RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

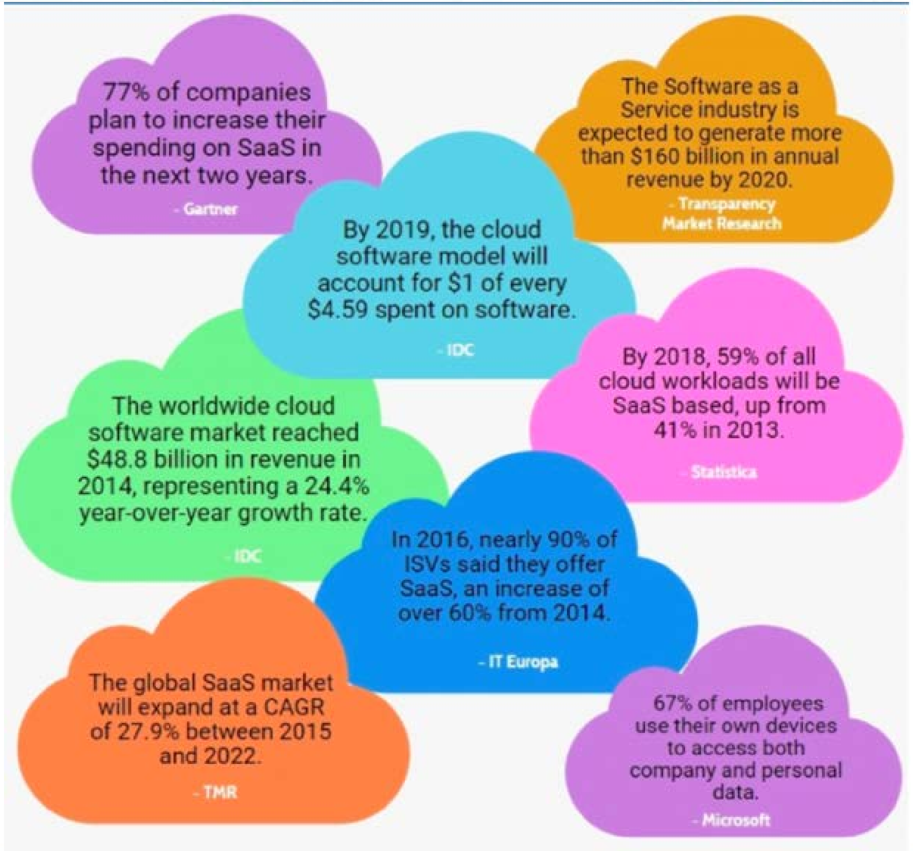
SESSION ID: CSV-F02

application security - this is the future that saas companies want

Caroline Wong, CISSP

Vice President of Security Strategy at Cobalt.io

SaaS is taking over the world



77% of companies plan to increase their spending on SaaS in the next two years.

- Gartner

The Software as a Service industry is expected to generate more than $160 billion in annual revenue by 2020.

- Transparency Market Research

By 2019, the cloud software model will account for $1 of every $4.59 spent on software.

- IDC

By 2018, 59% of all cloud workloads will be SaaS based, up from 41% in 2013.

- Statistica

The worldwide cloud software market reached $48.8 billion in revenue in 2014, representing a 24.4% year-over-year growth rate.

- IDC

In 2016, nearly 90% of ISVs said they offer SaaS, an increase of over 60% from 2014.

- IT Europa

The global SaaS market will expand at a CAGR of 27.9% between 2015 and 2022.

- TMR

67% of employees use their own devices to access both company and personal data.

- Microsoft

https://www.internetsearchinc.com/top-10-saas-technology-trends-for-2017/

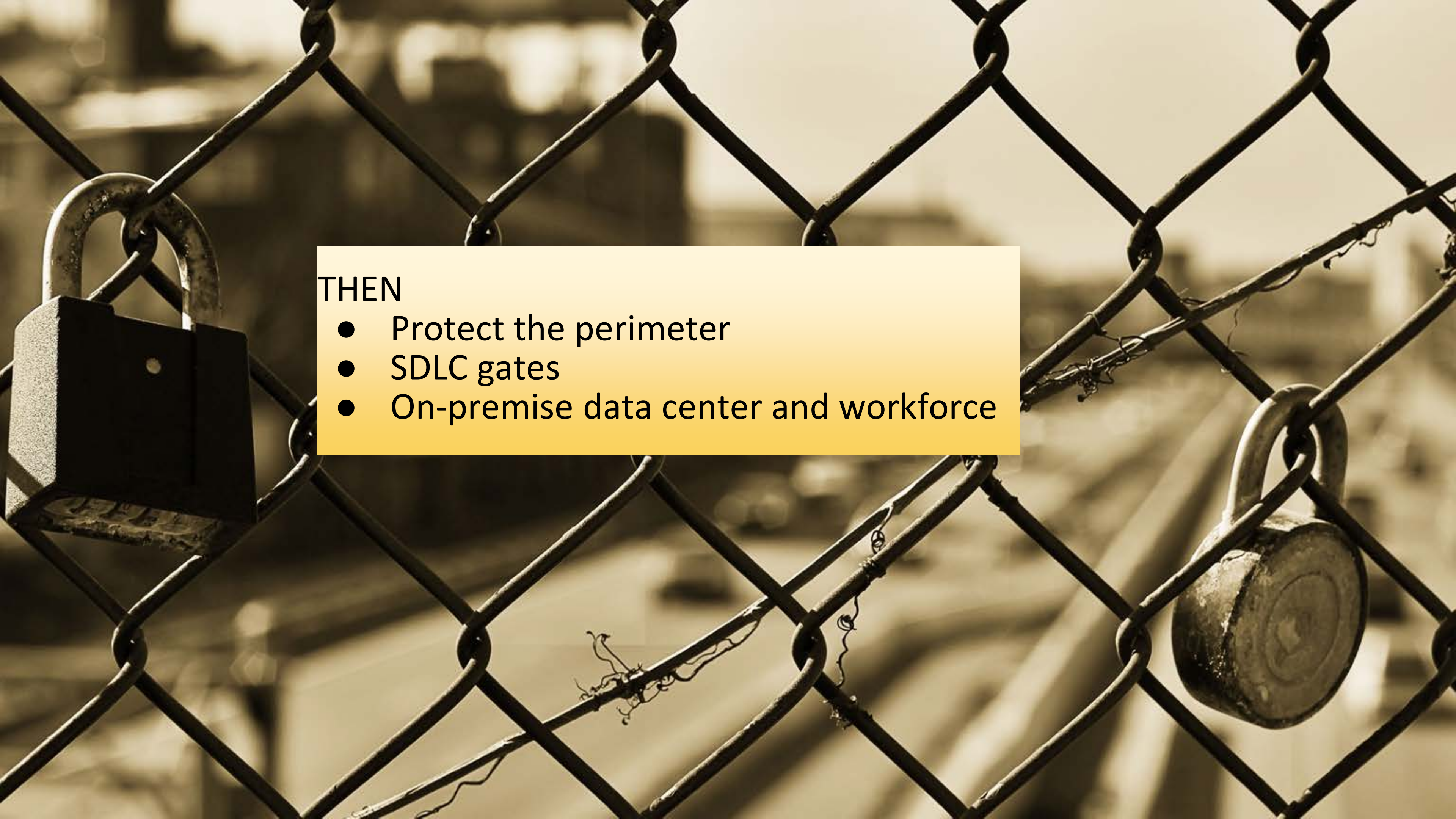
SaaS is taking over the world

It doesn’t happen often, every 10 to 15 years or so, but we are in the throes of the reordering of the $4 trillion corporate IT market.

And depending on which side of that transformation you sit, this is either the best time to be an enterprise technology company, or reason to start looking for a new line of work.

- Peter Levine, The SaaS Manifesto

How is the role of security changing?



THEN

- Protect the perimeter
- SDLC gates
- On-premise data center and workforce

NOW

- Vendor risk (goes both ways)
- Applications and APIs
- Mobile workforce and endpoints

Do you trust me?

BSIMM8 Structure

The BSIMM is organized as a set of 113 activities in a framework.

The Software Security Framework

The graphic below shows the software security framework (SSF) used to organize the 113 BSIMM activities. There are 12 practices organized into four domains.

The four domains are as follows:

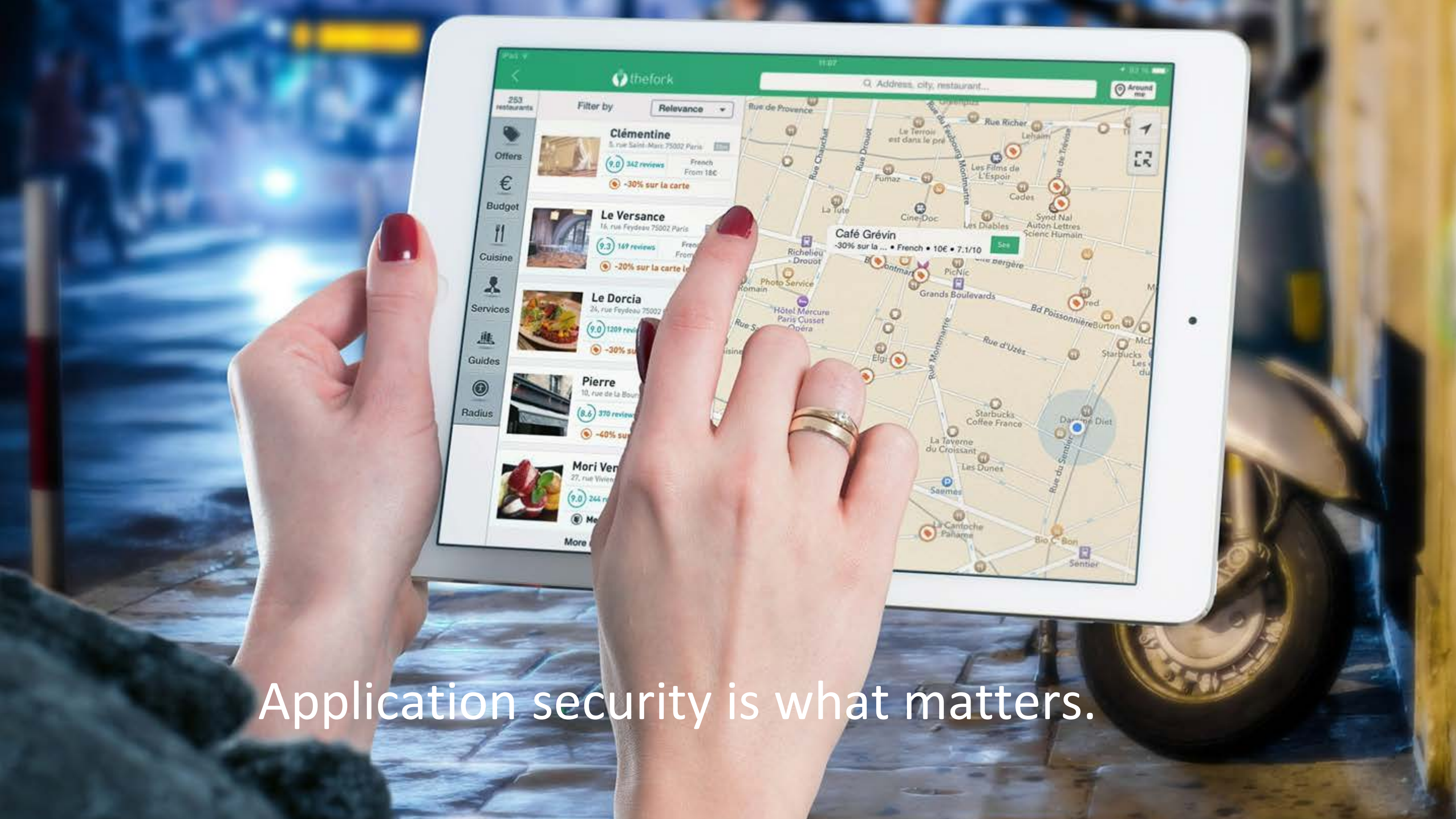
Governance: Practices that help organize, manage, and measure a software security initiative. Staff development is also a central governance practice.

Intelligence: Practices that result in collections of corporate knowledge used in carrying out software security activities throughout the organization. Collections include both proactive security guidance and organizational threat modeling.

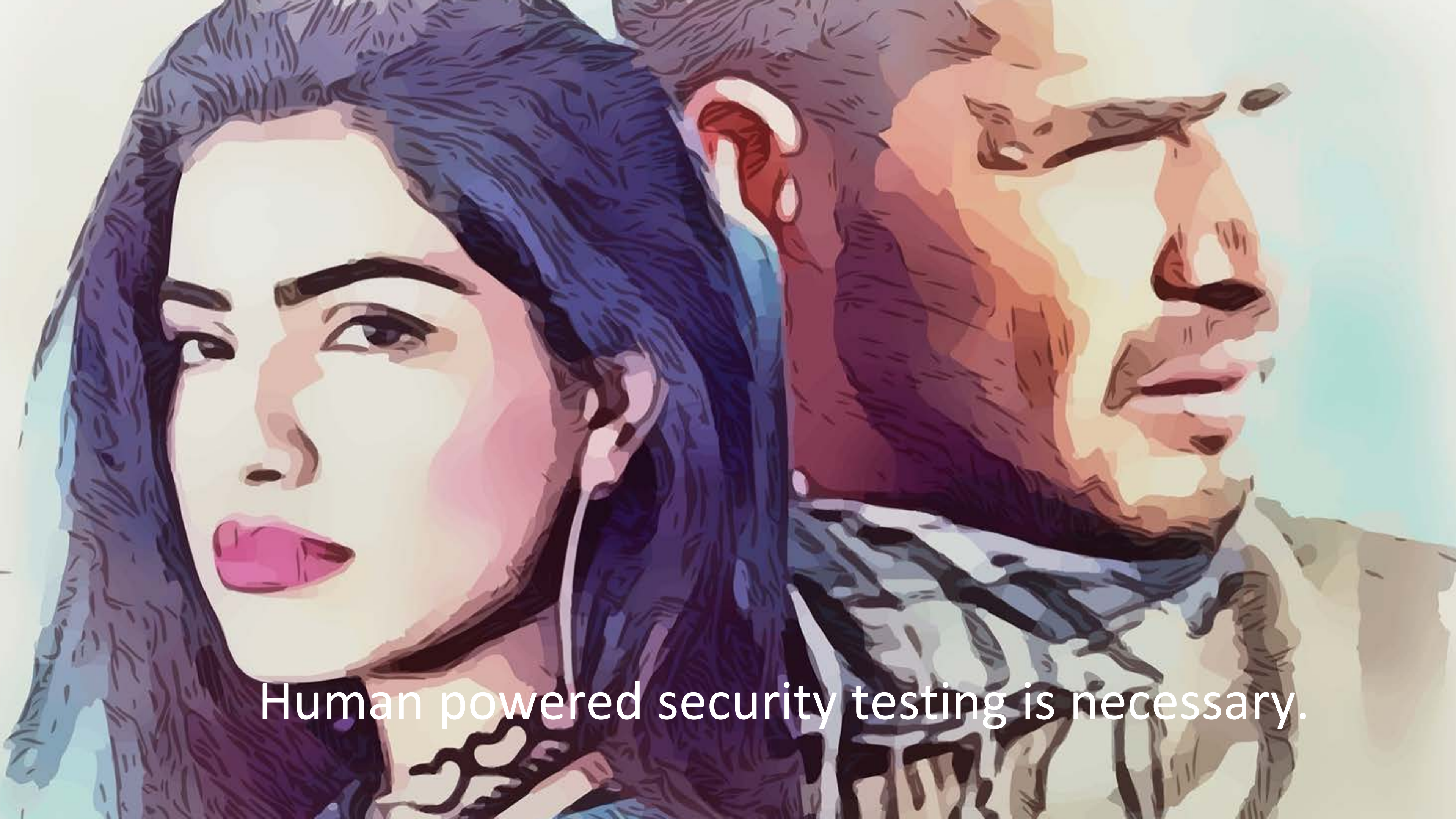
SSDL Touchpoints: Practices associated with analysis and assurance of particular software development artifacts and processes. All software security methodologies include these practices.

Deployment: Practices that interface with traditional network security and software maintenance organizations. Software configuration, maintenance, and other environment issues have direct impact on software security.

Secure software is business critical.



Application security is what matters.



Human powered security testing is necessary.

On demand specialization wins.

Agile companies need agile security solutions.

Apply what you have learned today

- Next week:
  - Find out what your SaaS company does about vendor security questionnaires
- In the next 3 months:
  - If you haven't ever pen tested your application(s), start planning one
  - Identify critical gaps in your security program (application security, manual security testing, etc.)
- In the next 6 months:
  - Execute a plan to address the gaps in your security program