Коротко о себе ☺

Школа 40, Чебоксары

ЧГУ, Кафедра пром. электроники

Дубна, Кафедра системного анализа

MBA, GEM, France, Innovation Management class

GRENOBLE ECOLE DE MANAGEMENT
TECHNOLOGY & INNOVATION

kaspersky 11+ лет

KasperskyOS

Руководитель платформы

Кибериммунитет

Дмитрий Лукиян
Руководитель платформы KasperskyOS

KasperskyOS

Кибериммунитет, зачем это, ну жили же без него…

Вызовы кибербезопасности начала XXI века

Вызовы кибербезопасности начала **XXI** века не могут быть полностью закрыты традиционными методами

Динамика роста киберугроз

Основные причины

- Устаревающее оборудование
- Обеспечение обратной совместимости
- Патчи
- Реактивное противодействие

ФСТЭК РФ, рекомендует следующие сроки устранения уязвимостей (2023):

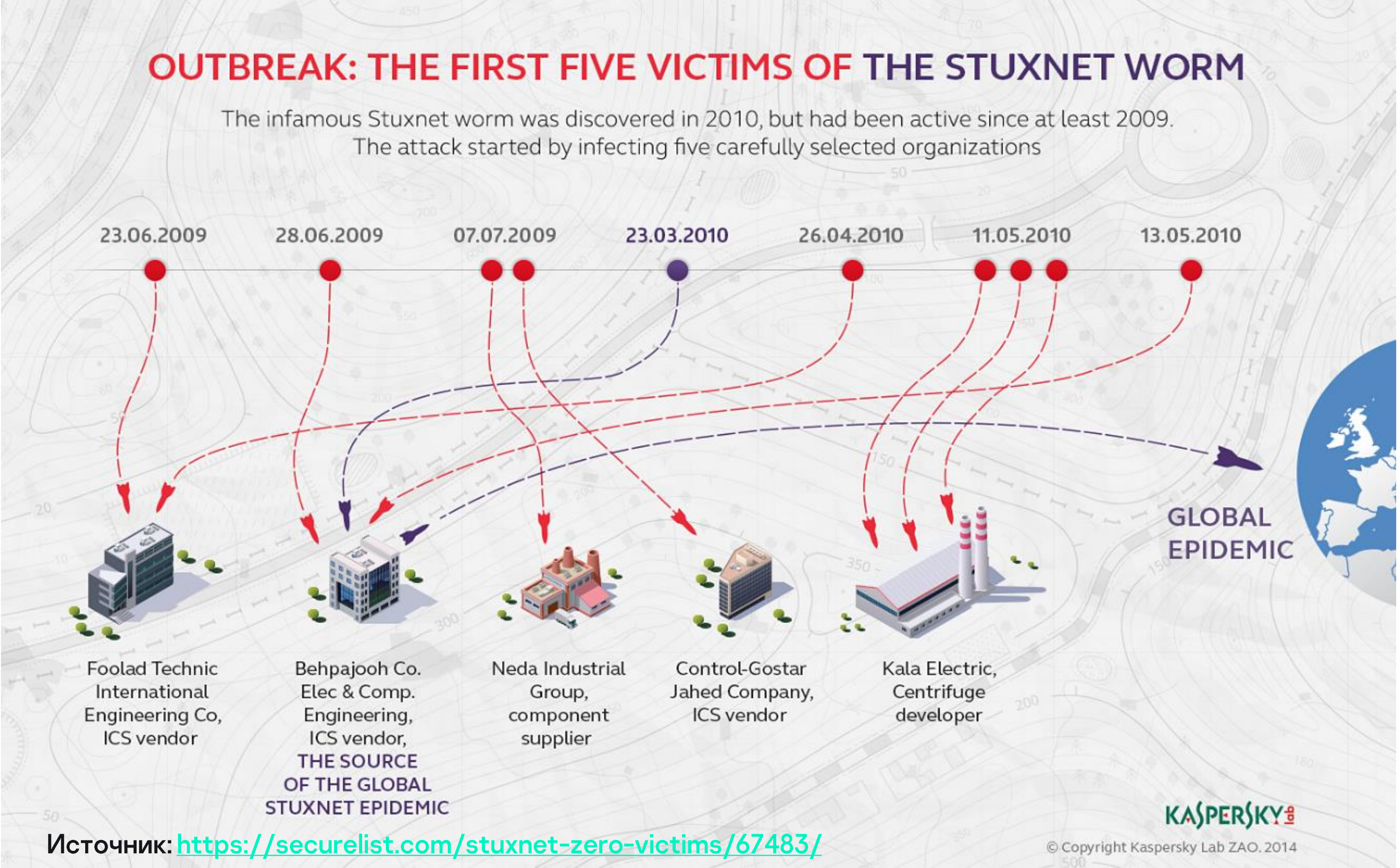
1. Критический уровень опасности: до 24 часов;
2. Высокий уровень опасности: до 7 дней;
3. Средний уровень опасности: до 4 недель;
4. Низкий уровень опасности: до 4 месяцев.

Stuxnet, 2010

Эксплуатация уязвимостей 0-дня (zero-day) ОС, срок обнаружения > года

Источник: https://securelist.com/stuxnet-zero-victims/67483/

Последовательность событий



Источник: https://securelist.com/stuxnet-zero-victims/67483/

Уязвимости 0-дня:

- [CVE-2010-2568](CVE-2010-2568)

Windows XP, Vista, and Windows 7 as well as Windows Server 2003 and 2008

Реактивное противодействие на примере мобильных ОС

Приложения

Проблема эффективно решена наложенными средствами ИБ **Лаборатории Касперского**

.APK файлы с вредоносной функциональностью, распространяемые под видом взломанных игр или приложений

Сторонние магазины приложений

Google play, через который распространяются приложения не несущие полезный функционал, но загружающее рекламу (Adlo)

Источник: https://securelist.ru/mobile-threat-report-2022/106860/

Уязвимости ОС

Пример: Триангуляция, 4 уязвимости 0-го дня в Apple iOS

Наложенные средства безопасности сокращают время обнаружения. **Триангуляция, была обнаружена SIEM системой Лаборатории Касперского - KUMA**

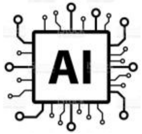
Решение задачи требует кардинальных изменений на уровне архитектуры ОС и средств разработки ОС

Источник: https://securelist.ru/trng-2023/

Новые технологии – новые возможности

Интернет вещей

Сети 5G



Машинное обучение

Дроны

уже сейчас помогают пожарным командам в поиске очагов возгорания

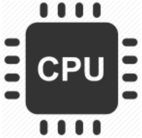
Роботы

позволяют добиться высокой эффективности производства и убрать людей с вредных производств

Автономный транспорт

увеличивает эффективность использования транспорта при значительном снижении аварийности

Новые технологии – новые вызовы ИБ



Вычислительные ресурсы

Вес

Расход мощности

Частые обновления

Решение фундаментальной проблемы

Secure by design

Конструктивно безопасные системы
Системы, способные самостоятельно противостоять киберугрозам за счет архитектуры

Кибериммунитет

Подход «Лаборатории Касперского» к реализации конструктивно безопасных систем

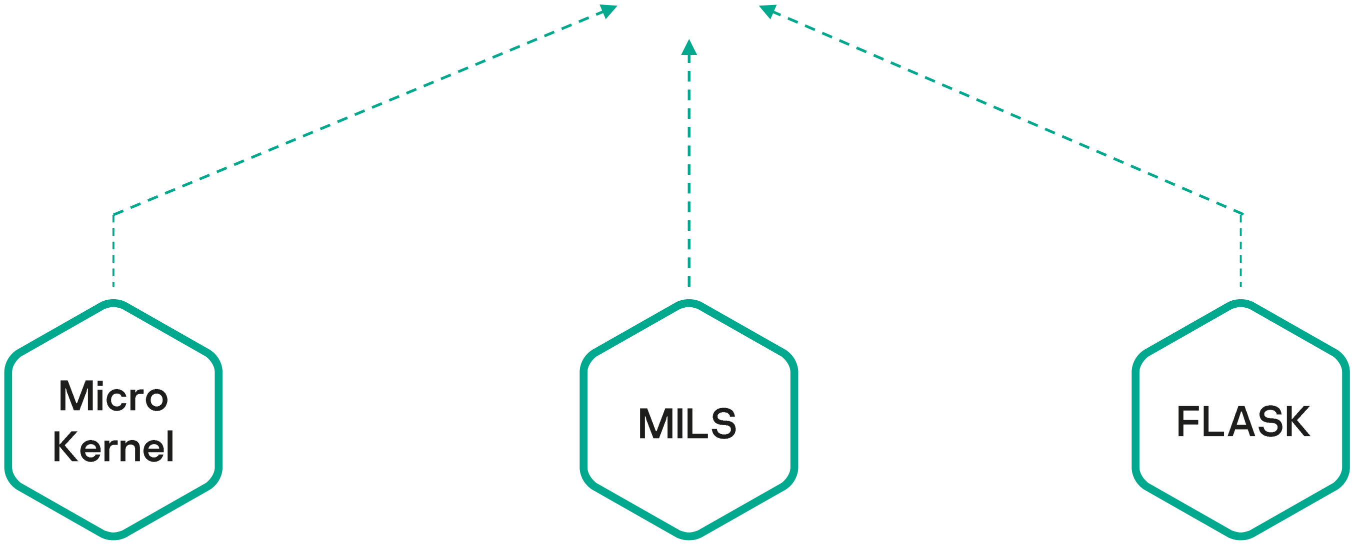
Сочетает в себе как методологию, так и технологии создания кибериммунных систем

KasperskyOS — наиболее эффективная среда для создания кибериммунных систем

От концепции к технологии

KasperskyOS

KasperskyOS базируется на научных концепциях, которые в совокупности наделяют ее уникальными свойствами. Эти свойства позволяют строить на базе ОС системы с высокими гарантиями ИБ.



Доверенная кодовая база (ДКБ)

Linux ДКБ
27+ миллионов
Строчек кода

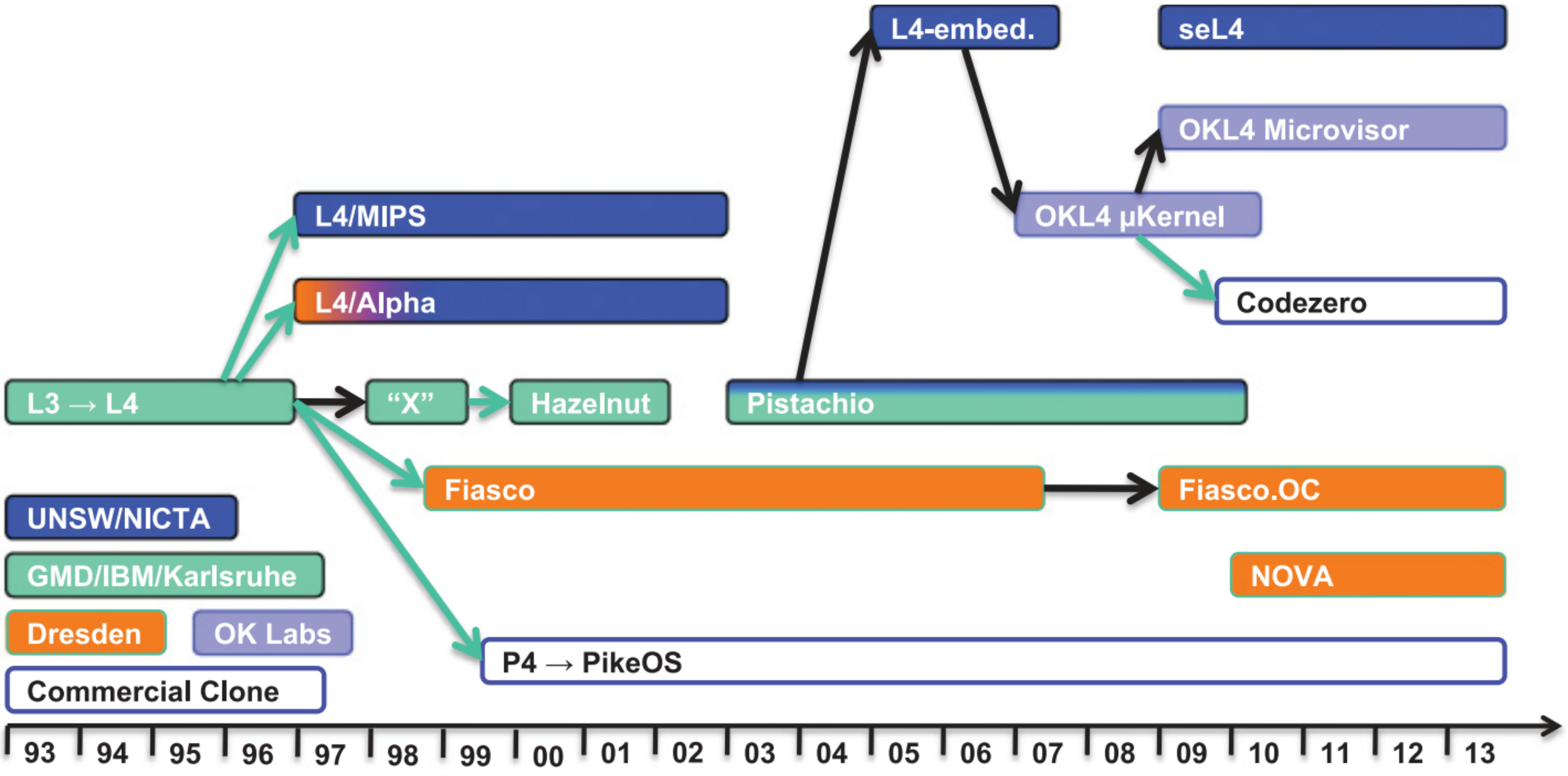
KasperskyOS ДКБ
Менее 100 тысяч
Строчек кода

VS

Монолитная архитектура

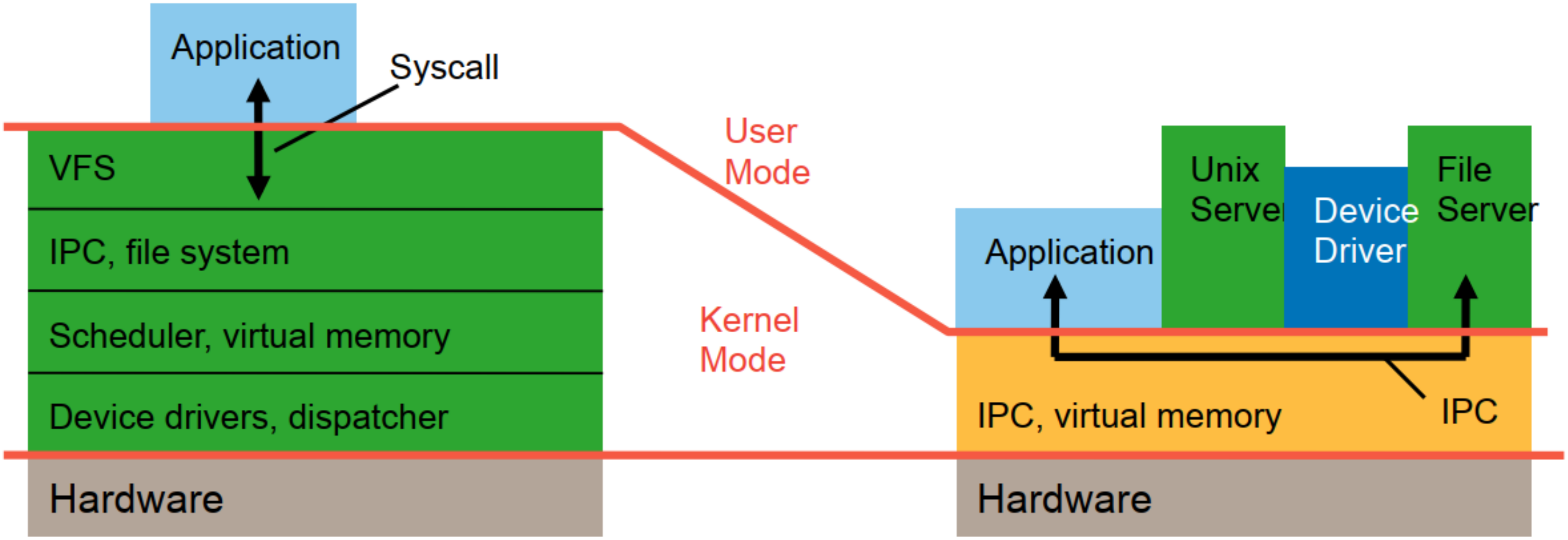
Микроядерная архитектура

История развития микроядерных ОС



Источник: GERNOT HEISER, L4 Microkernels: The Lessons from 20 Years of Research and Deployment

Архитектура монолитных и микроядерных ОС



Источник: Gernot Heiser UNSW/NICTA.

Преимущества микроядра в цифрах

96%

Критических эксплойтов
в Linux не являются критическими для микроядерной ОС.

57%

Эксплойтов
В Linux полностью нивелируются при верификации микорядра.

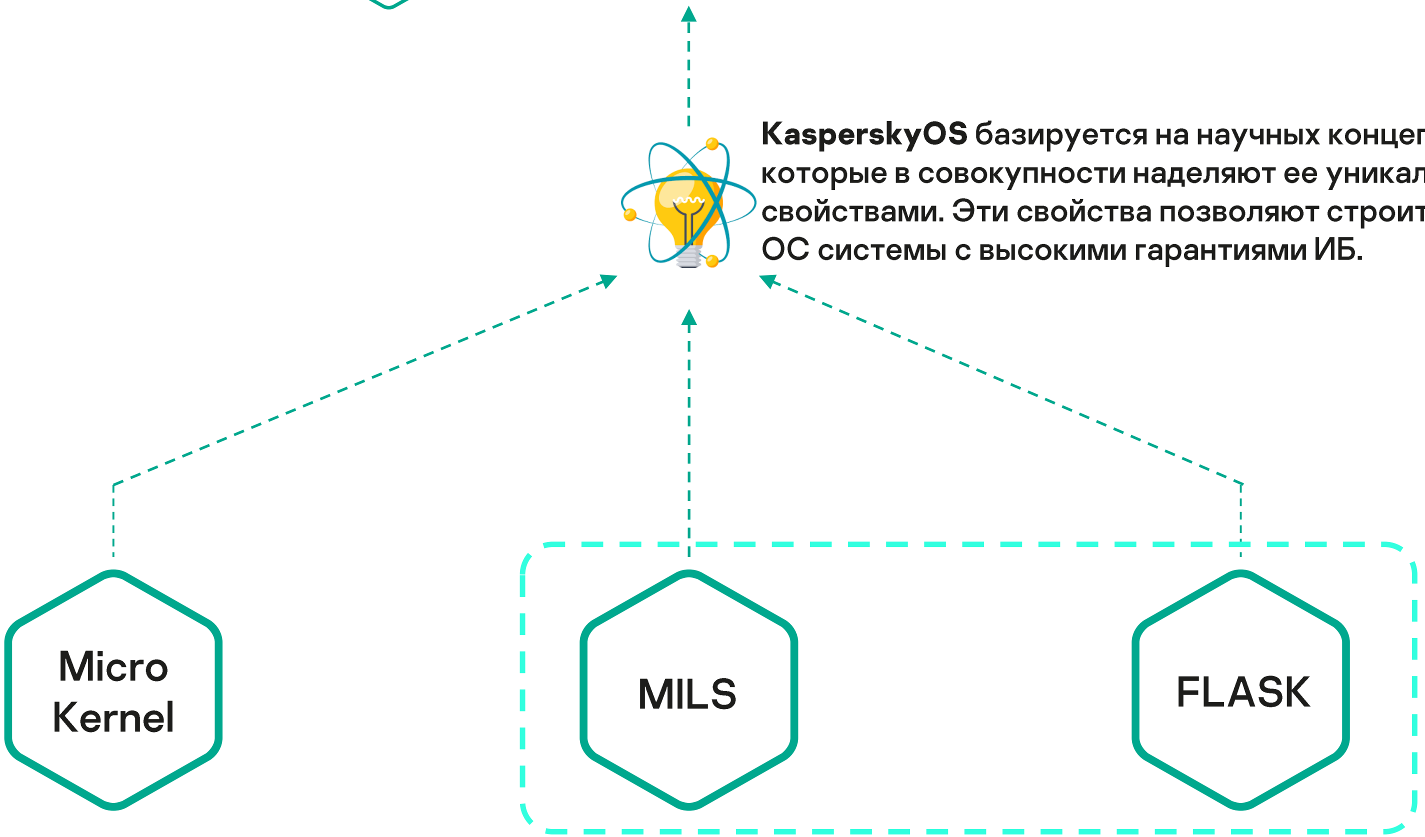
29%

Эксплойтов
в Linux не применимы к микроядерной архитектуре.

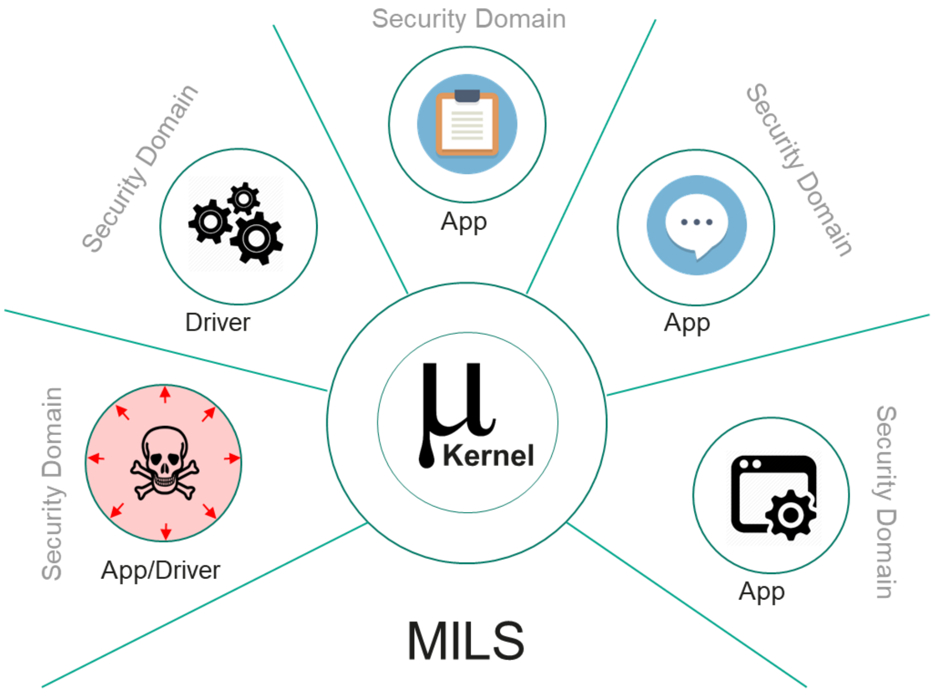
Источник: ACM, Simon Biggs, The Jury Is In: Monolithic OS Design Is Flawed - 2020

KasperskyOS

KasperskyOS базируется на научных концепциях, которые в совокупности наделяют ее уникальными свойствами. Эти свойства позволяют строить на базе ОС системы с высокими гарантиями ИБ.



Multi Independent Levels of Security (MILS)



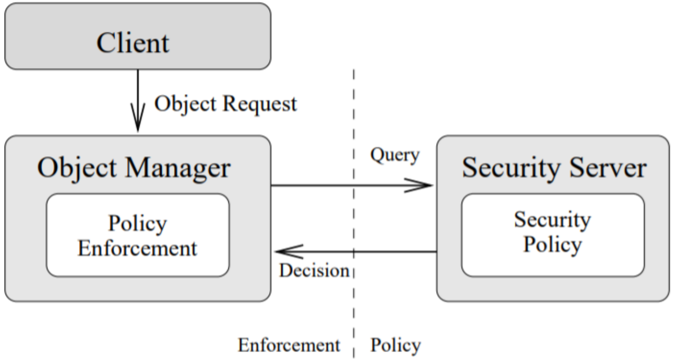
Подход, который позволяет

1. Обеспечить автоматическое купирование угрозы в рамках небольшого домена безопасности, которым может быть драйвер, приложение или его часть (даже библиотека)

2. Реализовать нивелирование вектора атаки, за счет архитектуры системы.

Продемонстрировано на примерах в следующих разделах презентации

FLASK (Flux Advanced Security Kernel)



Подход к построению ядра ОС, который позволяет

1. Разработчику сконцентрироваться на разработке бизнес логики приложения не думая о политиках безопасности.

2. Архитектору ИБ сконцентрироваться на разработке политик безопасности и их декларация в KasperskyOS.

Подход полностью аналогичен WEB когда разработчик (Java Script) думает о бизнес логике а дизайнер (CSS) о отображении.

Глобальное признание

Индикатор, что ты бежишь в правильном направлении

Признание в индустрии

industrial internet CONSORTIUM

“MILS Architectural Approach Supporting Trustworthiness of the IIoT Solutions”, 2021

Architectural approach behind KasperskyOS as a strategy for creating IT systems

Source

ARC Advisory Group

“From Cybersecurity to Cyber Immunity in IIoT”, 2021

An expert view on Kaspersky's Cyber Immunity concept: Kaspersky Cyber Immunity – a new approach to digital transformation

Source

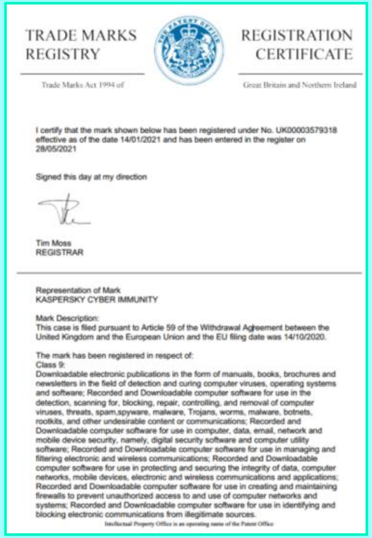
Gartner®

“Vendor to watch” for its KasperskyOS

Market Trends: Software-Defined Vehicles Will Disrupt the Automotive Supply Chain

Source

Kaspersky Cyber Immunity торговая марка



TRADE MARKS REGISTRY
REGISTRATION CERTIFICATE

Trade Marks Act 1994 of Great Britain and Northern Ireland

I certify that the mark shown below has been registered under No. UK00003579318 effective as of the date 14/01/2021 and has been entered in the register on 28/05/2021

Signed this day at my direction

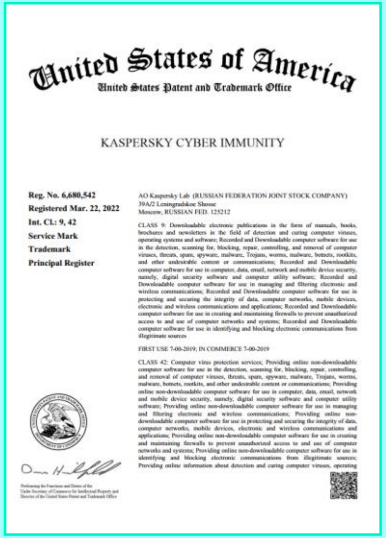
Tim Moss
REGISTRAR

Representation of Mark
KASPERSKY CYBER IMMUNITY

Mark Description:
This case is filed pursuant to Article 59 of the Withdrawal Agreement between the United Kingdom and the European Union and the EU filing date was 14/10/2020.

The mark has been registered in respect of:
Class 9:
Downloadable electronic publications in the form of manuals, books, brochures and newsletters in the field of detection and curing computer viruses, operating systems and software; Recorded and Downloadable computer software for use in the detection, scanning for, blocking, repair, controlling, and removal of computer viruses, threats, spam,spyware, malware, Trojans, worms, malware, botnets, rootkits, and other undesirable content or communications; Recorded and Downloadable computer software for use in computer, data, email, network and mobile device security, namely, digital security software and computer utility software; Recorded and Downloadable computer software for use in managing and filtering electronic and wireless communications; Recorded and Downloadable computer software for use in protecting and securing the integrity of data, computer networks, mobile devices, electronic and wireless communications and applications; Recorded and Downloadable computer software for use in creating and maintaining firewalls to prevent unauthorized access to and use of computer networks and systems; Recorded and Downloadable computer software for use in identifying and blocking electronic communications from illegitimate sources.

Intellectual Property Office is an operating name of the Patent Office



United States of America
United States Patent and Trademark Office

KASPERSKY CYBER IMMUNITY

Reg. No. 6,680,542
Registered Mar. 22, 2022
Int. Cl.: 9, 42
Service Mark
Trademark
Principal Register

AO Kaspersky Lab (RUSSIAN FEDERATION JOINT STOCK COMPANY)
39A/2 Leningradskoe Shosse
Moscow, RUSSIAN FED. 125212

CLASS 9: Downloadable electronic publications in the form of manuals, books, brochures and newsletters in the field of detection and curing computer viruses, operating systems and software; Recorded and Downloadable computer software for use in the detection, scanning for, blocking, repair, controlling, and removal of computer viruses, threats, spam, spyware, malware, Trojans, worms, malware, botnets, rootkits, and other undesirable content or communications; Recorded and Downloadable computer software for use in computer, data, email, network and mobile device security, namely, digital security software and computer utility software; Recorded and Downloadable computer software for use in managing and filtering electronic and wireless communications; Recorded and Downloadable computer software for use in protecting and securing the integrity of data, computer networks, mobile devices, electronic and wireless communications and applications; Recorded and Downloadable computer software for use in creating and maintaining firewalls to prevent unauthorized access to and use of computer networks and systems; Recorded and Downloadable computer software for use in identifying and blocking electronic communications from illegitimate sources

FIRST USE 7-00-2019; IN COMMERCE 7-00-2019

CLASS 42: Computer virus protection services; Providing online non-downloadable computer software for use in the detection, scanning for, blocking, repair, controlling, and removal of computer viruses, threats, spam, spyware, malware, Trojans, worms, malware, botnets, rootkits, and other undesirable content or communications; Providing online non-downloadable computer software for use in computer, data, email, network and mobile device security, namely, digital security software and computer utility software; Providing online non-downloadable computer software for use in managing and filtering electronic and wireless communications; Providing online non-downloadable computer software for use in protecting and securing the integrity of data, computer networks, mobile devices, electronic and wireless communications and applications; Providing online non-downloadable computer software for use in creating and maintaining firewalls to prevent unauthorized access to and use of computer networks and systems; Providing online non-downloadable computer software for use in identifying and blocking electronic communications from illegitimate sources; Providing online information about detection and curing computer viruses, operating

Performing the Functions and Duties of the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office

EUIPO
EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE

Registered / Enregistré 07/10/2022

No 018320558

EUROPEAN UNION INTELLECTUAL PROPERTY OFFICE
CERTIFICATE OF REGISTRATION

This Certificate of Registration is hereby issued for the European Union trade mark identified below. The corresponding entries have been recorded in the Register of European Union trade marks.

OFFICE DE L'UNION EUROPÉENNE POUR LA PROPRIÉTÉ INTELLECTUELLE
CERTIFICAT D'ENREGISTREMENT

Le présent Certificat d'Enregistrement est délivré pour la marque de l'Union européenne identifiée ci-joint. Les mentions et les renseignements qui s'y rapportent ont été inscrits au Registre des Marques de l'Union Européenne.

KASPERSKY CYBER IMMUNITY

The Executive Director / Le Directeur exécutif

Christian Archambeau

www.euipo.europa.eu

United Kingdom,
May 2021

United States,
March 2022

European Union,
October 2022

Глобальное признание партнёрами

Gitex 2022

Strategic cooperation between Centerm and Kaspersky aimed to development and delivery of cyber immune endpoints

World Leading Internet Scientific and Technological Achievements

"Technology innovation" award for Kaspersky Secure Remote Workspace – cyber immune thin clients based on KasperskyOS

Мы не одни

Google Fuchsia

Huawei HarmonyOS

И у нас есть особенность

KasperskyOS

KasperskyOS **фокусируется** на информационной безопасности

От технологии к продуктам

Развитие продуктов на базе KasperskyOS

Этап I: Статические киберимунные системы

Продукт

Прошивка для IoT Шлюзов

2021

Этап II: Статические киберимунные системы с Граф. интерфейсом

Продукт

Прошивка для Тонкий клиентов

2022

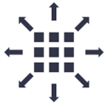
Этап III: Полудинамические Киберимунные системы

Мы сейчас здесь

Прототип

Платформ а для IoT Шлюзов

Прототип



Система дистрибуции приложений

Прототип

Платформа для Автомобильных шлюзов

2023-2024

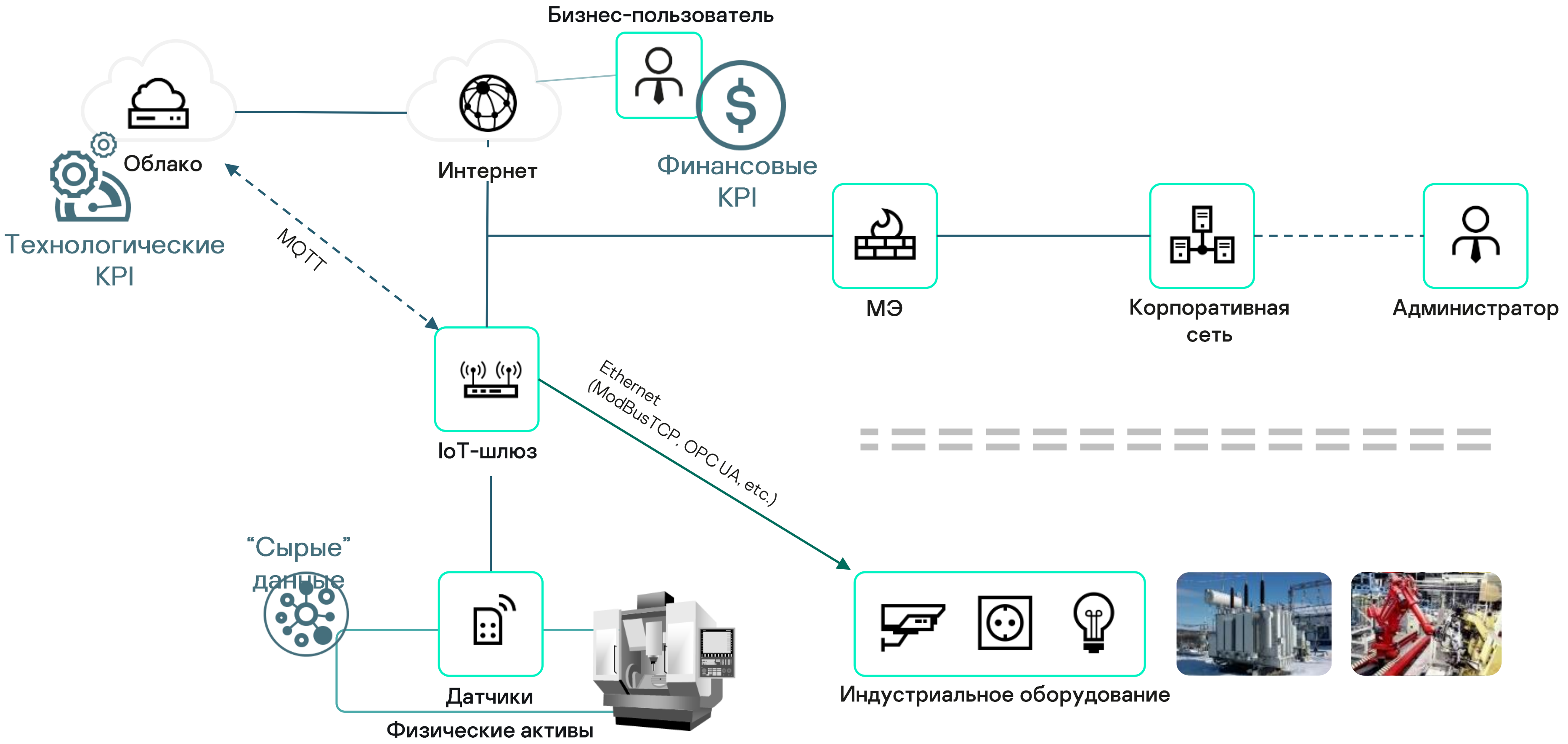
Этап IV: Открытые Динамические киберимунные системы

Прототип

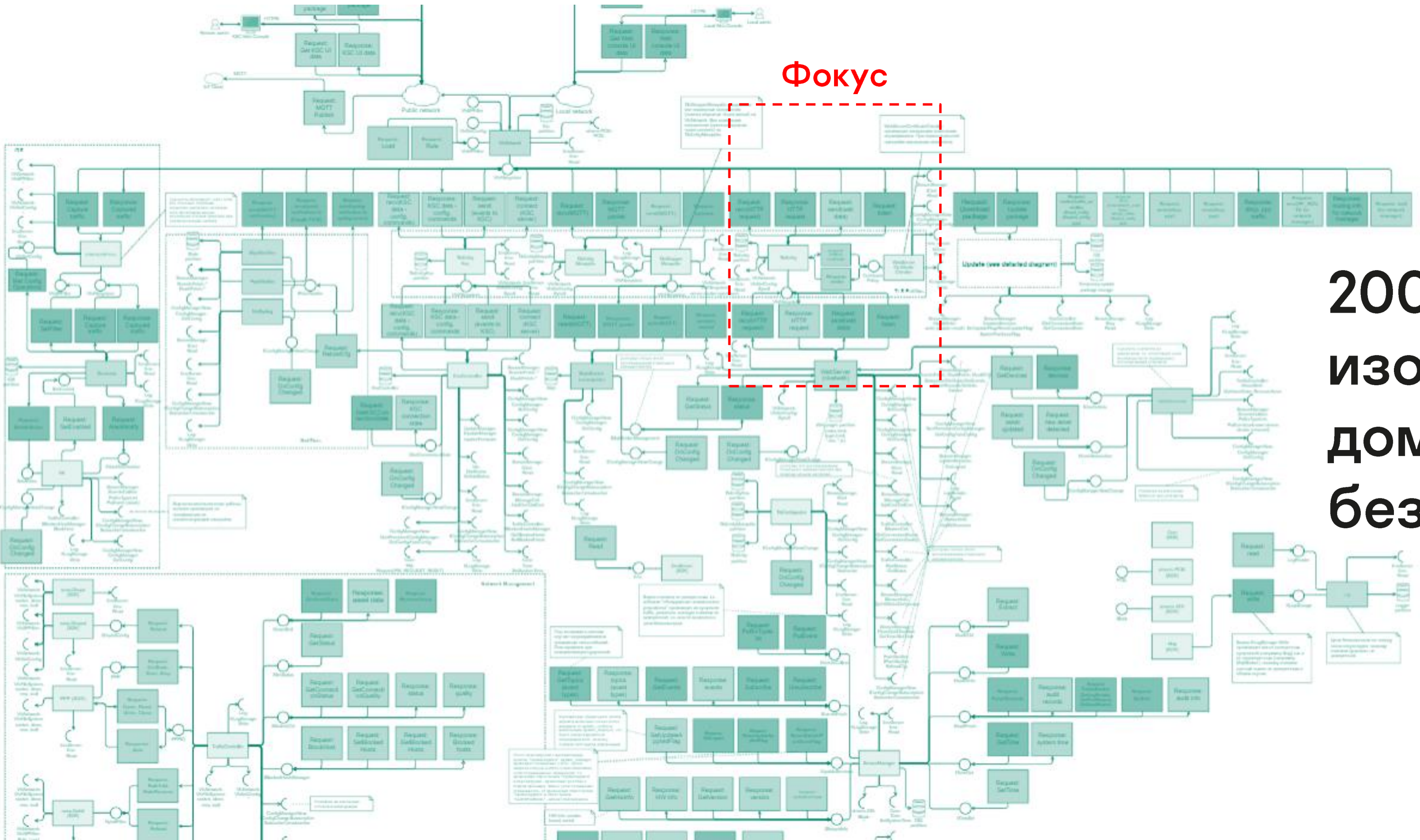
Платформа для мобильных устройств

2024+

Бизнес аспект цифровизации с использованием IoT/IIoT



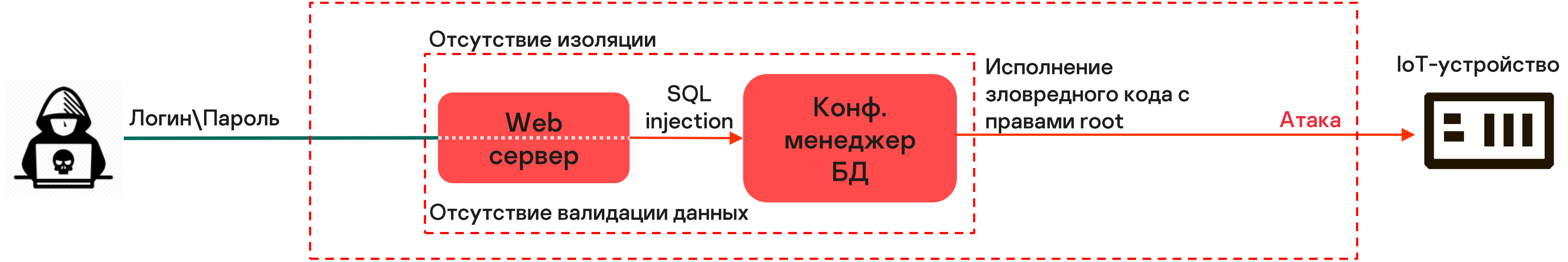
Архитектура промышленного шлюза на KasperskyOS



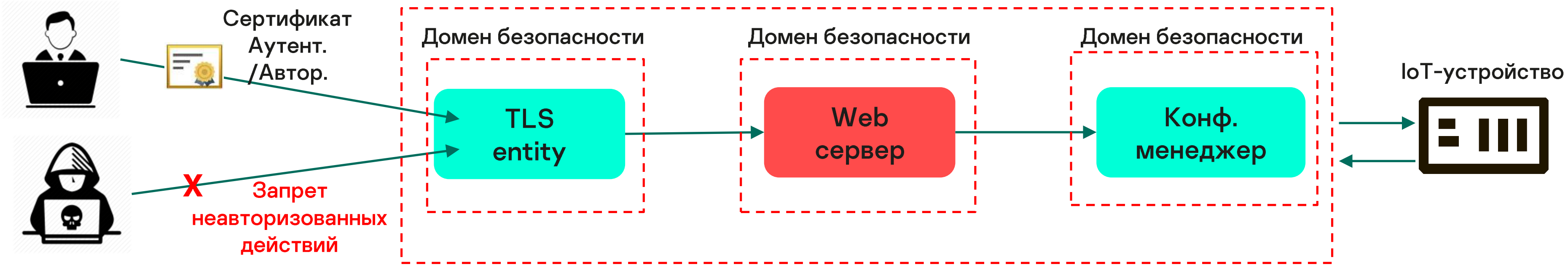
200+ изолированных доменов безопасности

Пример реакции кибериммунной системы на реальную RCE

Существующий шлюз с известной CVE-2021-42311 – Обычный шлюз

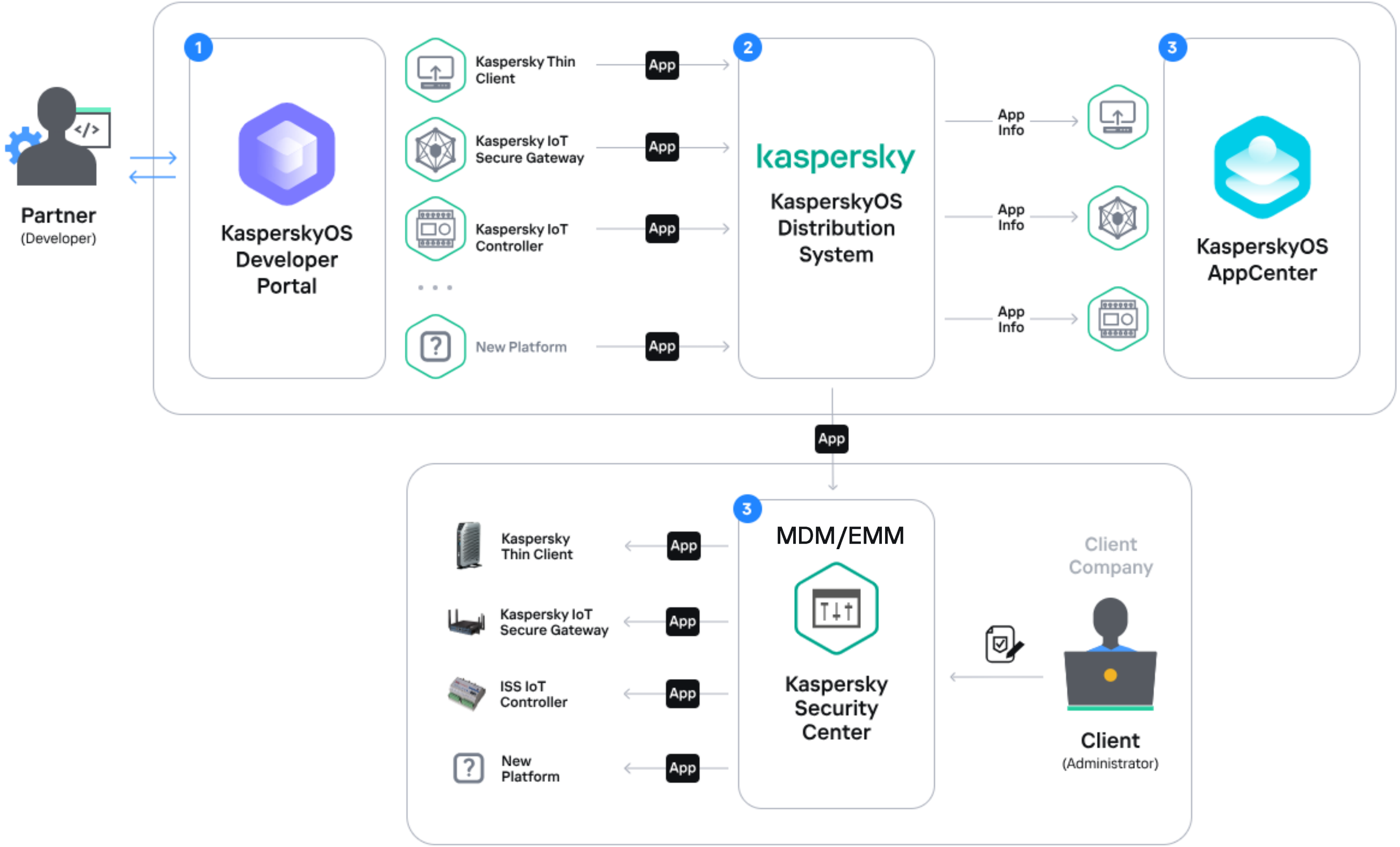


Шлюз на базе KasperskyOS – Кибериммунный шлюз



AppiCenter

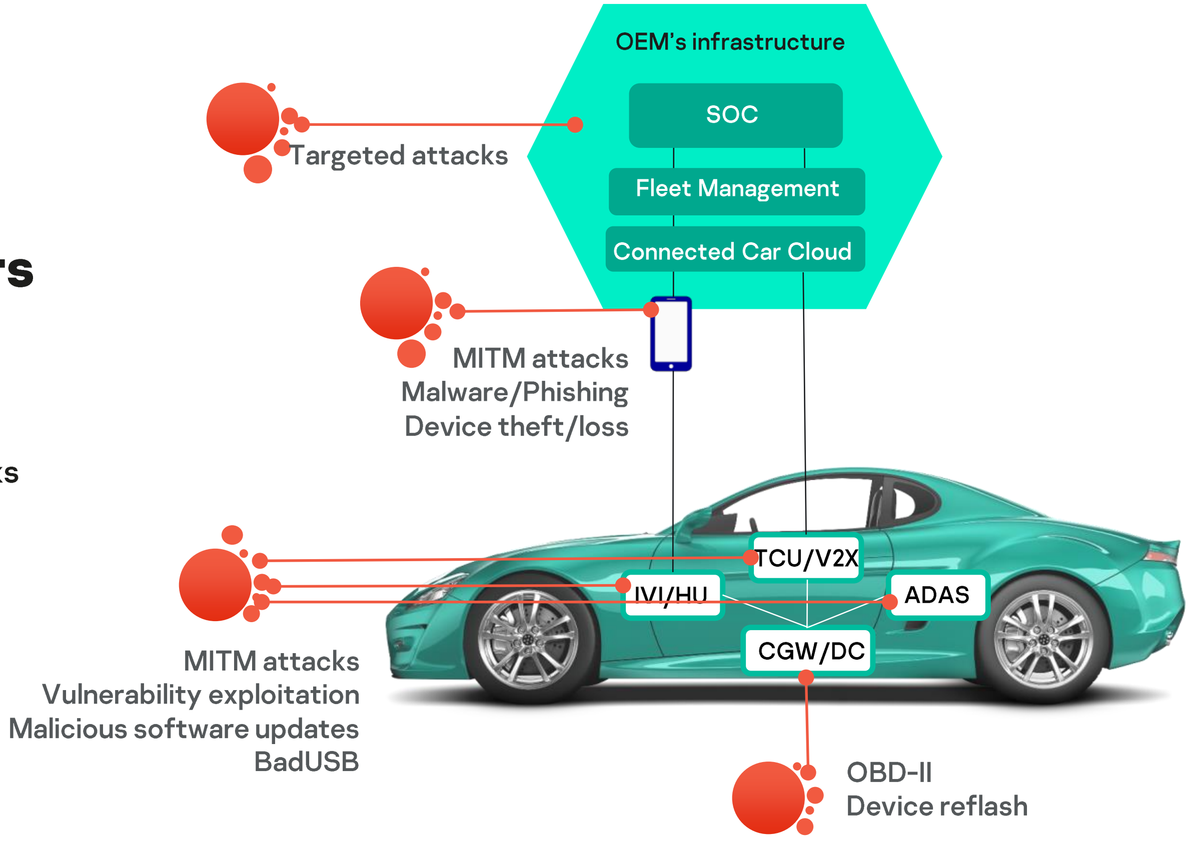
Q



Vehicle ecosystem threats

Diverse attack vectors

- Interior, short- & long-range attacks
- Mobile devices and apps
- Connected car infrastructure attacks



kaspersky

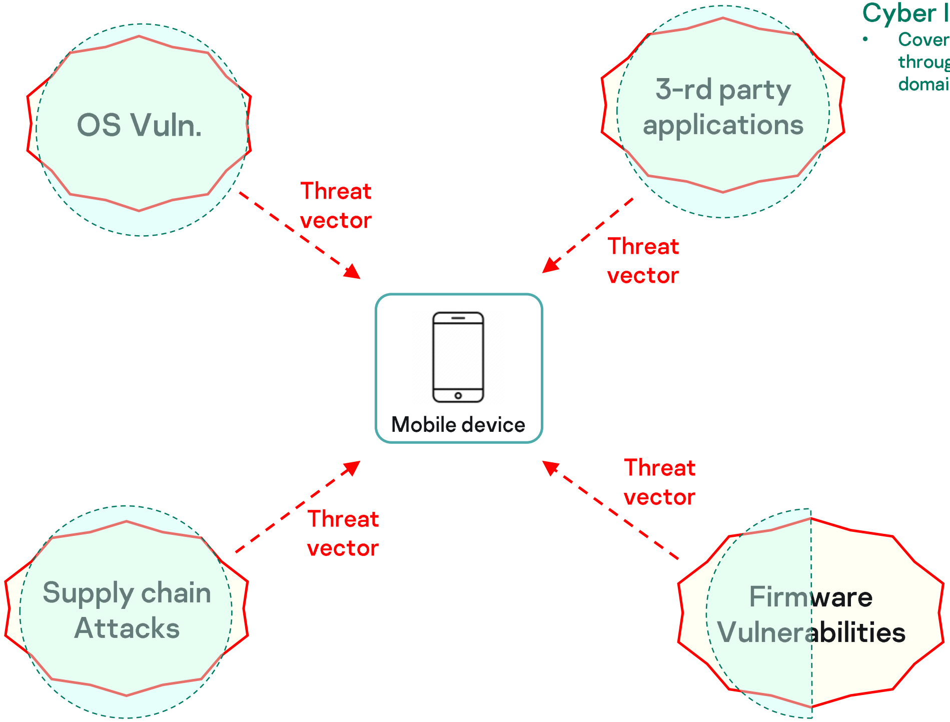
Mobile devices threat vectors (mostly associated with Industrial networks)

OS Vulnerabilities

- Life of Mobile devices in industrial more that 5 years. Most of the producers do not support software after 3 years.
- Legacy software, which prevent updates

Cyber Immunity

- Covers such threats through small TCB.



Cyber Immunity

- Covers such threats through isolated security domains.

Cyber Immunity

- Covers such threats through isolated security domains.

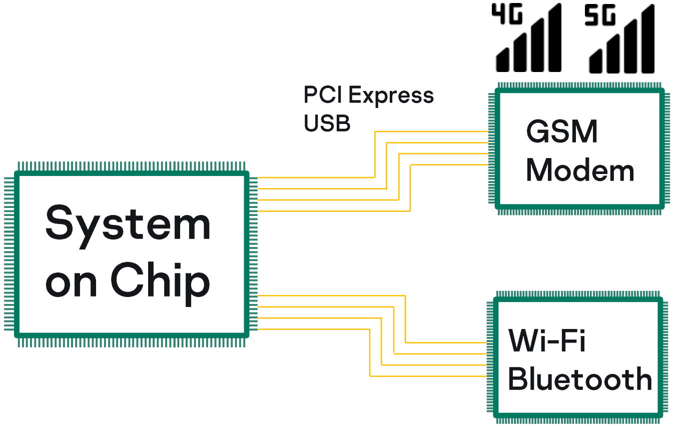
Vulnerabilities in firmware of GSM Modem, Wi-Fi, Bluetooth

- GSM Modem, Wi-Fi, Bluetooth components integrated directly into mobile chip. They use memory mapping interface. So it means, that vulnerability in such components can provide for potential intruder back door with full control.

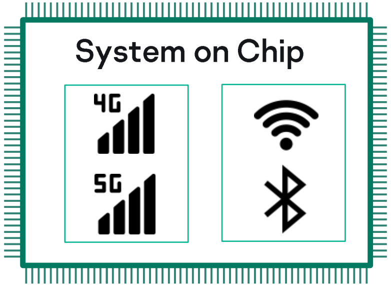
Cyber Immunity

- Partially covers such threats through isolated security domains.
- Smart hardware architecture required.

Vulnerabilities in firmware can be eliminated through secure by design in hardware



+ Security-first design with Cyber Immunity
+ Wireless interfaces are not SoC based, so wireless comms could be controlled
+ Typical implementation through Rockchip, NxP
- Higher power consumption
- Tablet as more suitable form factor
- More expensive device than mobile-SoC based one

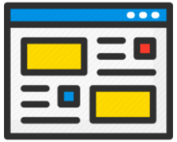


+ Universal design with Cyber Immunity
+ More variants to build smartphone device
+ Less expensive due to integrated peripherals
+ Better power efficiency
- We don’t have any experience with Unisoc yet

Вызовы

Сегодня

Web Приложения



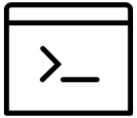
IoT Шлюз

QT приложения

Qt

Тонкий клиент

Консольные приложения



Контроллер

Завтра

Adaptive AUTOSAR

Автомобильный шлюз

Flutter

Платформа для мобильных устройств

Масштабируемость по оборудованию

Linux

Android

Windows

Исследовательский проект

Результаты на примере применения KasperskyOS на мобильных устройствах

- В рамках проекта было портировано 300 000+ строчек кода драйверов Linux
- Объем необходимых изменений для запуска в KasperskyOS < 5%

Драйверы акселерометра и гироскопа

- Исходный код под Linux: 7 100 стр.
- Объем изменений: 20 строчек;

Драйверы NFC

- Исходный код под Linux: 1 176 стр.
- Объем изменений: 0 строчек;

Программы обучения

Новости кибериммуннитета

Технические статьи кибериммунного мира