Cyberattacks on smart cities – it’s just a matter of time

Marat Nuriev

IoT Business Development

Facts About Kaspersky

Essentials

Founded in 1997 and led by Eugene Kaspersky

Present on 5 continents in 200 countries and territories

Provides innovative IT security solutions and services for business and consumers

Numbers

>20 million product activations per year

> 4000 highly qualified specialists

USD 698 million — global unaudited revenue in 2017*

Achievements and Industry Recognition

One of the four biggest endpoint security vendors**

Kaspersky Lab received the Platinum Award as part of the 2017 & 2018 Gartner Peer Insights Customer Choice Awards for Endpoint Protection Platforms***

Our solutions are the most tested and most awarded in independent tests and reviews****

> 400,000,000 users worldwide are protected by our technologies

industrial internet® CONSORTIUM

OpenFog®

* According to International Financial Reporting Standards (IFRS)
** IDC - Worldwide Endpoint Security Market Shares, 2015 - Nov 2016 US41867116
*** The Gartner Peer Insights Customers' Choice Logo is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice distinctions are determined by the subjective opinions of individual end-user customers based on their own experiences, the number of published reviews on Gartner Peer Insights and overall ratings for a given vendor in the market, as further described here and are not intended in any way to represent the views of Gartner or its affiliates.
****kaspersky.com/top3

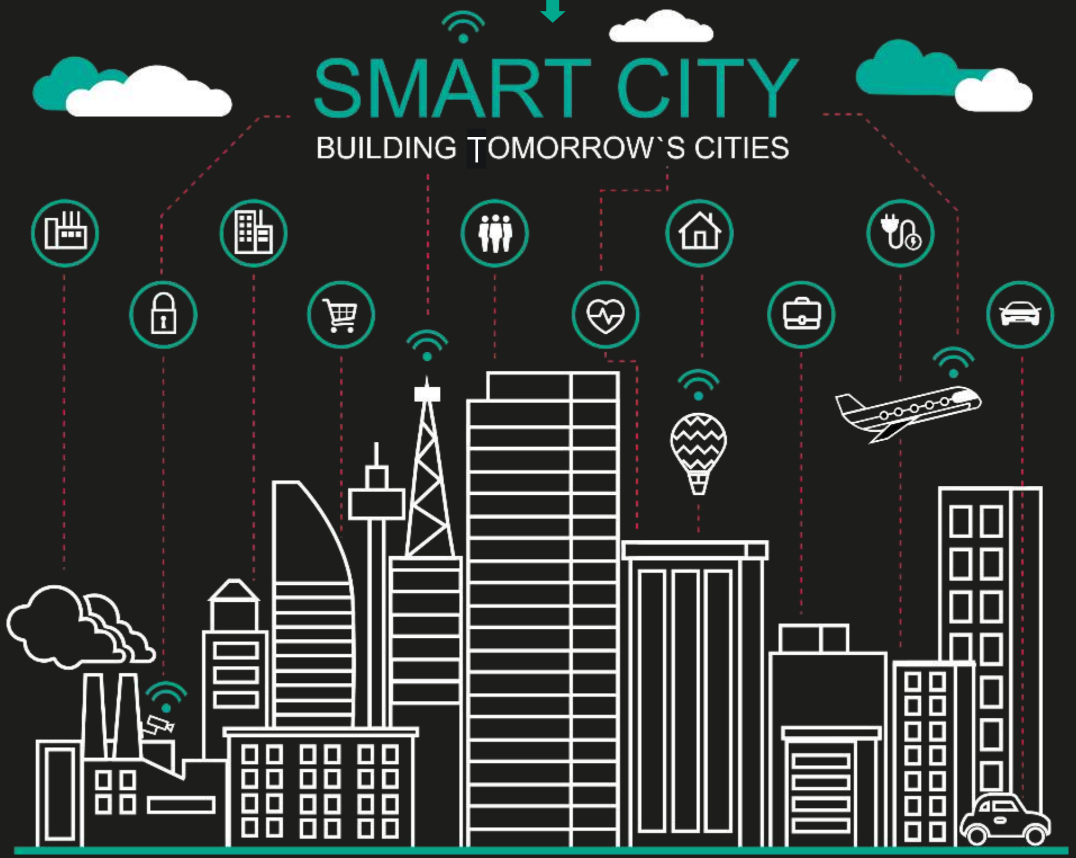
This is just computer game. Or not?

Why we talk about ‘smart cities’

Increase the productivity of urban services

Reduce costs and resource consumption

Improve the quality of life

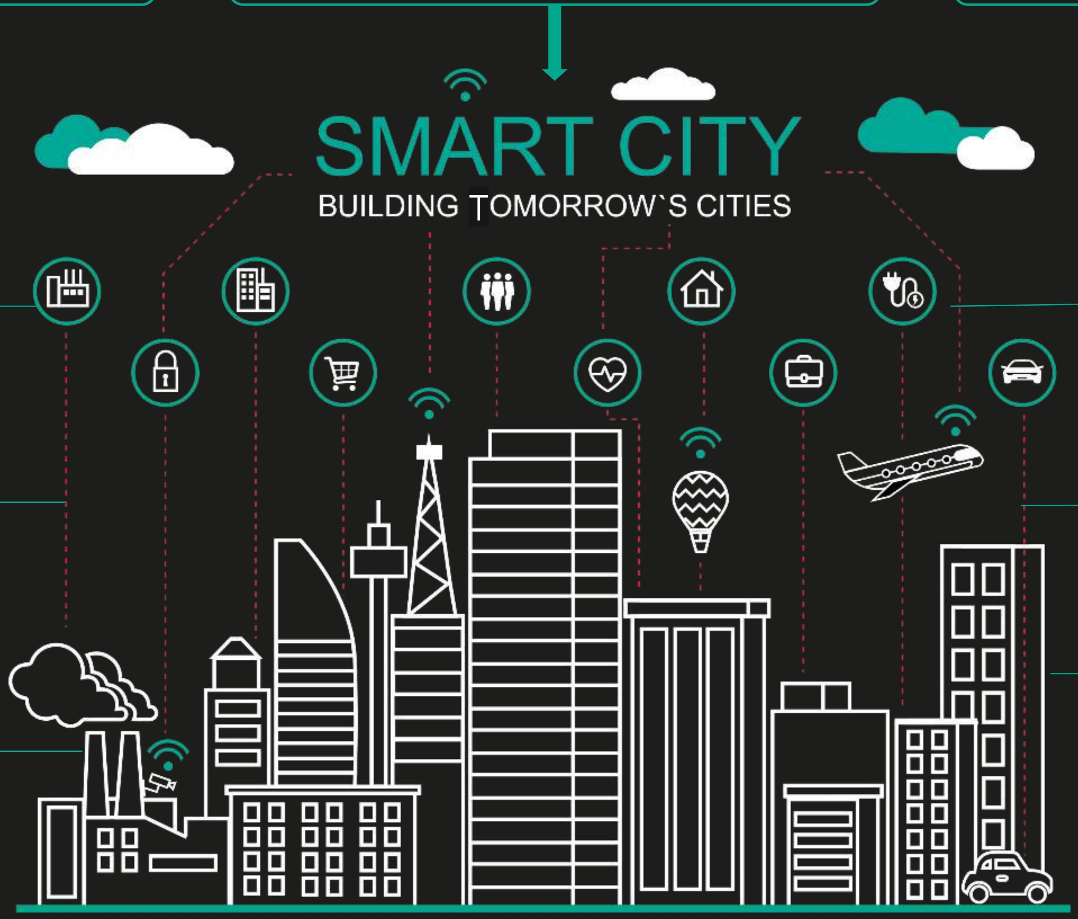


Why we talk about ‘smart cities’

Increase the productivity of urban services

Reduce costs and resource consumption

Improve the quality of life



City administration services

Transport and traffic management

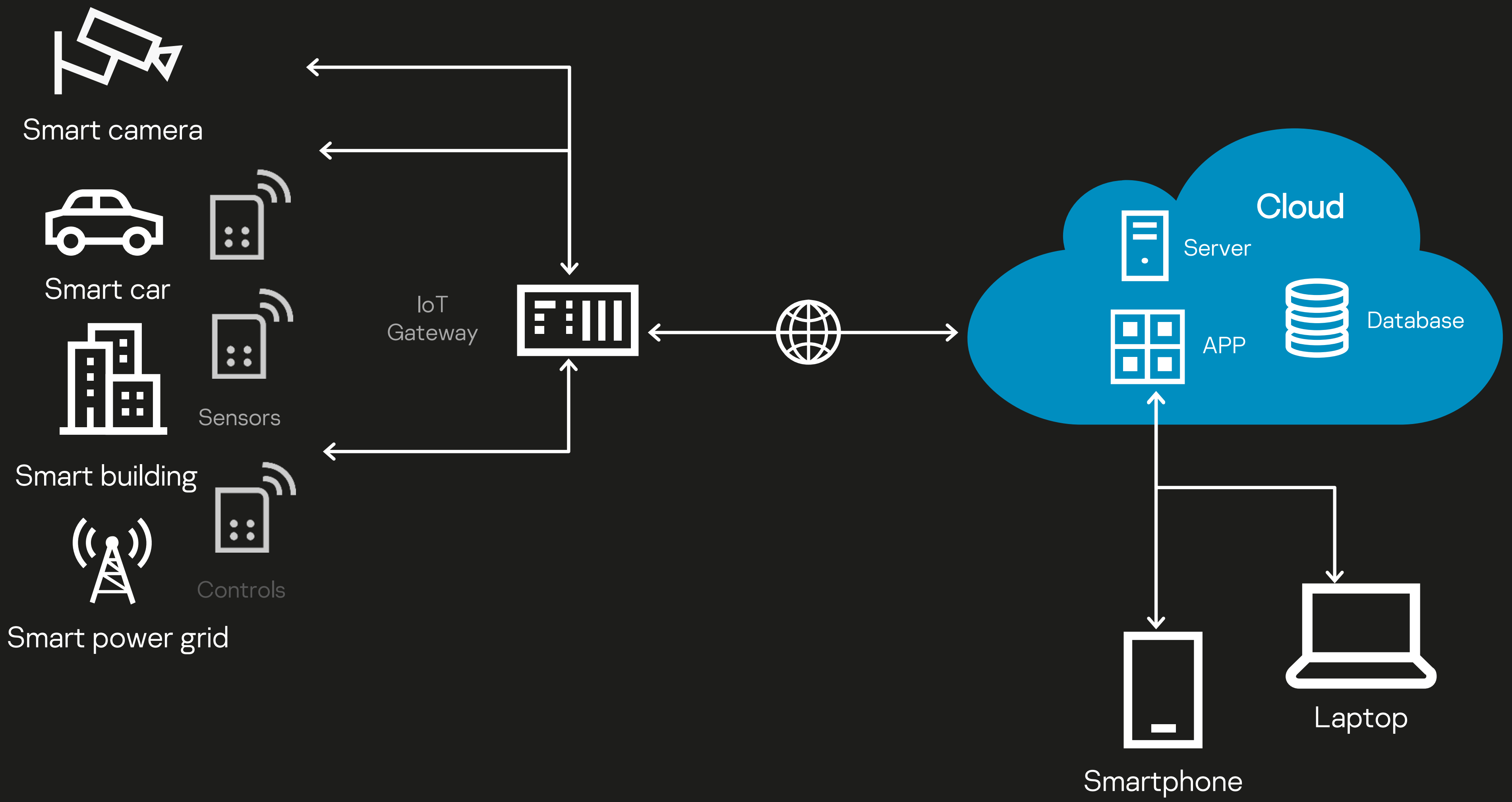
Utilities management: gas, water, electricity

Emergency prevention systems

Smart healthcare

CCTV

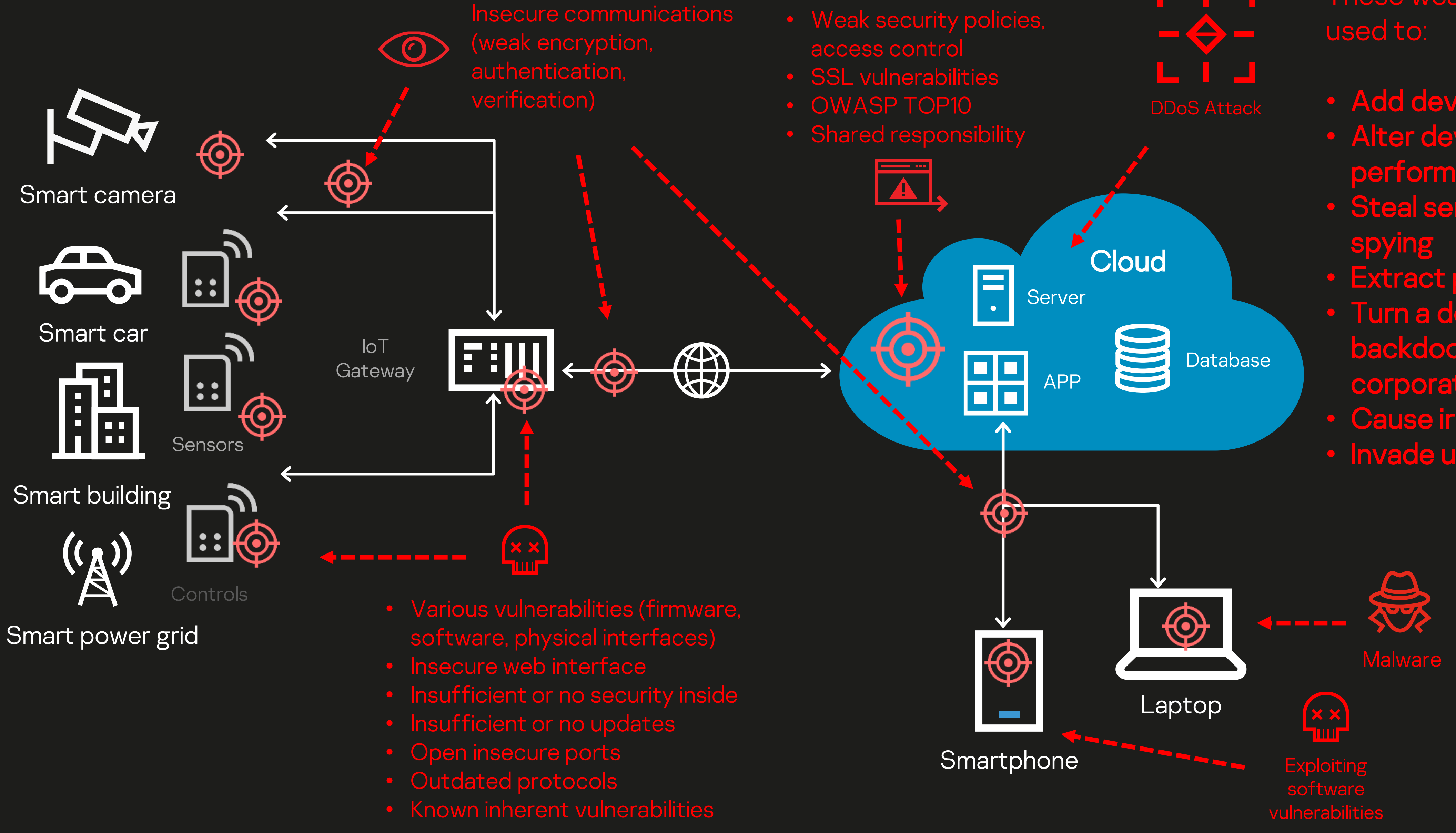
A smart city is based on IoT technologies



kaspersky

A smart city is based on IoT technologies

IoT is vulnerable



Insecure communications (weak encryption, authentication, verification)

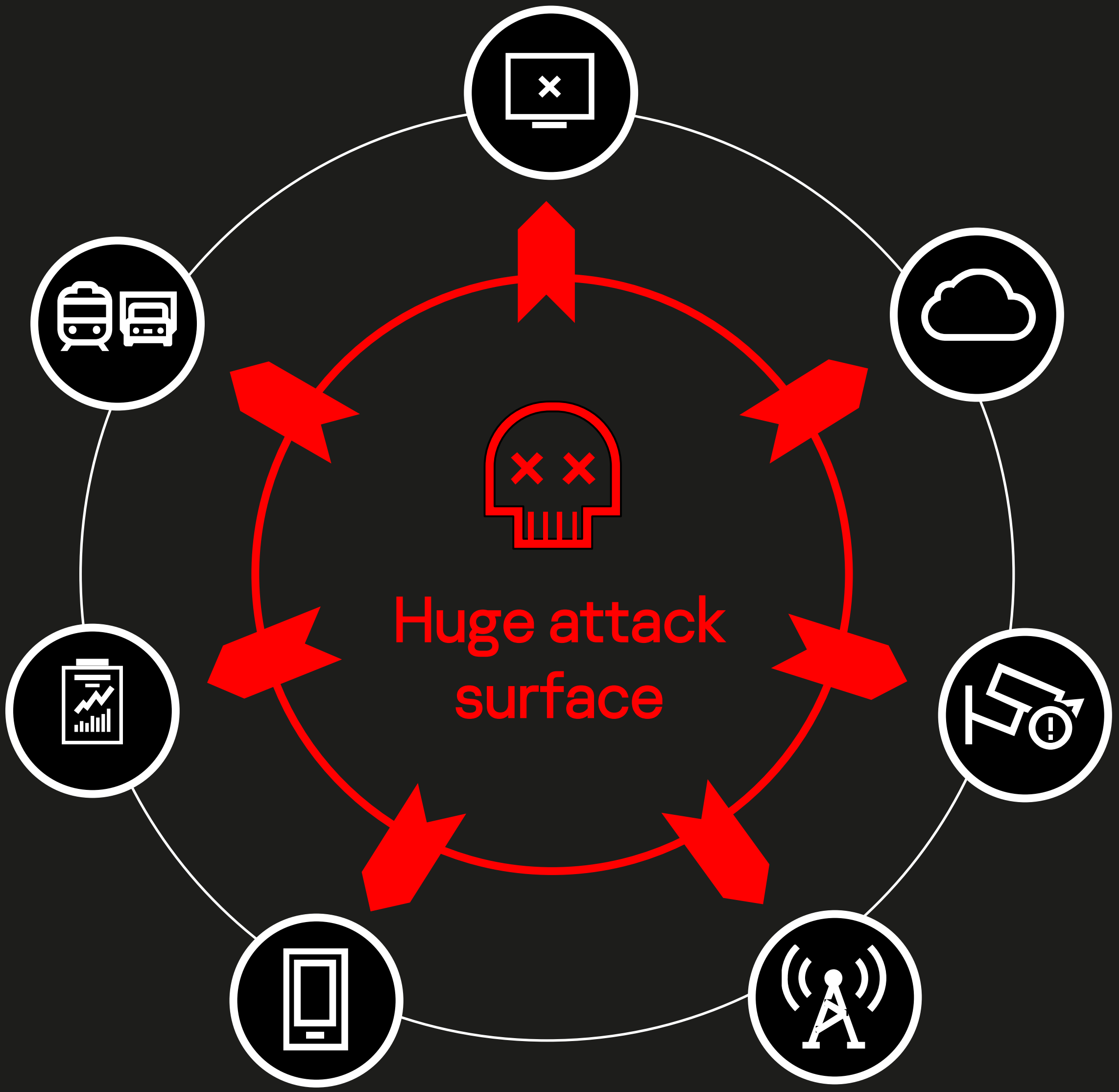
- Weak security policies, access control
- SSL vulnerabilities
- OWASP TOP10
- Shared responsibility

- Various vulnerabilities (firmware, software, physical interfaces)
- Insecure web interface
- Insufficient or no security inside
- Insufficient or no updates
- Open insecure ports
- Outdated protocols
- Known inherent vulnerabilities

These weaknesses can be used to:

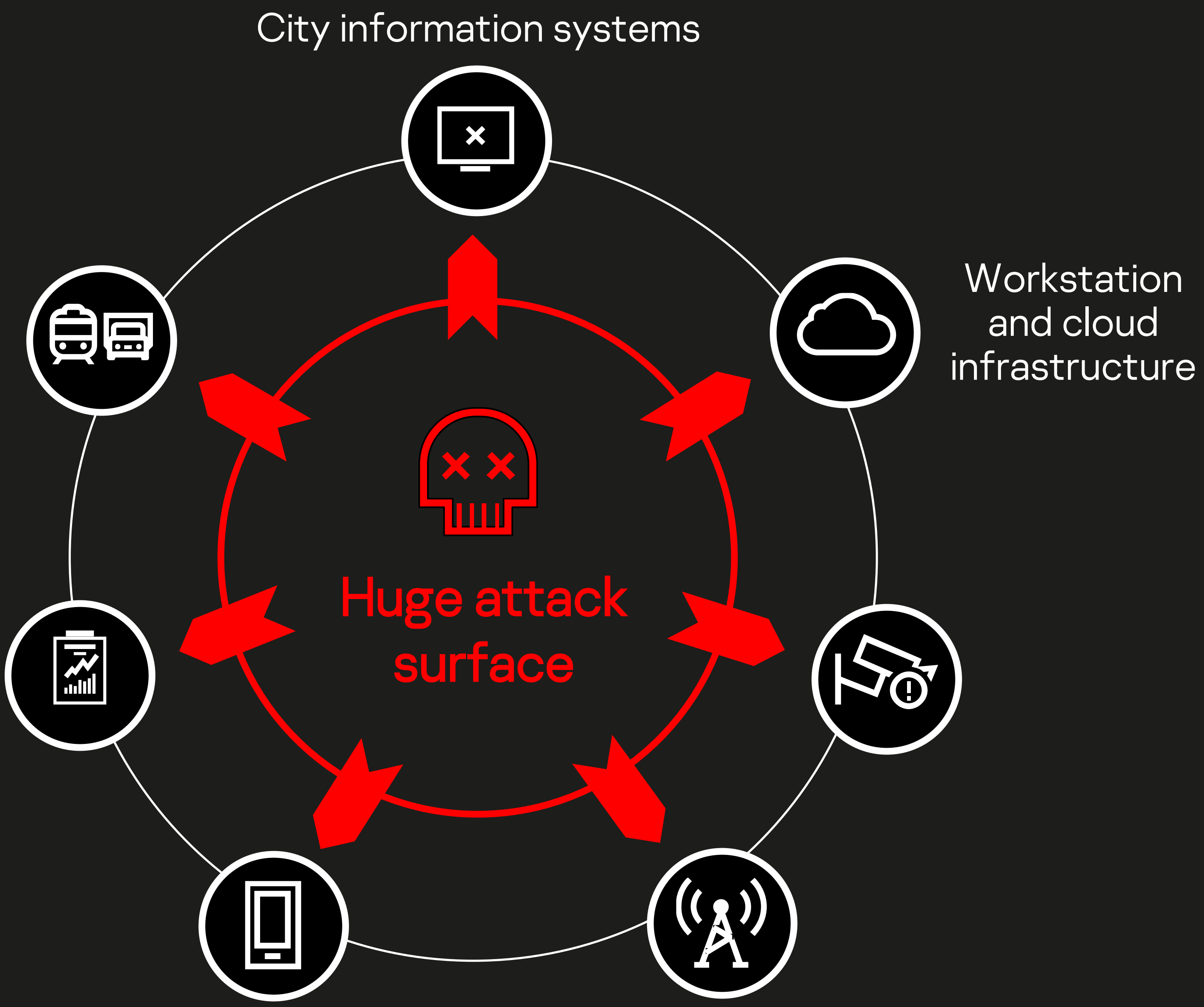
- Add devices to botnets
- Alter device behavior to perform spying, sabotage
- Steal sensitive data: spying
- Extract private credentials
- Turn a device into a backdoor to a user or corporate network
- Cause irreversible damage
- Invade user privacy

Advanced cyberthreats: All smart city systems are targets



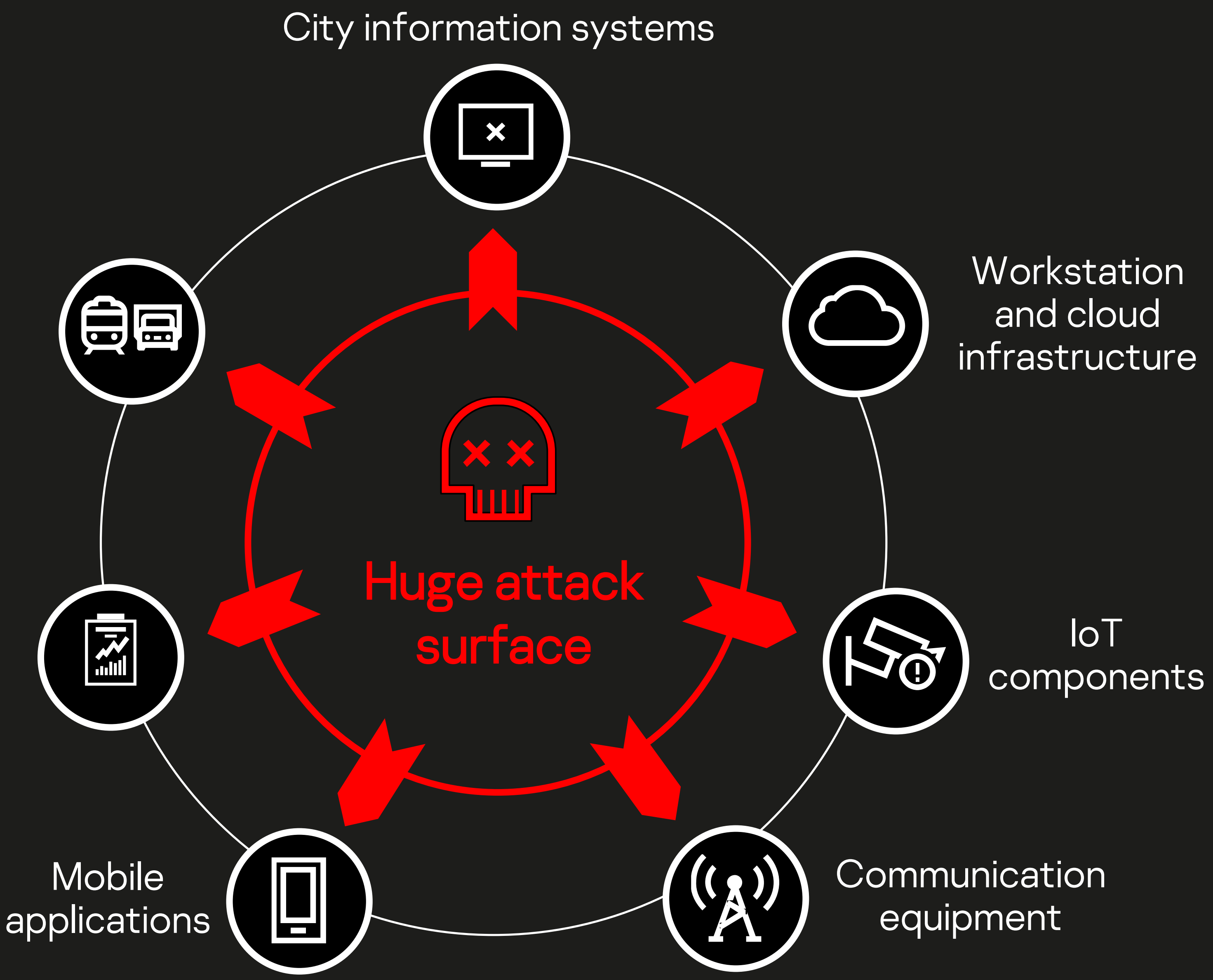
kaspersky

Advanced cyberthreats: All smart city systems are targets

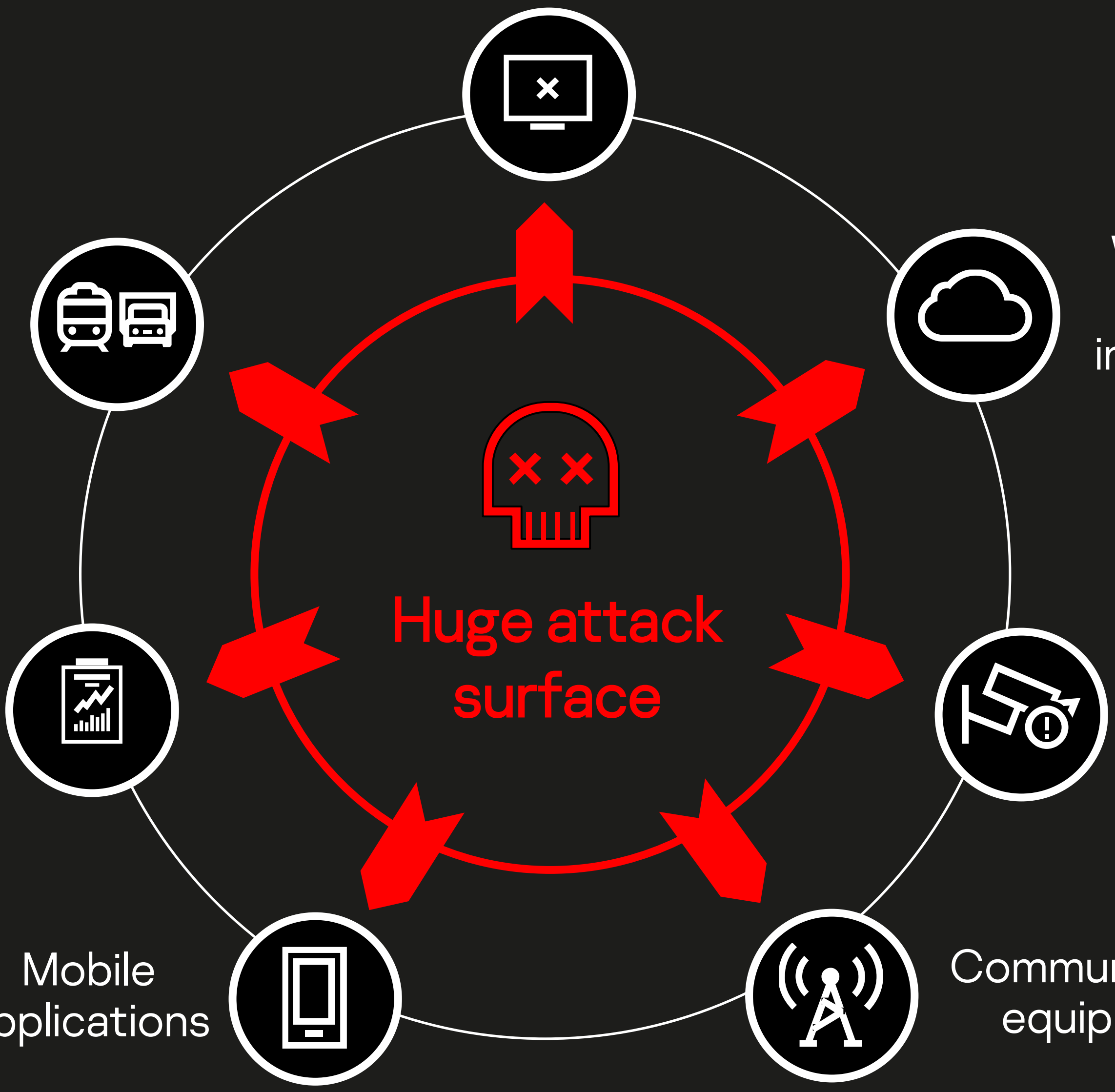


kaspersky

Advanced cyberthreats: All smart city systems are targets



Advanced cyberthreats: All smart city systems are targets



City information systems

Workstation and cloud infrastructure

IoT components

Communication equipment

Mobile applications

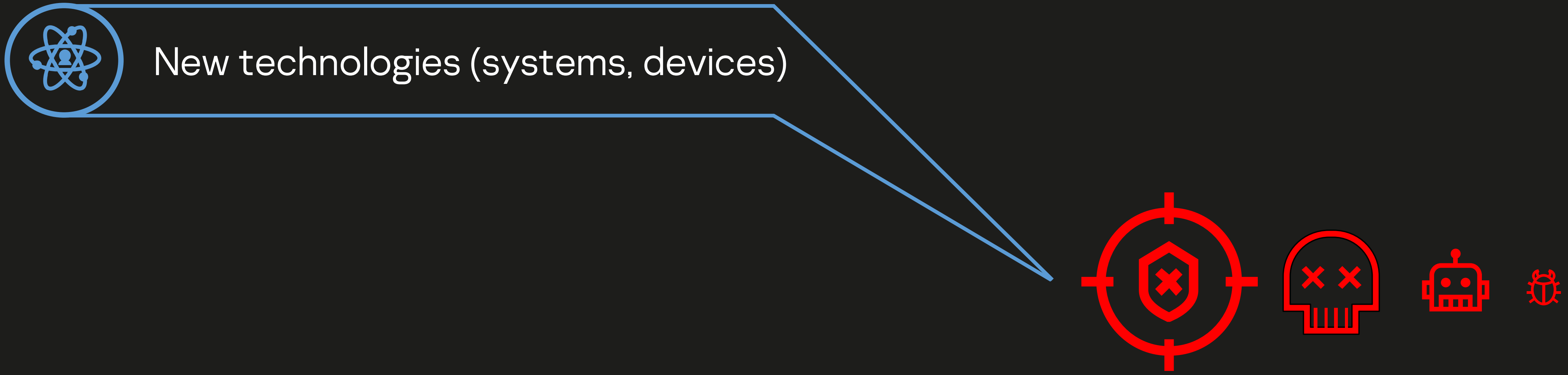
Smart grid and Utilities

Public transport and road infrastructure

Huge attack surface

kaspersky

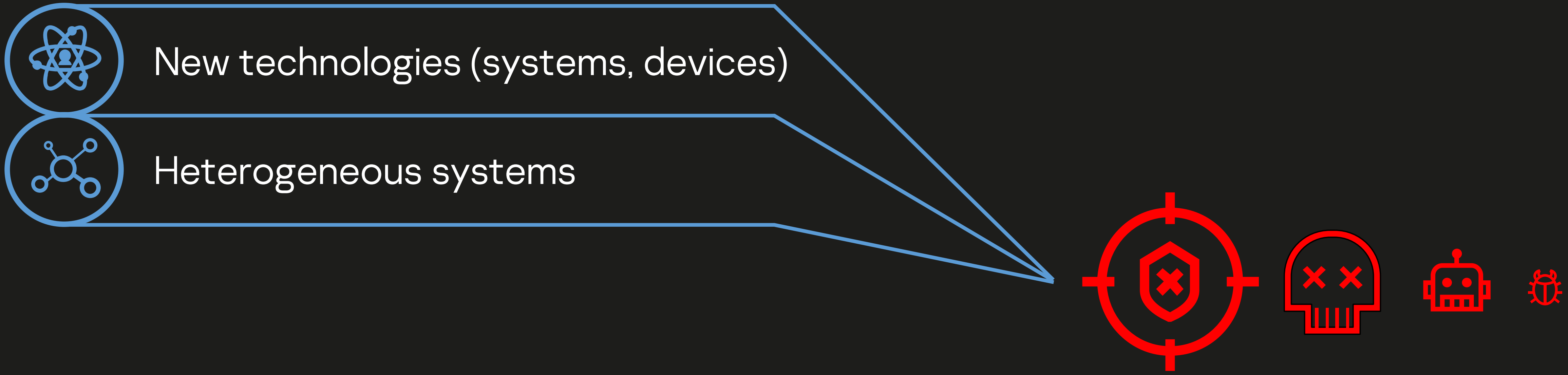
Advanced cyberthreats: Potential sources of problems



New technologies (systems, devices)

Exploitation of Vulnerabilities

Advanced cyberthreats: Potential sources of problems

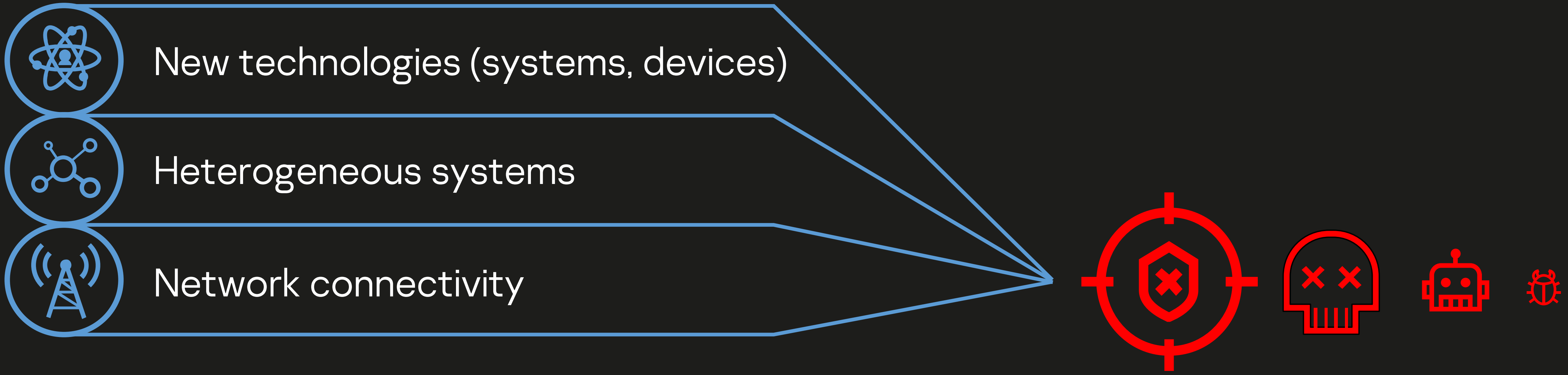


New technologies (systems, devices)

Heterogeneous systems

Exploitation of Vulnerabilities

Advanced cyberthreats: Potential sources of problems



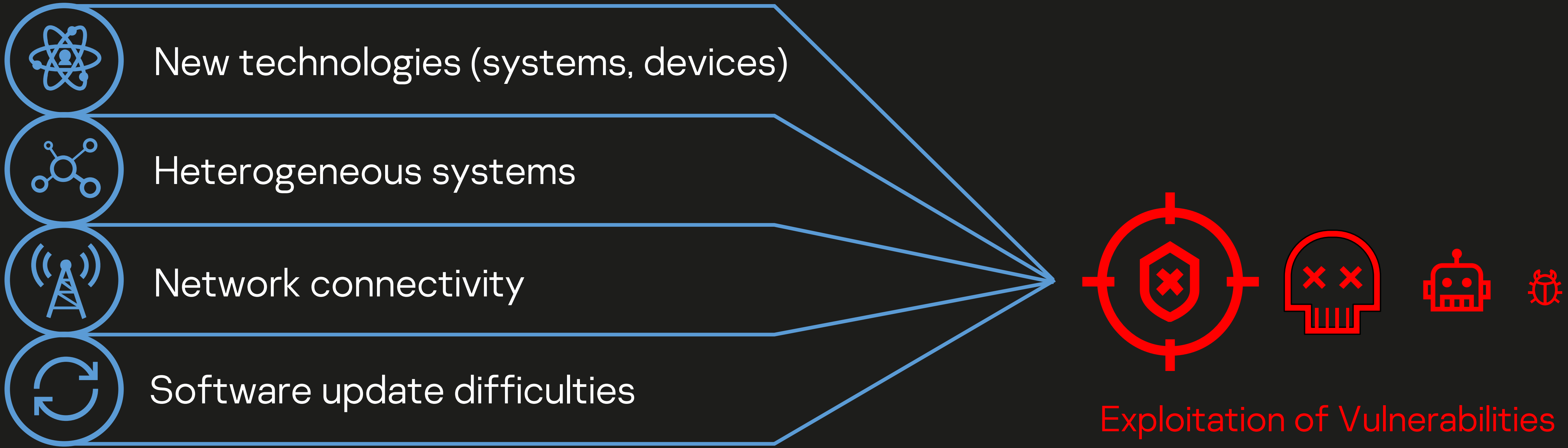
New technologies (systems, devices)

Heterogeneous systems

Network connectivity

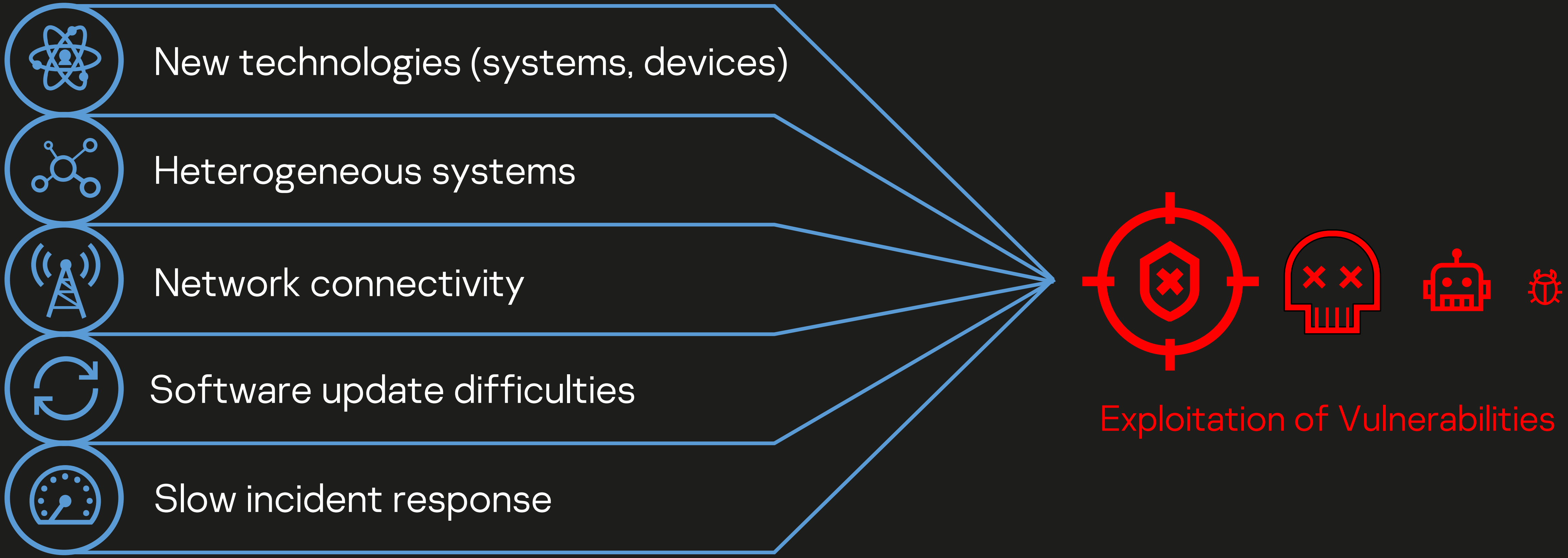
Exploitation of Vulnerabilities

Advanced cyberthreats: Potential sources of problems



New technologies (systems, devices)
Heterogeneous systems
Network connectivity
Software update difficulties
Exploitation of Vulnerabilities

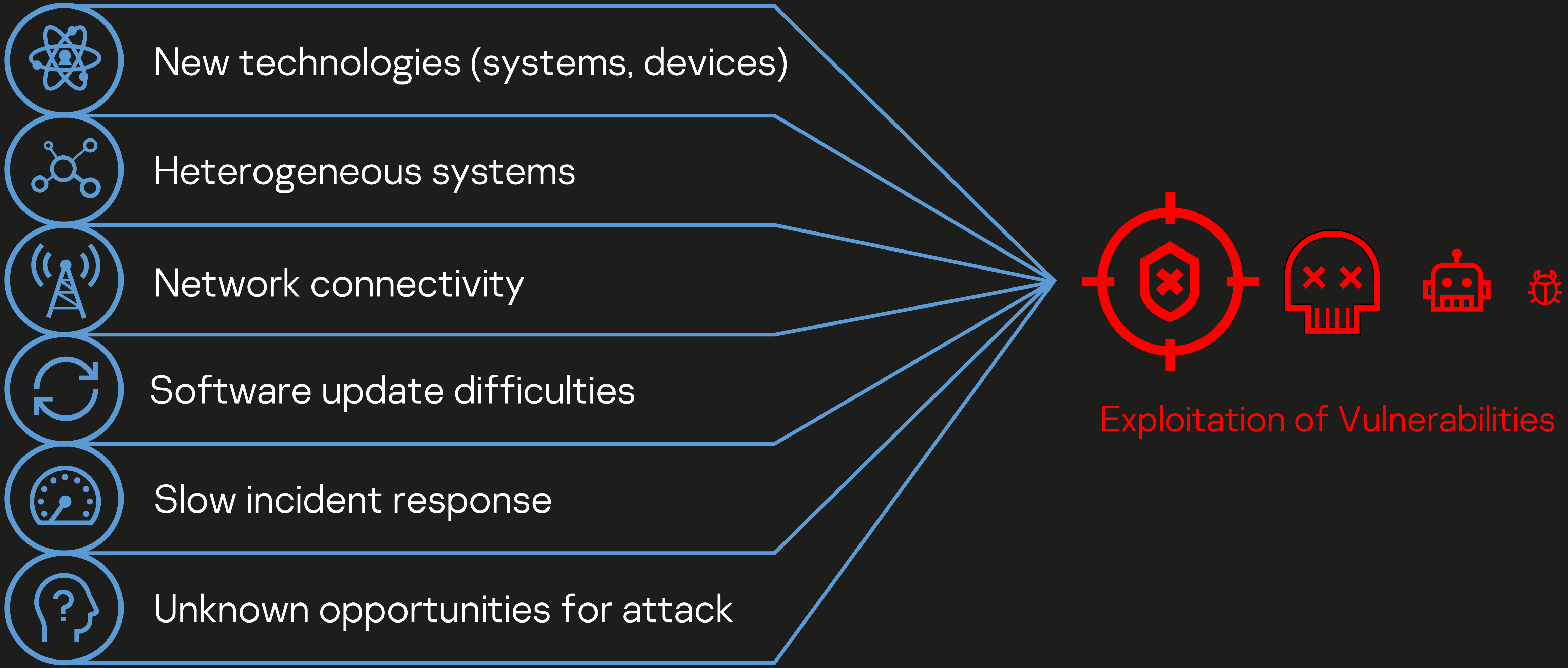
Advanced cyberthreats: Potential sources of problems



- New technologies (systems, devices)
- Heterogeneous systems
- Network connectivity
- Software update difficulties
- Slow incident response

Exploitation of Vulnerabilities

Advanced cyberthreats: Potential sources of problems



- New technologies (systems, devices)
- Heterogeneous systems
- Network connectivity
- Software update difficulties
- Slow incident response
- Unknown opportunities for attack

Exploitation of Vulnerabilities

Example: Attacks on traffic police cameras in Moscow region

January 2014. More than 100 traffic cameras in Moscow region disabled in cyber-incident

- Attack resulted in damage to file system of processing and control units, making it impossible to launch camera OS and software
- OS system logs damaged
- Malicious files detected
- Passwords to access OS changed with administrator rights.
- Outage - 5 days

https://www.interfax.ru/moscow/351263

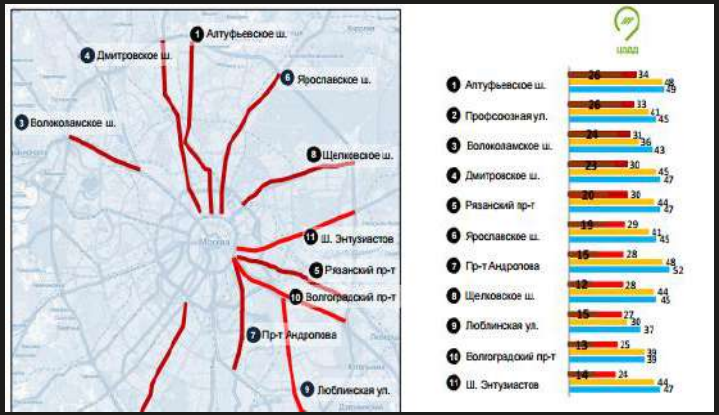
Kaspersky research: vulnerable cameras

- Many cameras have no protection from attacking or falsification of transmitted data.
- Wireless connectivity makes possible to perform Man-in-the-Middle attacks
- Attackers don’t need to be very skilled

https://securelist.com/does-cctv-put-the-public-at-risk-of-cyberattack/70008/

Kaspersky research: vulnerable traffic sensors

- Traffic sensors count the number of cars of varying size in each lane, determine their average speed, and send the data to a Traffic Control Center
- Some of sensor models use Bluetooth for data communication and configuration
- Sensor configurations tampering can affect traffic data and influence ‘smart’ traffic lights and other road equipment


1 Алтуфьевское ш.
4 Дмитровское ш.
6 Ярославское ш.
3 Волоколамское ш.
8 Щелковское ш.
Москва
11 Ш. Энтузиастов
5 Рязанский пр-т
10 Волгоградский пр-т
7 Пр-т Андропова
9 Люблинская ул.
ЦОДД
1 Алтуфьевское ш. 26 34 48 49
2 Профсоюзная ул. 26 33 41 45
3 Волоколамское ш. 24 31 36 43
4 Дмитровское ш. 23 30 45 47
5 Рязанский пр-т 20 30 44 47
6 Ярославское ш. 19 29 41 45
7 Пр-т Андропова 15 28 48 52
8 Щелковское ш. 12 28 44 45
9 Люблинская ул. 15 27 30 37
10 Волгоградский пр-т 13 25 39 39
11 Ш. Энтузиастов 14 24 44 47

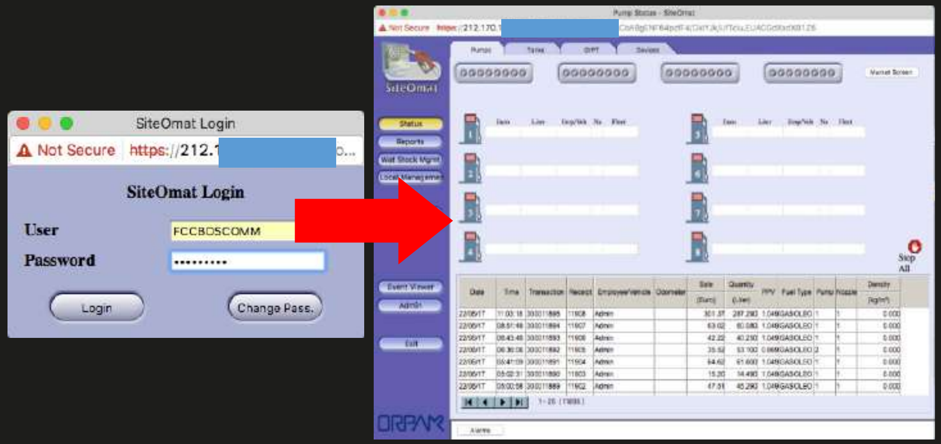
https://securelist.com/how-to-trick-traffic-sensors/74454/

Kaspersky research: vulnerable gas stations

Gas stations with Linux-based controller unit responsible for managing every component of the station, including dispensers, payment terminals and more.

WHAT an attacker can do:

- Shut down all fueling systems
- Cause fuel leaks and risk to life
- Change fuel prices
- Circumvent payment terminal to steal money
- Scrape vehicle license plates and driver identities
- Halt the station's operation until a ransom is paid
- Execute code on the controller unit



SiteOmat Login

Not Secure https://212.1[redacted]o...

SiteOmat Login

User FCCBOSCOMM

Password •••••••••

Pump Status - SiteOmat

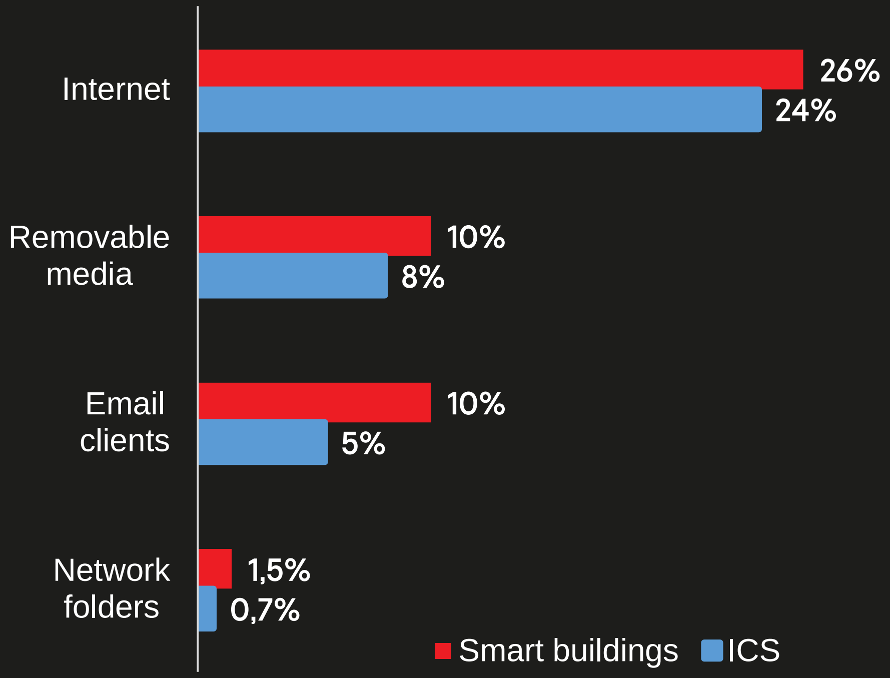
Not Secure https://212.170.1[redacted]

Date	Time	Transaction	Receipt	Employee/Vehicle	Odometer	Sale (Euro)	Quantity (Liter)	PPV	Fuel Type	Pump	Nozzle	Density (kg/m³)
22/06/17	11:03:18	300011895	11908	Admin		301.37	287.290	1.049	GASOLEO	1	1	0.000
22/06/17	08:51:48	300011894	11907	Admin		63.02	60.080	1.049	GASOLEO	1	1	0.000
22/06/17	08:43:48	300011893	11906	Admin		42.22	40.250	1.049	GASOLEO	1	1	0.000
22/06/17	06:36:06	300011892	11905	Admin		35.52	53.100	0.669	GASOLEO	2	1	0.000
22/06/17	05:41:09	300011891	11904	Admin		64.62	61.600	1.049	GASOLEO	1	1	0.000
22/06/17	05:02:31	300011890	11903	Admin		15.20	14.490	1.049	GASOLEO	1	1	0.000
22/06/17	05:00:58	300011889	11902	Admin		47.51	45.290	1.049	GASOLEO	1	1	0.000

https://securelist.com/expensive-gas/83542/

kaspersky

Kaspersky research : Smart building vulnerabilities



Sources of threats to building automation systems, H1 2019

Bad firmware update by a manufacturer of smart locks blocked all the doors of their clients

Vulnerability in smart security system linked to SSL certificates and access management

https://securelist.com/smart-buildings-threats/93322/
https://threatpost.com/smart-locks-bricked-by-bad-update/127427/
https://www.zdnet.com/article/security-flaw-internet-connected-home-security-system-remotely-control/

Example: Ransomware attack on city infrastructure

- November, 2016. San Francisco Municipal Transport Agency attacked by hackers who locked 2000+ computers and data, and forced to open all gates and allow passengers to ride for nothing

- June, 2019. Florida city pays $600,000 to hackers who seized control of its computer system

- June, 2019, Lake City was targeted by a malware attack known as “Triple Threat”, city government approved to pay $460,000

https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware
https://www.cbsnews.com/news/riviera-beach-florida-ransomware-attack-city-council-pays-600000-to-hackers-who-seized-its-computer-system/
https://www.lcfla.com/community/page/press-release-cyber-attack

Cybersecurity strategy for ‘smart cities’

The smart city development can be controlled by establishing the right principles to ensure long-term security for the overall operation of smart city components

Organizational

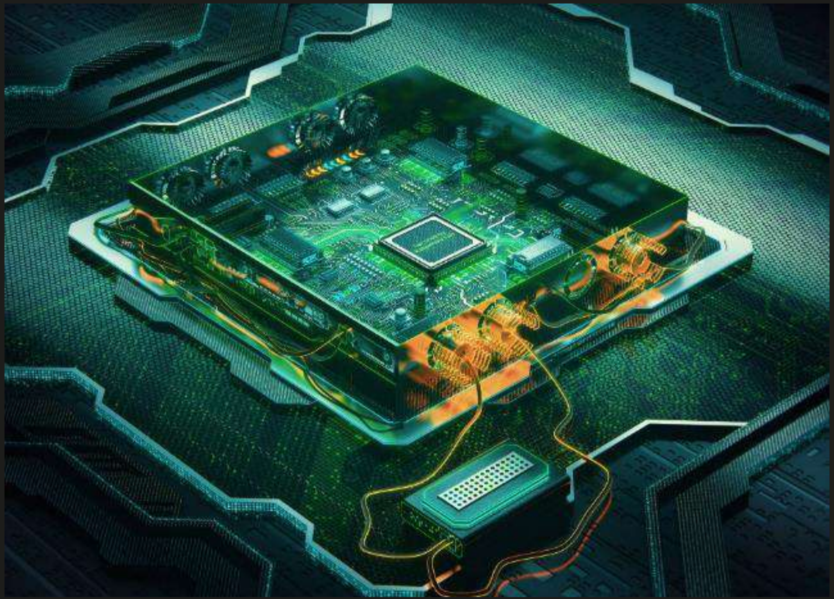
- Standardization (ISO/IEC)
- Education
- Threat analysis

Technological

- Timely implementation of cyberprotection
- Design based on IMMUNE systems

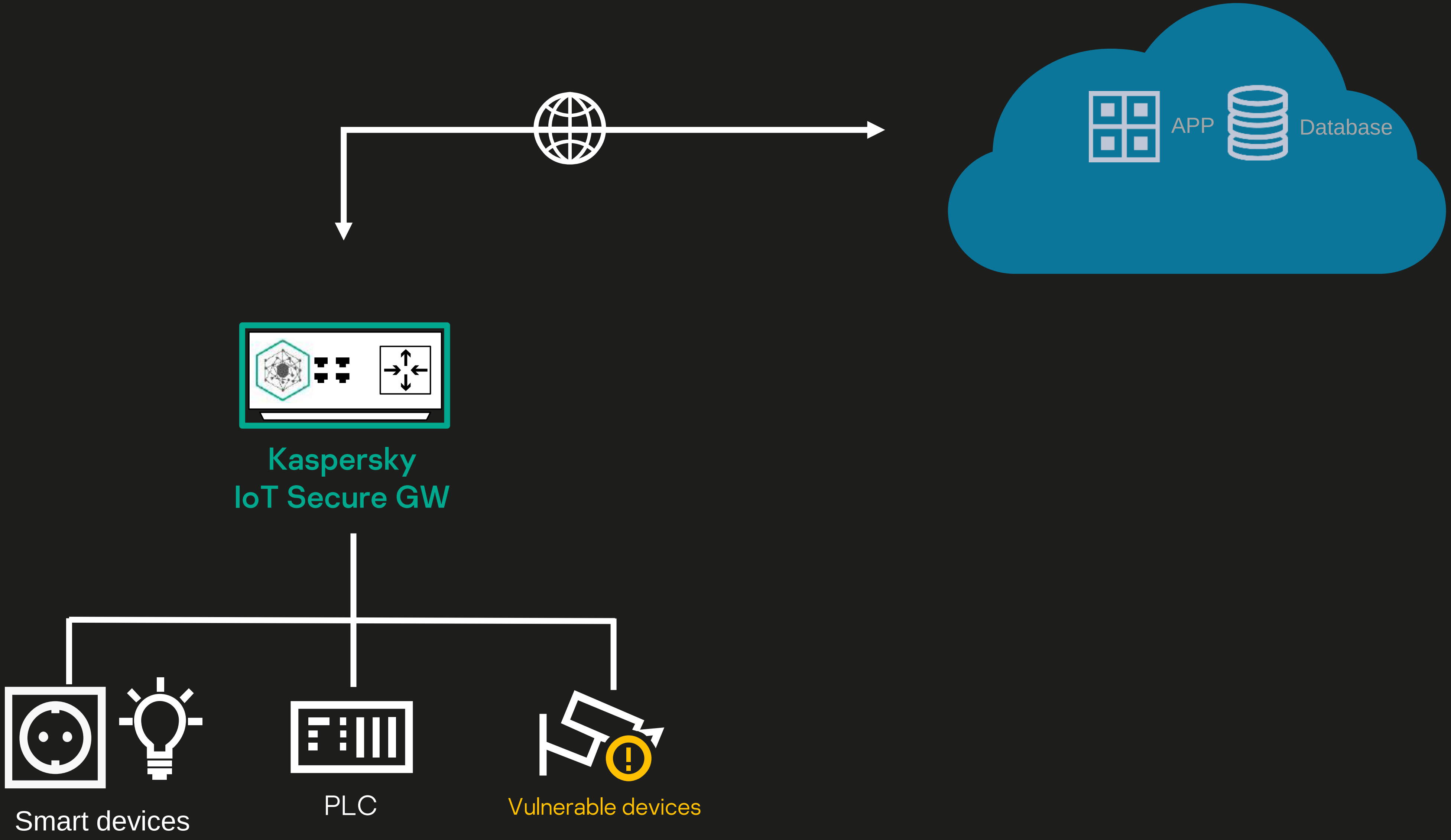
Kaspersky IMMUNITY principles

KasperskyOS®

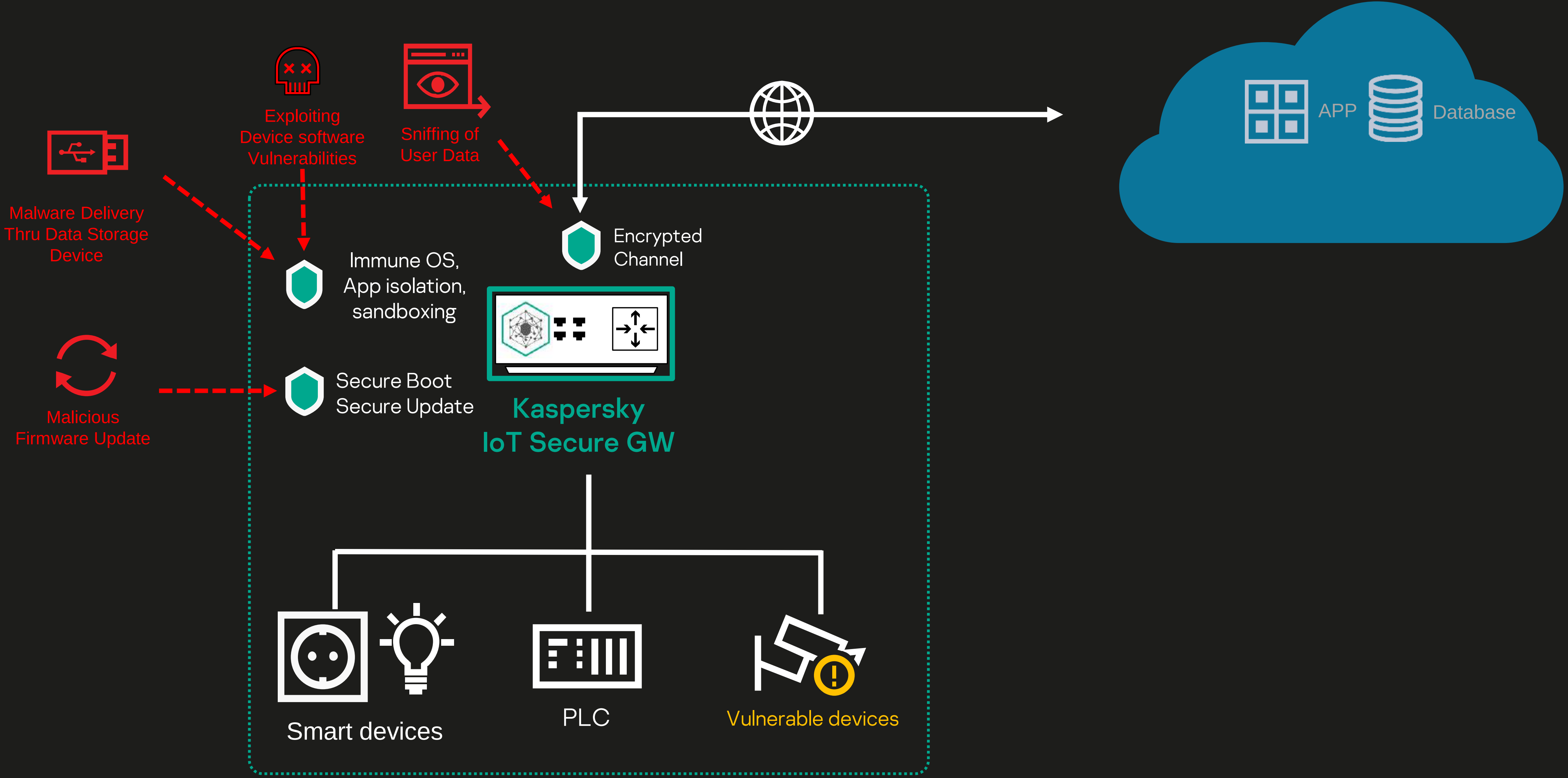


- Secure-by-design system
- Microkernel architecture
- Security layer isolation for all modules
- Trusted behaviour

How Kaspersky recommends protecting IoT infrastructure

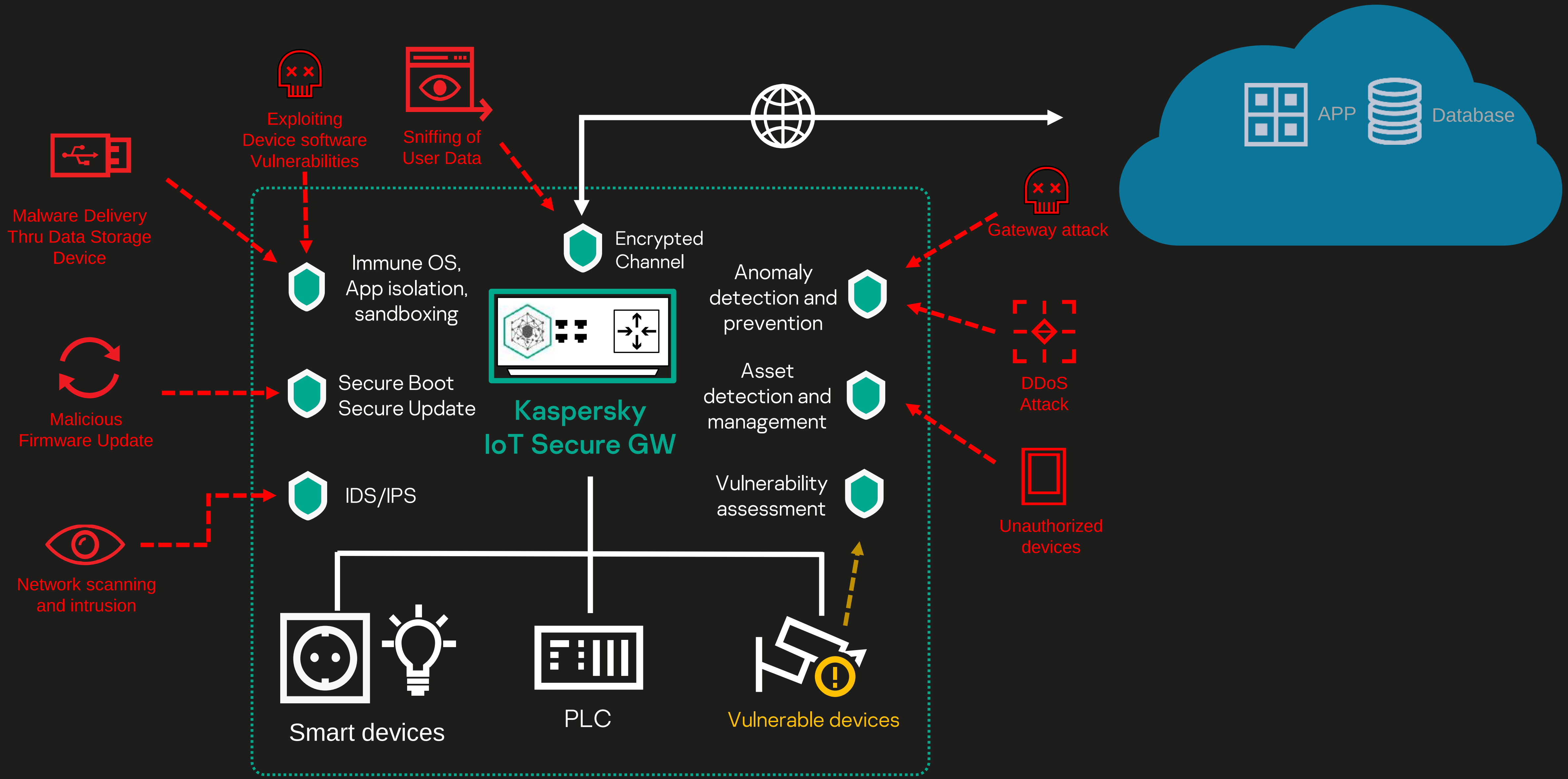


How Kaspersky recommends protecting IoT infrastructure



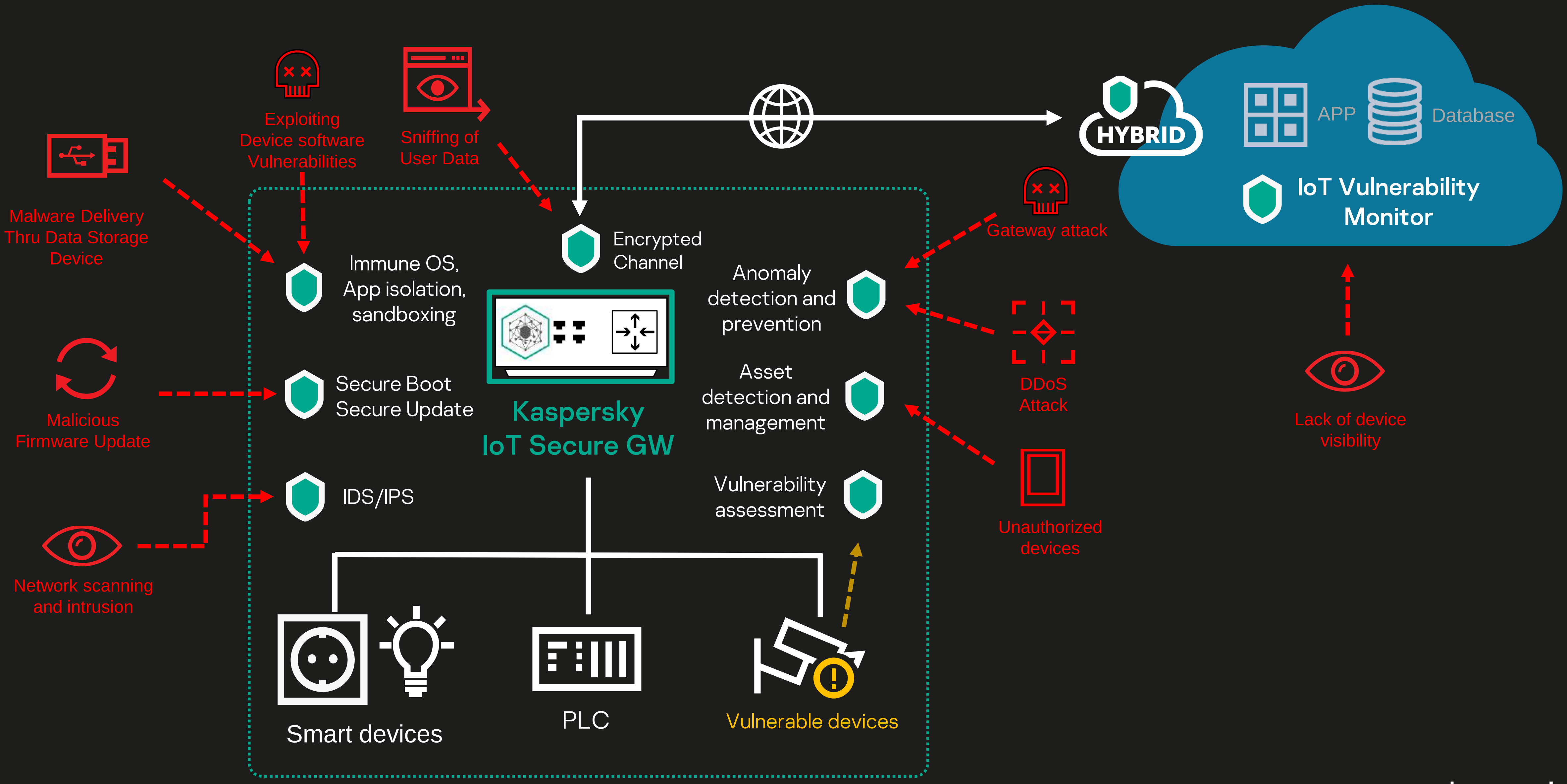
kaspersky

How Kaspersky recommends protecting IoT infrastructure



kaspersky

How Kaspersky recommends protecting IoT infrastructure



Exploiting Device software Vulnerabilities
Sniffing of User Data
Malware Delivery Thru Data Storage Device
HYBRID
APP
Database
IoT Vulnerability Monitor
Gateway attack
Encrypted Channel
Immune OS, App isolation, sandboxing
Anomaly detection and prevention
Kaspersky IoT Secure GW
Secure Boot Secure Update
Asset detection and management
DDoS Attack
Malicious Firmware Update
Lack of device visibility
IDS/IPS
Vulnerability assessment
Unauthorized devices
Network scanning and intrusion
Smart devices
PLC
Vulnerable devices

kaspersky

Conclusion

- A smart city is a dynamically developing concept
- It require cyberprotection capable of keeping pace with the development of modern technology
- Proper and effective development of this concept requires a long-term cybersecurity strategy

From Cybersecurity to Cyber-Immunity

kaspersky

kaspersky

IOT SOLUTIONS WORLD CONGRESS

Visit us at IoTSolutionsWorldCongress2019 : Hall 2, Stand 437

Thank you!

kaspersky.com