SENAI
SÃO PAULO

5G NA INDÚSTRIA: A QUESTÃO DA SEGURANÇA CIBERNÉTICA

CONIC 26/08/21

Agenda:

- Cenário global
- Ações SENAI SP em Cibersegurança e 5G
- Vulnerabilidades no chão de fábrica

Segundo relatório da McAfee:

“O custo do cibercrime global atingiu mais de U$ 1 trilhão...”

Fonte: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

Falhas na Segurança Cibernética causam:

- **Interrupção de serviços críticos**
- **Paralisação na cadeia produtiva**
- **Queda na produtividade**
- **Quebra na continuidade do negócio**
- **Danos à imagem da empresa**

Ataque Cibernético – Colonial Pipeline

Menu Search **Bloomberg** Sign In **Subscribe**

Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
4 de junho de 2021, 16:58 GMT-3

Fonte: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Ataque Cibernético - JBS

CNBC

Search quotes, news & videos | SIGN IN

MARKETS | BUSINESS | INVESTING | TECH | POLITICS | CNBC TV | WATCHLIST | PRO | MAKE IT | USA · INTL

Meat supplier JBS paid ransomware hackers $11 million

PUBLISHED WED, JUN 9 2021•7:43 PM EDT | UPDATED WED, JUN 9 2021•8:42 PM EDT

NBC NEWS | Kevin Collier

SHARE

Signage outside the JBS Beef Production Facility in Greeley, Colorado, U.S., on Tuesday, June 1, 2021.

Michael Ciaglo | Bloomberg | Getty Images

Fonte: https://www.cnbc.com/2021/06/09/jbs-paid-11-million-in-response-to-ransomware-attack-.html

SENAI

Ataque Cibernético – Reservatório de água na Flórida

A hacker tried to poison the water supply in a Florida community that serves 15,000 people, officials said

Madison Hall Feb 8, 2021, 8:05 PM

Fonte: https://www.businessinsider.com/hacker-tried-to-poison-water-supply-in-oldsmar-florida-2021-2

Tecnologias de ponta Hannover Messe 2019

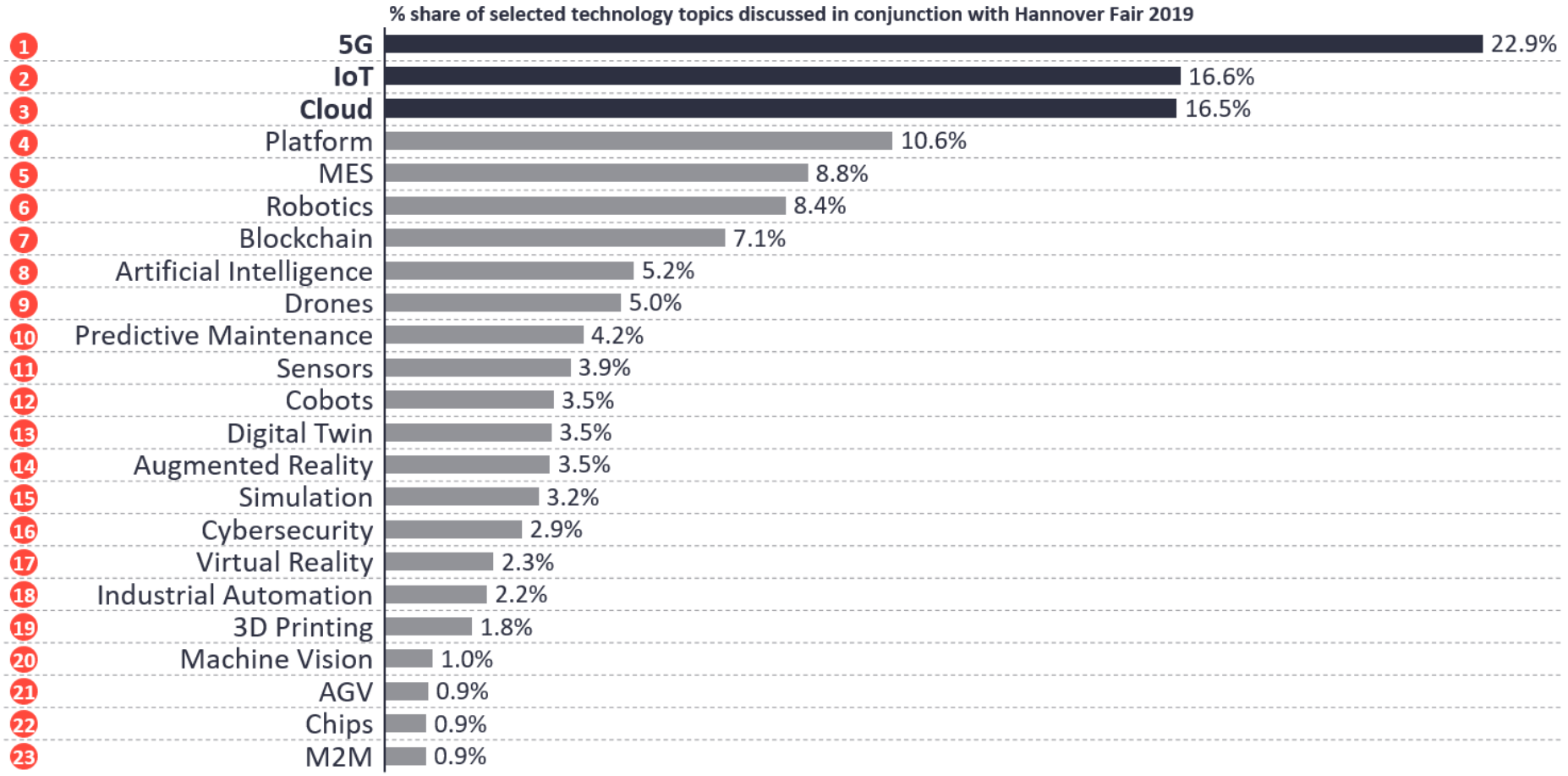
IOT ANALYTICS

Insights that empower you to understand IoT markets

HANNOVER MESSE

Hannover Fair 2019: Top technologies

Share-of-voice in the media



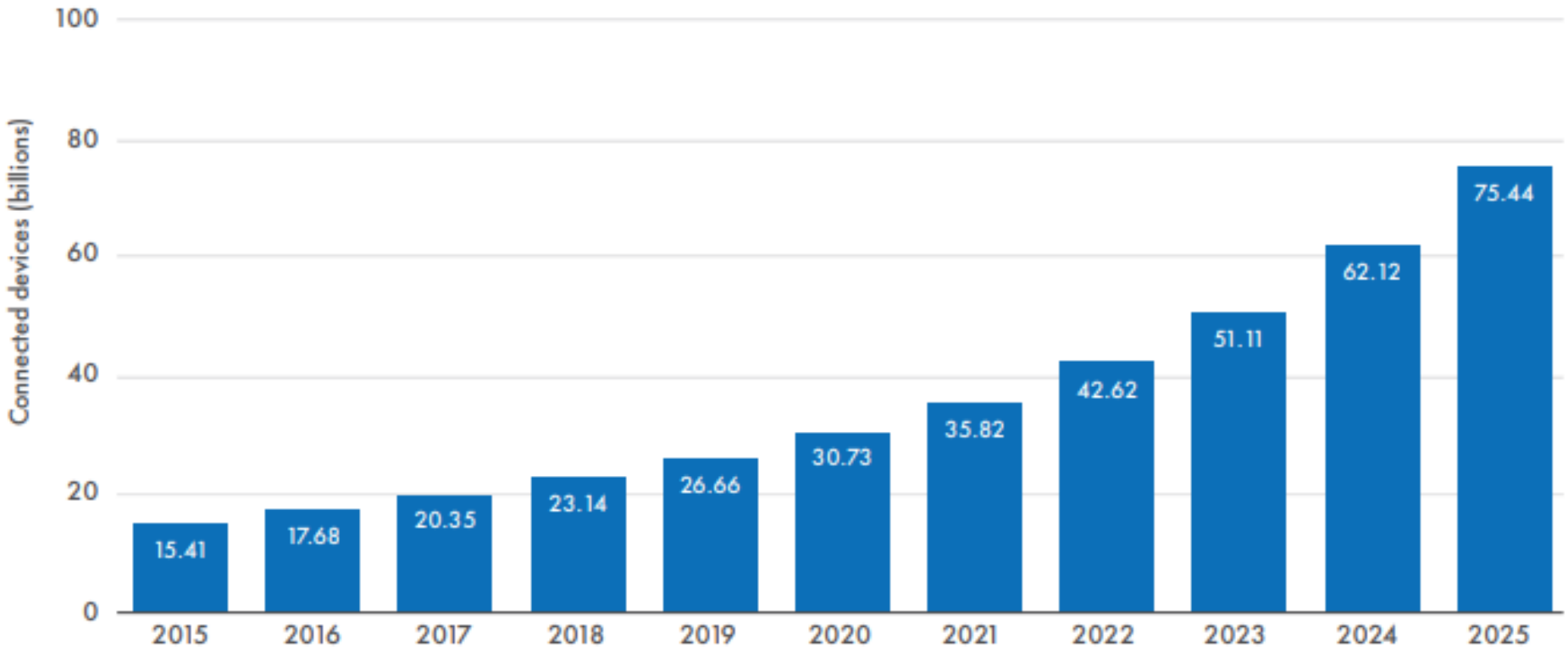
Note: Analyzed were all press articles and announcements 3 weeks prior and the week during the fair that specifically mentioned the fair and the topic Total adds up to more than 100%

Source(s): IoT Analytics Research, Google News

SENAI

Aumento exponencial de dispositivos conectados - IoT

Fig 3 **Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)**



Source: Statista

SENAI SÃO PAULO - 2021

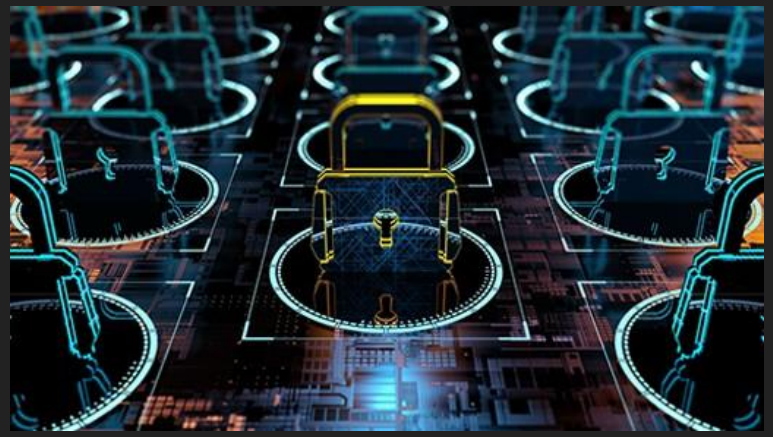
Internet of Threats - Internet das ameaças (Kaspersky Hannover 2021)

Não é novidade o impacto dos grandes ataques cibernéticos nas empresas do mundo todo.

As indústrias começaram a perceber que não é uma questão de "se", mas sim "quando". Há preocupação crescente com segurança de sistemas e proteção de dados a medida que ocorre a migração para a era digital.

Internet of Threats

Apresentado pela primeira vez durante o evento, o KasperskyOS, sistema operacional desenvolvido pela Kaspersky será embarcado em gateways IoT. Com uma arquitetura de sistemas diferenciada, ele é apresentado como produto Cyber-Imune em meio ao que denominam Internet das ameaças.

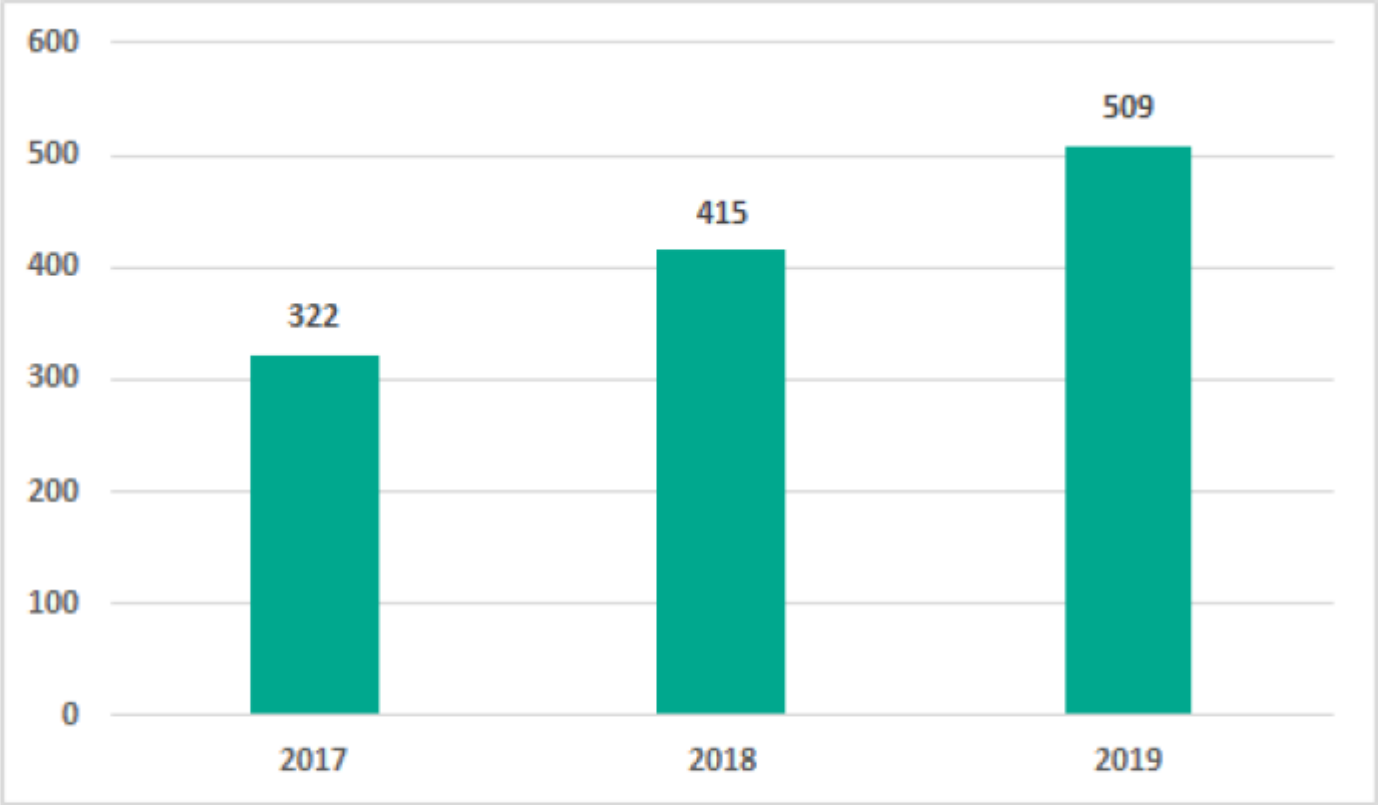


Segurança em todos os níveis

Os novos produtos focam no monitoramento da saúde dos equipamentos bem como na segurança da conectividade. As soluções do futuro englobam gestão de energia, otimização dos sistemas de resfriamento
e utilizam I.A. para detectar anomalias, sejam nos setpoints dos equipamentos ou no fluxo de informação trafegada na rede.

Vulnerabilidades vêm crescendo !

Number of vulnerabilities in different ICS components, as published on the US ICS-CERT website



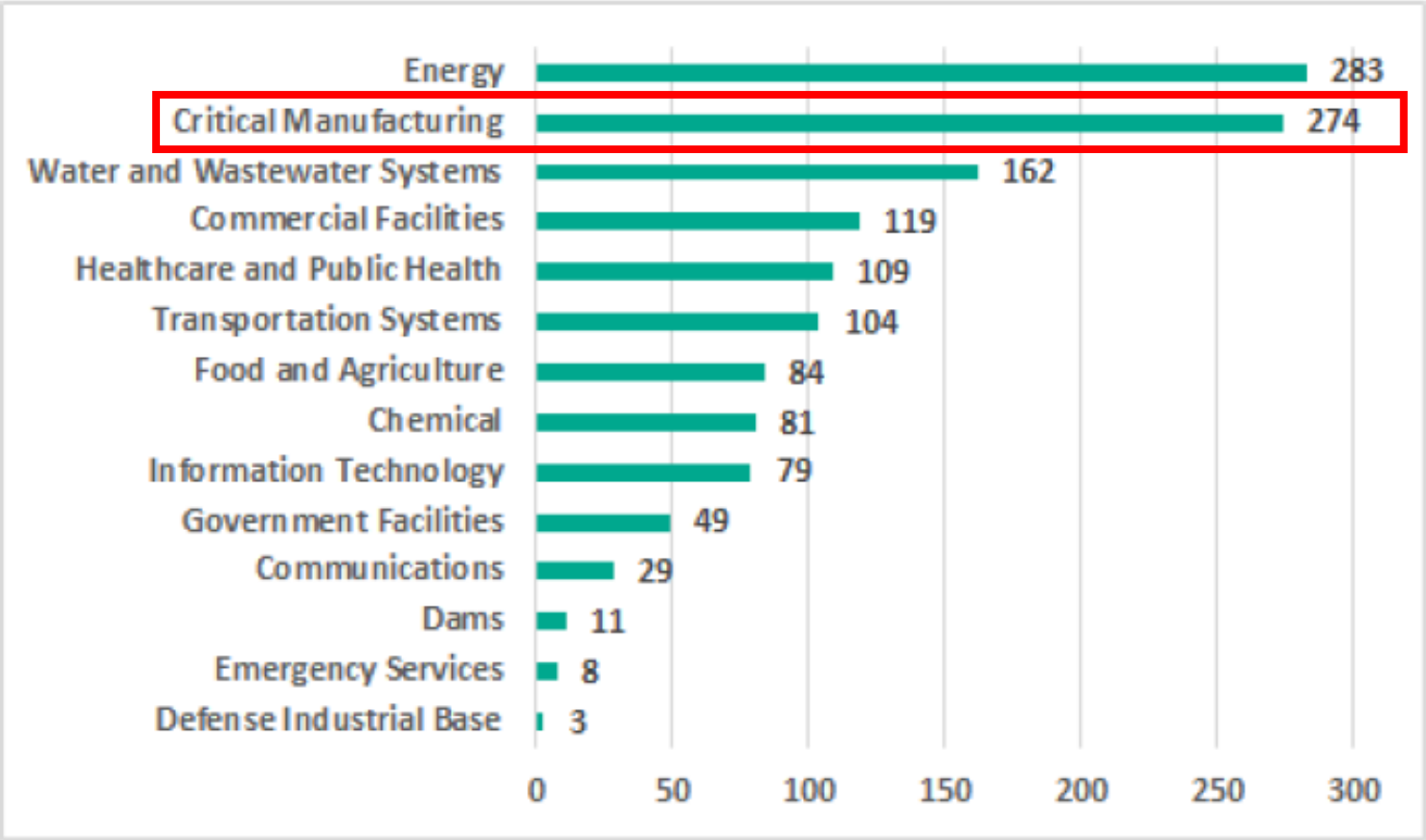
Analysis by industry

The largest number of vulnerabilities affect industrial control systems in the energy sector (283), systems used to control industrial processes at various enterprises categorized as critical infrastructure facilities in the US (274); and water supply and sewage systems (162).

THREAT LANDSCAPE FOR INDUSTRIAL AUTOMATION SYSTEMS. H2 2019 3 © KASPERSKY, 1997 – 2020

Setores produtivos afetados - USA

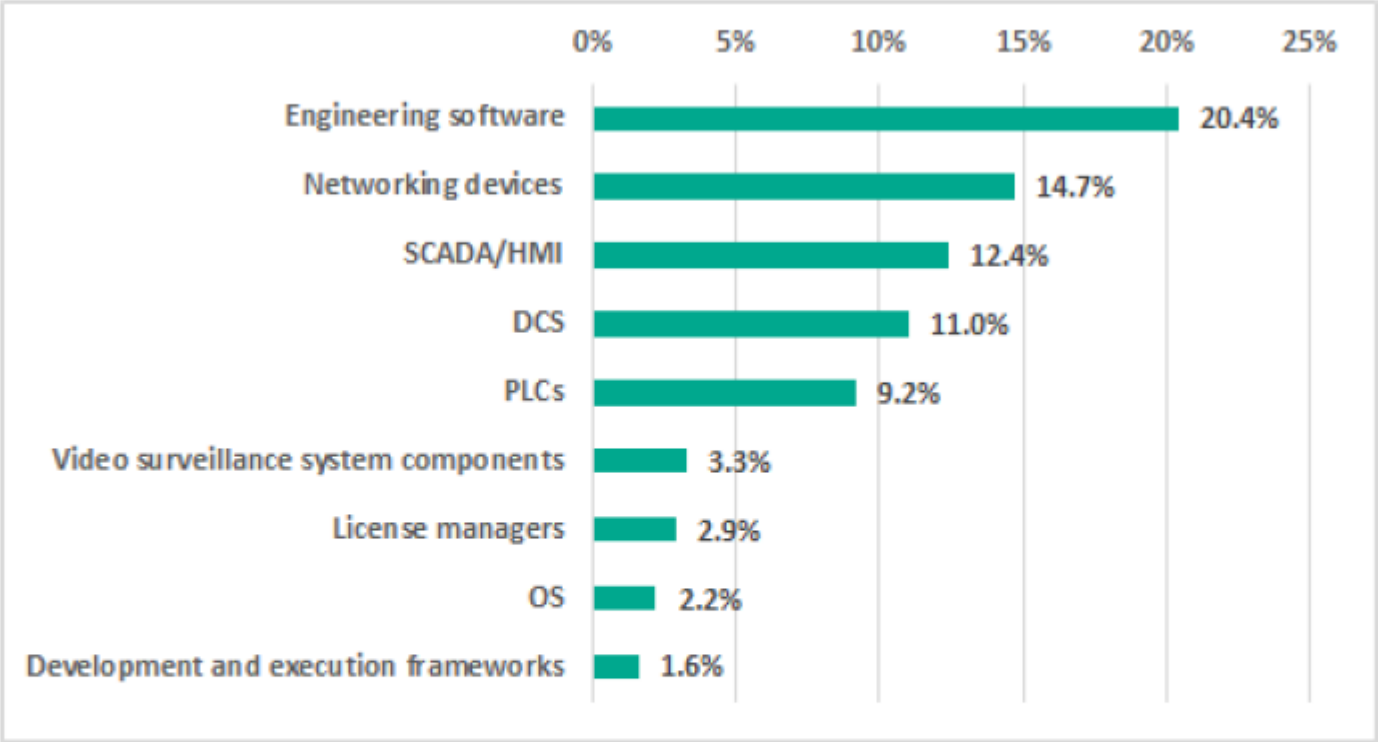
Number of vulnerable products used in different industries (according to US ICS-CERT classification). Vulnerabilities published in 2019



THREAT LANDSCAPE FOR INDUSTRIAL AUTOMATION SYSTEMS. H2 2019 3 © KASPERSKY, 1997 – 2020

Muitas vulnerabilidades são de Terceira parte!

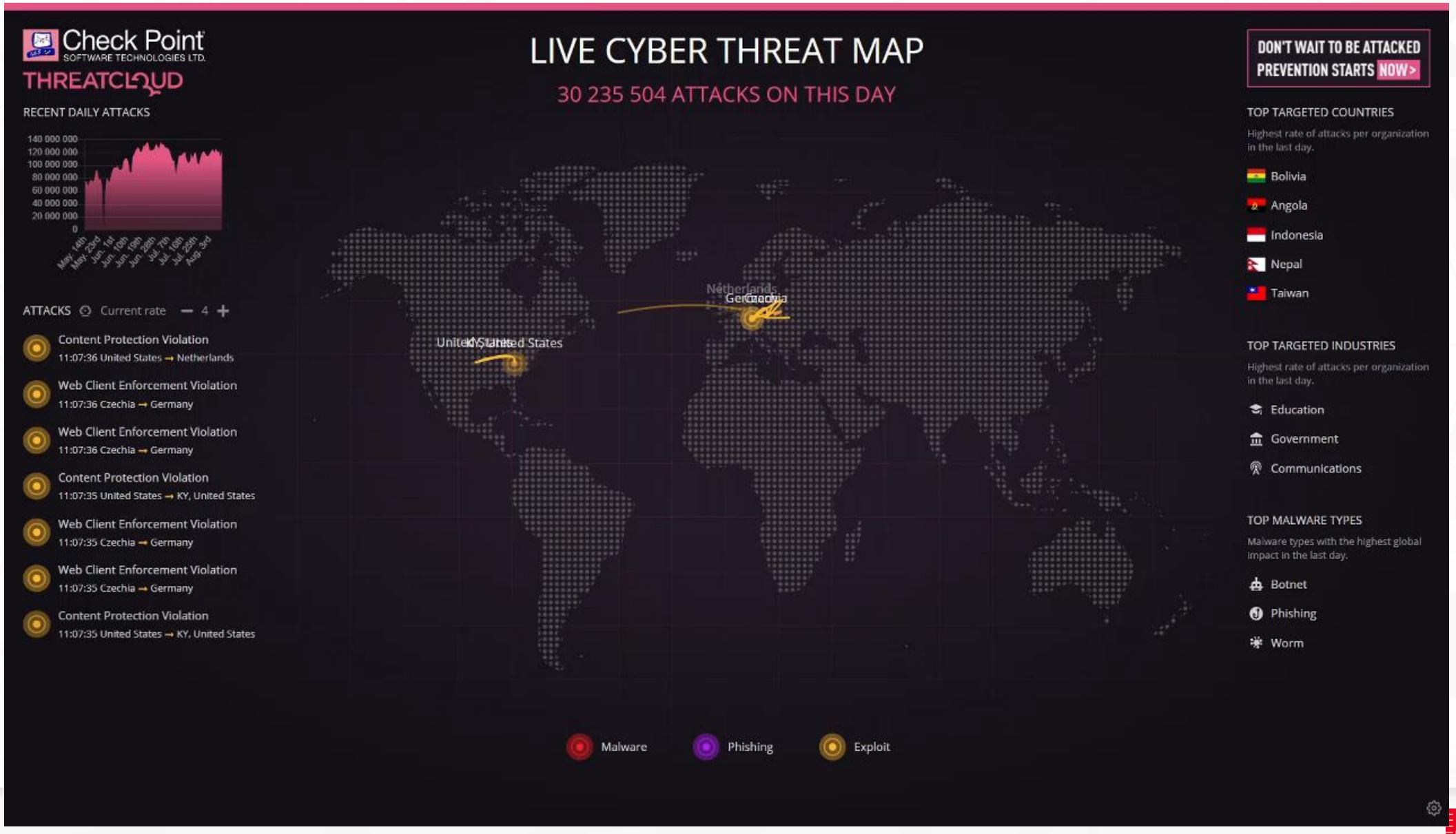
Percentage of vulnerabilities identified in various ICS components to all vulnerabilities. Vulnerabilities published in 2019



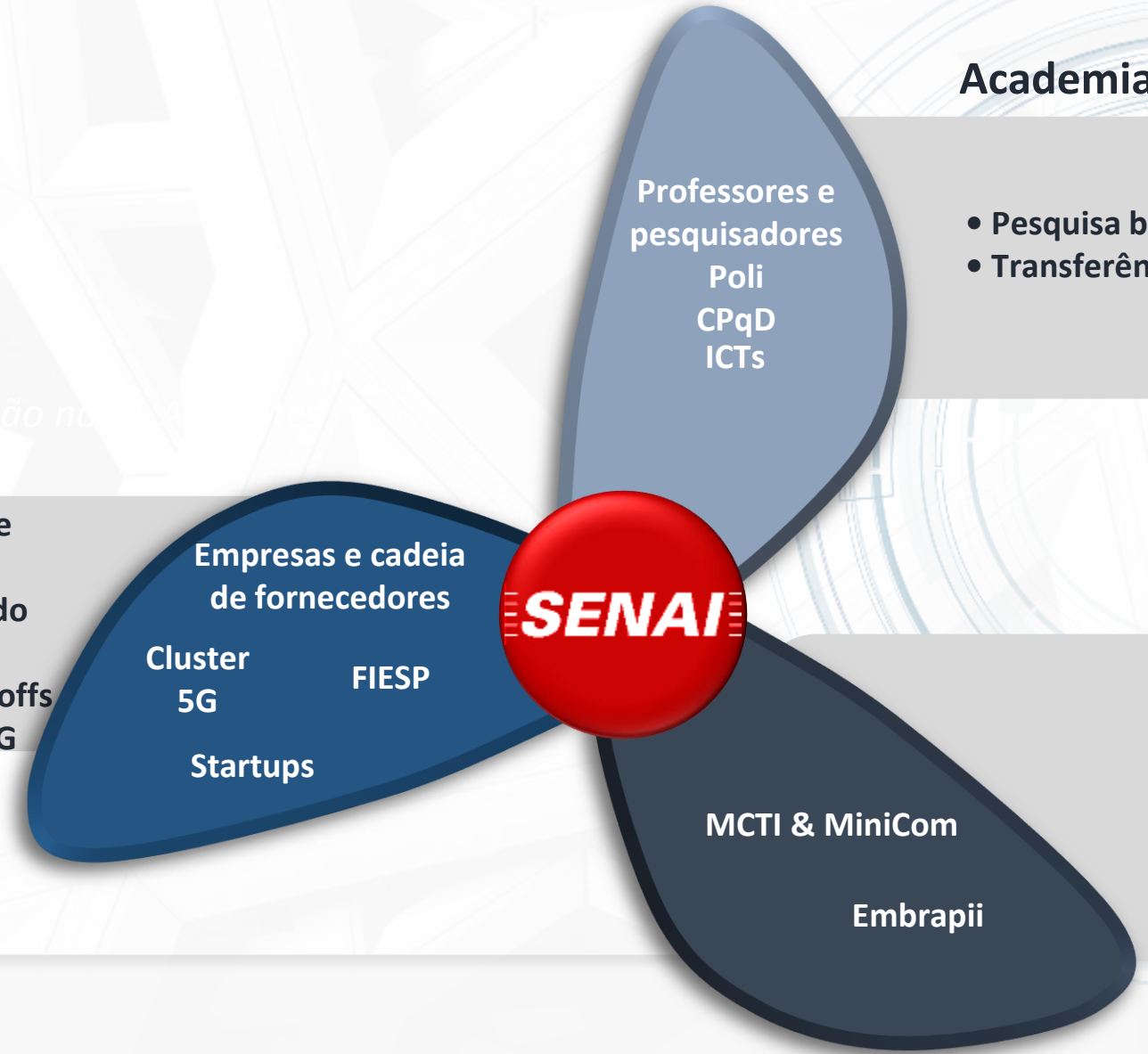
Security issues in industrial automation systems are often due to vulnerabilities in third-party common software components used by vendors in many ICS solutions. Such components include operating systems (OS), license managers, modules implementing various security mechanisms, as well as frameworks used to develop and execute industrial control system software.

THREAT LANDSCAPE FOR INDUSTRIAL AUTOMATION SYSTEMS. H2 2019 3 © KASPERSKY, 1997 – 2020

A densidade de Ciber ataques está aumentando!



Estratégia SENAI de hélice tripla para Conectividade digital



Academia

- Pesquisa básica
- Transferência de tecnologia

Industria

- Competitividade
- Inovação
- Conhecimento do mercado
- Startups e Spinoffs
- Cluster Brasil 5G

Governo

- Fomento para P&D
- Participação em programas estratégicos: IoT , Câmara da Indústria 4.0

Estratégia SENAI SP para Conectividade Digital

- O SENAI SP iniciou um amplo programa de Conectividade digital, no âmbito da assistência tecnológica às empresas, com atuação fundamentada em parcerias com o setor industrial e outros ICTs, incluindo ações de P&D em:

- Desenvolvimento e integração das tecnologias visando a democratização da Transformação Digital na Indústria do Brasil, notadamente nas tecnologias habilitadoras da Indústria 4.0 e conectividade 5G de alta performance em ambiente “Aberto”;

- Programas de capacitação, eventos tecnológicos, desenvolvimento de provas de conceito e outras atividades em parceria com ICTs e empresas;

- Transformação da rede de facilidades do SENAI em uma referência no estado da arte em termos de conectividade digital na tecnologia 5G para indústria e sociedade.

Ações SENAI SP em Cibersegurança e 5G

SENAI

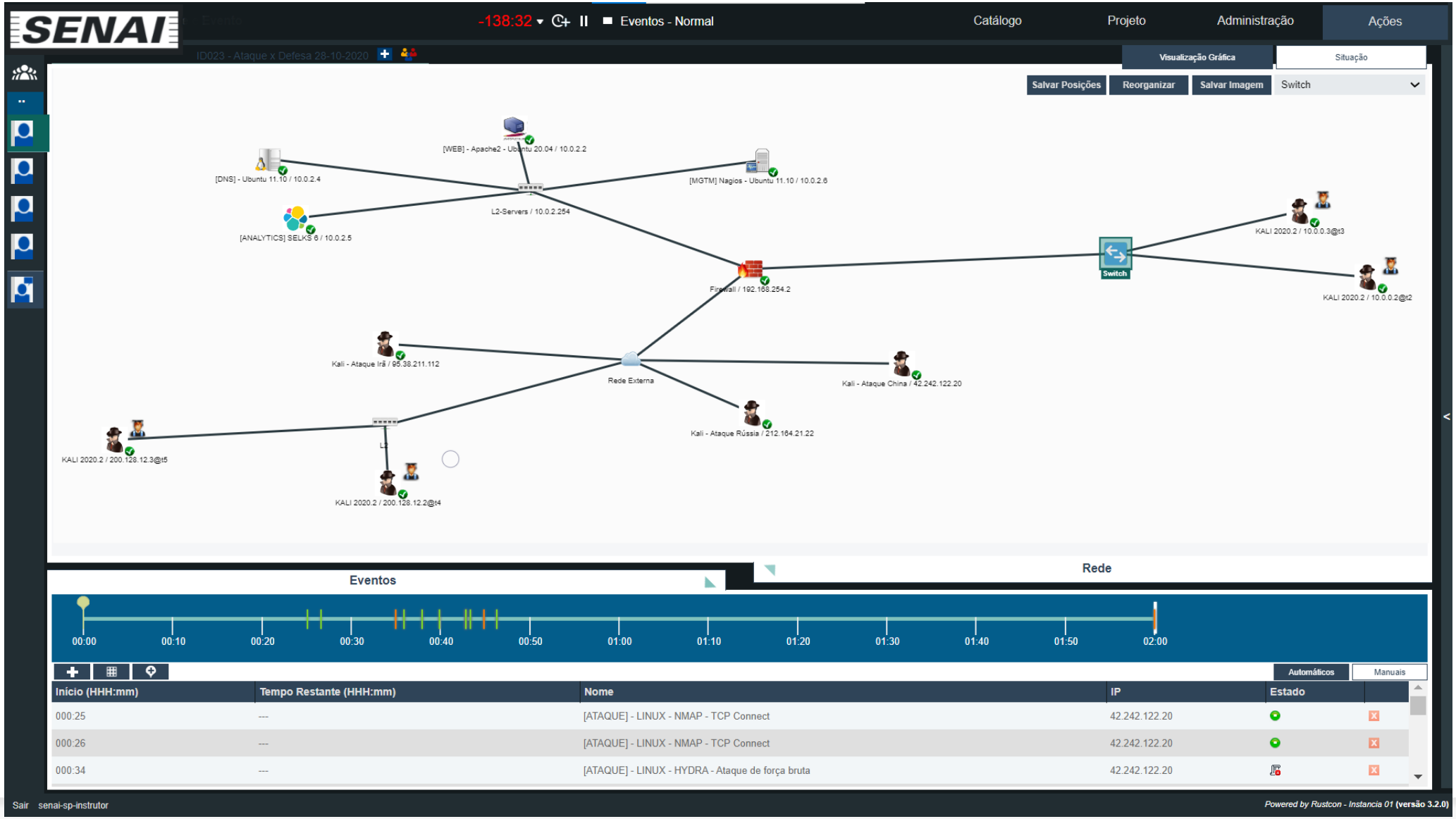
Missão FIESP ao NCFTA - USA

Laboratório de Malware NCFTA - USA

Laboratório de Segurança Cibernética – Escola SENAI de T.I.

Plataforma SOAR (Security Orchestration Automation and Response)

Simulador Hiper-realista de Ataque e Defesa Cibernética



SENAI

Estratégia de parceria com a Raytheon Technologies

Raytheon Technologies

Ryan Bagby
Executive
International Business

Shane Powell
Engineering Fellow - Cybersecurity

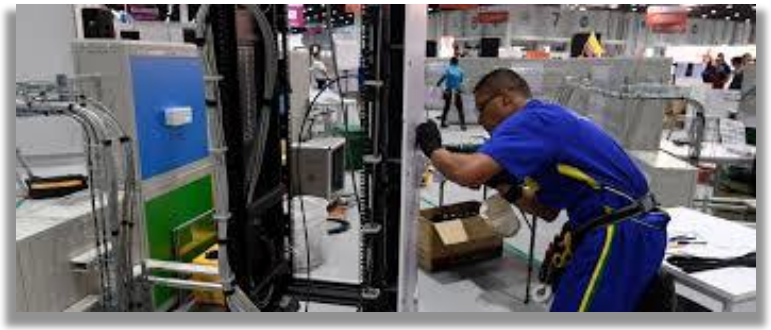
05/20/2021

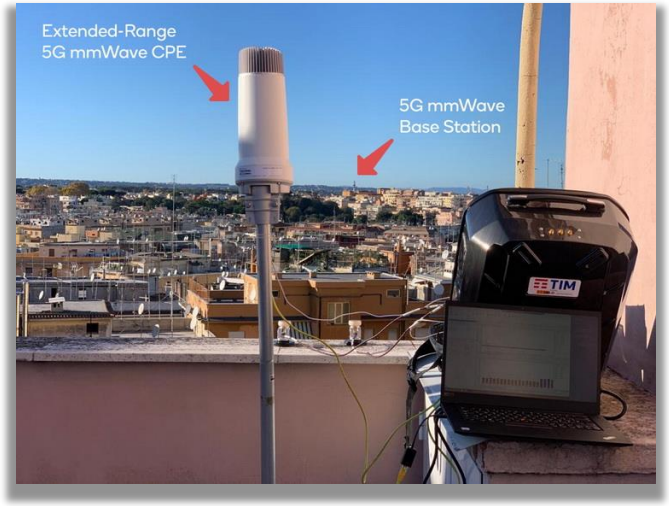
SENAI

Futuro Centro SENAI de Conectividade Digital São Paulo – Vila Mariana

Exemplo de configuração :
Bell Nokia Labs

Labs especializados em parceria com empresas e ICTs (Open Lab)





Caso SENAI – Bolha 5G no chão de fábrica

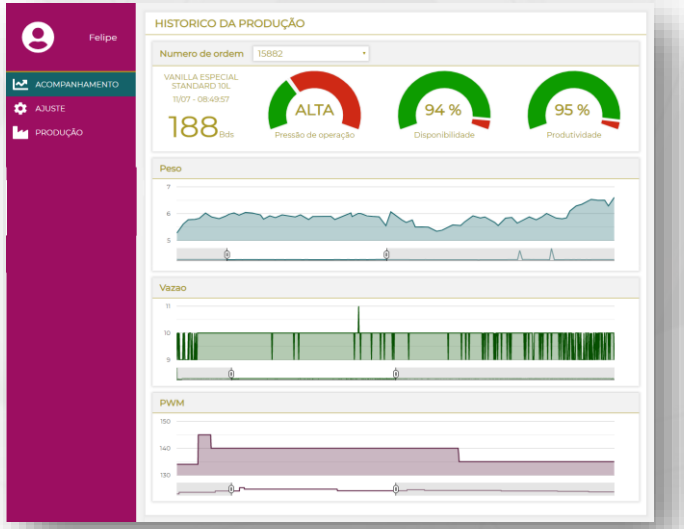
Casos implementados

1 – Solução de mobilidade para controle e monitoramento

2 – Realidade Aumentada

3 – Fábricas Flexíveis por meio de AIVs e Cobots

4 – Gestão de Ativos / Predição e Prescrição (AI)



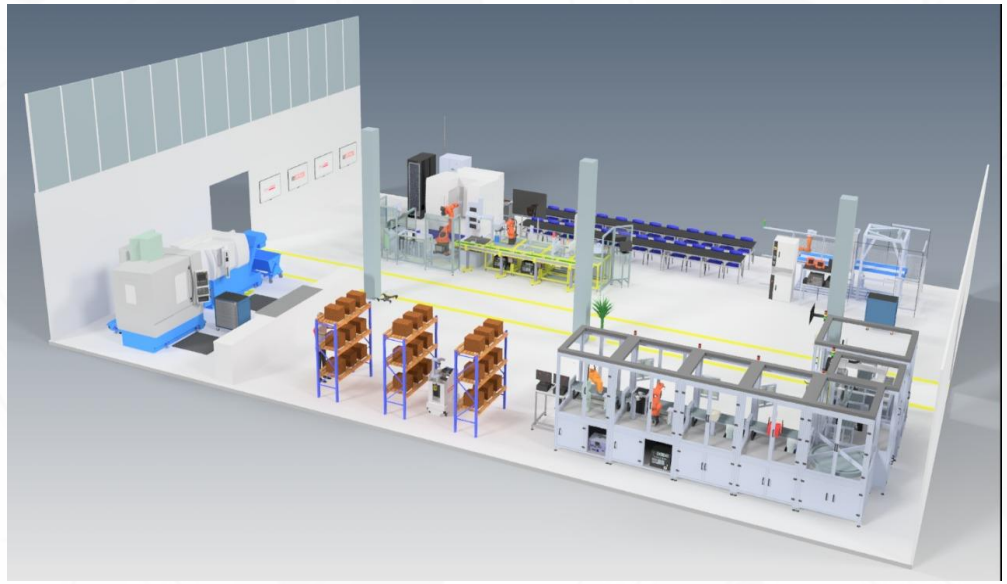
Projeto para compartilhamento de ativos e Laboratórios SENAI usando 5G

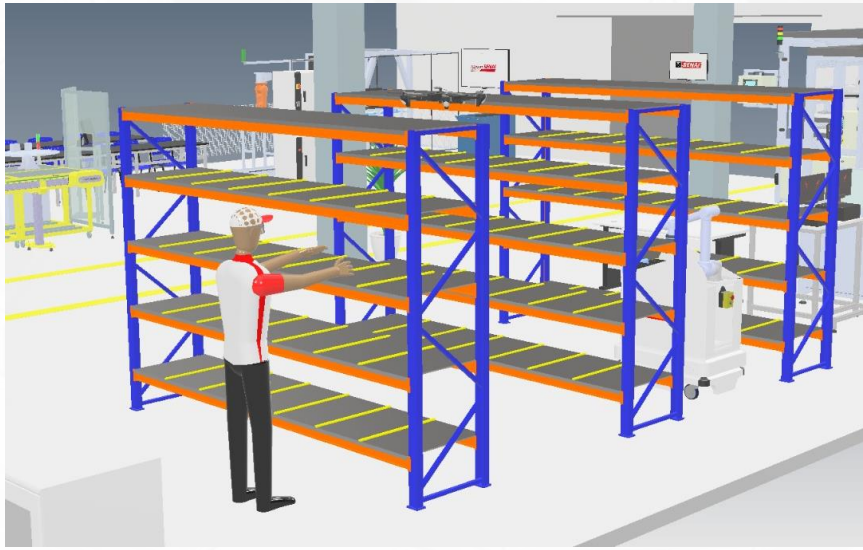
No compartilhamento virtual (Cyber Full) os equipamentos serão acessados e utilizados remotamente por meio de tecnologias de redes remotas de acesso para conectividade e câmeras especiais incluindo 5G.

Caso de uso – 5G Logística - Openlab de São Caetano

A utilização de drones integrados em uma rede privada 5G e realizando processamento de imagens através de aplicações em computação de borda e nuvem, proporcionará com que todas as informações sejam analisadas a qualquer momento e em qualquer lugar, obtendo assim uma solução de inventário em tempo real

ESTRUTURA DO WAREHOUSE





Vulnerabilidades no chão de fábrica

O 5G vai potencializar as vulnerabilidades

- **Baixa latência e grande densidade de objetos conectados – IoT**
- **Ataques maliciosos em sistemas industriais, incluindo Sistemas de controle, e Sistemas supervisórios e de aquisição de dados (SCADA) estão crescendo rapidamente nos últimos anos.**

Lufthansa's maintenance subsidiary Lufthansa Technik uses a private 5G network at its Hamburg headquarters for remote engine-parts inspection.

PHOTO: LUFTHANSA TECHNIK AG / PHOTOGRAPHER: JAN BRANDES

Ambiente Industrial predominantemente massivo e crítico

eMBB
Banda Larga Móvel Aprimorada

uRLLC
Comunicações de baixa latência e ultra confiáveis

mMTC
Comunicações massivas em máquinas

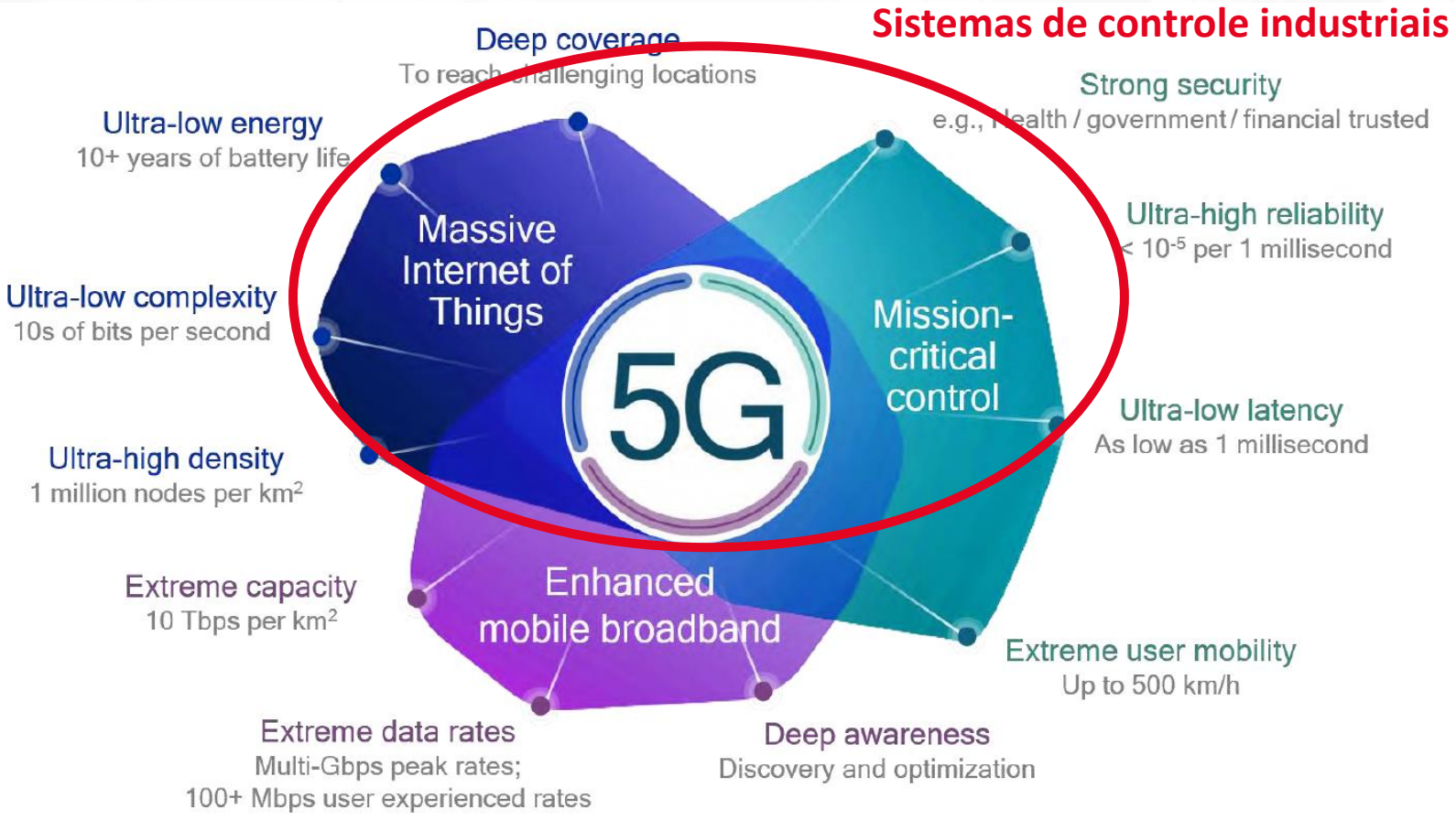
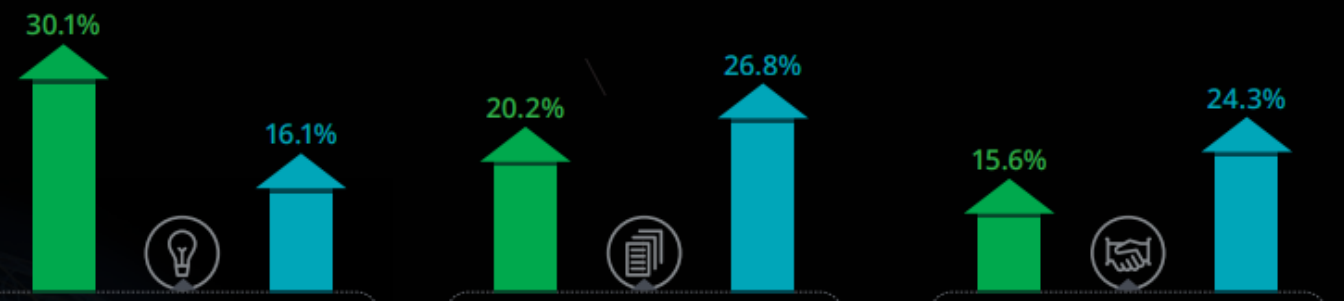


Image source: [Qualcomm white paper: Making 5G NR a reality]

Which do you think poses the greatest cybersecurity challenge to your organization's adoption of 5G?

Votes received: 582 (302 using 5G; 280 planning to adopt 5G in next 12 months)



Talent – 5G adoption will require appropriately skilled security professionals for implementation and maintenance without which establishment and operationalization of 5G may be hindered

Data – 5G adoption can enable a vast increase in the amount and diversity of data created from more enabled segments (e.g., IoT, ERP, and PHI) and associated risk of mismanagement of data, requiring updates to organizational data security management programs

Third parties – With increased cross-sector, enterprise-supplier, real-time collaboration with third parties and others in the external supply chain, 5G enablement increases dependency on third parties with the potential to impact production and productivity

Cost of adoption – Cyber risk associated with 5G deployment cannot be adequately mitigated against without incorporating an appropriate strategic approach and long-term strategy for upgrading legacy IT infrastructure and outdated systems

Adoption without cyber – 5G adoption can increase the attack surface, opening up the organization to greater risk without cyber provisions

Deloitte.

Yes, we currently use 5G

Yes, we plan to begin use of 5G during the next 12 months

Don't know/not applicable = 16.2% using 5G; 8.9% planning to adopt 5G in next 12 months

SENAI

Evolução do conceito de Cibersegurança para Imunidade Cibernética (vulnerabilidade no gateway)

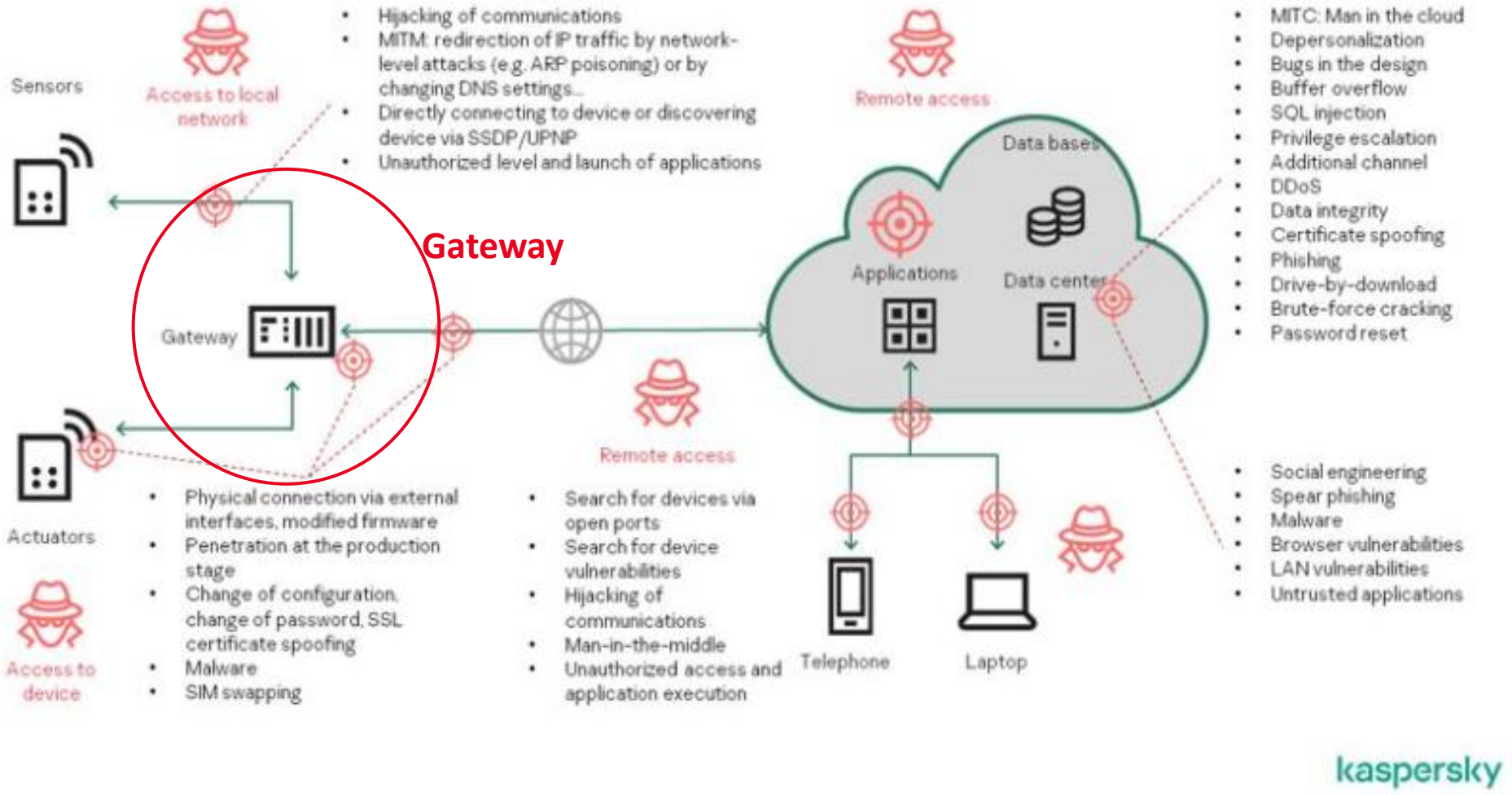


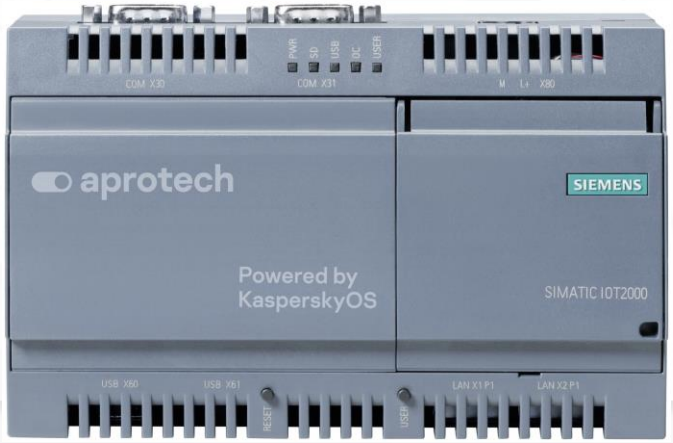
Exhibit 3 - Potential IoT Infrastructure Attack Scenarios (Courtesy Kaspersky)

Conceito de imunidade cibernética

Exemplo:

Hardware platforms
Kaspersky IoT Secure Gateway 100

Kaspersky IoT Secure Gateway 100, based on KasperskyOS, is a key element in the industrial digital transformation. It quickly and securely connects devices from the OT level to the level of enterprise IT. It is the world's first **industrial internet of things (IIoT) gateway with Cyber Immunity**, "innate" resistance to most types of cyberattacks.
The device is specially designed for industrial use and meets all the proven SIMATIC quality standards — durability, reliability and robustness.



5 G na industria – a questão da segurança cibernética

Conclusão:

Política de segurança cibernética 5G daqui para frente !

Para aproveitar ao máximo essa tecnologia, os formuladores de políticas devem trabalhar com o setor privado para implementar medidas eficazes de prevenção e controle 5G.

Primeiro, para construir redes 5G seguras e protegidas, os governos e empresas precisam adotar estruturas de confiança zero.

Um sistema de segurança cibernética que usa essa estrutura tem quatro características:

1- Limitar o acesso a todas as interações
2- Regulamentar todas as interações
3- Particionar ativos por meio de pequenos segmentos e
4- Monitorar regularmente os sistemas de segurança.

Os mecanismos de proteção e monitoramento de ponta a ponta da estrutura de confiança zero garantirão que todas as atividades na rede 5G sejam seguras.

Overcoming Cyber Threats in a 5G World CHRISTOPHER MARTIN· MARCH 2021 CPO MAGAZINE

5G NA INDÚSTRIA: A QUESTÃO DA SEGURANÇA CIBERNÉTICA

CONIC 26/08/21

Osvaldo Lahoz Maia
Gerência de Inovação e Tecnologia
omaia@sp.senai.br

SENAI SÃO PAULO - 2021