

Protecting Smart Buildings

The next frontier of critical infrastructure security

Suzanne Rijnbergen - MBA



Who am I?



Global Director Professional Services @SecurityMatters (ForeScout)

> 13y experience in cybersecurity

- * Fox-IT
- * Netherlands Forensics Institute
- * TNO
- * KPN

Passion for technology

- * Privacy
- * Intelligence
- * MBA





- * Introduction to (Building Automation) Security
- * Threat landscape: Risks to Building Automation Systems
- * First hand experience
- * What to do now? How to reduce security risks?



*Cybersecurity is to be prevented from the danger or damage caused by disruption of ICT or misuse of ICT. The risk of damage due to misuse, disruption or interruptions may consist of the limitation of the **availability and reliability** of ICT, the violation of the integrity of ICT information and the damage to the integrity of that information.*

It is about

- **Availability**
- **Reliability**
- **Integrity**

Hackaanval op Kamerleden via MH17- mail



AUTORITEIT
PERSOONSGEGEVENS



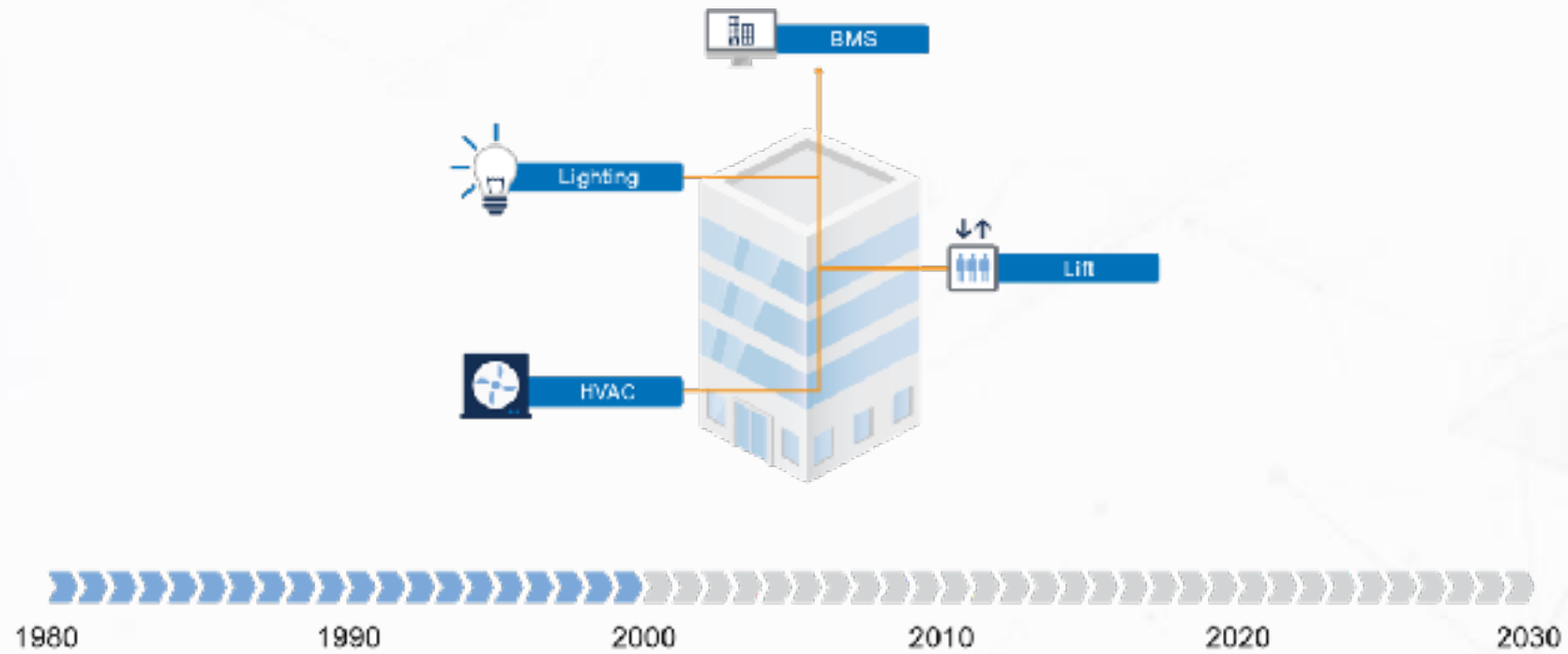
ABN en Rabobank getroffen door DDoS- aanval

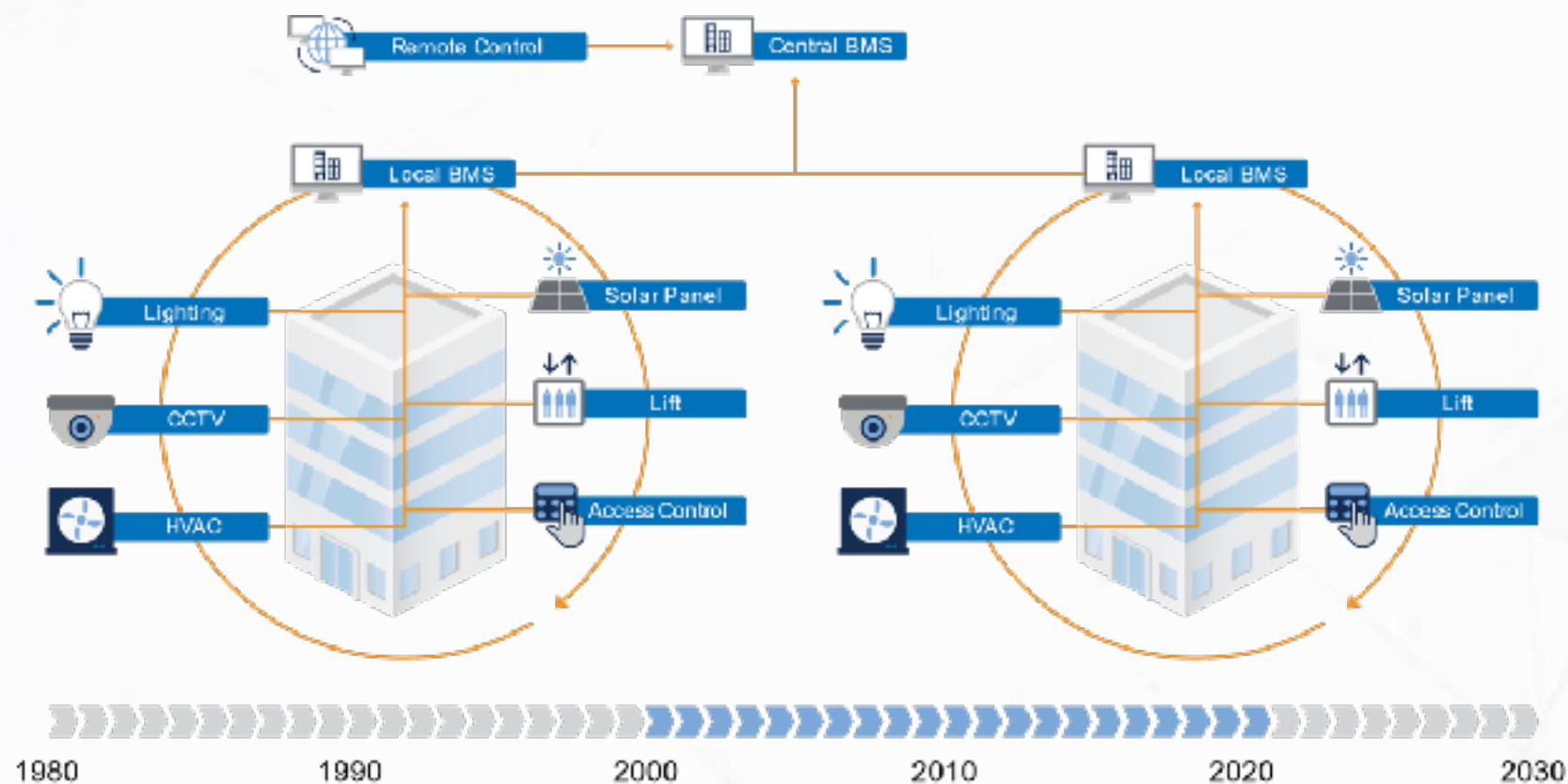


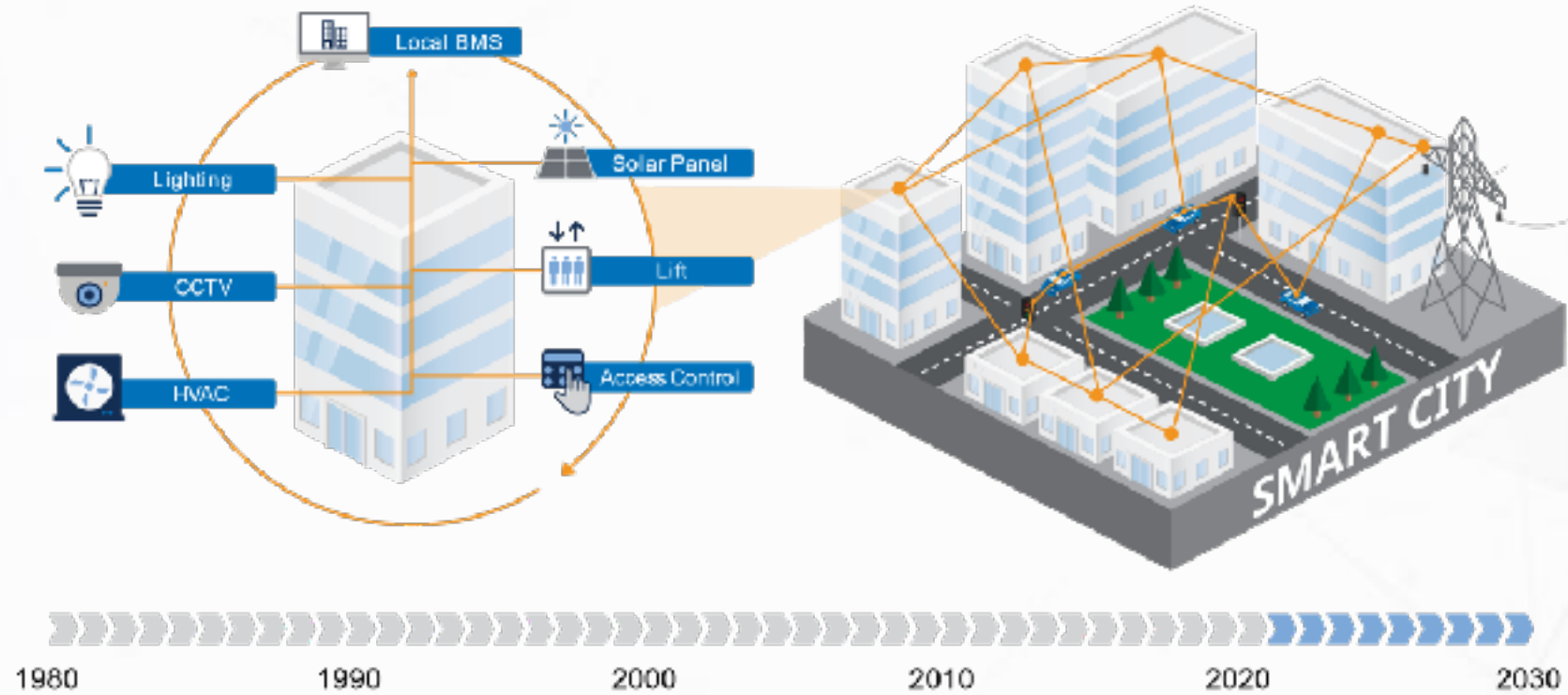
Why cybersecurity?



Don't argue with idiots....







Why cybersecurity for Building Management Systems?



We need to learn and cooperate....



Threat Landscape



Hackers Designed a 'Master Key' to Unlock Millions of Hotel Room Doors

 Bill Cameron
4/25/18 9:15am • Filed to: HOSPITALITY ▾

  
781K 51 6

PARIS/NEW YORK

Could hackers really take over a hotel? WIRED explains

Reports this week claimed an Austrian hotel was hit by ransomware that locked its bedroom doors, but the claims weren't entirely accurate


 > Technology Intelligence

CCTV vulnerability could allow cyber criminals to hack video surveillance recordings

November 8, 2016 14:20

Update: Let's Get Cyberphysical: Internet Attack shuts off the Heat in Finland

Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank

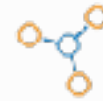
 Oscar Williams-Gruet, Business Insider
© 15.04.2018, 09.08



Legacy Systems

- 60% of buildings have systems that are 20 years old
- No encryption
- No authentication

Why should we worry?



Legacy Systems

- 60% of buildings have systems that are 20 years old
- No encryption
- No authentication

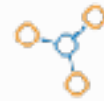
Connectivity

- More connection = more vulnerabilities
- Default open ports
- Default passwords



Legacy Systems

- 60% of buildings have systems that are 20 years old
- No encryption
- No authentication



Connectivity

- More connection = more vulnerabilities
- Default open ports
- Default passwords



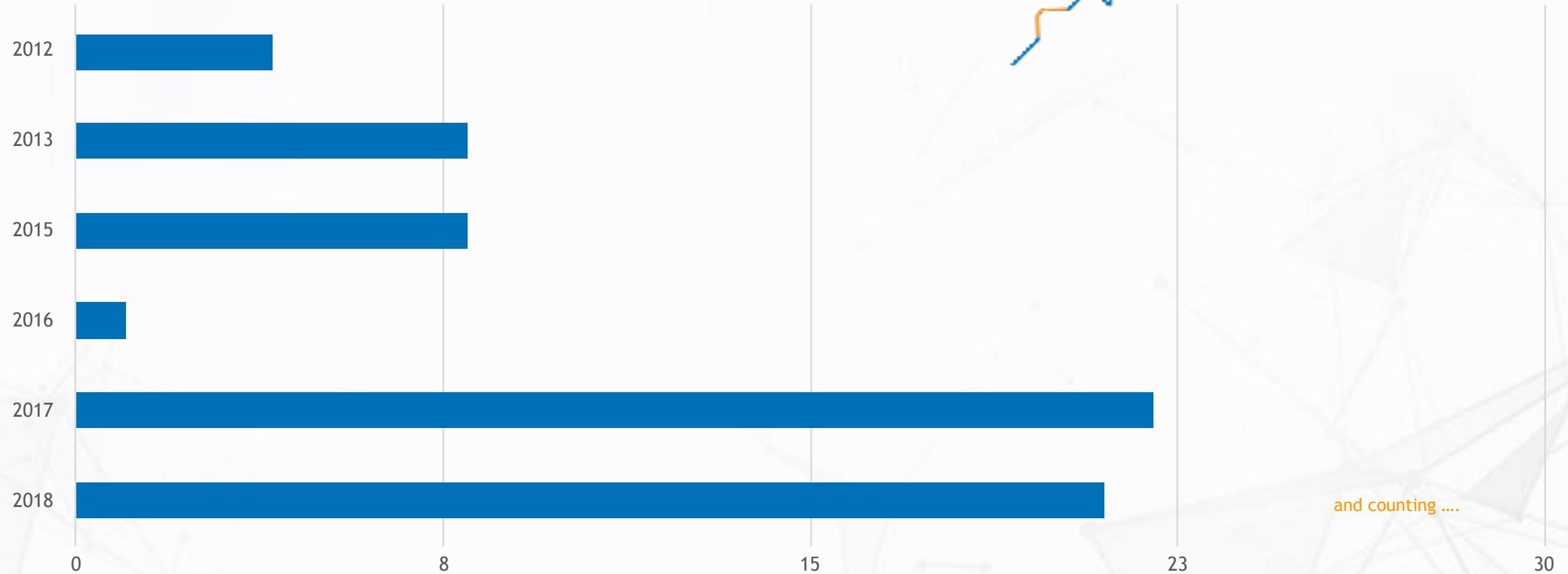
Critical Buildings

- Airports
- Data centers
- Hospital & Public spaces

Why the fuss?



Vulnerabilities are on the rise





2012: Target Hack

2013: Google Wharf Australia hacked

2016: Lappeenranta DDOS attack

2016-2017: 4x hack on Seehotel Austria

2017: >70% of all CCTV in Washington DC hacked

2018: Cameras in gymnasium Brabant hacked

2018: AIVD hacked 'CozyBear' through CCTV systems





First-hand experience: a cyber security exercise

Exercise setup



1

Take a small team of security students.



2

Give them a few **controllers** and **software** used in Smart Buildings



BMS



PLCs

3

Select devices from top vendors and with realistic distribution of firmware versions



4

Let them play for a few days

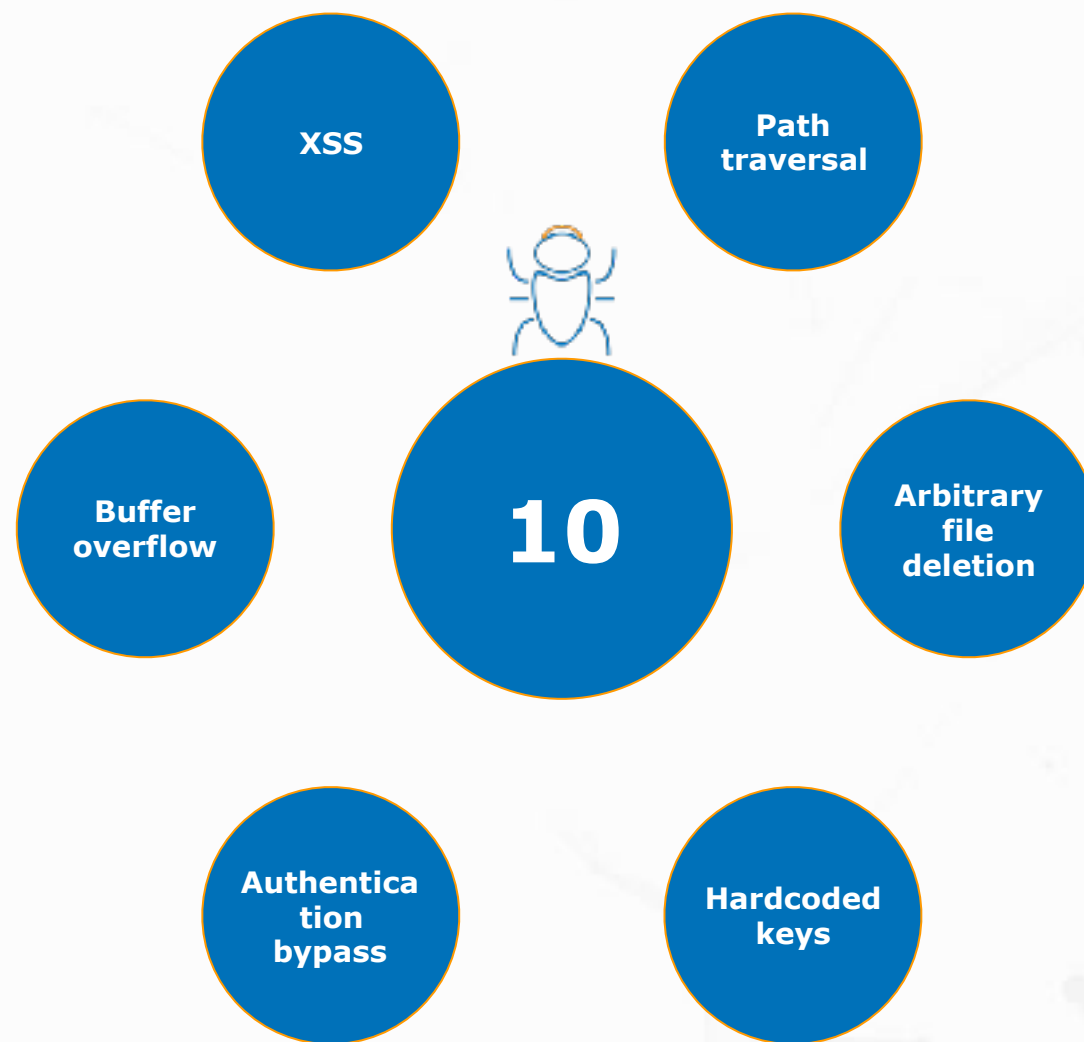


5

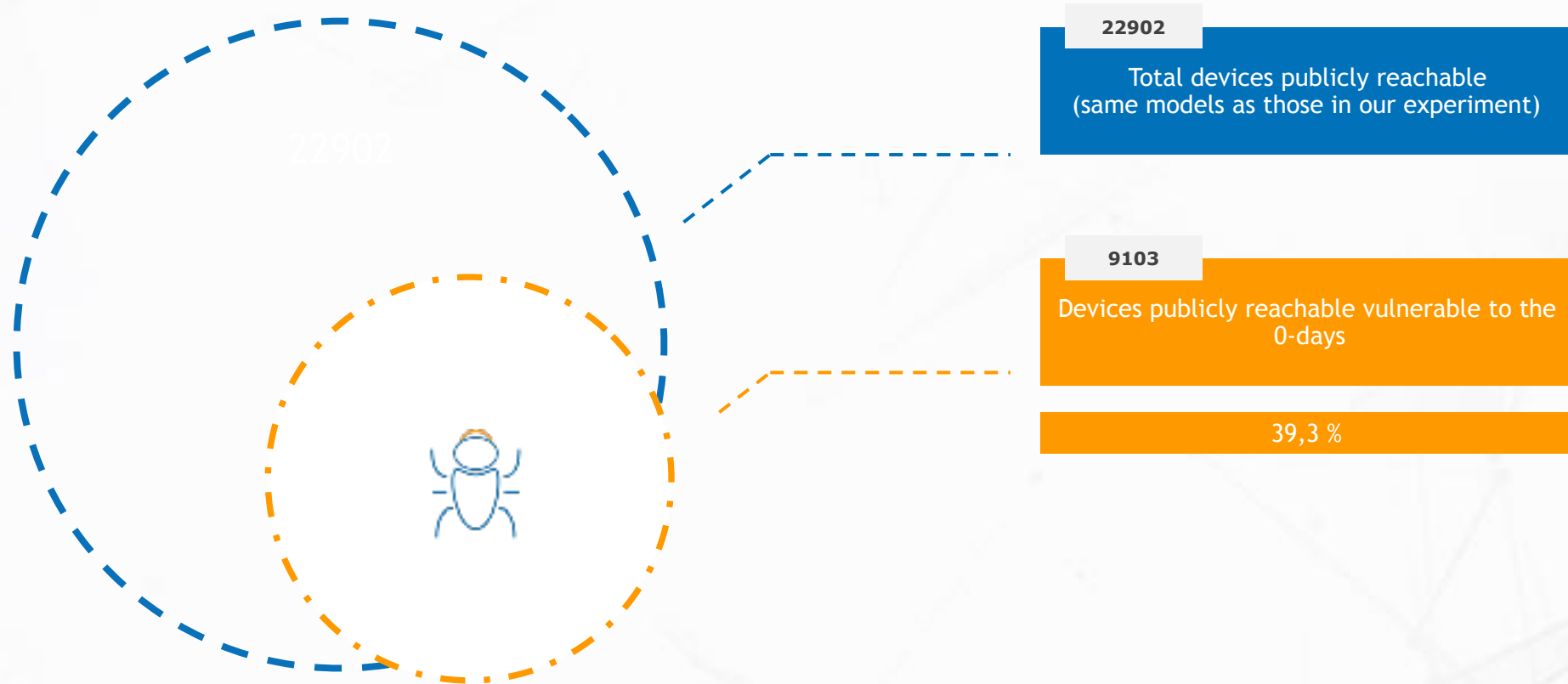
How many 0-days will they find?

?





How many devices with those 0-days are publicly reachable?

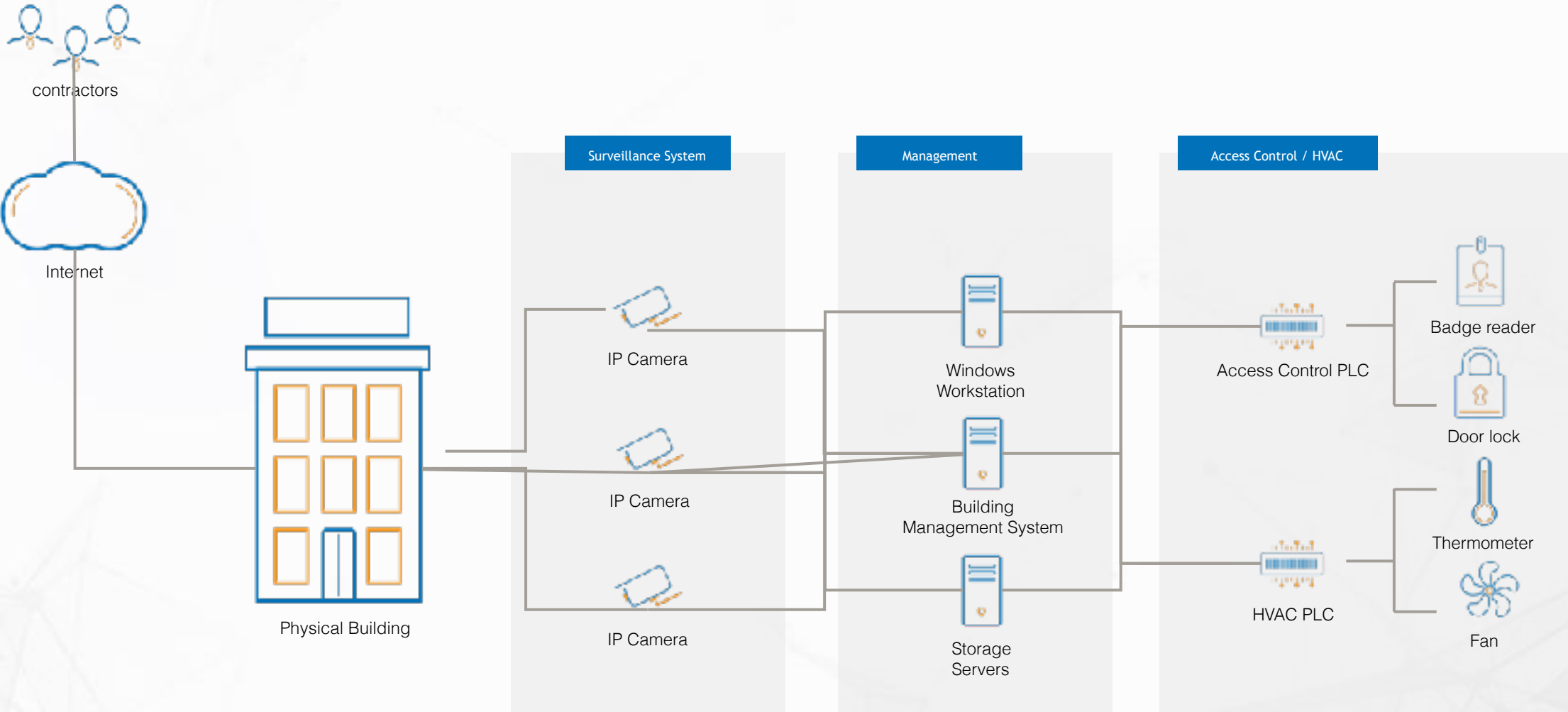


Infographic obtained by:
aggregating data from Shodan and
Censys

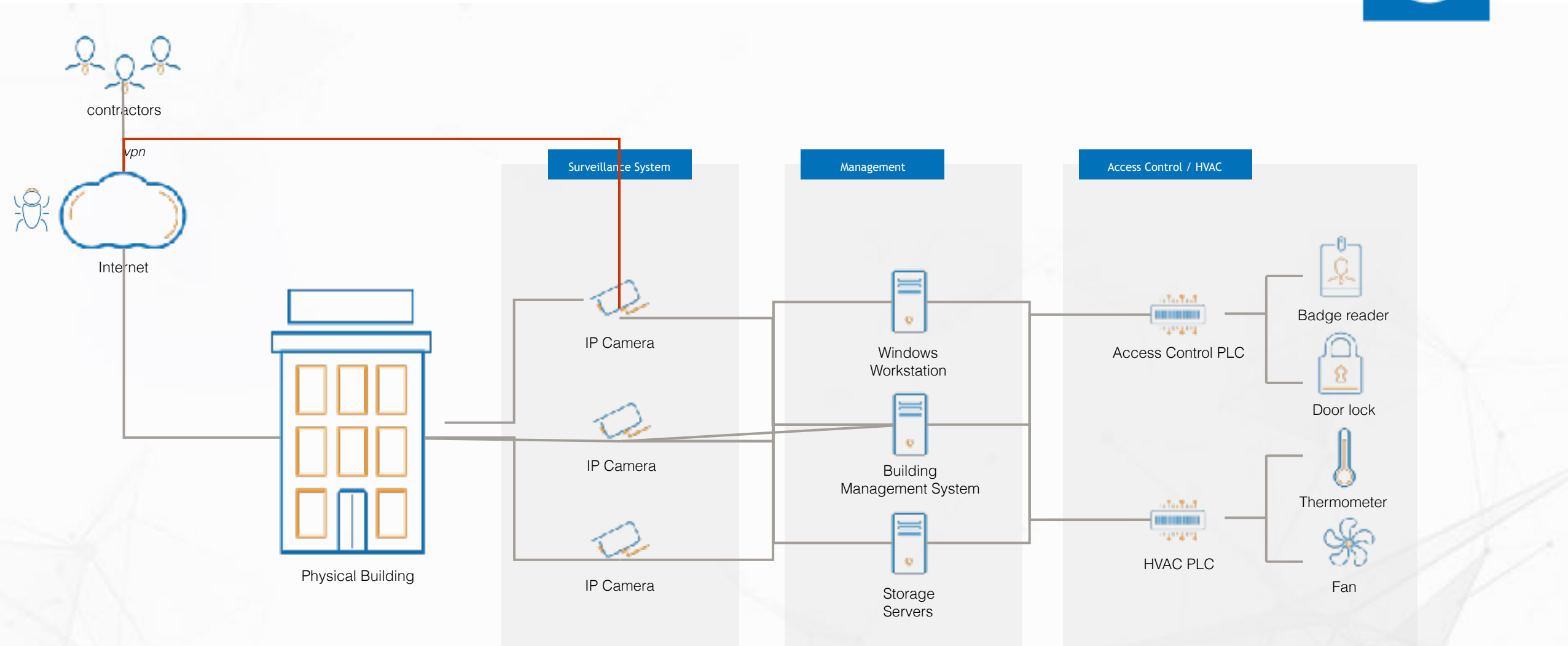


WHAT IS THE DANGER BEHIND EXPOSED DEVICES?

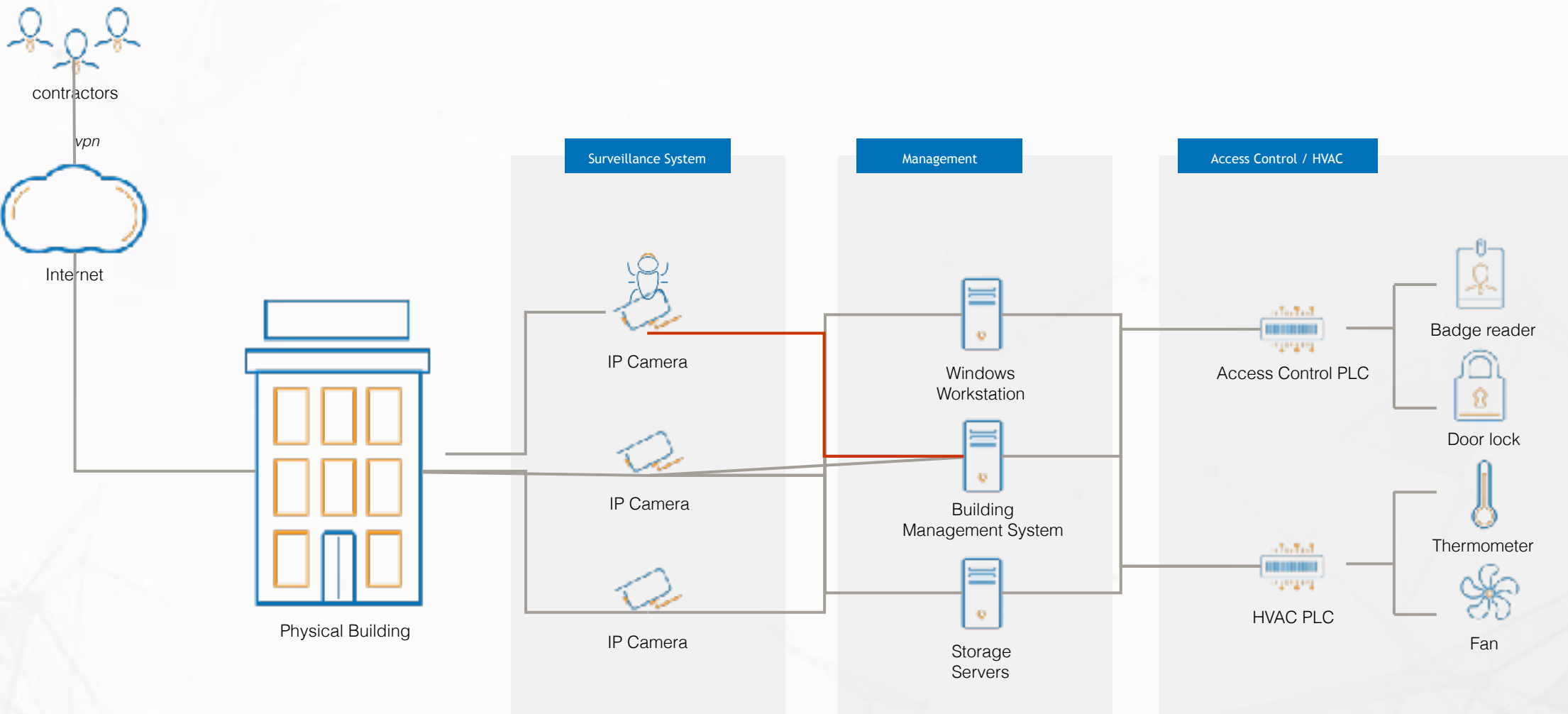




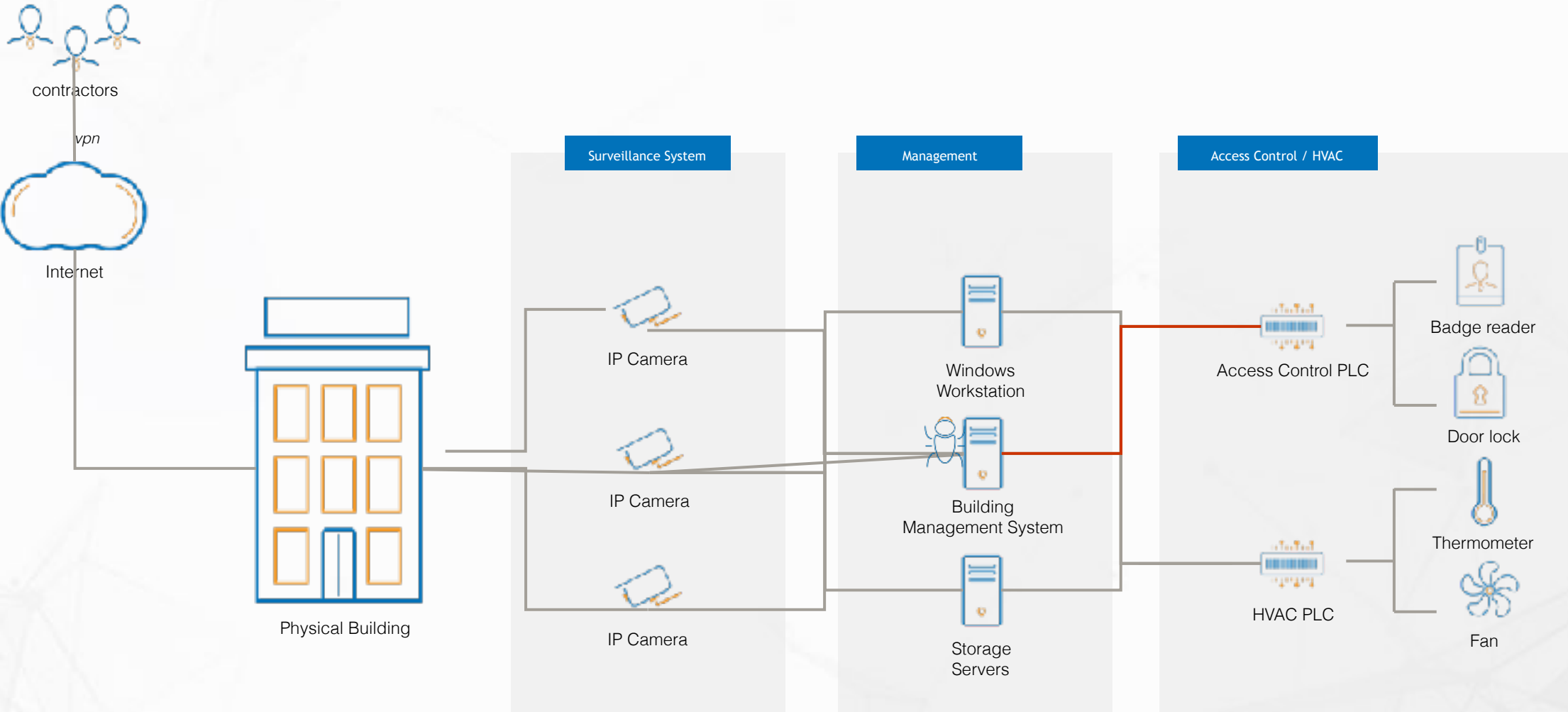
Gain Access



Lateral Movements



Lateral Movements





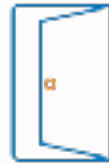
Turning off cameras to cover malicious physical actions

Delete recordings that could serve as evidence

Using cameras as botnet (Mirai)



THAT'S NOT IMPOSSIBLE



Add/remove user credentials

Allow access to restricted areas to unauthorized users

Deny access to critical areas to authorized users



WHO LEFT THE DOOR OPENED?



Change the settings for the temperature

Increase temperature to damage medical labs ..

.. or cause data centers to go offline



POWER BELONGS TO THOSE WHO TAKE IT (OFF)



How to reduce security risks?



Threat Intelligence Consumption



Asset Identification & Network Monitoring

Active Cyber
Defense Cycle



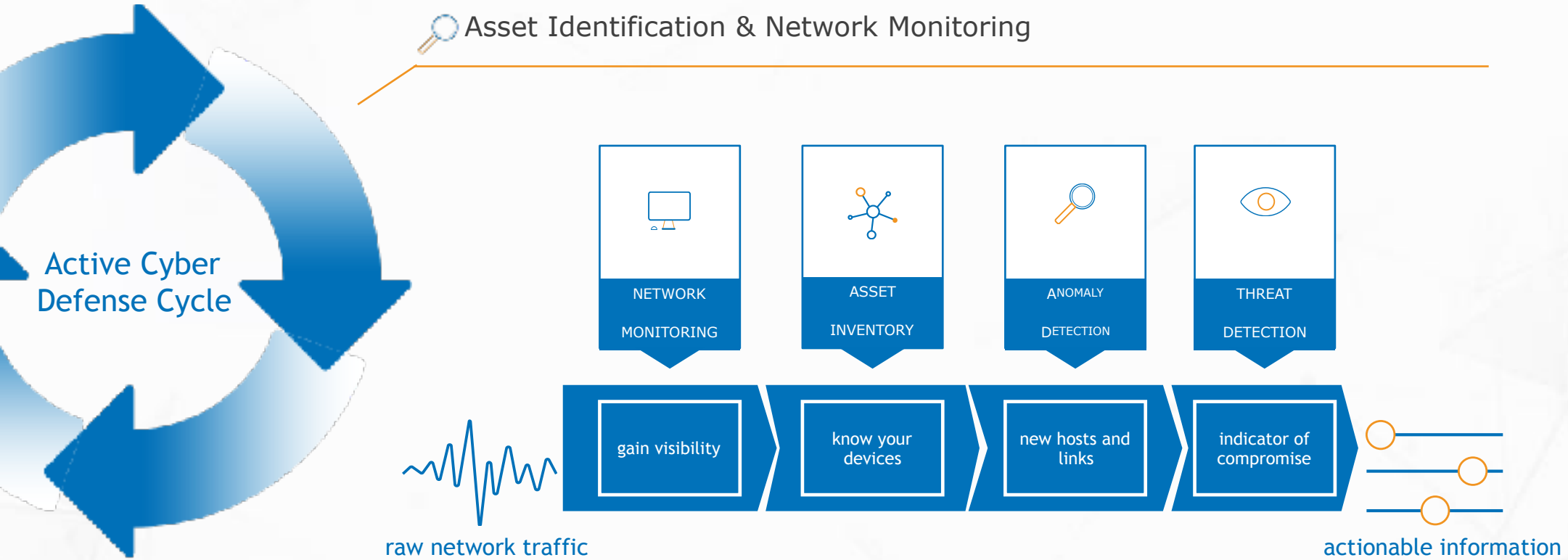
Threat and Environment Manipulation



Incident Response



 Asset Identification & Network Monitoring





Real-world examples



Headquarter of a financial institute



About 500 devices in the Building Automation Network



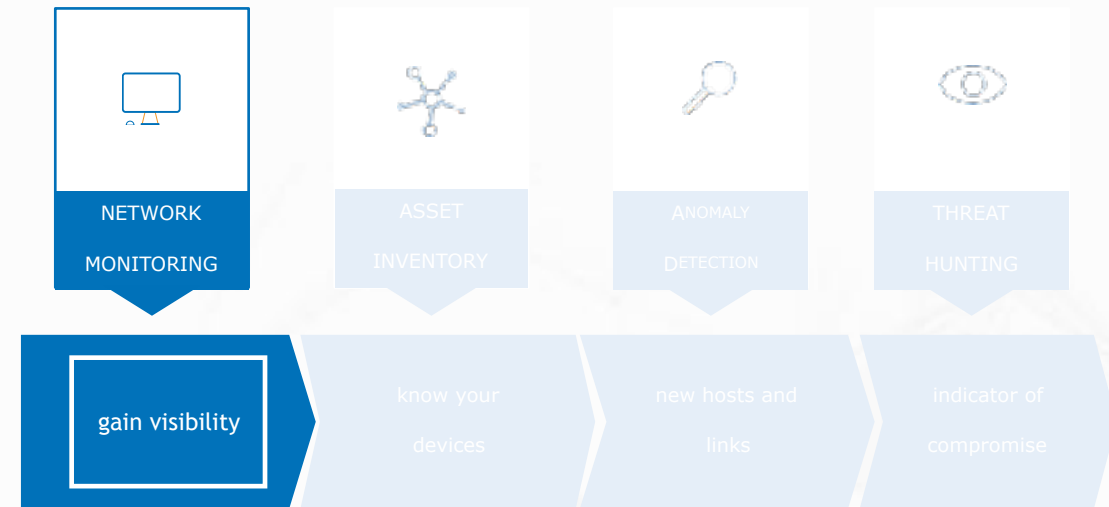
Monitored systems include HVAC, Surveillance and Access Control



Unwanted SMB traffic in the network

Identification of maintenance operations not adhering to policies (e.g. supplier connecting own laptop to network)

Unwanted communication links between IT and OT networks (firewall misconfiguration)

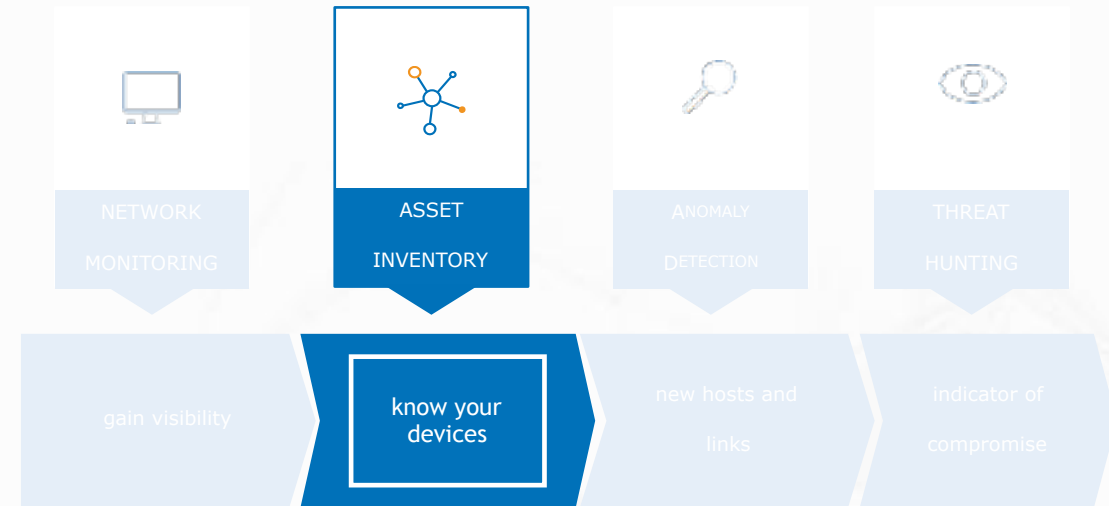




Automatic inventory of network assets and their status

Identified hundreds of BACnet devices with only outbound communication flows

Identified multiple vulnerable hosts and controllers with outdated firmware

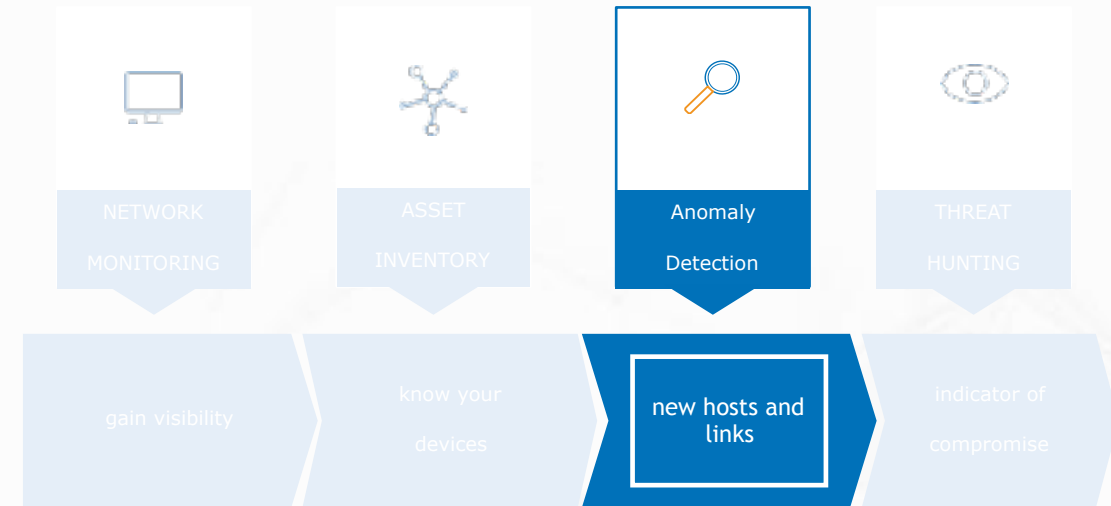




Detect unusual traffic direction (inbound traffic to IP Cameras)

Detect IP-cameras using HD recording (high bandwidth consumption)

Identify out-of-range values for critical variables

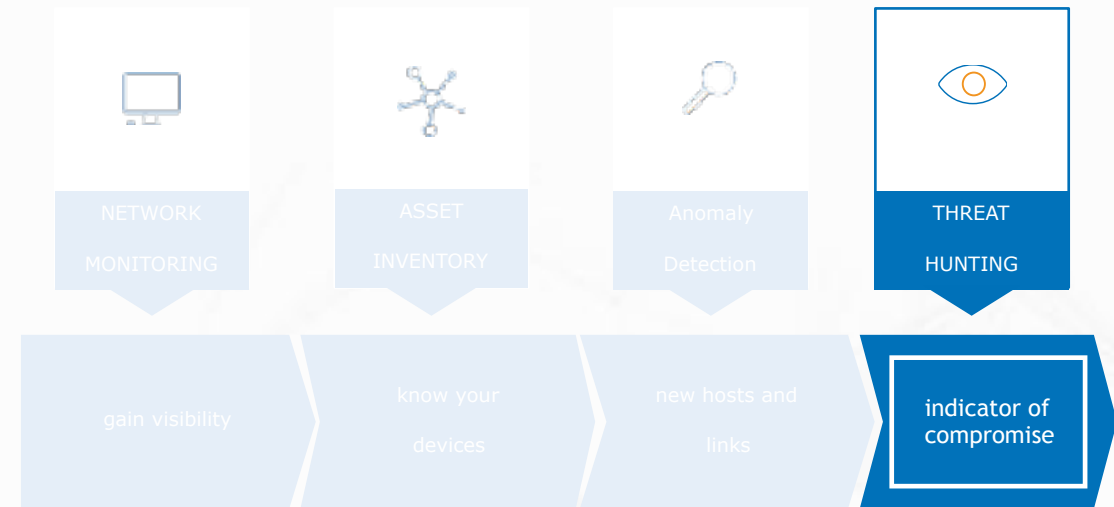




Detect changes to the logic of controllers

Detected usage of UpnP

Detected weak passwords to access IP-cameras





Wrapping up



Landscape	Visibility	Detection
<ul style="list-style-type: none">Smart building rely on legacy systems	<ul style="list-style-type: none">See what your network devices are doing	<ul style="list-style-type: none">Catch known and unknown threats
<ul style="list-style-type: none">Cyber risks for smart buildings are on the rise	<ul style="list-style-type: none">Assess risks, threats and vulnerabilities	<ul style="list-style-type: none">Pinpoint weak spots and current inefficiencies
<ul style="list-style-type: none">Building automation networks are vulnerable	<ul style="list-style-type: none">Understand the current resilience state of your network	<ul style="list-style-type: none">Gather all evidence required for incident response

Q & A

Stay in touch with our team!

-  info@secmatters.com
-  [@sec_matters](https://twitter.com/sec_matters)
-  [company/securitymatters](https://www.linkedin.com/company/securitymatters)

