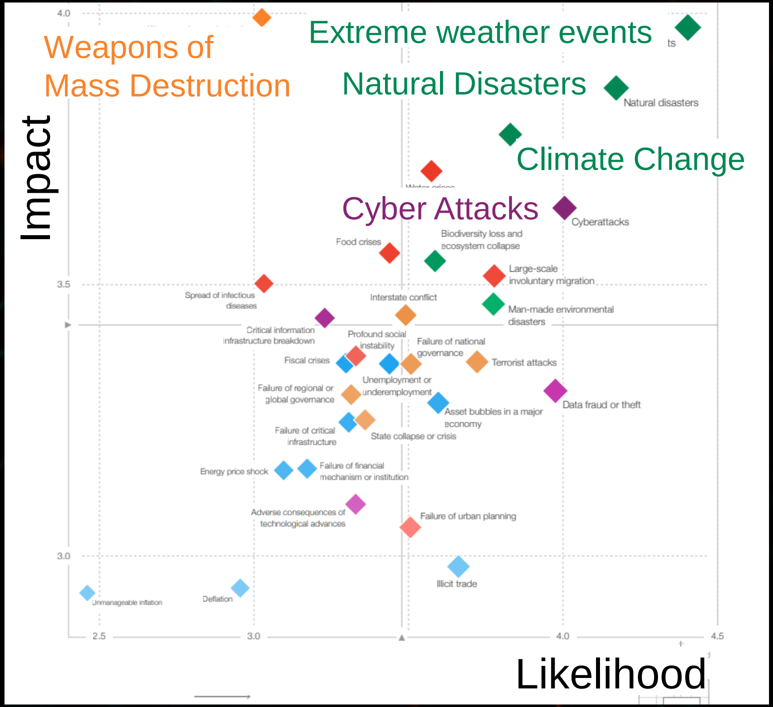
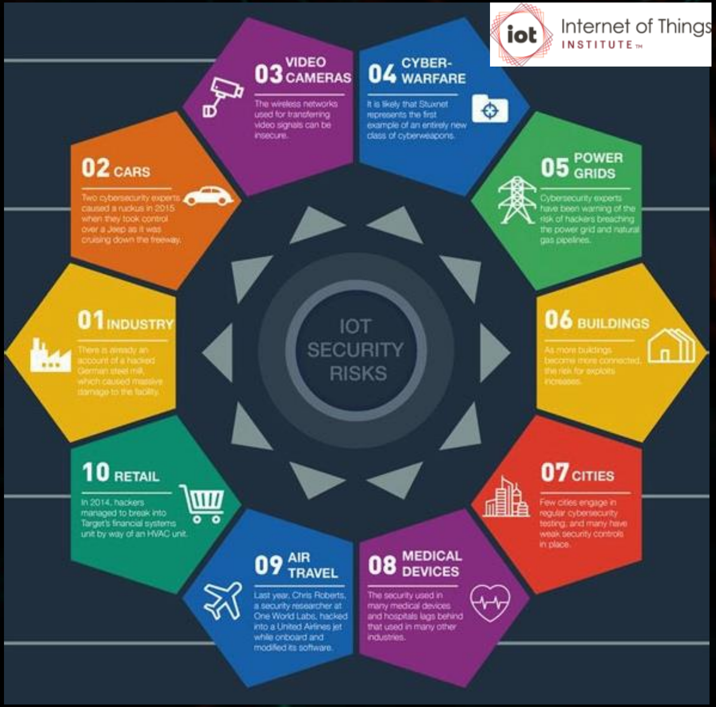
IoT Security for Critical Information Infrastructures

Andrey Tikhonov

THE SCALE OF EVENTS



World Economic Forum 2018



01 INDUSTRY
There is already an account of a hacked German steel mill, which caused massive damage to the facility.

02 CARS
Two cybersecurity experts caused a ruckus in 2015 when they took control over a Jeep as it was cruising down the freeway.

03 VIDEO CAMERAS
The wireless networks used for transferring video signals can be insecure.

04 CYBER-WARFARE
It is likely that Stuxnet represents the first example of an entirely new class of cyberweapons.

05 POWER GRIDS
Cybersecurity experts have been warning of the risk of hackers breaching the power grid and natural gas pipelines.

06 BUILDINGS
As more buildings become more connected, the risk for exploits increases.

07 CITIES
Few cities engage in regular cybersecurity testing, and many have weak security controls in place.

08 MEDICAL DEVICES
The security used in many medical devices and hospitals lags behind that used in many other industries.

09 AIR TRAVEL
Last year, Chris Roberts, a security researcher at One World Labs, hacked into a United Airlines jet while onboard and modified its software.

10 RETAIL
In 2014, hackers managed to break into Target's financial systems unit by way of an HVAC unit.

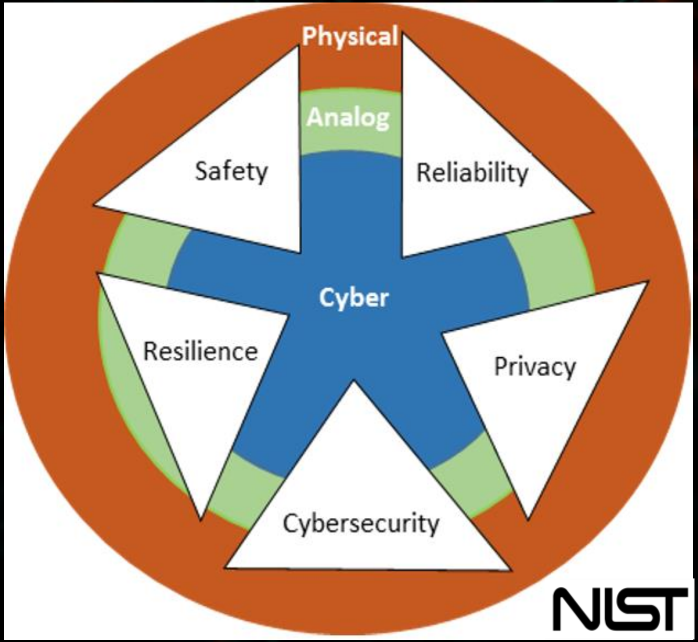
Top-10 IoT Security Targets

1

IoT and Critical Information Infrastructures

EVOLUTION OF SECURITY IN ”SMART” SYSTEMS

CYBER-PHYSICAL SYSTEMS



SECURITY DOMAINS

EVOLUTION OF “TRUST NETWORKS”

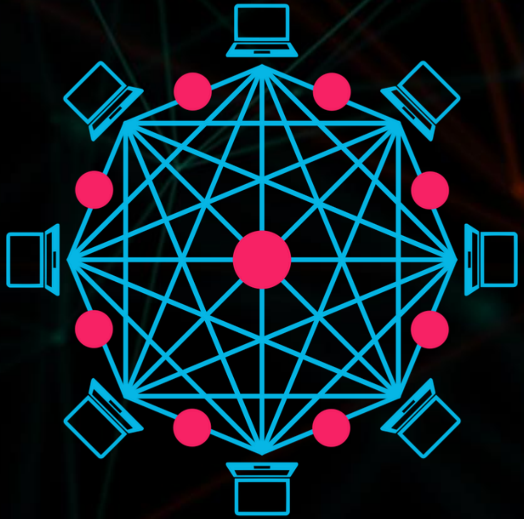
CENTRALISED

INSTITUTIONAL
(AUTHORITY)

DECENTRALISED

INTERPERSONAL
(SOCIAL CONTROL)

DISTRIBUTED



BLOCKCHAIN
(AUTONOMOUS)

PROTECTING THE CRITICAL INFORMATION INFRASTRUCTURE

The State emphasises the protection of Key Information Infrastructure in public communications and information services, i.e telecommunications, energy, finance, transportation, water conservation, public services and e-governance, as well as other critical information infrastructure that could cause serious damage to national security, the national economy and public interest if destroyed, functionality is lost or data is leaked (Articles 31, 187)

Federal Law on Critical Information Infrastructure

China's Network Security Law and Key Information Infrastructure

Department for Digital, Culture Media & Sport

Secure by Design: Improving the cyber security of consumer Internet of Things Report

Policy of Critical Information Infrastructure Protection Information Security Strategy for Protecting the Nation

HOW WE FIT WITH THE REGULATORY TREND

- Priorities to the **nationally certified** technologies and solutions or even direct requirements for their use in CII Protection

↔

- **Security by design** not only contributes to trust but makes the verification and thus certification of technologies easier

- Cyberspace and **CII sovereignty** (cross-border data transmission rules + in-house control of key technologies)

↔

- Increasing trustworthiness level for solutions on a base of clear **trust architecture** specific to the regulation

- **General auditing and supervising the protection of CII**, from the classification of CII systems to on-site checks

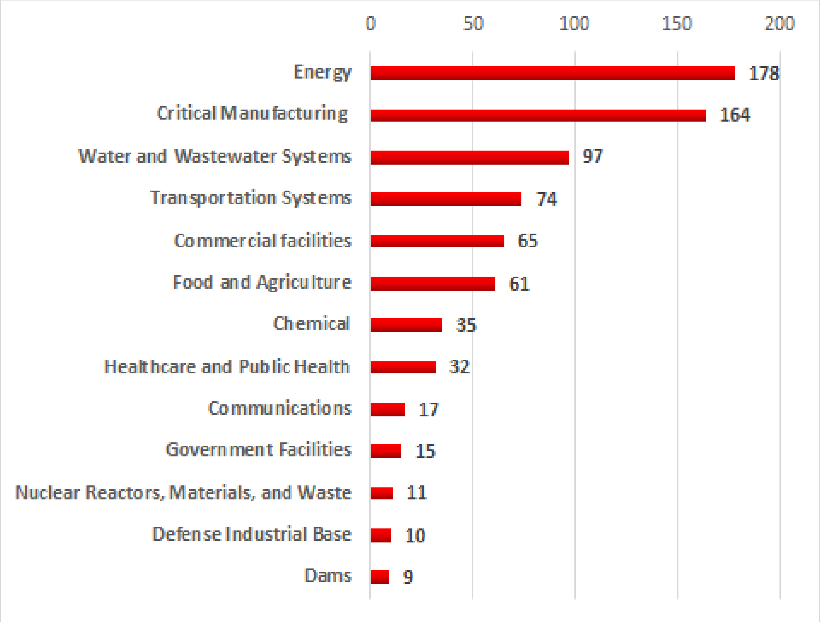
↔

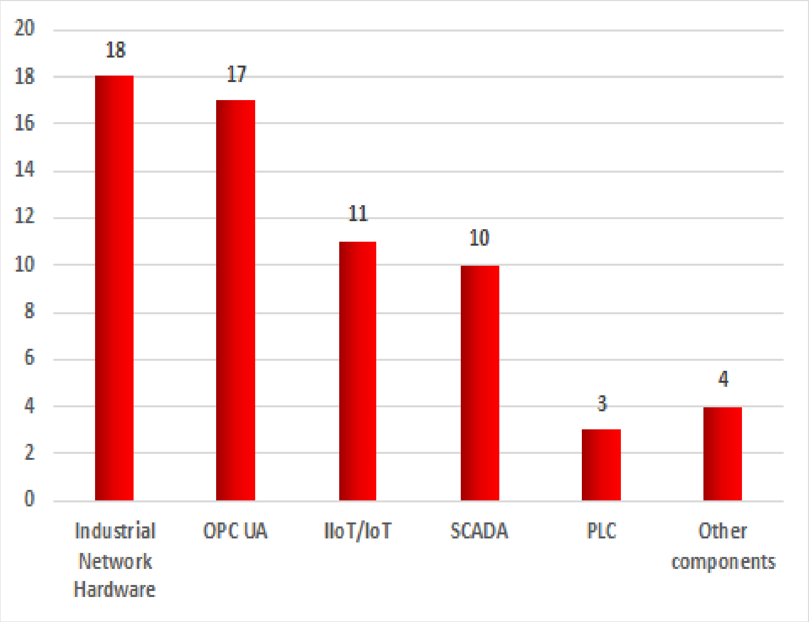
- Combination of state-of-the-art solutions with services supporting the proper **security maturity level**

2 IoT VULNERABILITIES, THREATS AND RISKS

IoT VULNERABILITIES

Kaspersky Lab ICS CERT identified 63 vulnerabilities in industrial and IIoT/IoT systems in 2017





BY INDUSTRY

BY COMPONENT

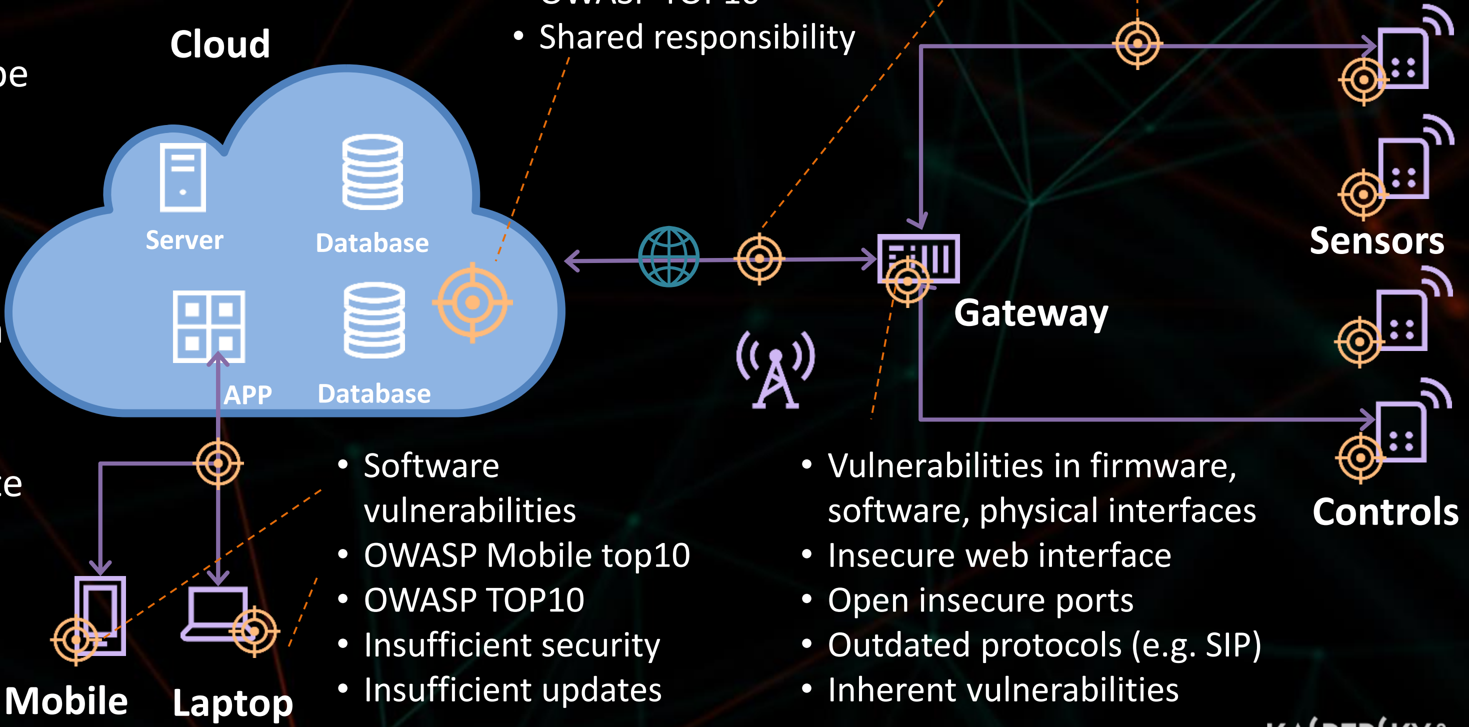
Source: https://ics-cert.kaspersky.com/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017

IoT VULNERABILITIES

Adversary

Weaknesses can be used for:

- BotNets
- Backdoors
- Privacy violation
- Data theft
- Spying
- Extracting private credentials



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

Insecure communications (week encryption, authentication, verification, etc)

- Software vulnerabilities
- OWASP Mobile top10
- OWASP TOP10
- Insufficient security
- Insufficient updates

- Vulnerabilities in firmware, software, physical interfaces
- Insecure web interface
- Open insecure ports
- Outdated protocols (e.g. SIP)
- Inherent vulnerabilities

◎ **Threat surface**

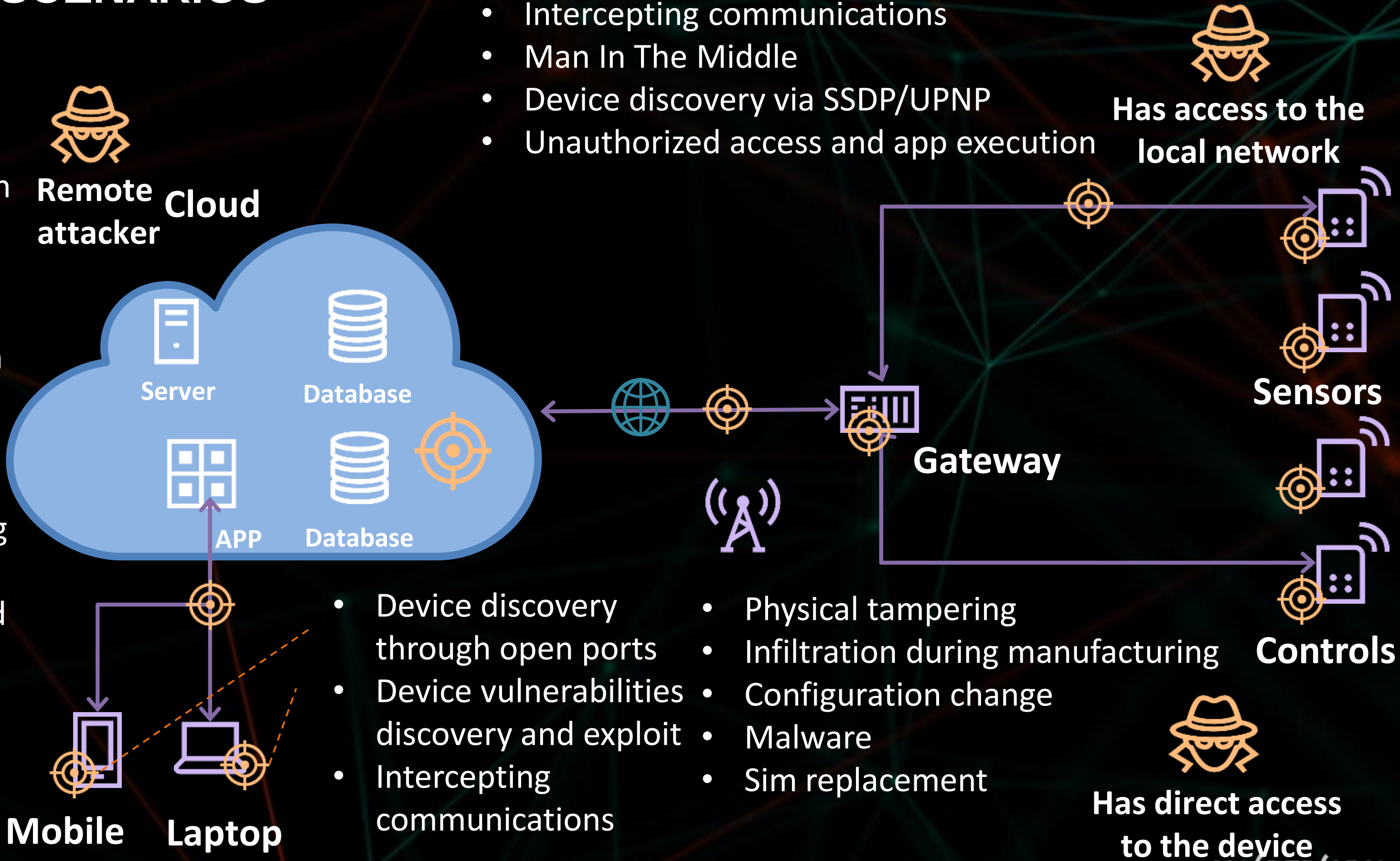
IOT ATTACK SCENARIOS

- MITC: Man in the Cloud
- User impersonation
- Plant backdoors
- Buffer overflow
- SQL Injection
- Privilege escalation
- Side channel
- DDoS
- Data integrity
- Certificate spoofing
- Phishing
- Drive-By-Download
- Brute Force
- Password reset

- Intercepting communications
- Man In The Middle
- Device discovery via SSDP/UPNP
- Unauthorized access and app execution

- Device discovery through open ports
- Device vulnerabilities discovery and exploit
- Intercepting communications

- Physical tampering
- Infiltration during manufacturing
- Configuration change
- Malware
- Sim replacement



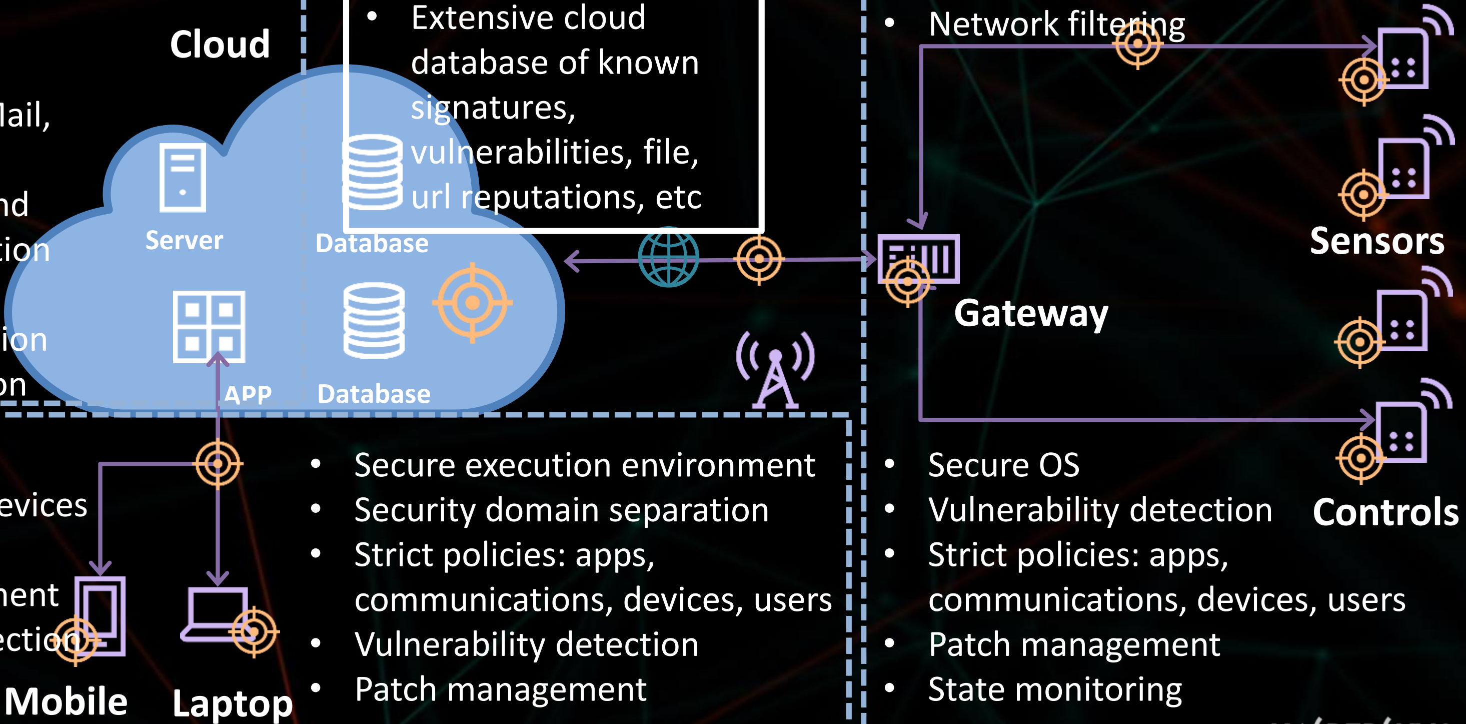
◎ Attack surface

IOT SECURITY ELEMENTS

- DDOS protection
- Advanced persistent threat protection
- Various servers protection: Web, Mail, File...
- Virtual machines and hypervisors protection
- Secure Hypervisor
- Security Orchestration
- Perimeter protection

- **SECURITY CENTER**
- Intelligence services
- Extensive cloud database of known signatures, vulnerabilities, file, url reputations, etc

- Communication anomalies and violations detection (DPI, Machine Learning)
- Intrusion detection
- Network filtering



- Whitelisting: apps, communications, devices
- Antivirus
- Reputation assessment
- Vulnerabilities Detection
- Firewall

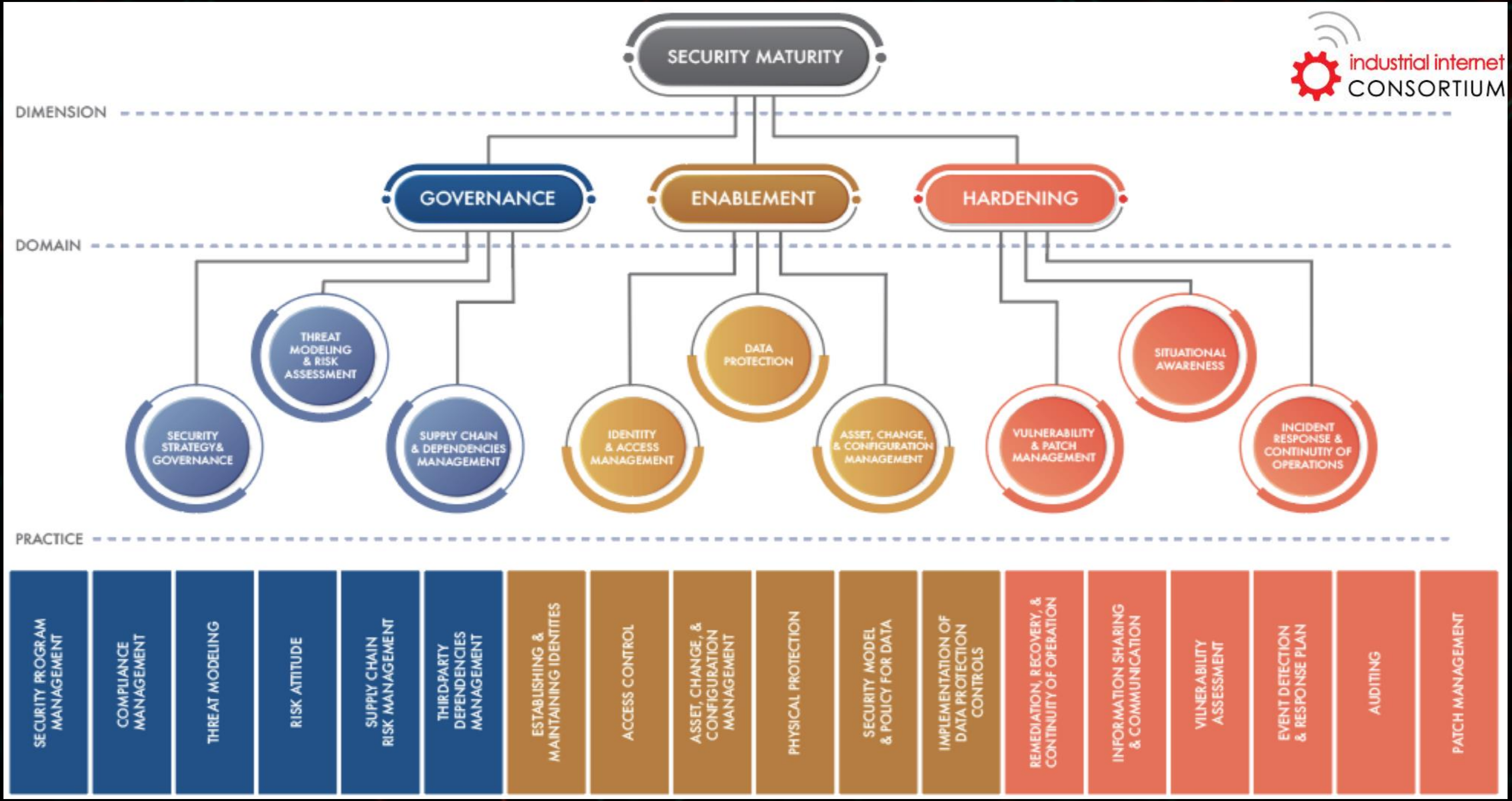
- Secure execution environment
- Security domain separation
- Strict policies: apps, communications, devices, users
- Vulnerability detection
- Patch management

- Secure OS
- Vulnerability detection
- Strict policies: apps, communications, devices, users
- Patch management
- State monitoring

3

BEST PRACTICES

IIC IoT SECURITY MATURITY MODEL



industrial internet CONSORTIUM

SECURITY MATURITY

DIMENSION

GOVERNANCE

ENABLEMENT

HARDENING

DOMAIN

SECURITY STRATEGY& GOVERNANCE

THREAT MODELING & RISK ASSESSMENT

SUPPLY CHAIN & DEPENDENCIES MANAGEMENT

IDENTITY & ACCESS MANAGEMENT

DATA PROTECTION

ASSET, CHANGE, & CONFIGURATION MANAGEMENT

VULNERABILITY & PATCH MANAGEMENT

SITUATIONAL AWARENESS

INCIDENT RESPONSE & CONTINUTIY OF OPERATIONS

PRACTICE

SECURITY PROGRAM MANAGEMENT

COMPLIANCE MANAGEMENT

THREAT MODELING

RISK ATTITUDE

SUPPLY CHAIN RISK MANAGEMENT

THIRD-PARTY DEPENDENCIES MANAGEMENT

ESTABLISHING & MAINTAINING IDENTITES

ACCESS CONTROL

ASSET, CHANGE, & CONFIGURATION MANAGEMENT

PHYSICAL PROTECTION

SECURITY MODEL & POLICY FOR DATA

IMPLEMENTATION OF DATA PROTECTION CONTROLS

REMEDIATION, RECOVERY, & CONTINUITY OF OPERATION

INFORMATION SHARING & COMMUNICATION

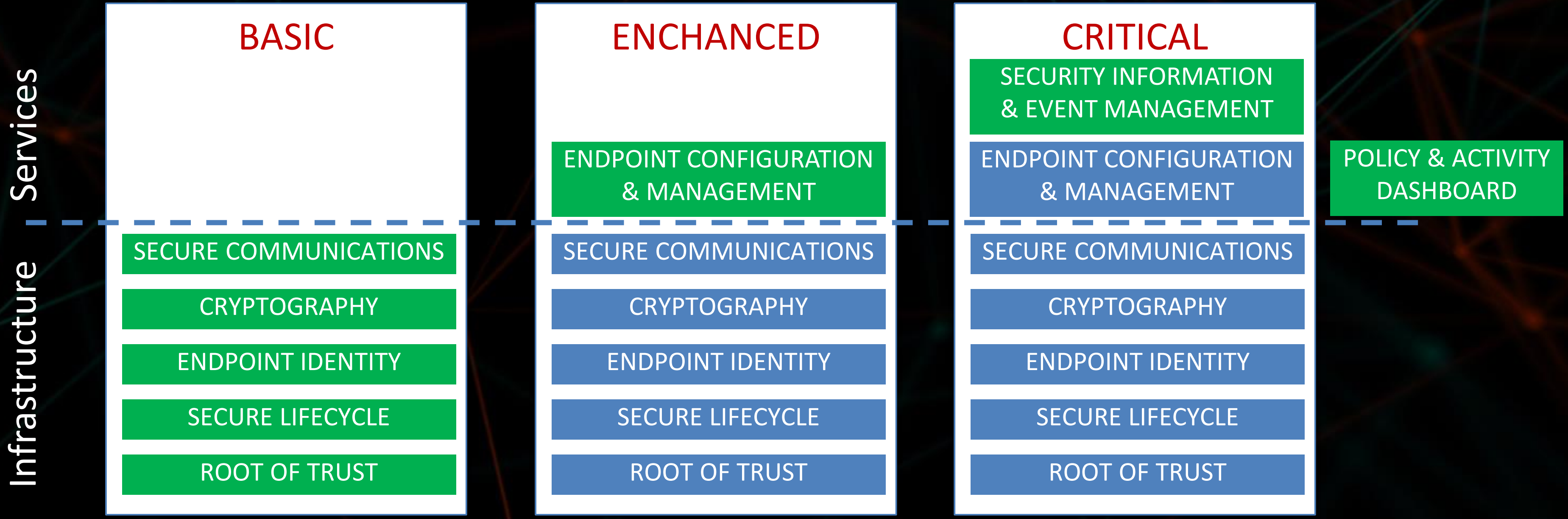
VILNERABILITY ASSESSMENT

EVENT DETECTION & RESPONSE PLAN

AUDITING

PATCH MANAGEMENT

IIC ENDPOINT SECURITY BEST PRACTICES



Services

Infrastructure

BASIC

- SECURE COMMUNICATIONS
- CRYPTOGRAPHY
- ENDPOINT IDENTITY
- SECURE LIFECYCLE
- ROOT OF TRUST

ENCHANCED

- ENDPOINT CONFIGURATION & MANAGEMENT
- SECURE COMMUNICATIONS
- CRYPTOGRAPHY
- ENDPOINT IDENTITY
- SECURE LIFECYCLE
- ROOT OF TRUST

CRITICAL

- SECURITY INFORMATION & EVENT MANAGEMENT
- ENDPOINT CONFIGURATION & MANAGEMENT
- SECURE COMMUNICATIONS
- CRYPTOGRAPHY
- ENDPOINT IDENTITY
- SECURE LIFECYCLE
- ROOT OF TRUST

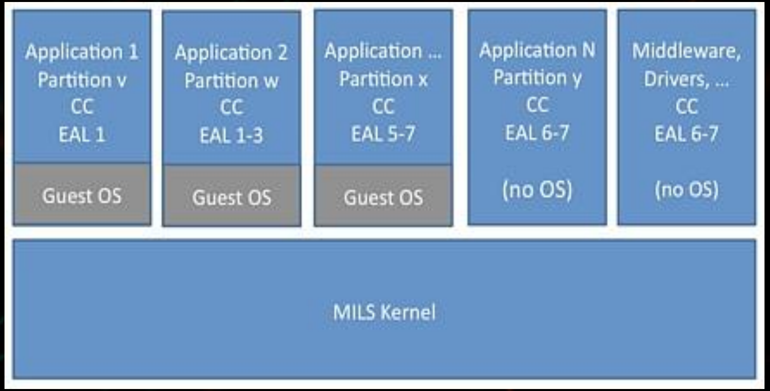
POLICY & ACTIVITY DASHBOARD

Intentional violation using simple means and limited resources

Intentional violation using sophisticated means and sufficient resources

Intentional violation using sophisticated means and large resources

MILS - MULTIPLE INDEPENDENT LEVELS OF SECURITY



Application 1
Partition v
CC
EAL 1
Guest OS

Application 2
Partition w
CC
EAL 1-3
Guest OS

Application ...
Partition x
CC
EAL 5-7
Guest OS

Application N
Partition y
CC
EAL 6-7
(no OS)

Middleware,
Drivers, ...
CC
EAL 6-7
(no OS)

MILS Kernel

EURO MILS

D-MILS

CITADEL
CRITICAL INFRASTRUCTURE PROTECTION USING ADAPTIVE MILS

THALES

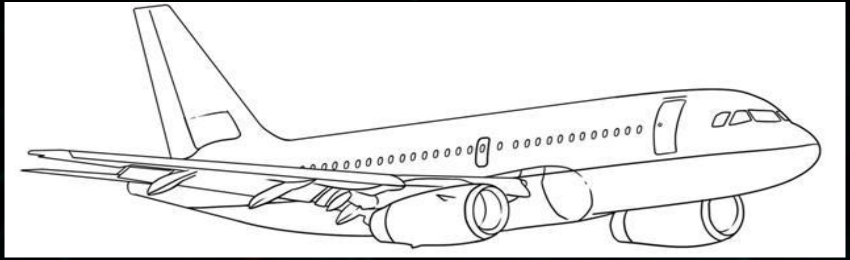
AIRBUS GROUP

TECHNIKON

SYSGO
EMBEDDING INNOVATIONS

Green Hills®

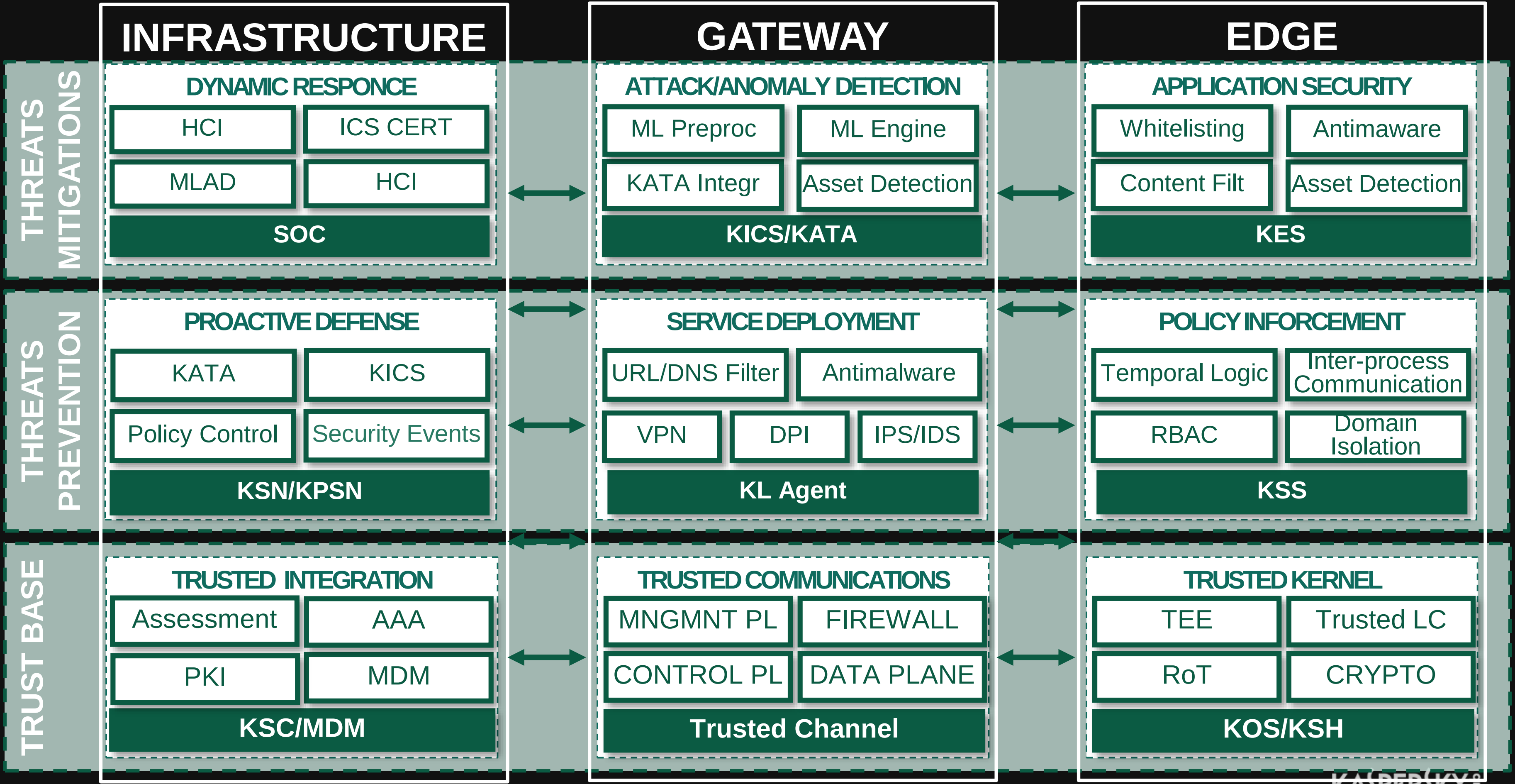
WIND RIVER



4

PRACTICAL STEPS

	INFRASTRUCTURE	GATEWAY	EDGE
THREATS MITIGATION	DYNAMIC SITUATIONAL AWARENESS Event Management	ATTACK ANOMALY DETECTION Monitoring and Filtering	SECURE DESIGN & IMPLEMENTATION Endpoint Security
THREATS PREVENTION	PROACTIVE DEFENSE Global Support	CASE BASED PROTECTION Security Service Delivery	SECURITY POLICY ENFORCEMENT Policy Enforcement
TRUST BASE	TRUSTED TAMPERPROOF INTEGRATION Assessment and Integration	TRUSTED TAMPERPROOF COMMUNICATIONS Connectivity Management	TRUSTED TAMPERPROOF KERNEL TEE



	INFRASTRUCTURE	GATEWAY	EDGE
THREATS MITIGATIONS	**DYNAMIC RESPONCE** HCI ICS CERT MLAD HCI **SOC**	**ATTACK/ANOMALY DETECTION** ML Preproc ML Engine KATA Integr Asset Detection **KICS/KATA**	**APPLICATION SECURITY** Whitelisting Antimaware Content Filt Asset Detection **KES**
THREATS PREVENTION	**PROACTIVE DEFENSE** KATA KICS Policy Control Security Events **KSN/KPSN**	**SERVICE DEPLOYMENT** URL/DNS Filter Antimalware VPN DPI IPS/IDS **KL Agent**	**POLICY INFORCEMENT** Temporal Logic Inter-process Communication RBAC Domain Isolation **KSS**
TRUST BASE	**TRUSTED INTEGRATION** Assessment AAA PKI MDM **KSC/MDM**	**TRUSTED COMMUNICATIONS** MNGMNT PL FIREWALL CONTROL PL DATA PLANE **Trusted Channel**	**TRUSTED KERNEL** TEE Trusted LC RoT CRYPTO **KOS/KSH**

TOOLS FOR SECURITY BY DESIGN

KASPERSKYOS

- Most secure solution (all components are isolated and controlled)
- Requires rethinking and redevelopment of architecture of every component
- Requires (at least) porting of applications or complete rewriting of them
- Limited support of hardware (embedded systems only)

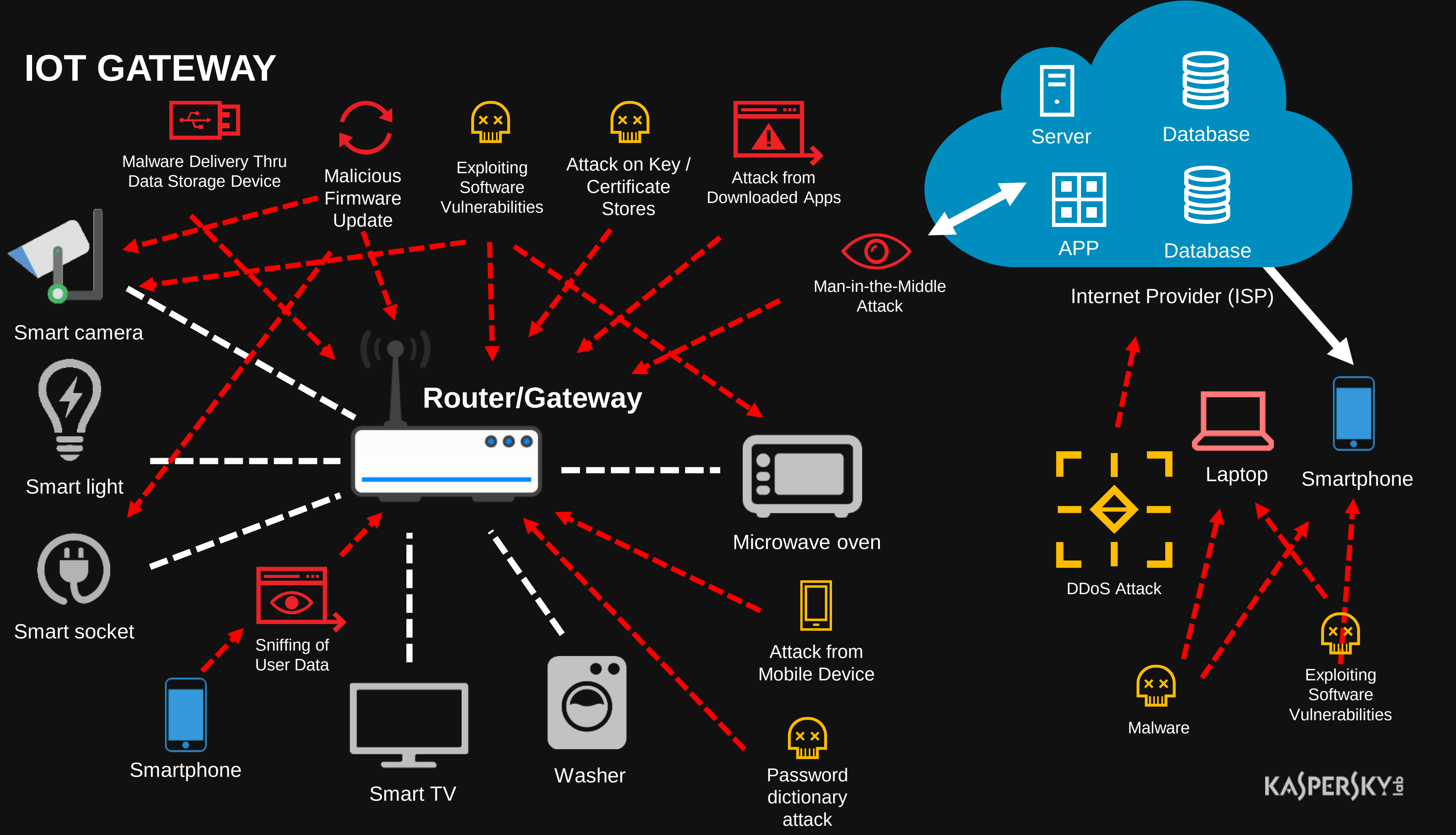
SECURE HYPERVISOR

- Good level of security (isolation of VMs and critical functions, limited control of communications)
- Requires rethinking and redeveloping of applications’ architecture only
- Requires re/development some critical functions
- Wide range of hardware supported (not only embedded systems)

KSS FOR LINUX

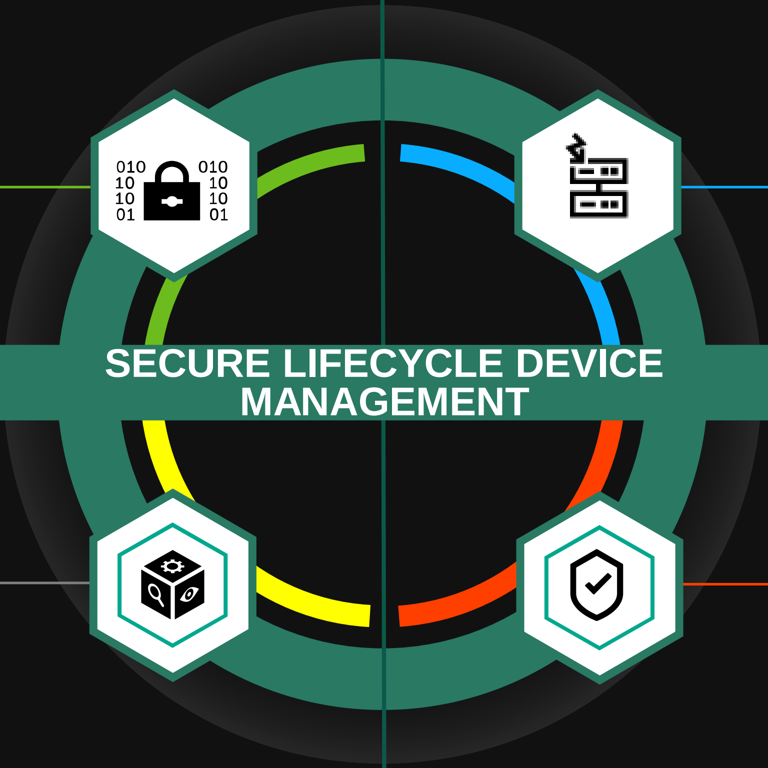
- Good level of security (isolations of Linux containers, control only inter containers communications)
- Requires rethinking and redeveloping of applications’ architecture only
- Requires minimum re/development
- Runs virtually on all Linux with containers support

IOT GATEWAY


Malware Delivery Thru Data Storage Device
Malicious Firmware Update
Exploiting Software Vulnerabilities
Attack on Key / Certificate Stores
Attack from Downloaded Apps
Server
Database
APP
Database
Man-in-the-Middle Attack
Internet Provider (ISP)
Smart camera
Router/Gateway
Smart light
Microwave oven
Laptop
Smartphone
DDoS Attack
Smart socket
Sniffing of User Data
Attack from Mobile Device
Smartphone
Smart TV
Washer
Password dictionary attack
Malware
Exploiting Software Vulnerabilities
KASPERSKY lab

KASPERSKY SECURE IoT GATEWAY

SECURE LIFECYCLE DEVICE MANAGEMENT



Secure Boot

Boots only verified firmware

- Firmware is digitally signed and encrypted
- Bootloader is verified
- Only trusted OS is loaded

Secure Update

Guarantee integrity and authenticity of the firmware delivery

- Failsafe rollback
- Firmware lifecycle support

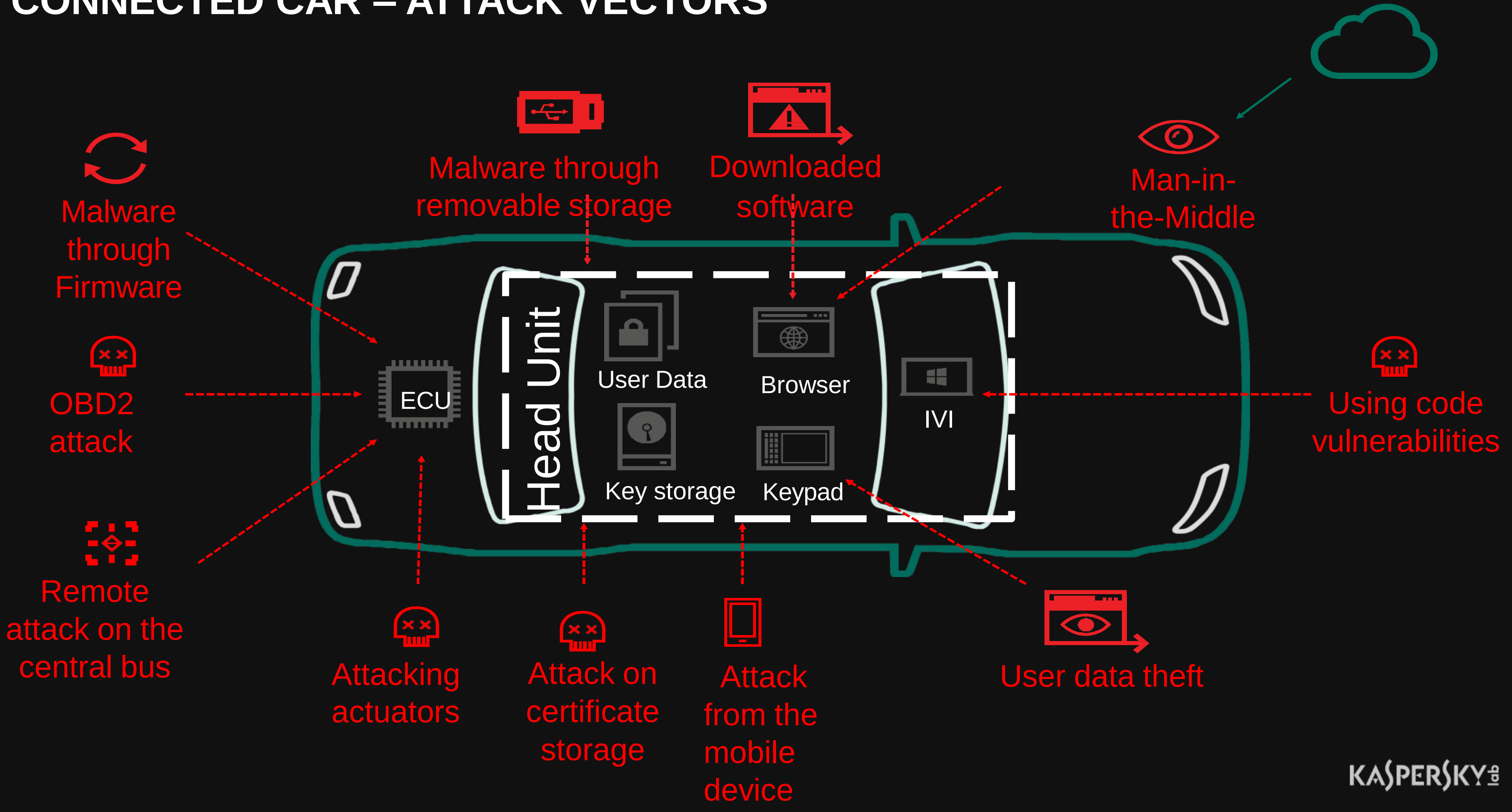
Security Services

- Kaspersky Security Network
- Threat Data Feeds
- Firmware Checking
- Vulnerability Assessment

Secure OS

- Security policies enforcement by independent engine
- Controls interactions across the system
- Security domains separation

CONNECTED CAR – ATTACK VECTORS



Malware through Firmware

OBD2 attack

Remote attack on the central bus

Attacking actuators

Attack on certificate storage

Attack from the mobile device

Malware through removable storage

Downloaded software

Man-in-the-Middle

Using code vulnerabilities

User data theft

	Threat vectors	KL Technologies
Car Cloud Services	• Man in-The-Middle-Attack • Attack From Downloaded Apps	Server Security, Solutions for Data Centers, DDoS Protection, Security Assessment Services (SAS)
Network Access	• Sniffing of User Data • Attack From Downloaded Apps • Exploiting Software Vulnerabilities	Security and Vulnerability Mgmt (SVM), IDS & IPS, Mobile SDK, Security Assessment Services (SAS),
Car Gateway	• Attack from Apps in Mobile Device • Exploiting SW Vulnerabilities • Malicious Firmware Update • Malware Delivery Thru Data Storage Devices	IPS technology can be transformed to IDS, Security and Vulnerability Mgmt, Anti-Malware, Security Asmnt. Services, Kaspersky Secure Hypervisor, Kaspersky Security System SDK (IPS), KasperskyOS
Car Network	• Compromised Engine Actuator • Attack on Vehicle Bus	Security Assessment Services, Kaspersky Security System SDK (IPS)
ECU	• Attack on Key, • Malicious Firmware Update • Attack on Vehicle Bus	Kaspersky Security System SDK (IPS), Encryption, Security Hypervisor, Security Assessment Services, KasperskyOS

5

IN CONCLUSION

TAKEAWAYS

- Market: Critical Information Infrastrucuture
- Regulation: National Landscape
- International Cooperation: ITU, IIC, GSMA, GP
- Principle: Security by Design
- Foundation: Integrated Security

LET’S TALK?

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com