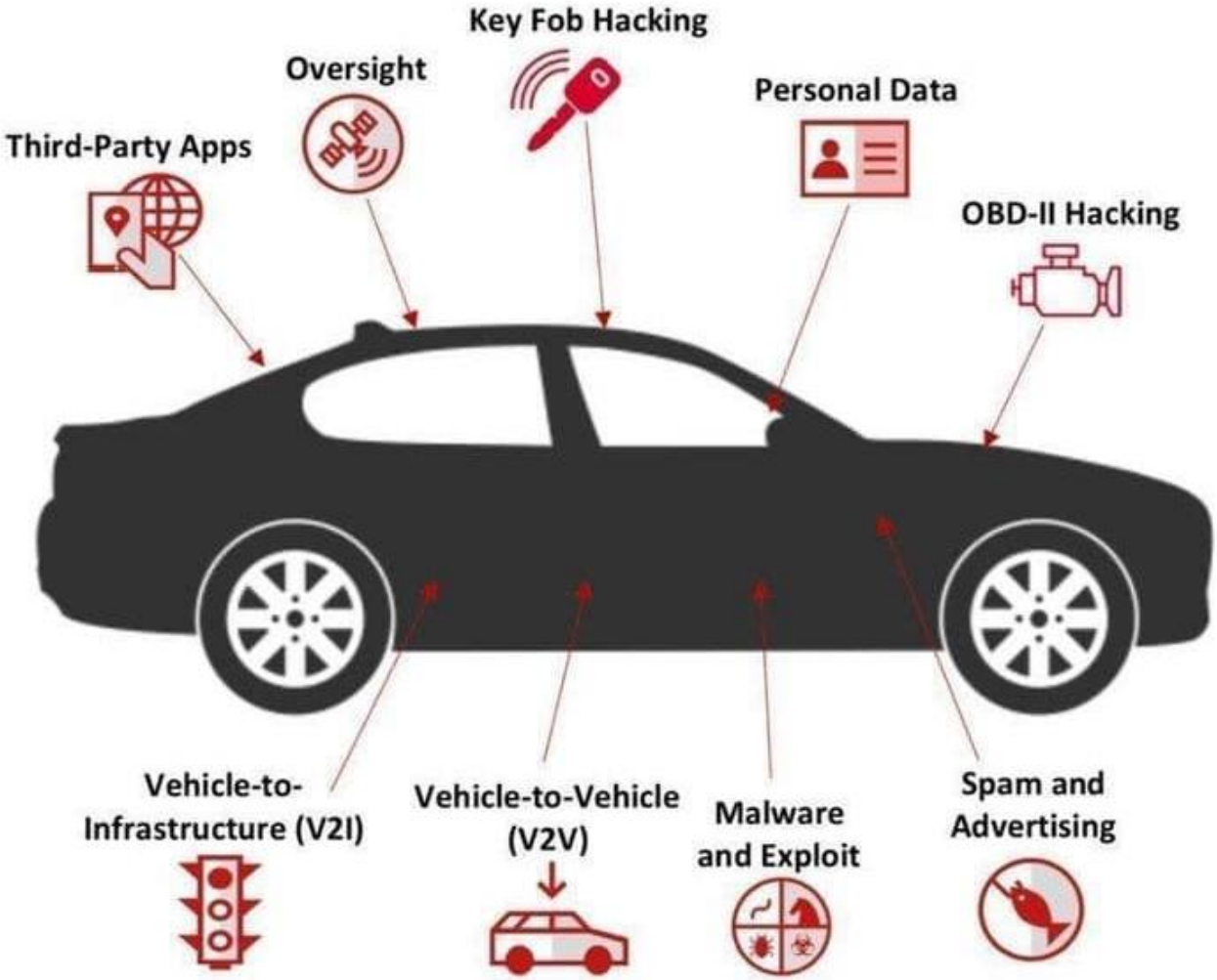


Source: Symantec (2018)

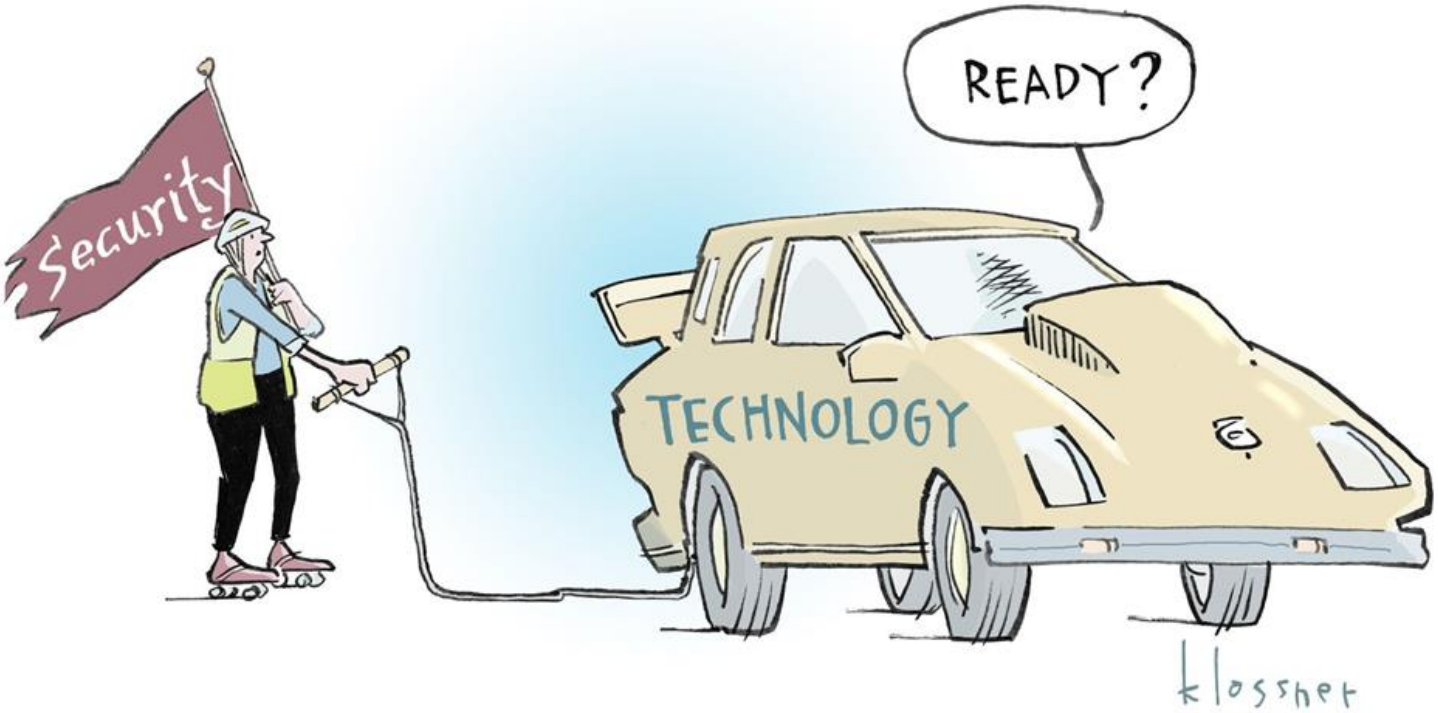
IoT Vulnerabilities

- Access
  - Default passwords, password & access controls
- Patching / firmware updates
- Configuration - Code manipulation
- No / weak encryption
- DDoS – No protection against
- Protocols
  - e.g. unsecure implementation
- Unreliable Interfaces
  - SQL injection,
  - XSS
- Privacy

Risk – Smart Car



IIoT Security



Thank you

"CAN I INTEREST YOU IN A FIREWALL FOR YOUR TOASTER?"

Barend Pretorius barend.pretorius@gmail.com