Product Security Comes of Age

TOREON

This slide deck was meant to be presented, not serve as a reference.

Catch the next run of this talk at ISACA Belgium on 03/12/26,
or have a look at my other presentations on the topic of CRA and product security

Scan	Talk	Link
	Product Security Comes of Age Live online - with ISACA Belgium	isaca.be/events/product-security-comes-of-age
	CRA Webinar 1 – Intro the CRA Toreon – Webinar Recording	youtube.com/watch?v=IdGOt1yqArA
	CRA Webinar 2 – Getting Started Toreon – Webinar Recording	youtube.com/watch?v=JNhJP_Z9leg
	CRA – Risk-based Selection of Security Requirements CRACY – Webinar Recording	youtube.com/watch?v=RpUU2eaNSlo

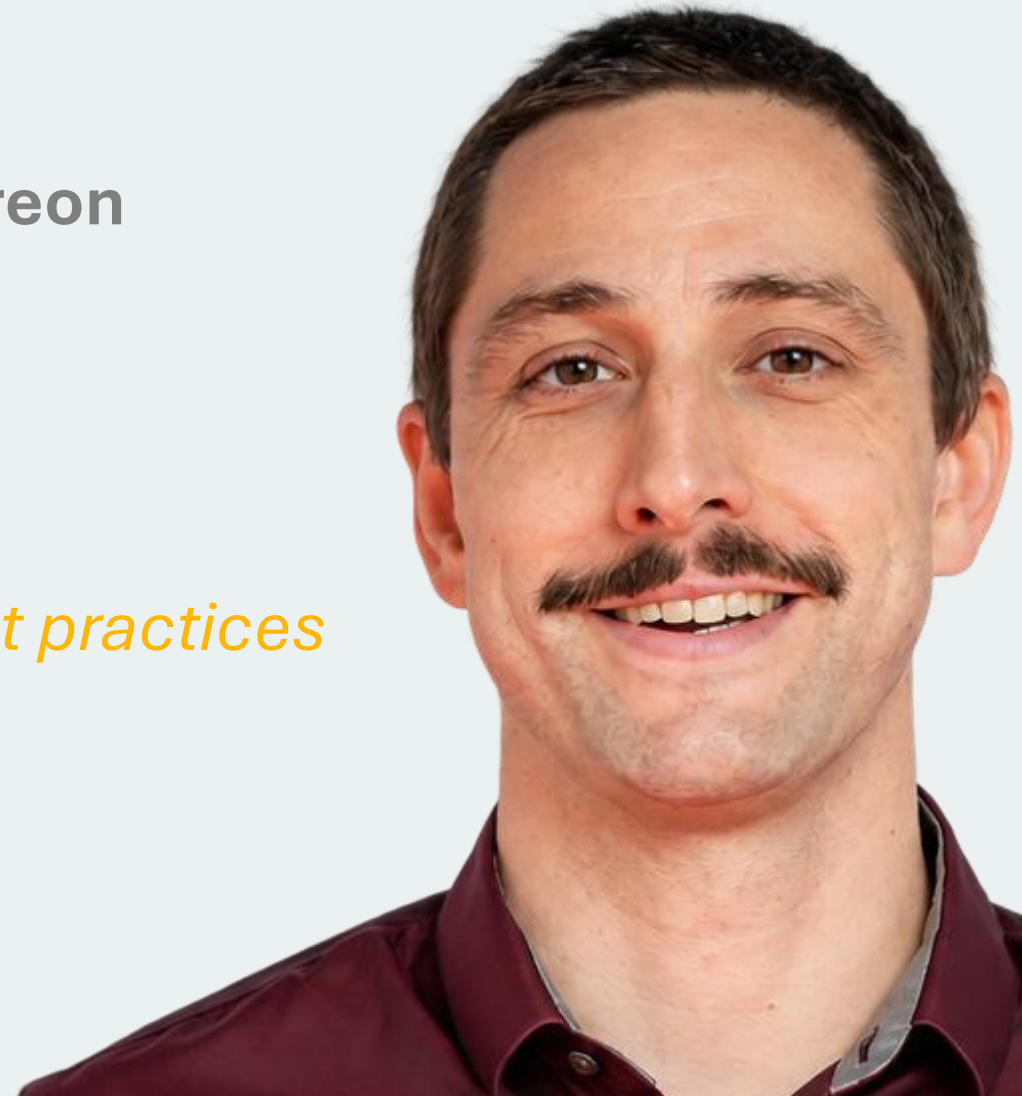
Maxim Baele

Principal Consultant Product Security @Toreon

I help organizations build secure products

Volunteer @OWASP

I help build a community around security best practices



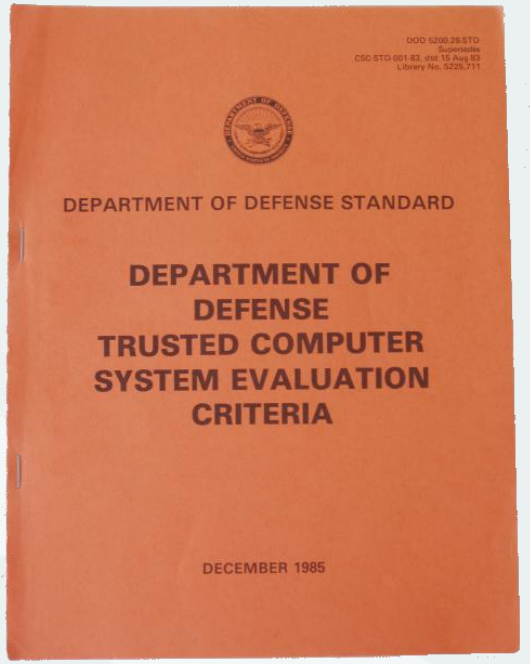
The domain of

“product security”

is coming of age

(at this very moment!)





1980’s

CITICORP



1990’s

flickr

OWASP TOP10

2000’s



Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	■	■	■	■
Client & end-point protection	■	■	■	■/□
Identity & access management	■	■	■/□	■/□
Application level controls	■	■	■/□	□
Network controls	■	■/□	□	□
Host infrastructure	■	■/□	□	□
Physical security	■	□	□	□

■ Cloud Customer □ Cloud Provider

2010’s





2020’s

In marketing and economics, a **product** is any object, service, or system offered to a market to satisfy a customer's need or want

Source: wikipedia.org Product_(business)

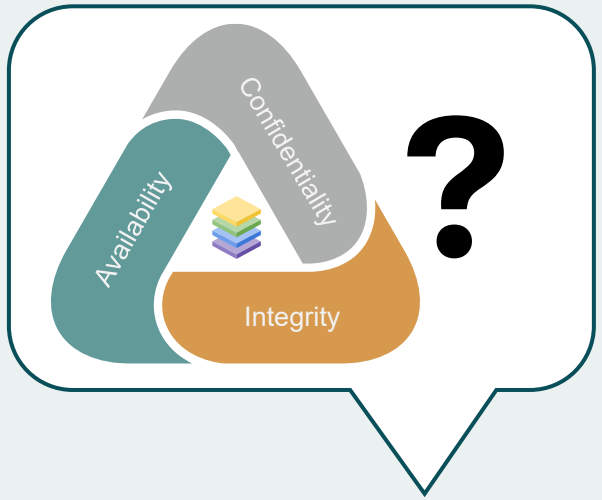


A ‘**Product with Digital Elements**’ means a software or hardware product and its remote data processing solutions,
including software or hardware components being placed on the market separately

Source: Cyber Resilience Act (EU Reg 2024/2847)



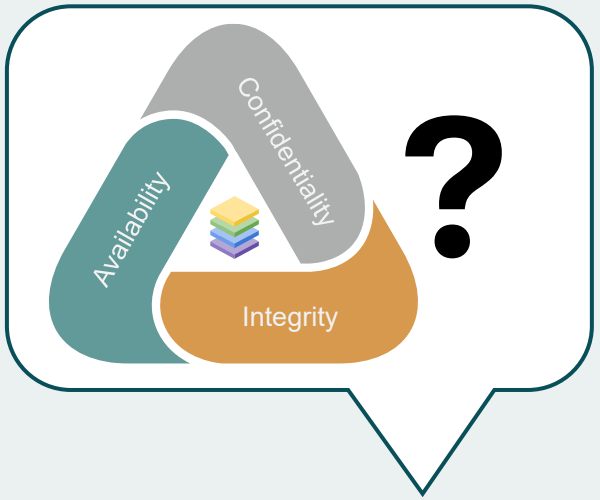

Project step
Jan
Feb
Mar
Apr
May
June
July
Aug
Sep
Oct
Nov
Dec



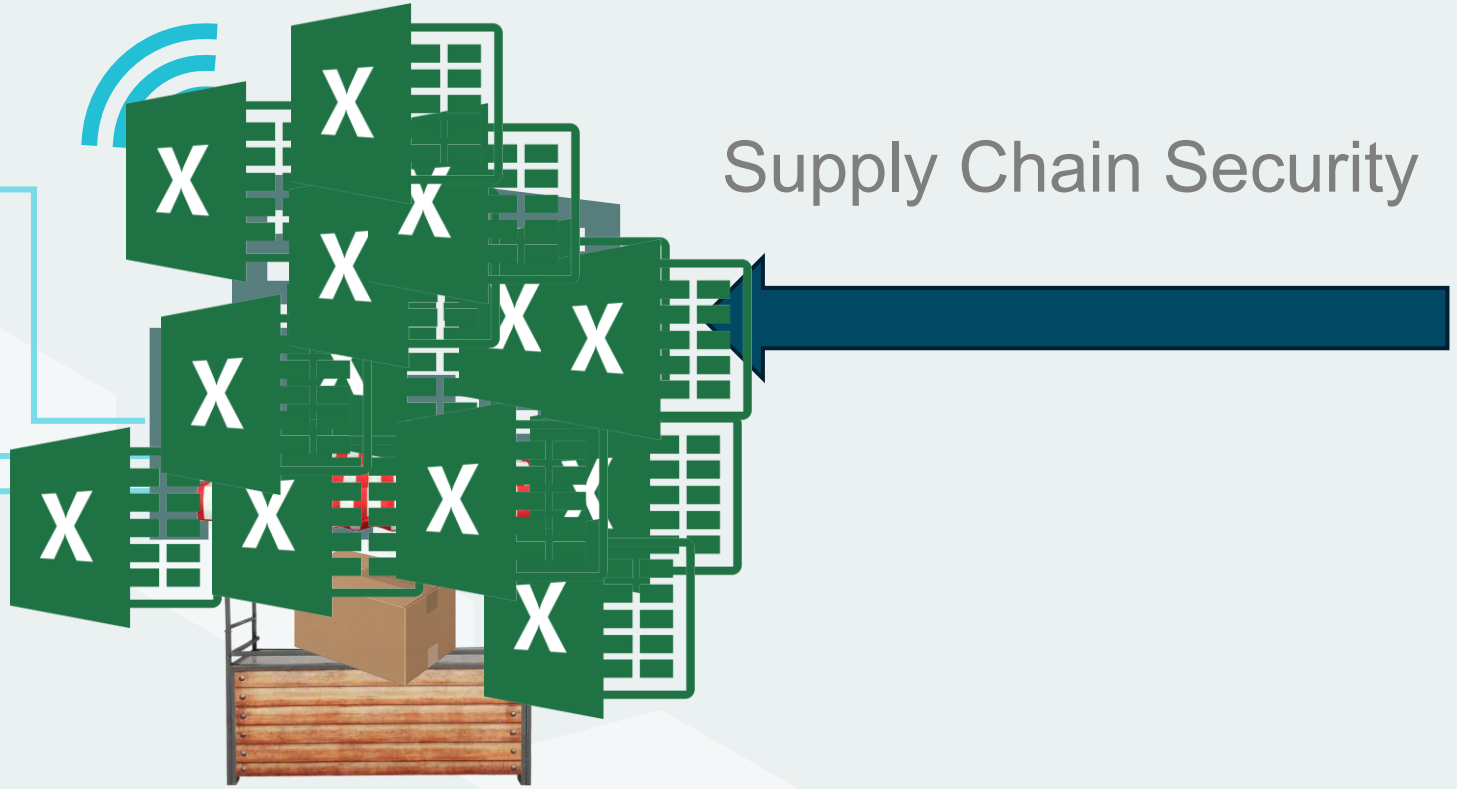
Supply Chain Security







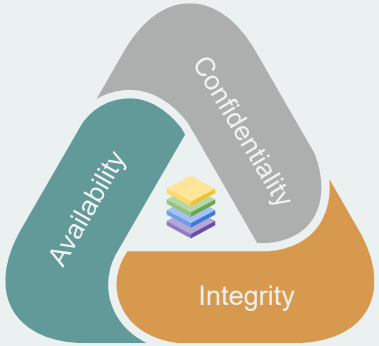
Supply Chain Security






Confidentiality
Availability
Integrity
?
Product Security





?









Build the product with security built in

Communicate transparently on security

Provide security updates, handle incidents and support it during its expected life



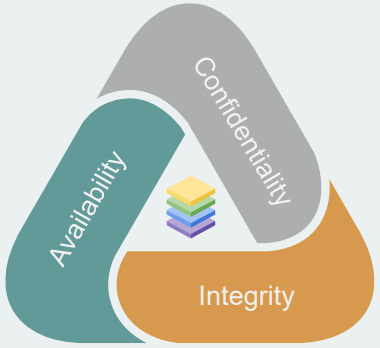












?

Build the product with security built in



Build the product with security built in

→ “The right amount of security is *just enough* security” ™

…for your markets you sell into
…for the intended purpose of the product
…for the reasonable foreseeable lifetime of the product



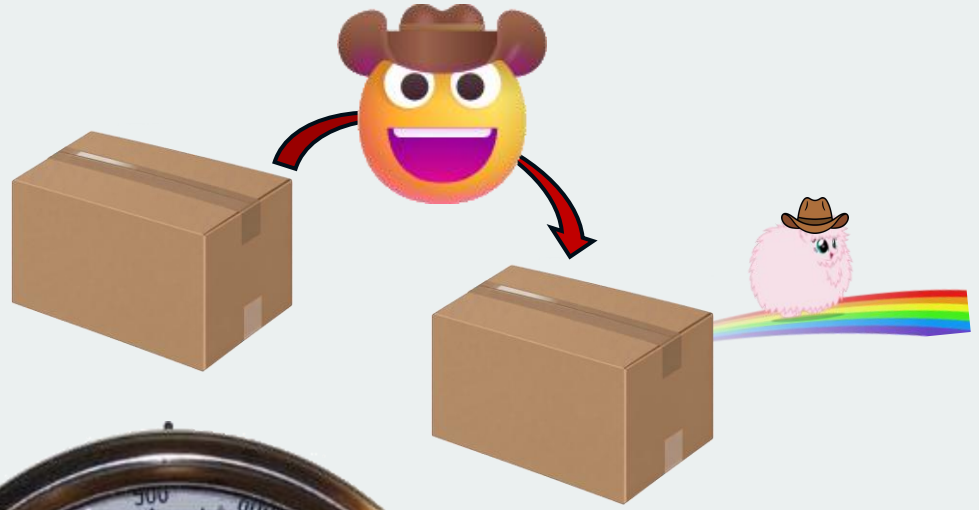


Build the product with security built in



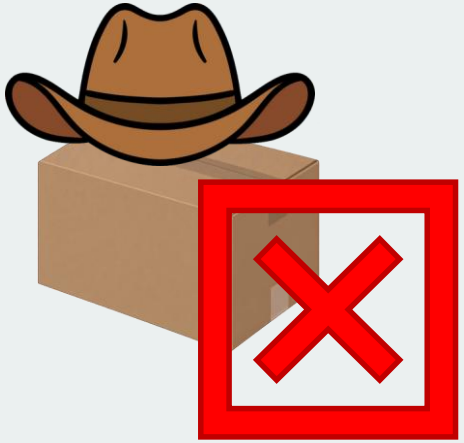


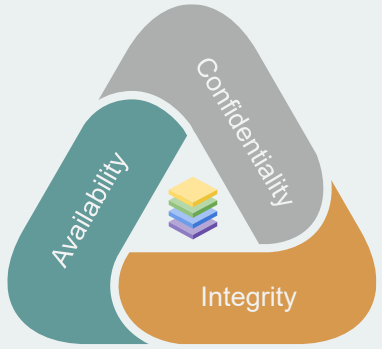
Build the product with security built in







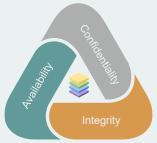


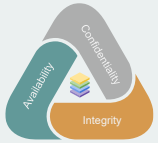


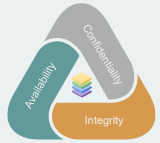
?

Build the product with security built in



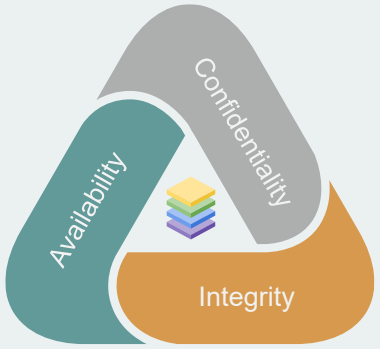






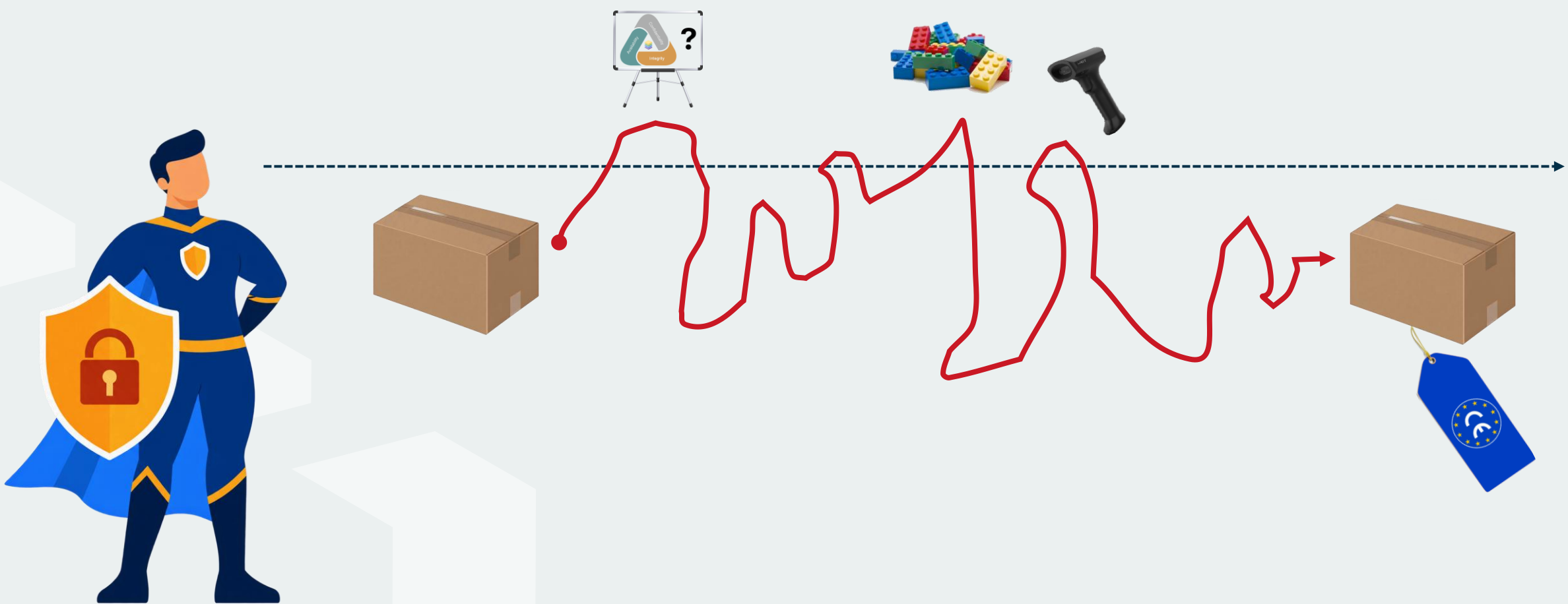


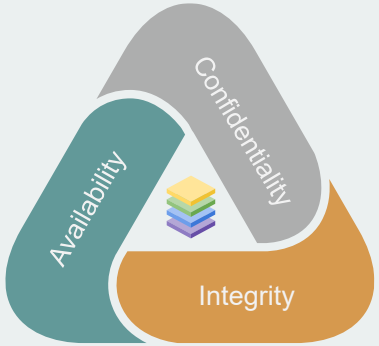
→ Establish and maintain a secure development lifecycle



?

Build the product with security built in





?

Build the product with security built in





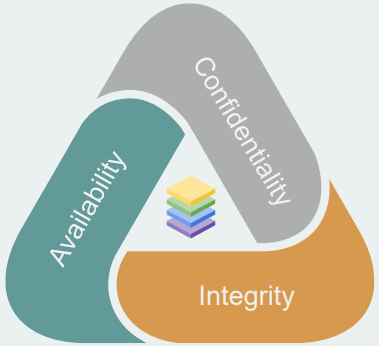


Market
→ Legislation and standards

Business
→ Policies

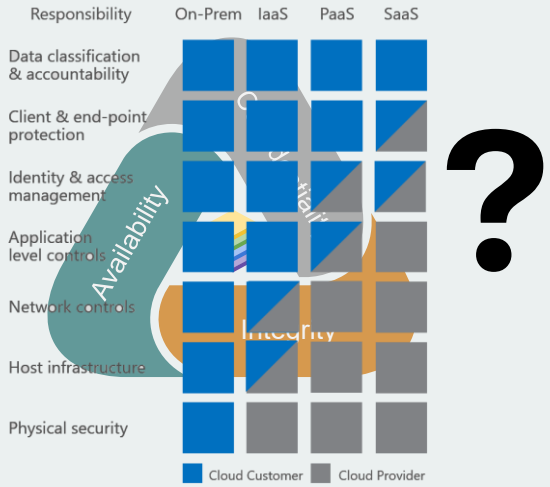
Product
→ Processes

Technical
→ Implementation



?

Communicate transparently on security



?

Communicate transparently on security

→ Establish a shared responsibility model



What is the product's expected security context?
What is the threat model taken into account?

How can the user securely manage the product?
What did the manufacturer do to support this?



OPERATION

⚠ WARNING:
Battery tools are always in operating condition. Therefore, switch should always be locked when not in use or carrying at your side.

KICKBACK

See Figures 6 - 9.

Kickback occurs when the blade stalls rapidly and the saw is driven back towards you. Blade stalling is caused by any action which pinches the blade in the wood.

⚠ DANGER:
Release switch immediately if blade binds or saw stalls. Kickback could cause you to lose control of the saw. Loss of control can lead to serious injury.

To guard against kickback, avoid dangerous practices such as the following.

- Setting blade depth incorrectly.
- Sawing into knots or nails in workpiece.
- Twisting the blade while making a cut.
- Making a cut with a dull, gummed up, or improperly set blade.
- Supporting the workpiece incorrectly.
- Forcing a cut.
- Cutting warped or wet lumber.
- Operating the tool incorrectly or misusing the tool.

To lessen the chance of kickback, follow these safety practices.

- Keep the blade at the correct depth setting. The depth setting should not exceed 1/4 in. below the material being cut.
- Inspect the workpiece for knots or nails before cutting. Never saw into a knot or nail.
- Make straight cuts. Always use a straight edge guide when rip cutting. This helps prevent twisting the blade.
- Use clean, sharp, and properly set blades. Never make cuts with dull blades.
- Support the workpiece properly before beginning a cut.
- Use steady, even pressure when making a cut. Never force a cut.
- Do not cut warped or wet lumber.
- Hold the saw firmly with both hands and keep your body in a balanced position so as to resist the forces if kickback should occur.

⚠ WARNING:
When using the saw, always stay alert and exercise control. Do not remove the saw from the workpiece while the blade is moving.

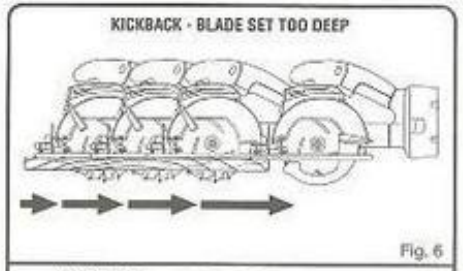
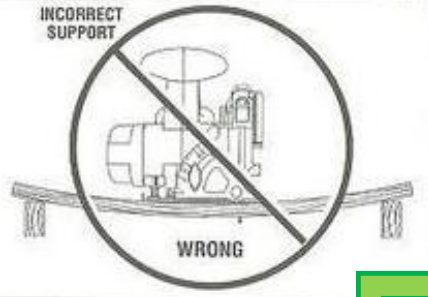


Fig. 6



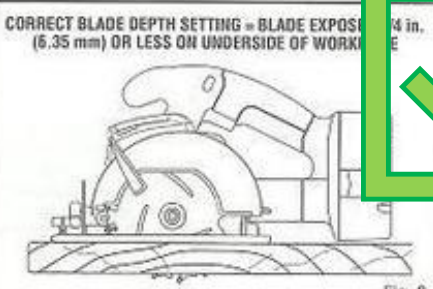


Fig. 8

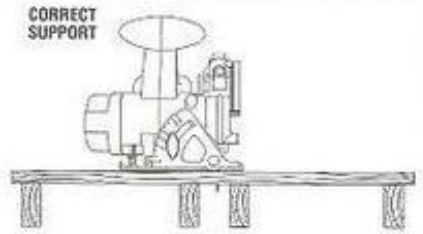
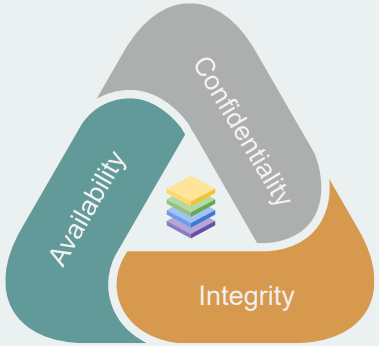


Fig. 9

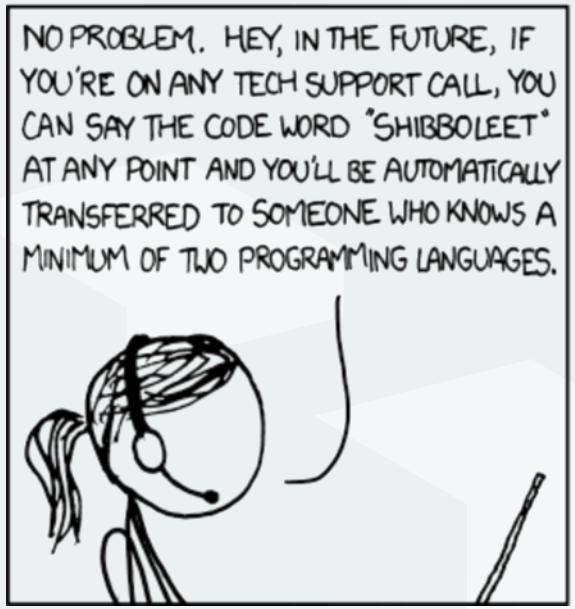


?

Communicate transparently on security

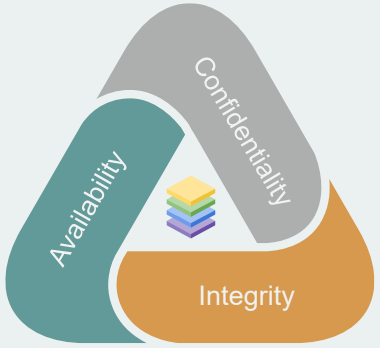
(bidirectional)

→ Provide multiple levels of communication



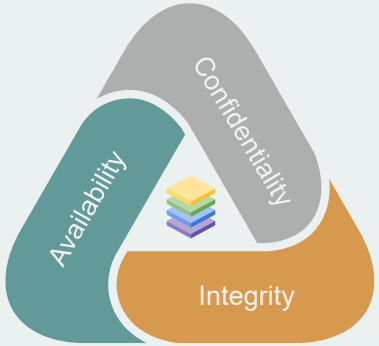
Vulnerability alerts
Root cause analysis for issues/incidents
Release Notes
Product Security Documentation
Security whitepaper
SBOM, VEX… and TEA!





?

Provide security updates, handle incidents and support it during its expected life



?

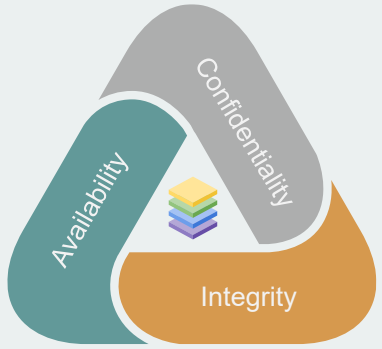
Provide security updates, handle incidents and support it during its expected life

→ Have a defined product lifecycle and support period



EOS (End Of Sale)
EOL (End Of Life)
EOSL (End of Service Life)





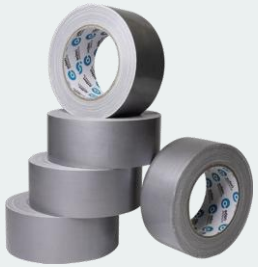
?

Provide security updates, handle incidents and support it during its expected life





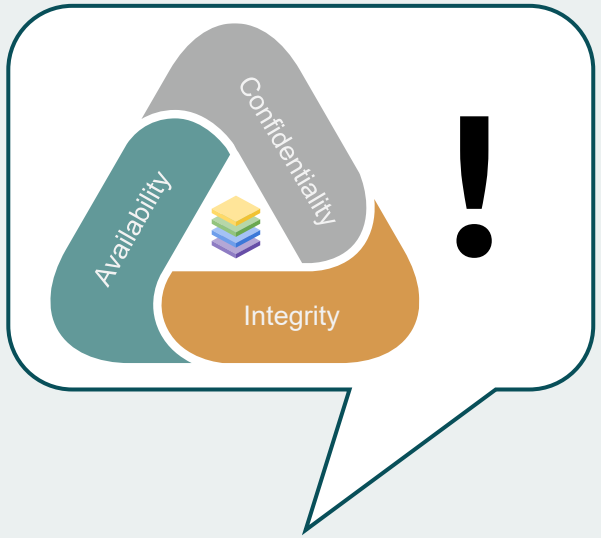


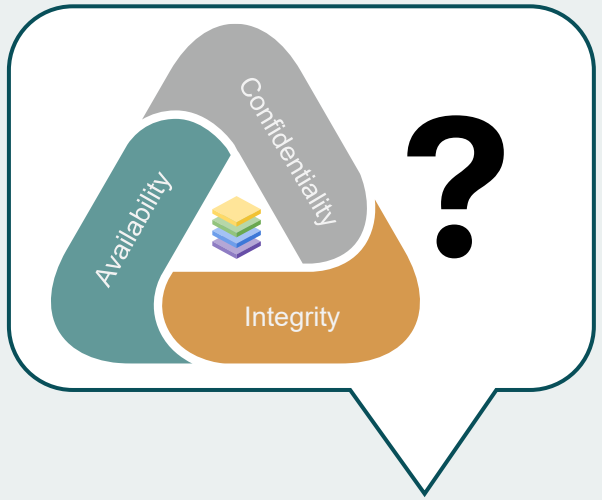




→ Prepare, receive, verify, remediate, distribute

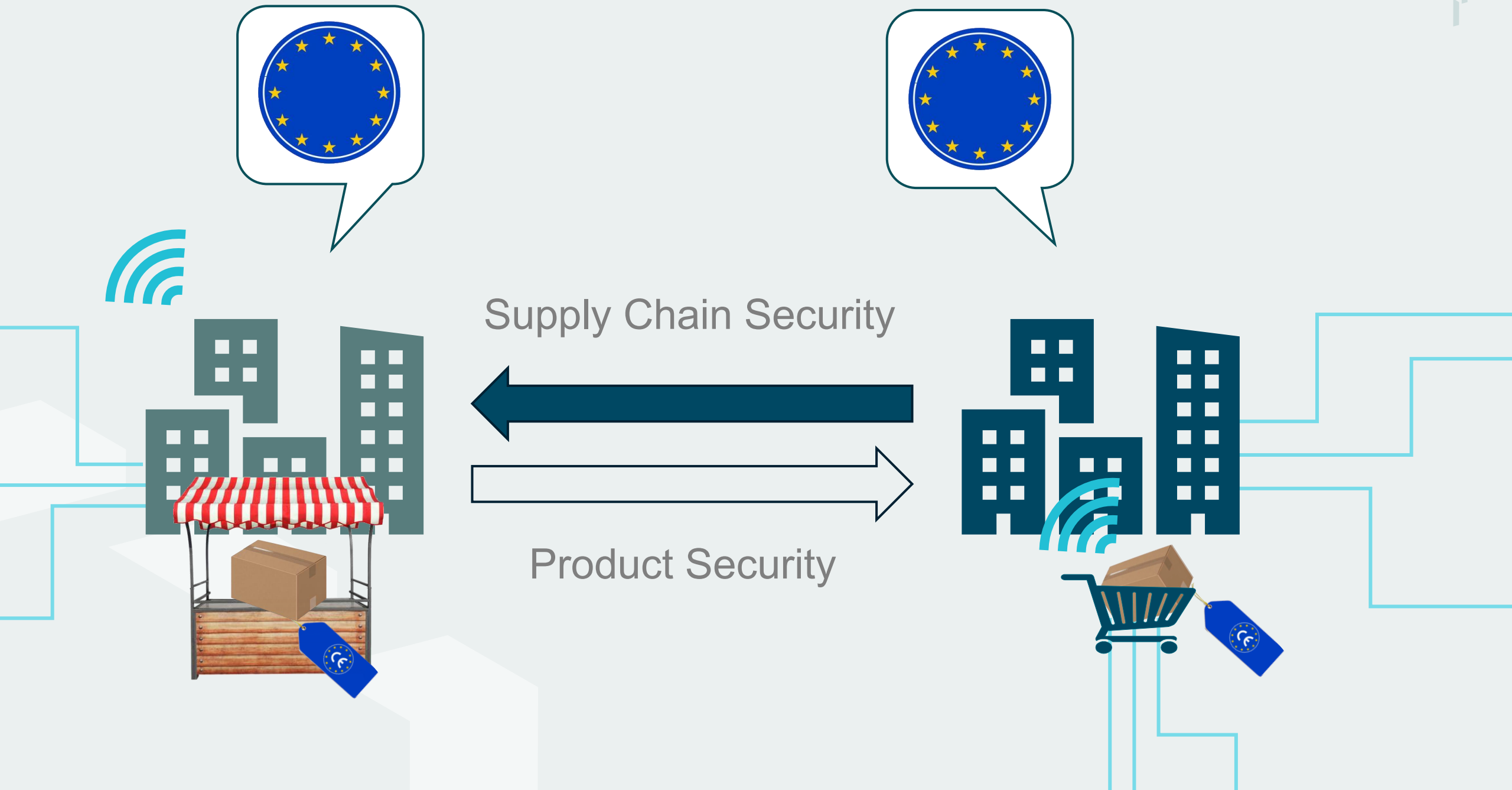






Supply Chain Security

Product Security


Supply Chain Security
Product Security

The domain of “product security” is coming of age

(at this very moment!)

Because we have built a common language around it,

start to agree on what the best practices are,

drive further formalization through legislation and standardization,

...and are make it (officially) someone’s job.

This slide deck was meant to be presented, not serve as a reference.

Catch the next run of this talk at ISACA Belgium on 03/12/26,
or have a look at my other presentations on the topic of CRA and product security

Scan	Talk	Link
	Product Security Comes of Age Live online - with ISACA Belgium	isaca.be/events/product-security-comes-of-age
	CRA Webinar 1 – Intro the CRA Toreon – Webinar Recording	youtube.com/watch?v=IdGOt1yqArA
	CRA Webinar 2 – Getting Started Toreon – Webinar Recording	youtube.com/watch?v=JNhJP_Z9leg
	CRA – Risk-based Selection of Security Requirements CRACY – Webinar Recording	youtube.com/watch?v=RpUU2eaNSlo

Contact

TOREON

Grotehondstraat 44 1/1
2018 Antwerpen
België

+32 3 369 33 96

Courbevoie 13
1348 Ottignies-Louvain-la-Neuve
Belgique

+32 1 079 00 10

www.toreon.com

toreon

info@toreon.com

toreon_BE