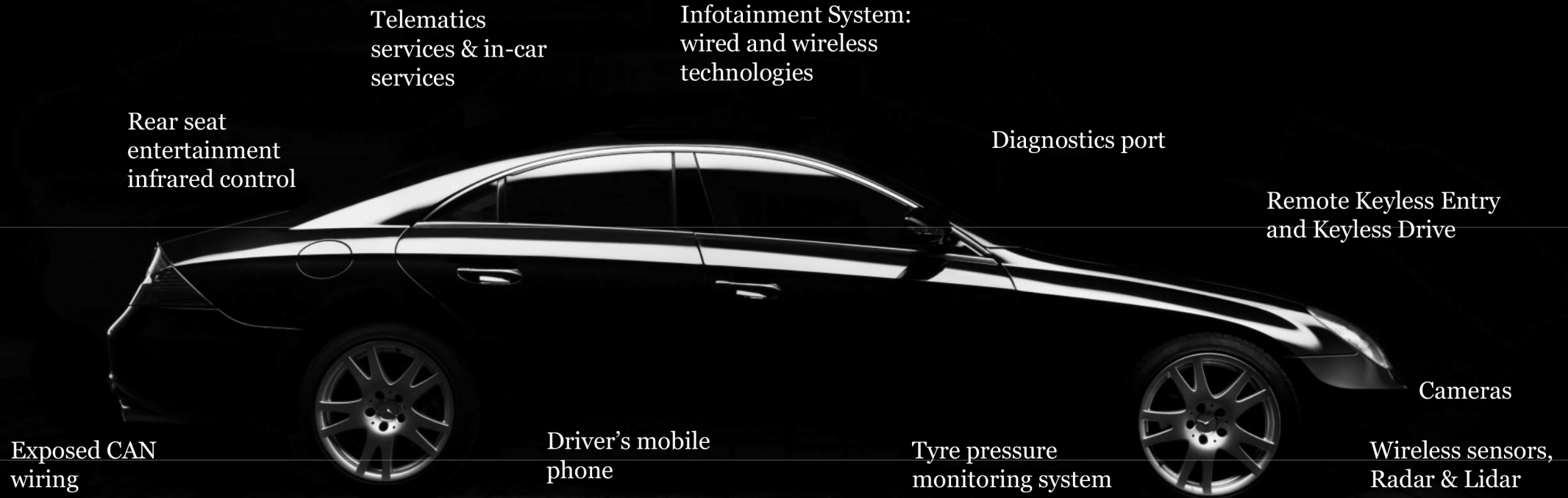




KNIGHTEC

THE SOUL OF DIGITALIZATION

Connected cars – Attack surfaces



Godfrey Shirima & Kit Gullbrandson



- Product Cybersecurity Consultant.
- Positions / Assignments:
Project Manager – Data Integrity Assignment at McNeil
- Information Security Auditing, Risk Management, Penetration Testing.
- Pencil Artist
- Amateur Photographer
- Reading – Book Club Moderator

- Business Unit Manager Software and Cybersecurity
- 30 years in the SW-industry
- Naïve when it comes to my own smart home
 - Robot vacuum cleaner, Alexa, Smart lamps, ...
- “Shoemaker’s children”



Agenda

Security challenges when the industry gets connected

Security culture and awareness

Cybersecurity examples from different industries

Security challenges when the industry gets connected

Threat Actors & Attack Surface

Nation States

Cybercriminals

Hactivists (Anonymous)

Competitors

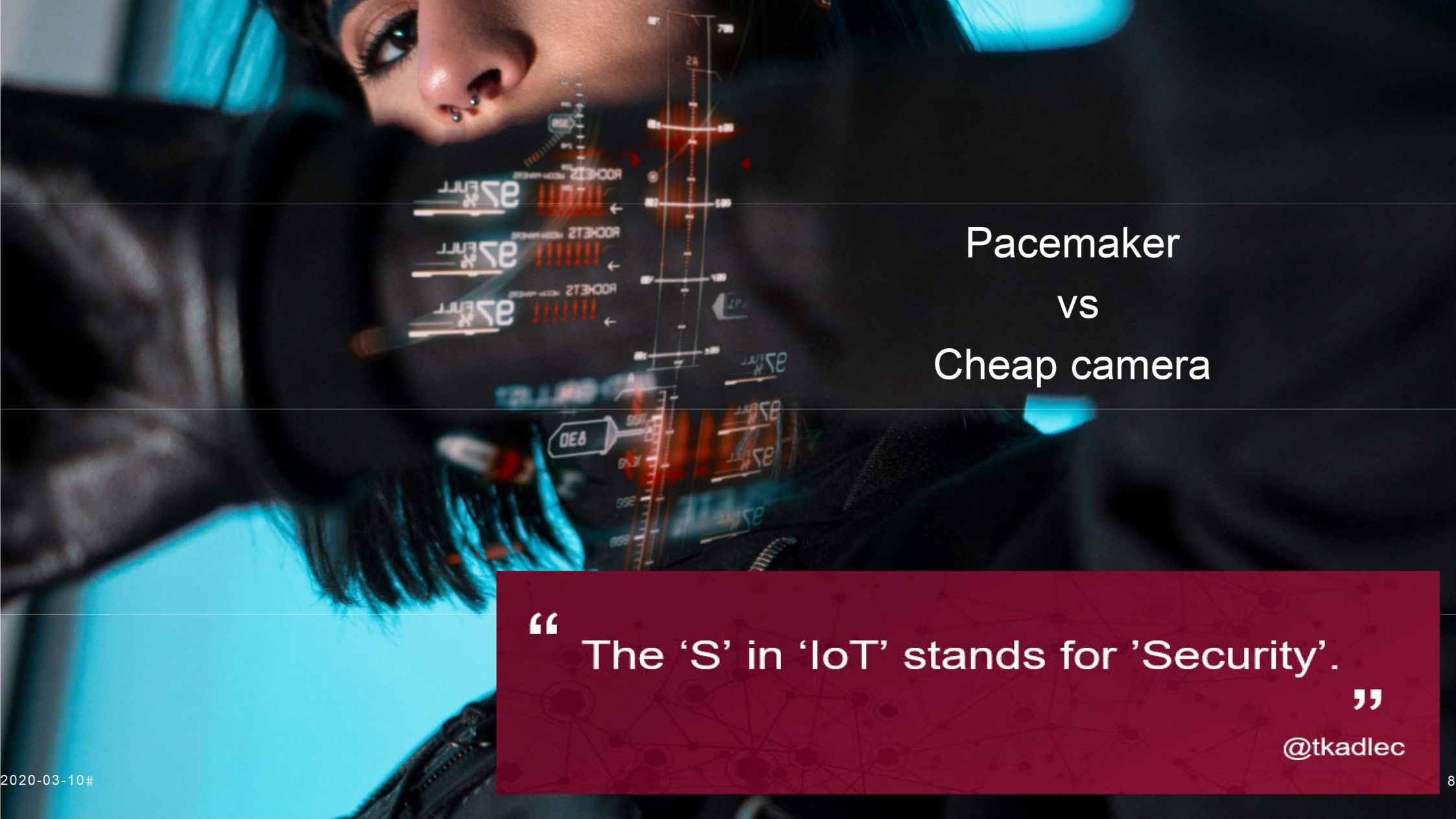
Insider Threats

BYOD Challenges

Data Breaches

Example: In July, 2019 Orvibo Smart Home products data breach

2 Billion Records exposed



Pacemaker vs Cheap camera

“ The ‘S’ in ‘IoT’ stands for ‘Security’.

”

@tkadlec

Security culture and awareness



- Top Down Security Mentality
- Security by Design
- Security Standards & Best Practices Adoption
- Cyber Security Trainings

65%

Verizon Data Breach Investigations Report 2019

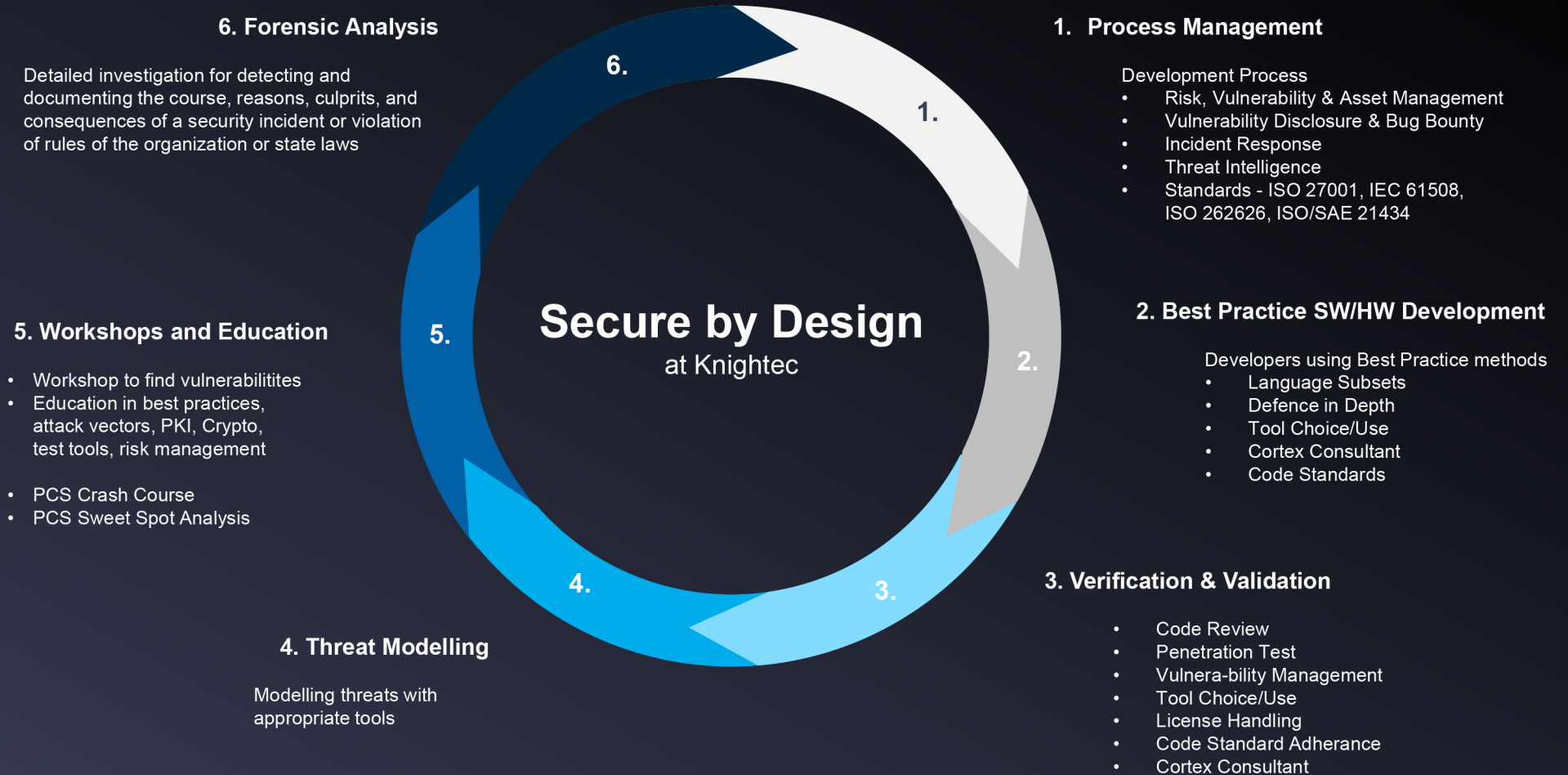
30%



Quick Wins

- Security Updates & Patching
- Passwords...Passwords... Passwords
- Multi-Factor Authentications
- BYOD risks mitigations controls

Examples from the industry



Pharmaceutical Industry

Cybersecurity Project Management

Background

Helping a customer to close Data Integrity gaps for applicable automation systems. The gaps were identified internally and Knightec is tasked to facilitate gaps closure by involving interested parties and act as trusted advisor on how the project could be successfully completed.

Secure by Design

- Vast experience in information security
- Knowledge of standards and best practices

Solution and Results

Project is ongoing and we are able to close significant number of gaps

Automotive Industry

Cybersecurity Management System (ISO/SAE 21434) UNECE Requirements

Background

The entire automotive industry will be affected by new UNECE (United Nations Economic Commission for Europe) requirements that will become EU directives and thus national legislation throughout the EU which will mean, among other things, a certified CSMS (Cybersecurity Management System) in accordance with ISO/SAE 21434.

Secure by Design

Knightec provides support to multiple work streams in

- product development
- product maintenance
- type approval
- cybersecurity risk management
- cybersecurity asset management
- vulnerability management
- threat intelligence
- vulnerability disclosure
- incident response

Solution and Result

A structured approach to cybersecurity work will be necessary throughout the organization for all companies that want to sell vehicles in the future.

Manufacturing Industry

Security Review and Security Update of Communications module

Background

The customer wanted to conduct an independent security review of their own developed communication module using a Bluetooth interface.

Secure by Design

- Security Review and threat analysis
- Best Practice SW/HW Development
- Bluetooth communication
- Key handling (PKI)
- Penetration testing

Solution and Results

The unit was analyzed based on possible attack vectors, which were then penetration tested. The module showed weaknesses that could be exploited for unauthorized access.

The software of the communication module was updated and new methods and configurations were added to establish a more reliable and secure Bluetooth connection.

The result was a product where the risks for security breaches had been reduced to a minimum.

Swedish Police Force

Forensic Analysis of Tachograph Manipulation Device

Background

The Police had found an unknown device during a routine control. They suspected that the device was used to manipulate signals to tachographs in order to make it possible for the truck driver to continue driving without any tachograph registration.

The purpose of the analysis was to determine if it was possible to use program analysis to find out how the device is working and in what way it could be activated.

Secure by Design

- Forensic Analysis
- Reverse Engineering
- Static program analysis
- HW design analysis

Solution and Result

The processor type was identified and further analysis showed that the processor was locked and no further information about how the device software was working. Analysis of the CAN buses resulted in the information that when the CAN buses were connected no data was sent in either direction from the device.

The conclusion of this analysis was that the device is most certainly used for manipulating a tachograph.

Thanks for listening!

KNIGHTEC

THE SOUL OF DIGITALIZATION