



From Bugs to Breaches: How to be a Security Tester

(and why you can't talk about it)



Benjámín Krivácsy



BSc and MSc degree in
Mechatronics Engineering
in BME



Working at Bosch
for 5+ years



Specialized in
security testing

Gergő Roznár



Academic studies
at BME



Working for Bosch
since 2018



Specialized in
security testing



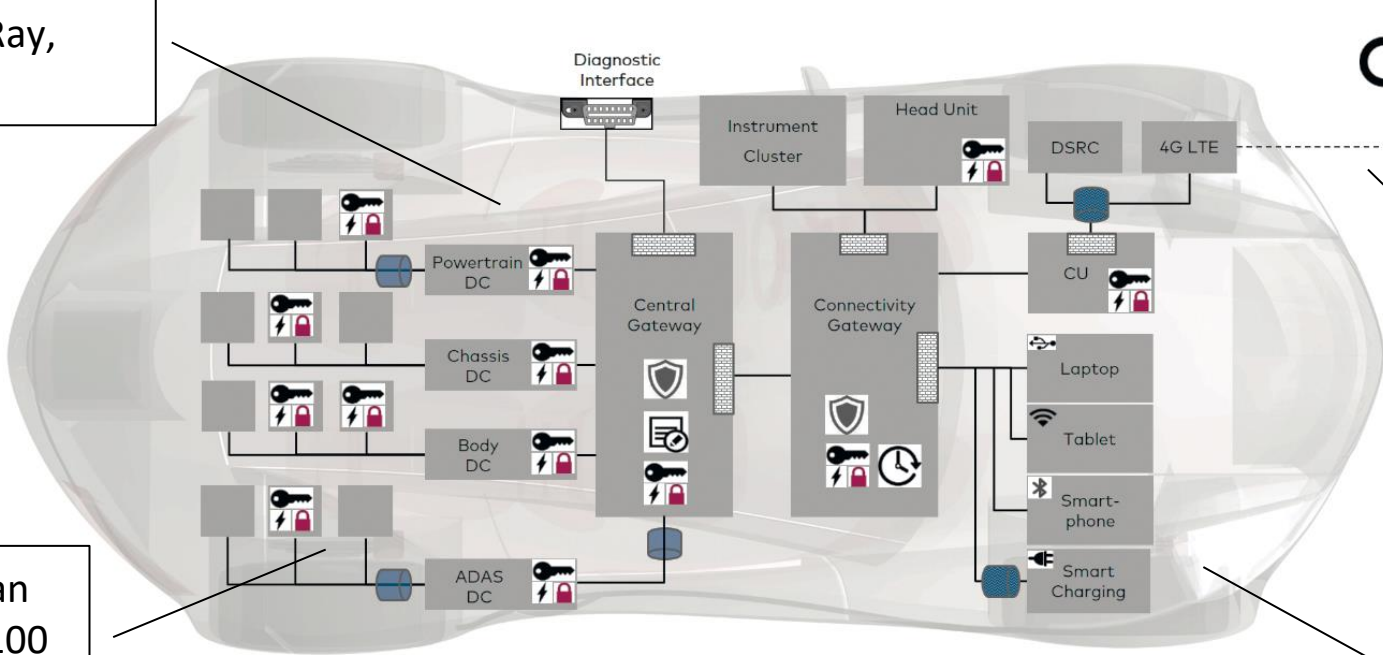
Our journey...



Why security testing is relevant in the automotive industry?

Higher complexity \Rightarrow Growing attack surface

Communication channels
(LIN, CAN, FlexRay,
Ethernet)



FOTA (Firmware
Over-The-Air)

Modern vehicles can
contain more than 100
ECUs

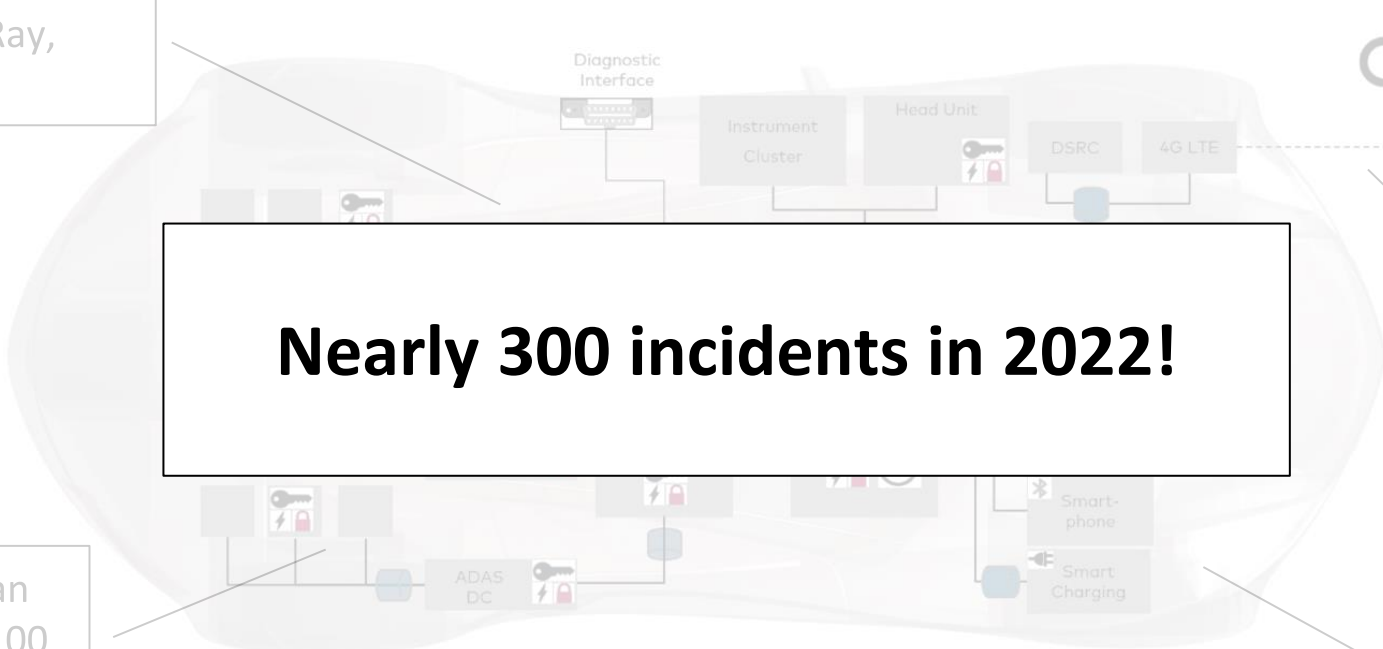
Connecting external
devices to the car

Source: https://www.infineon.com/dgdl/Infineon-ISP-Use-Case-Cyber-security-mechanisms-for-connected-vehicles-ApplicationBrochure-v02_19-EN.pdf?fileId=5546d462647e95a60164889affd74a5e

Why security testing is relevant in the automotive industry?

Higher complexity ⇒ Growing attack surface

Communication channels
(LIN, CAN, FlexRay,
Ethernet)



Nearly 300 incidents in 2022!

FOTA (Firmware
Over-The-Air)

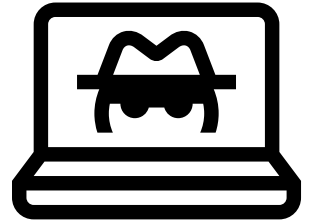
Modern vehicles can
contain more than 100
ECUs

Connecting external
devices to the car

Source: https://www.infineon.com/dgdl/Infineon-ISP-Use-Case-Cyber-security-mechanisms-for-connected-vehicles-ApplicationBrochure-v02_19-EN.pdf?fileId=5546d462647e95a60164889affd74a5e

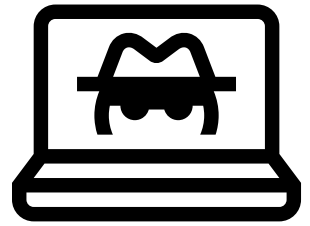
How can we reduce the probability of security risks?

Our source of information and experience



How can we reduce the probability of security risks?

Our source of information and experience

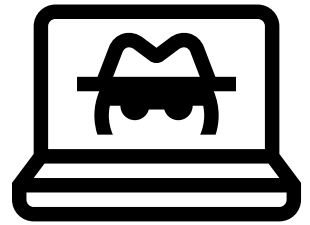


Follow the security standards

- UNECE's certification for CSMS (Cyber Security Management System)
- ISO/SAE 21434 – Road vehicles - Cybersecurity engineering
- For other areas there are also specific standards (e.g. ISO 27001 and 27002, IEC 62443, NIST)

How can we reduce the probability of security risks?

Our source of information and experience



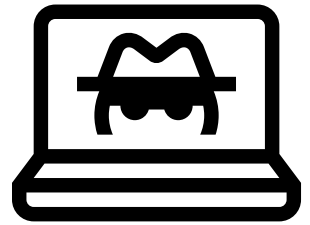
Follow the security standards

- UNECE's certification for CSMS (Cyber Security Management System)
- ISO/SAE 21434 – Road vehicles - Cybersecurity engineering
- For other areas there are also specific standards (e.g. ISO 27001 and 27002, IEC 62443, NIST)

Audits

How can we reduce the probability of security risks?

Our source of information and experience



Follow the security standards

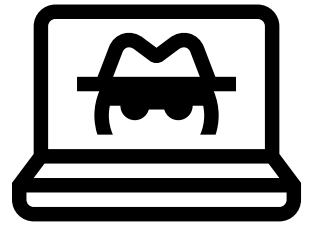
- UNECE's certification for CSMS (Cyber Security Management System)
- ISO/SAE 21434 – Road vehicles - Cybersecurity engineering
- For other areas there are also specific standards (e.g. ISO 27001 and 27002, IEC 62443, NIST)

Audits

Security related trainings

How can we reduce the probability of security risks?

Our source of information and experience



Follow the security standards

- UNECE's certification for CSMS (Cyber Security Management System)
- ISO/SAE 21434 – Road vehicles - Cybersecurity engineering
- For other areas there are also specific standards (e.g. ISO 27001 and 27002, IEC 62443, NIST)

Audits

Security related trainings

Consider the Security testing in the planning phase!

Product security testing timeline



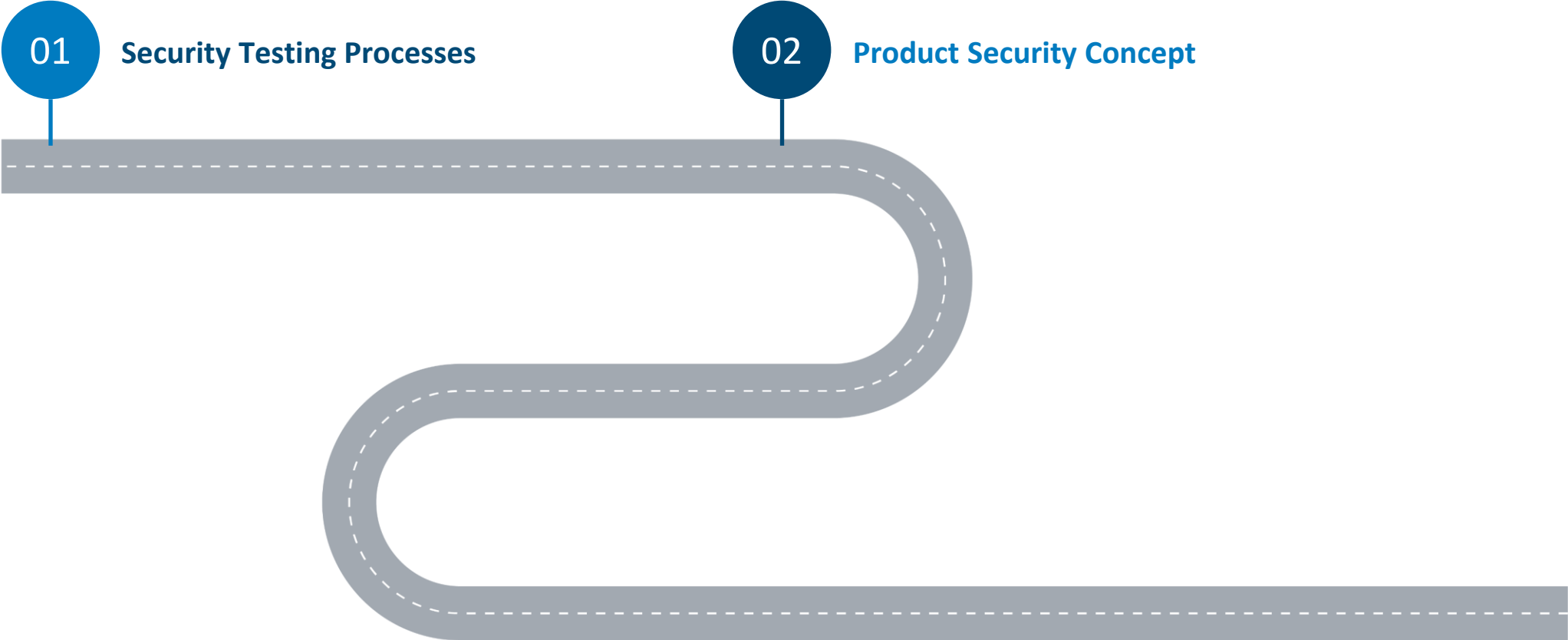
Product security testing timeline

01

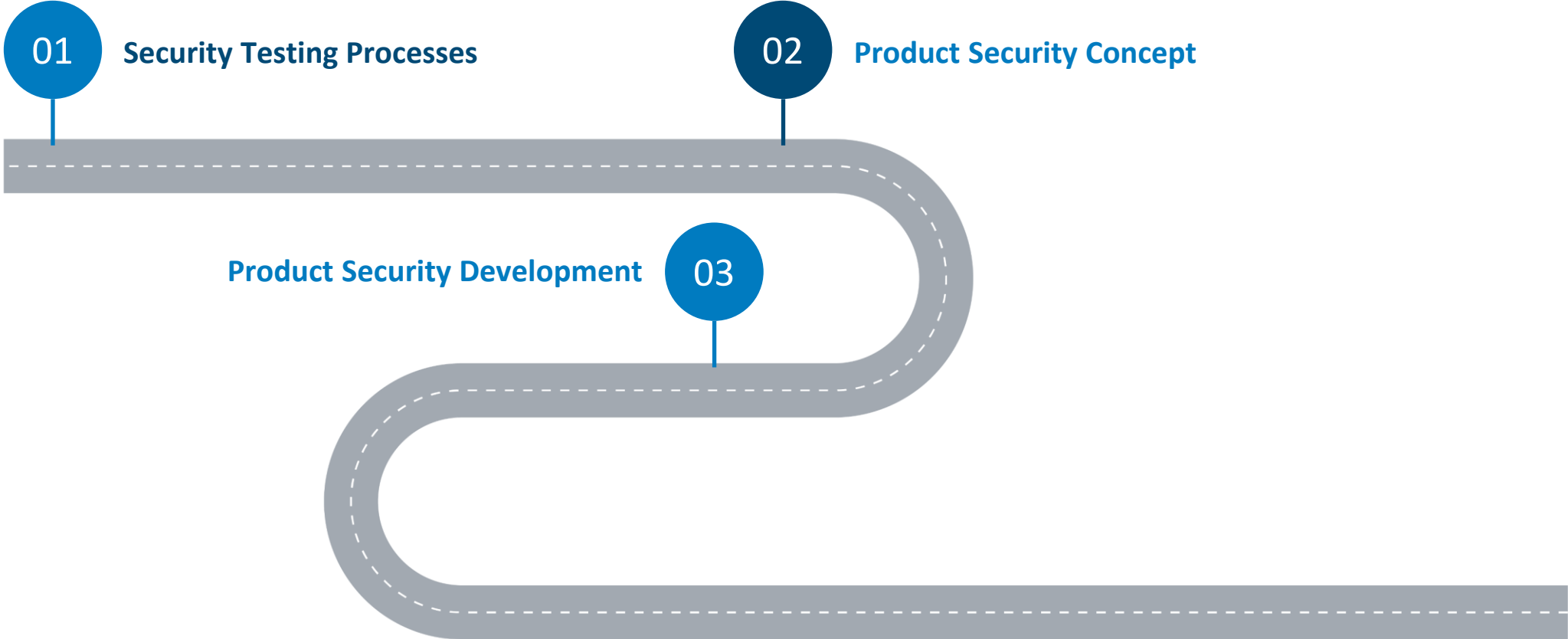
Security Testing Processes



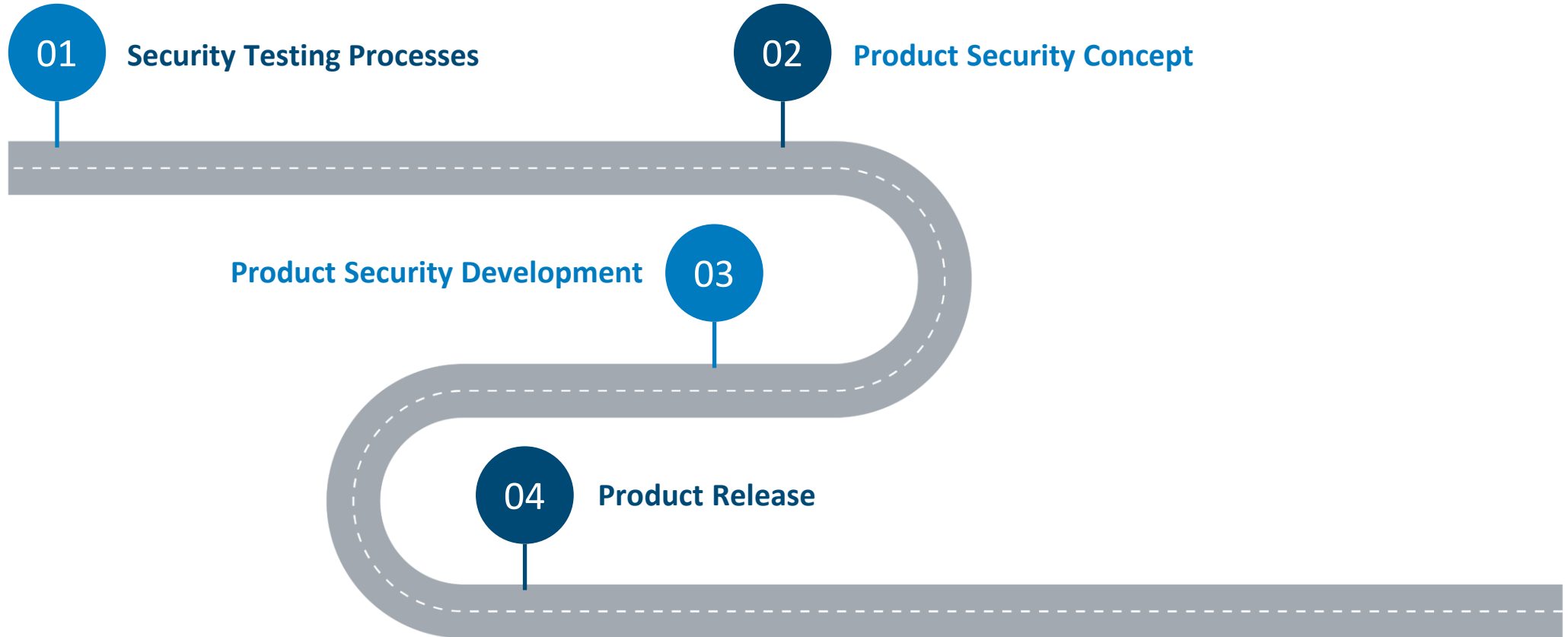
Product security testing timeline



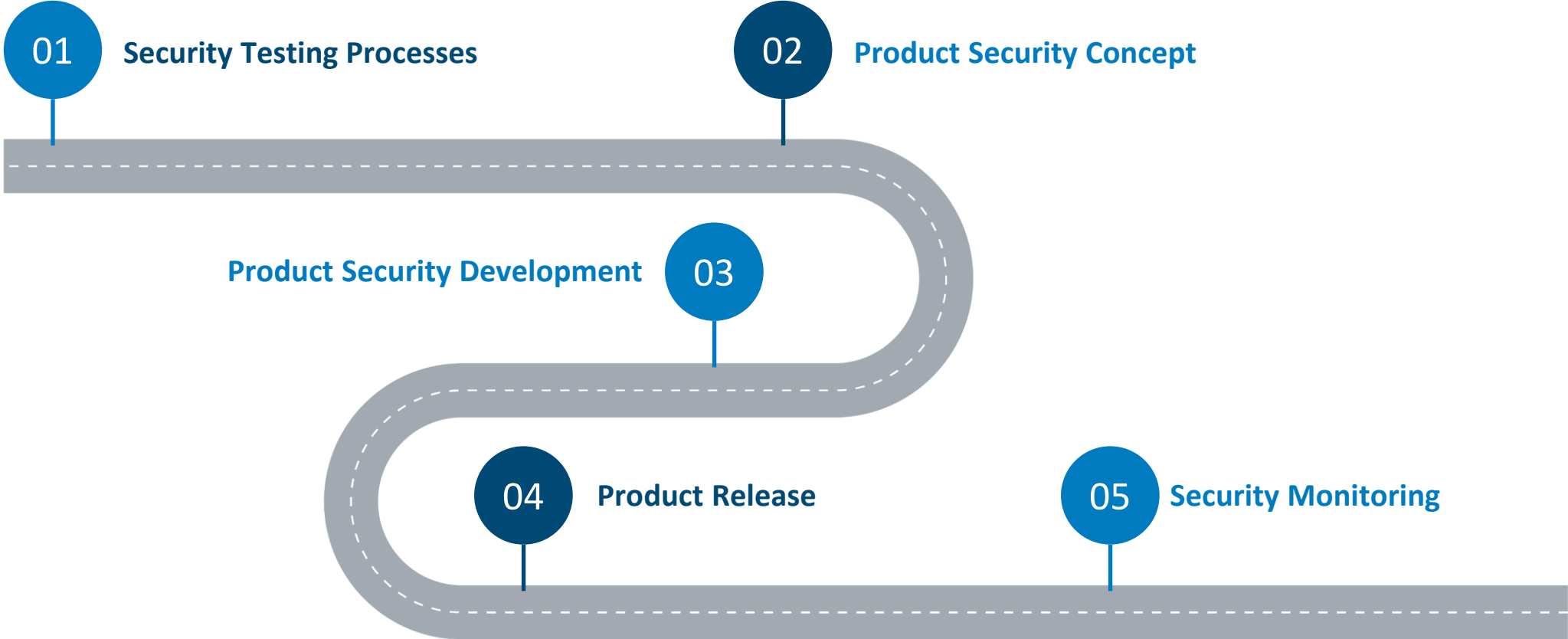
Product security testing timeline



Product security testing timeline



Product security testing timeline



What did we find different? Standard vs Security Testing



What did we find different?

Standard vs Security Testing

Deep understanding of the functionalities is necessary.



What did we find different?

Standard vs Security Testing

Information sharing is encouraged.

Deep understanding of the functionalities is necessary.



What did we find different?

Standard vs Security Testing

Information sharing is encouraged.

Deep understanding of the functionalities is necessary.

Sensitive information shall be severely restricted.



What did we find different?

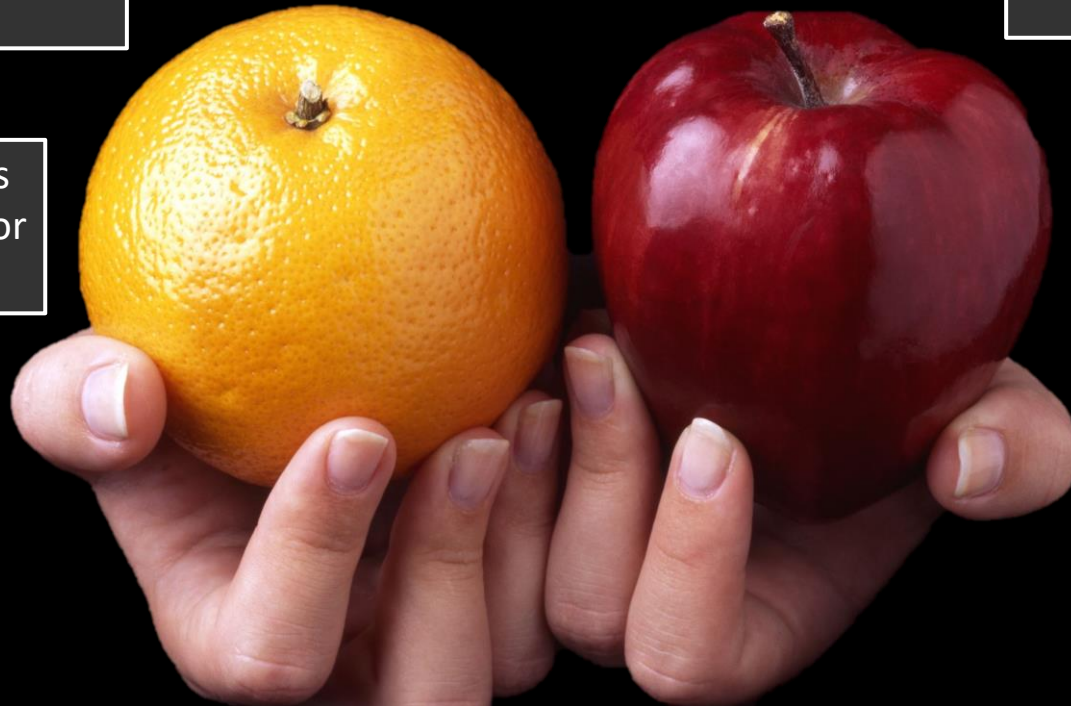
Standard vs Security Testing

Information sharing is encouraged.

Deep understanding of the functionalities is necessary.

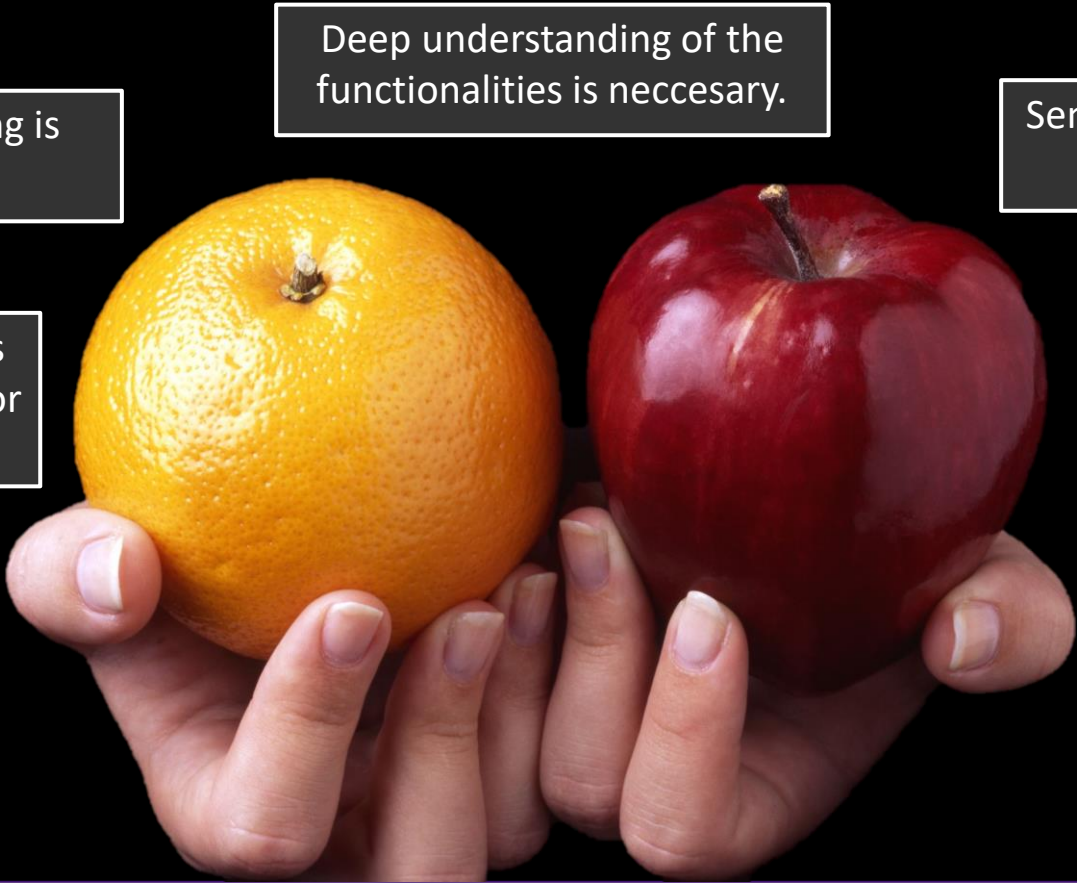
Sensitive information shall be severely restricted.

Well defined requirements coming from stakeholders or legal entities.



What did we find different?

Standard vs Security Testing



Information sharing is encouraged.

Deep understanding of the functionalities is necessary.

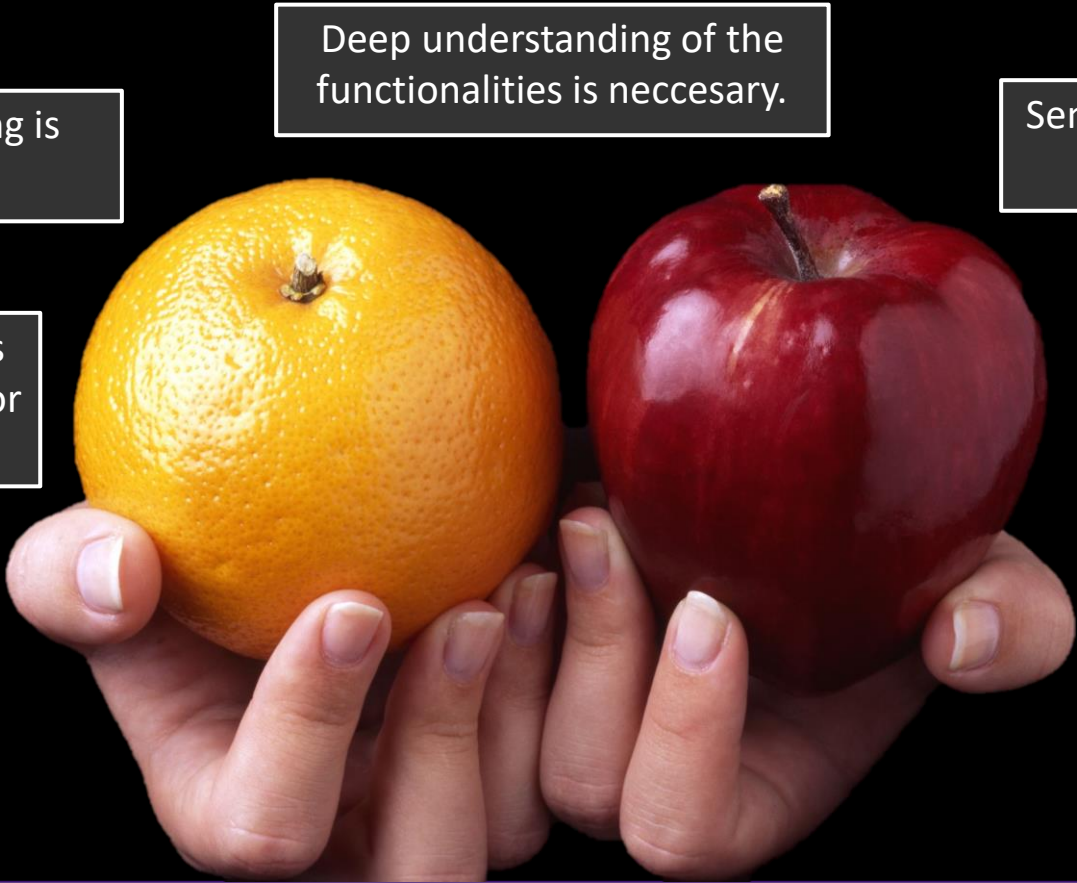
Sensitive information shall be severely restricted.

Well defined requirements coming from stakeholders or legal entities.

Requirements are harder to define.

What did we find different?

Standard vs Security Testing



Information sharing is encouraged.

Deep understanding of the functionalities is necessary.

Sensitive information shall be severely restricted.

Well defined requirements coming from stakeholders or legal entities.

Requirements are harder to define.

The main focus is on requirement based testing.

What did we find different?

Standard vs Security Testing

Information sharing is encouraged.

Deep understanding of the functionalities is necessary.

Sensitive information shall be severely restricted.

Well defined requirements coming from stakeholders or legal entities.

Requirements are harder to define.

The main focus is on requirement based testing.

Security testing is often a second class citizen.



Security testing methods


Test techniques based on ISO 29119

+

Test techniques based on ISO 21434

- Defensive Coding Tests
 - Fuzzing Tests
 - Side Channel Attacks
- Functional Security Tests
 - Service Scanning
 - Vulnerability Scan
 - Penetration Test

...



Access to rights and information
is quite complicated...

Access to rights and information
is quite complicated...

What are the
necessary
rights and tools for
my work?

Access to rights and information
is quite complicated...

What are the
necessary
rights and tools for
my work?

What are the base
knowledge
that I should
acquire?

Access to rights and information
is quite complicated...

What are the
necessary
rights and tools for
my work?

What are the base
knowledge
that I should
acquire?

How and where should I
store the secure data?

Access to rights and information is quite complicated...

What are the
necessary
rights and tools for
my work?

What are the base
knowledge
that I should
acquire?

Who should I ask
about it?

How and where should I
store the secure data?

Aspects of security

Safety of
customer
assets

Aspects of security



**Safety of
customer assets**



**Safety of
company assets**



Due diligence

Mistakes and breaches
can happen anytime.



Flexibility

And anywhere...



Problems can come in
different shapes and
sizes.

Working with other domains



Security is often needed at
non-security related
problems.

Professional Isolation

Our final conclusion

How to be a Security Tester



- 1 Find the right opportunity
- 2 Gather knowledge
- 3 Prepare yourself for challenges
- 4 Be creative
- 5 Enjoy being a security tester

Thank you very much for
attention!

Q&A time