Living risk-based security at SAP, the solved challenges and the open ones

Dr. Paul El Khoury – CISSP
Co-Owner of SAP Product Standard Security, SAP SE

September 2015

Security Assessment for Systems, Services, and Infrastructures (SASSI 2015)

SAP – Helping the world run better!

For More than 40 Years, SAP Has Helped the World Run Better and Improve People's Lives

For the world

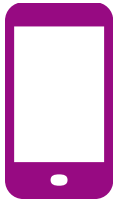
74%

of the world's transaction revenue touches an SAP system

For business

98%

SAP customers represent 98% of the top 100 most valued brands in the world



For you

97%

Mobile solutions from SAP reach 97% of the world's mobile subscribers via text messaging

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Who am I?

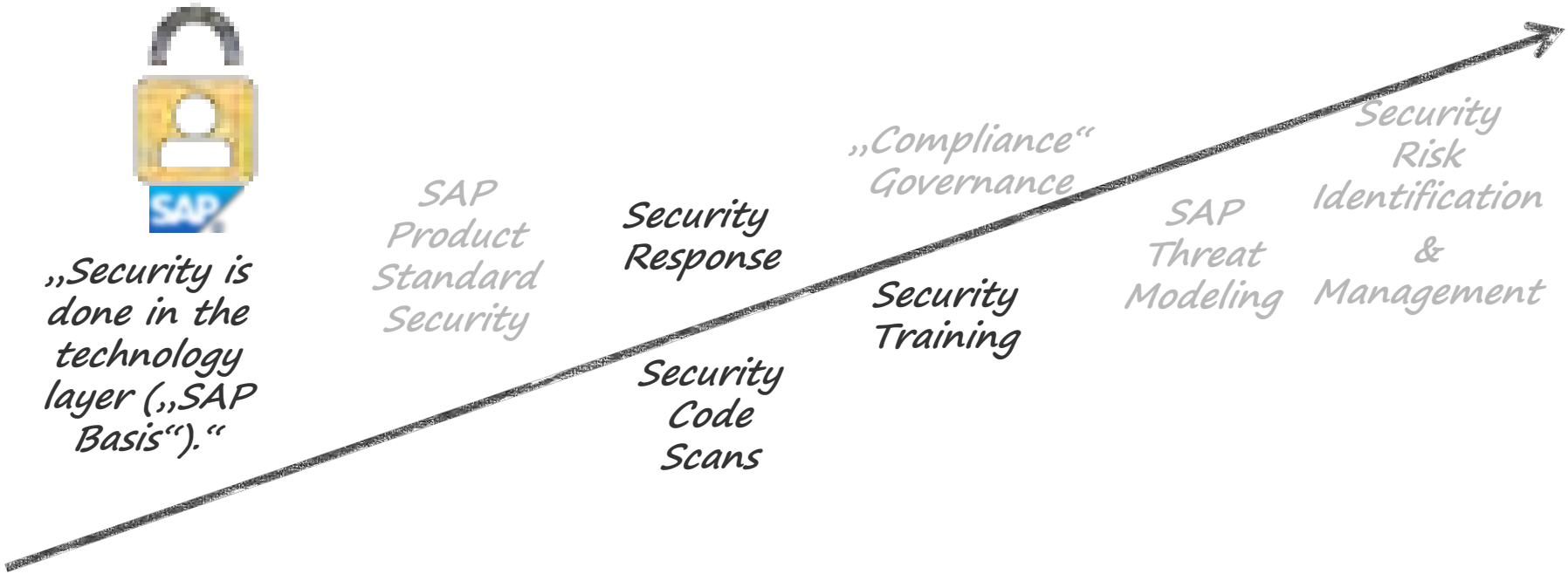
- ✓ **Joined SAP in 2006**
- ✓ **Holds a Ph.D. in Computer Science from the Université of Claude Bernard Lyon 1**

- ✓ **Is currently co-owner of the SAP Product Standard Security**
- ✓ **Leads the Product Security Risk Identification and Management**

- ✓ ***Earlier:***
  - ✓ Lead SAP Threat Modeling methodology,
  - ✓ Co-defined the secure storage on device used by all SAP mobile applications
  - ✓ Have held the position of governor of the SAP patch day

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

We have come a long way …



Awareness … Needs … Tools … Skills … Accountability …

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

We have come a long way …

Awareness … Needs … Tools … Skills … Accountability …

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP Product Innovation Lifecycle an over-simplified view

The past

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP Product Innovation Lifecycle an over-simplified view

The past

- Central Product Security Team (CPST) **defines** the **Product Standard Security** serving as baseline

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP Product Innovation Lifecycle an over-simplified view

The past

- Central Product Security Team (CPST) **defines** the **Product Standard Security** serving as baseline
- Development Teams **Plan** their compliance to the **Product Standard Security** and store the compliance in **Product Standard Compliance** tool

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP Product Innovation Lifecycle an over-simplified view

The past

- Central Product Security Team (CPST) **defines** the **Product Standard Security** serving as baseline
- Development Teams **Plan** their compliance to the **Product Standard Security** and store the compliance in **Product Standard Compliance** tool

*For every deviation a description of the **risk** taken and action item with a name and a date… are added to the tool supporting the PIL*

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP Product Innovation Lifecycle an over-simplified view

The past

- Central Product Security Team (CPST) **defines** the **Product Standard Security** serving as baseline
- Development Teams **Plan** their compliance to the **Product Standard Security** and store the compliance in **Product Standard Compliance** tool
- Development Teams **executes** on the plan

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP Product Innovation Lifecycle an over-simplified view

The past

- Central Product Security Team (CPST) **defines** the **Product Standard Security** serving as baseline
- Development Teams **Plan** their compliance to the **Product Standard Security** and store the compliance in **Product Standard Compliance** tool
- Development Teams **executes** on the plan
- Development Teams may have **implemented** or **deviated** from their agreed plan

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP Product Innovation Lifecycle an over-simplified view

The past

- Central Product Security Team (CPST) **defines** the **Product Standard Security** serving as baseline
- Development Teams **Plan** their compliance to the **Product Standard Security** and store the compliance in **Product Standard Compliance** tool
- Development Teams **executes** on the plan
- Development Teams may have **implemented** or **deviated** from their agreed plan

*For every deviation a description of the **risk** taken and action item with a name and a date… are added to the tool supporting the PIL*

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP Product Innovation Lifecycle an over-simplified view

The past

- Central Product Security Team (CPST) **defines** the **Product Standard Security** serving as baseline
- Development Teams **Plan** their compliance to the **Product Standard Security** and store the compliance in **Product Standard Compliance** tool
- Development Teams **executes** on the plan
- Development Teams may have **implemented** or **deviated** from their agreed plan
- If CPST during security validation **finds no violation of agreed security level** then shipment is authorized

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

“Winter is coming!...” (John Snow - Games of Thrones)

- **SAP’s strategy embarked with speed into Mobile application development**
- **SAP acquired several mid-to-large size companies with divers software portfolio**
- **SAP’s strategy promoted SAP HANA to partners and strengthen partnership offerings**
- **SAP’s strategy embarked with speed into Cloud and recently into Internet of Things offering**

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Wind of change…

- **#1: Ownership of the (security) risk moves with the Product Owners / Service Owners, i.e. CPST main objective is primarily “advising” rather than primarily “governing”**

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Wind of change…

- **#1: Ownership of the (security) risk moves with the Product Owners / Service Owners, i.e. CPST main objective is primarily “advising” rather than primarily “governing”**
- **#2: Refine the way security risks are identified and managed**

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Very important 3rd fact that we considered!

Developers are creators not builders!

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Wind of change…

- #1: Ownership of the (security) risk moves with the Product Owners / Service Owners, i.e. CPST main objective is primarily “advising” rather than primarily “governing”
- #2: Refine the way security risks are identified and managed
- **#3: Invest in the people: Need to strengthen security experts, up skill and enable all the development teams**
  - Creating a collaboration environment and a network of security experts
  - Creating a reliable channel for disseminating security information
  - Allowing easier access to the huge security knowledge base
  - Identifying security risks, understanding the underlying impact and managing them appropriately
  - Teach methods for building misuse cases and thinking like hackers
  - Teach how to build security test plans
  - …

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

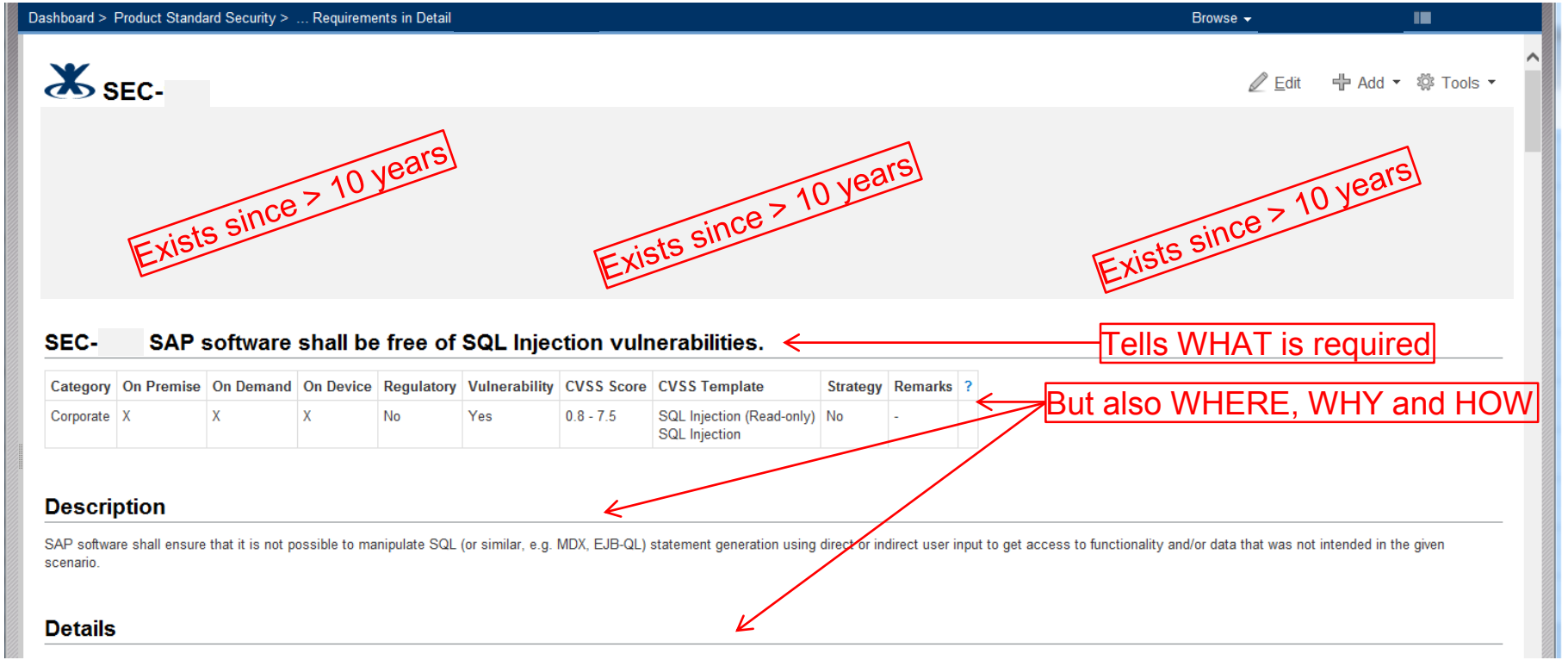
Very important 4th fact - external to SAP!

Declare compliance to ISO 27034

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The common denominator: SAP Product Standard Security

A Requirement Example



© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP Product Standard Security

Could no longer serve as a standalone planning means

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Feedback / Design thinking statements

From Developers, Architects and Security Experts

- Uncover the security threats and create transparency to decision makers
- Improve targeted security test cases / Improve true-positives in Code Scanning
- Up skill the development team and fits to our development

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP Threat Modeling and Security Risk Identification & Management

SAP Threat Modeling

- is a systematic approach to uncover security threats at design time to reach a secure design
- outcome is targeted for architects, developers and security experts

Security Risk Identification & Management

- is a method based on SAP Threat Modeling
- outcome is targeted for decision makers, lead architects and security experts

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Analyzing Risks: Security Risk Identification & Management + SAP Threat Modeling
Comparison

Security Risk Identification & Management

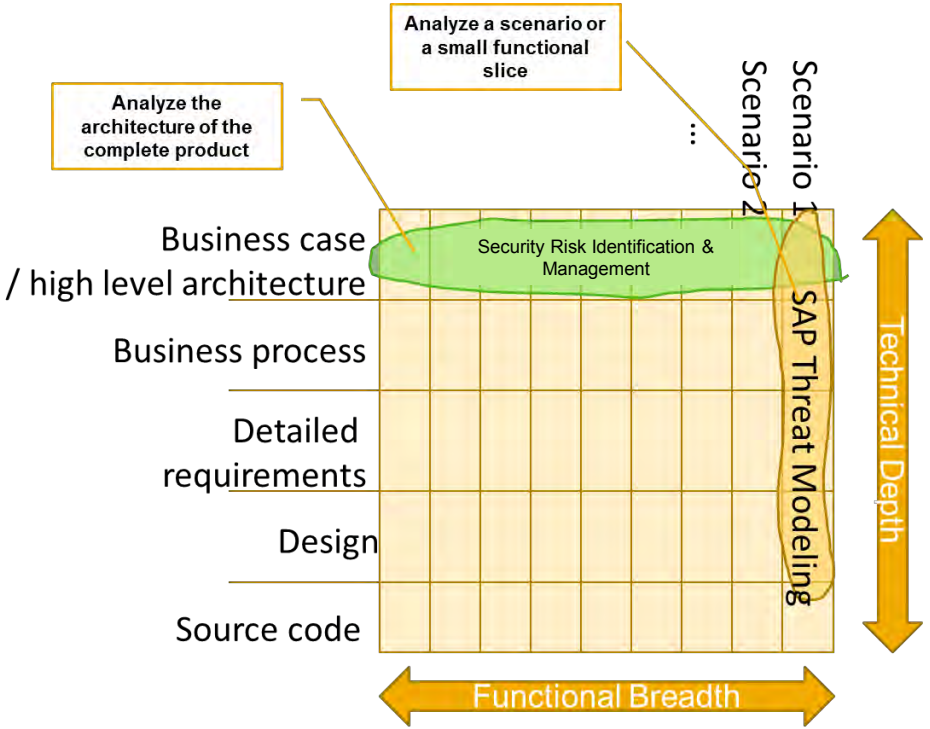
- Focus on complete product / service
- Analyze according to 10 security themes
- Document risk and risk response

=> High-level approach

SAP Threat Modeling

- Focus on critical scenarios
- Analyze these scenarios in detail
- Document threats, their risk, proposed mitigations and test cases

=> Very detailed, no coverage for huge applications



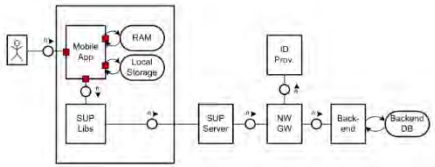
© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The common methodology

- Self-contained
- Timeboxed
- As simple as possible
- Clear workshop structure
- Clear outcome and documentation
- Decision and Follow-Up
- Mitigations by the Program

1

Understand the Architecture



Asset and Software centric view

2

Analyze potential Threats

Add an Attacker centric view

3

Put Threats on the Backlog & reprioritize

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

The seven steps of Security Risk Identification & Management

Risk Identifcation

1. Get common understanding about the architecture
2. Define the assets to be protected
3. Identify all risks in context of the product

Risk Analysis

4. Describe the risk incl.impact and mitigation alternatives
5. Rate the risks
6. Write documentation and present the risks to PO
7. Decide on the risks and document decisions

Workshop settings

Mandatory:
Program Lead Architect
Security Expert

Optional:
Lead Developer(s)
Product Owner (PO)

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Standardizing the Methods Across SAP

For SAP Threat Modeling

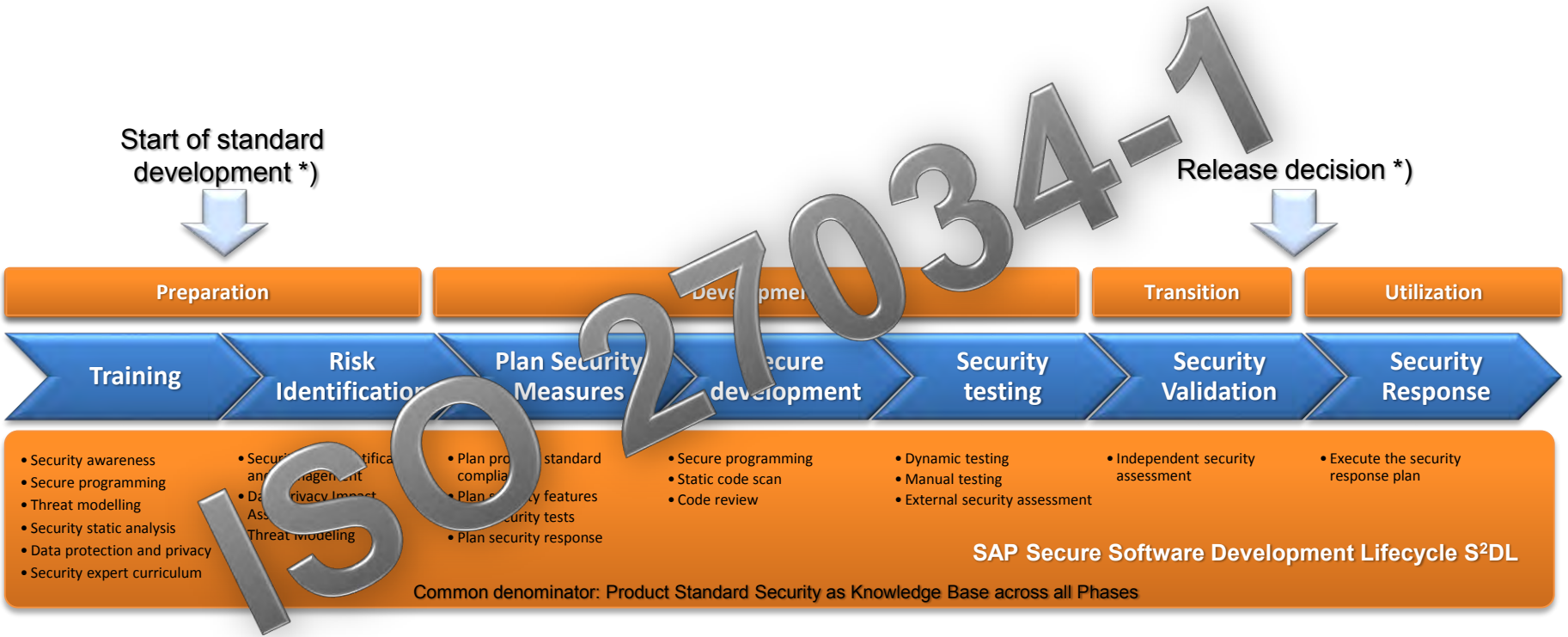
- 3 days class room training (200+ experts trained)
- Experts support projects across their development line
- Results and Decisions are reusable / understandable

For Security Risk Identification & Management

- Blended Learning with a prerequisite to have a certified Threat Modeling expert as a Security Risk Identification & Management lead

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

SAP Secure Software Development Lifecycle S²DL



*) In accordance to new I2M decision points

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Open challenges

- ✓ Cloud Solutions
  - ✓ Development and the hosting of software are tightly integrated
  - ✓ Even shorter development and release time-frames
- ✓ Security Monitoring plan with SAP Enterprise Threat Detection
  - ✓ Creating “monitoring plan” from SAP Threat Modeling reports
- ✓ Internet of Things
  - ✓ Security Threats are standard, but the capabilities and solutions have a high dependency on devices and scenarios!

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

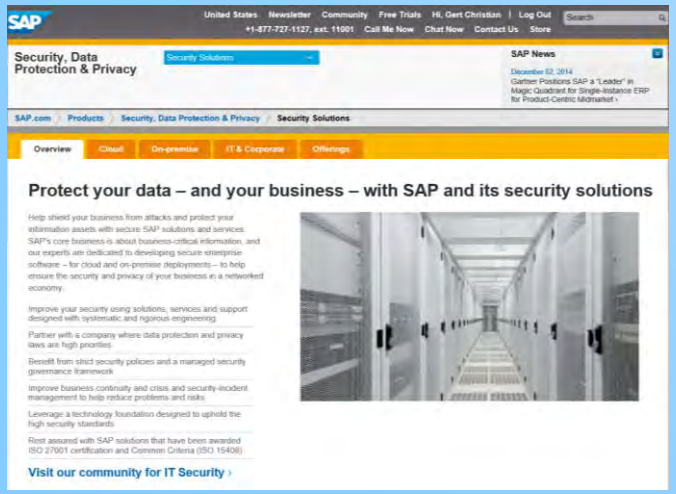
Summary

- ✓ The current SAP **S²DL** is a Risk-Based Security process
  - ✓ It helps SAP to scale with secure development to the various use cases
  - ✓ Reaching Risk-Based Security at SAP required a specific organizational infrastructure
- ✓ Security Risk Identification & Management and SAP Threat Modeling are the heart of Risk-Based Security process
  - ✓ Same methodology to identify security risks by different target user groups
  - ✓ Threat Modeling on the architecture for critical use cases
  - ✓ Security Risk Identification & Management for a complete product or solution
- ✓ Suitable risk description and rating focusing on affected assets and potential cost

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Where to Find More Information

www.sap.com/security



- Cloud
- On premise
- IT & Corporate
- Offerings

www.sap.com/security

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

Thank you!

Dr. Paul El Khoury, CISSP
Co-Owner of SAP Product Standard Security, SAP SE

paul.el.khoury@sap.com

© 2015 SAP SE or an SAP affiliate company. All rights reserved.