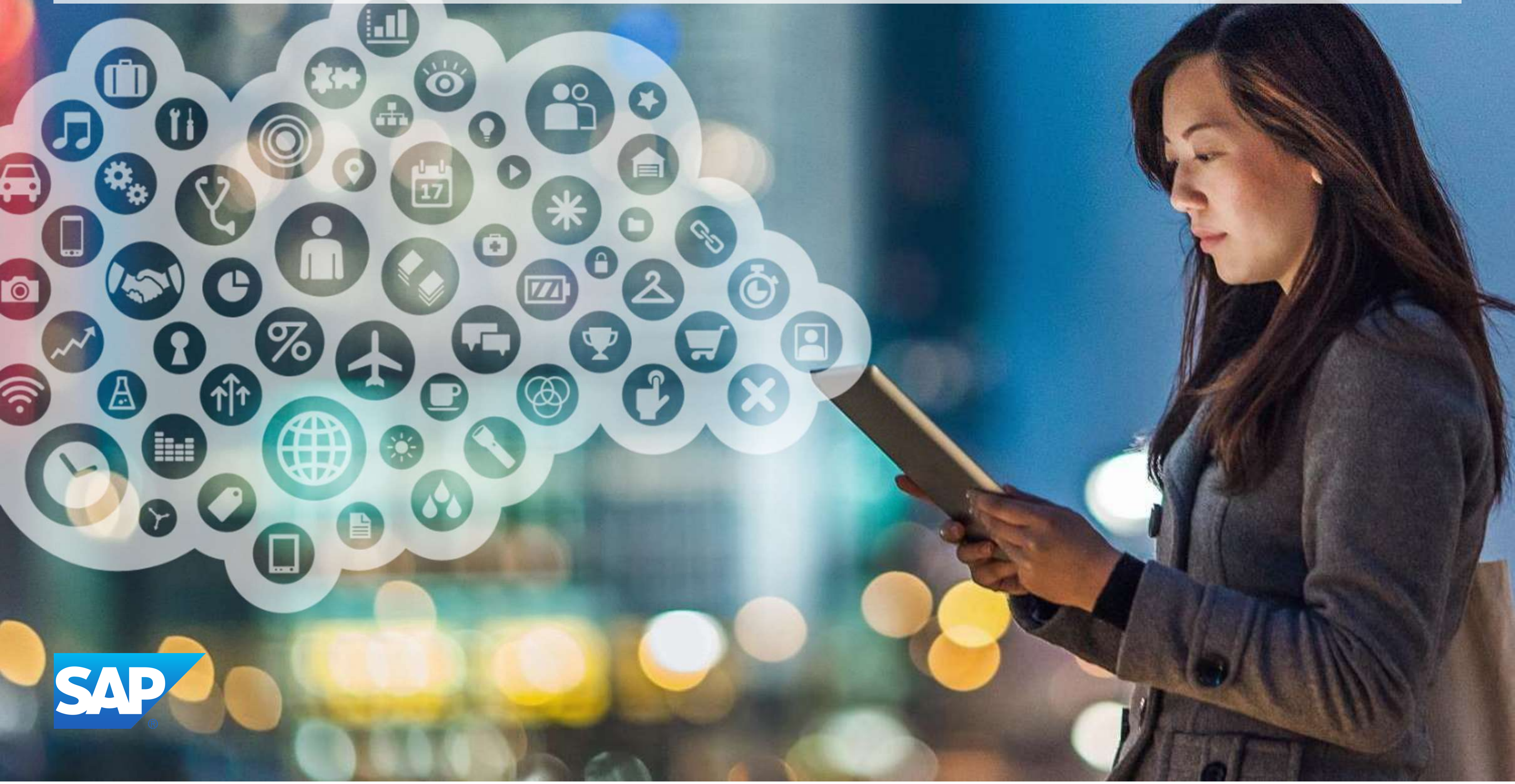
Public

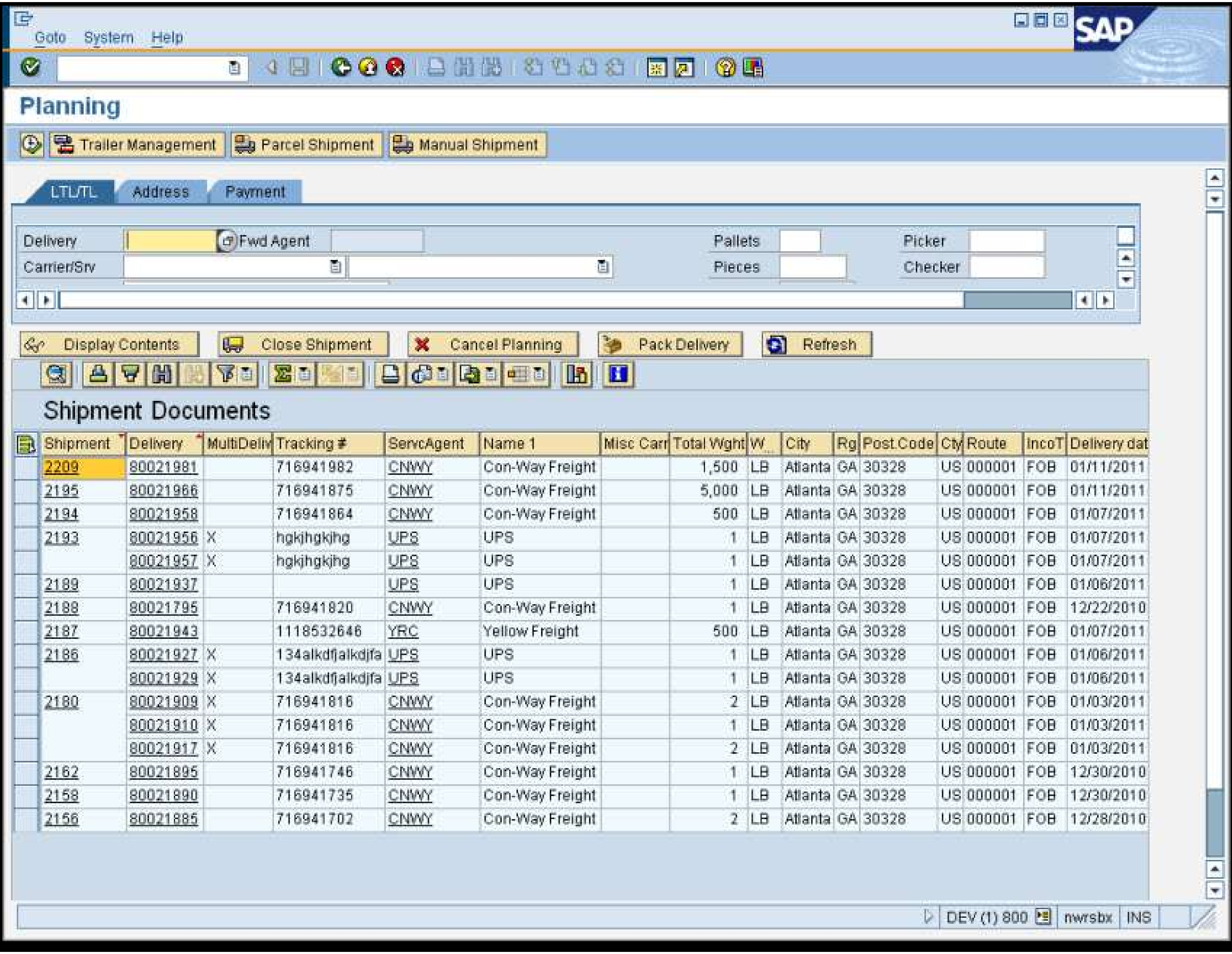
Evolving role of PSIRT in the Cloud

Vic Chung, SAP
March 2, 2017



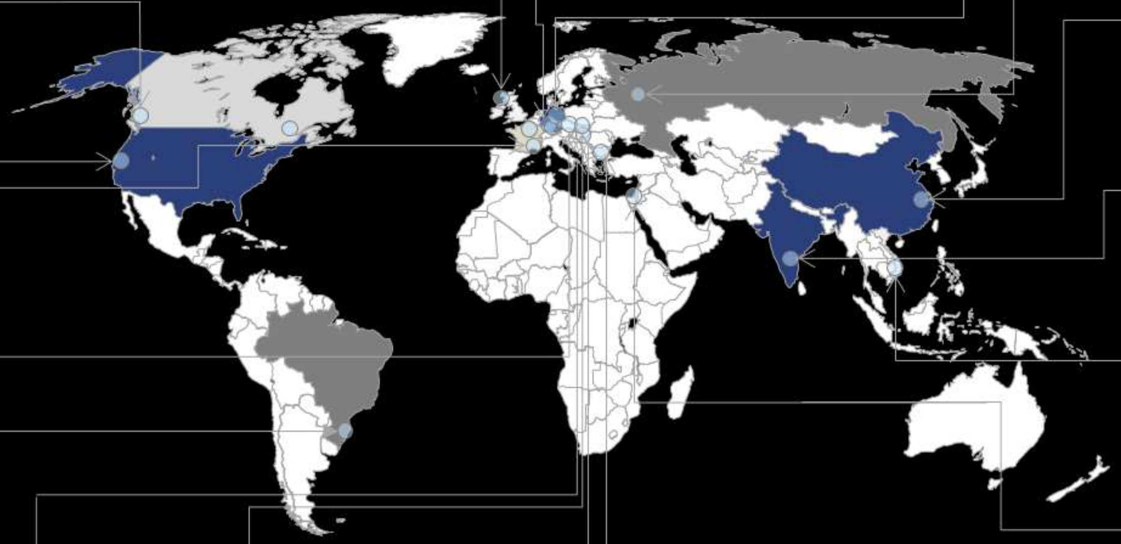
TRUMP
INTERNATIONAL HOTEL & TOWER
VANCOUVER
RESPECT, DIGNITY, ACCEPTANCE

SAP



Shipment Documents

Shipment	Delivery	MultiDeliv	Tracking #	ServcAgent	Name 1	Misc Carr	Total Wght	W	City	Rg	Post.Code	Cty	Route	IncoT	Delivery dat
2209	80021981		716941982	CNWY	Con-Way Freight		1,500	LB	Atlanta	GA	30328	US	000001	FOB	01/11/2011
2195	80021966		716941875	CNWY	Con-Way Freight		5,000	LB	Atlanta	GA	30328	US	000001	FOB	01/11/2011
2194	80021958		716941864	CNWY	Con-Way Freight		500	LB	Atlanta	GA	30328	US	000001	FOB	01/07/2011
2193	80021956	X	hgkjhgkjhg	UPS	UPS		1	LB	Atlanta	GA	30328	US	000001	FOB	01/07/2011
	80021957	X	hgkjhgkjhg	UPS	UPS		1	LB	Atlanta	GA	30328	US	000001	FOB	01/07/2011
2189	80021937			UPS	UPS		1	LB	Atlanta	GA	30328	US	000001	FOB	01/06/2011
2188	80021795		716941820	CNWY	Con-Way Freight		1	LB	Atlanta	GA	30328	US	000001	FOB	12/22/2010
2187	80021943		1118532646	YRC	Yellow Freight		500	LB	Atlanta	GA	30328	US	000001	FOB	01/07/2011
2186	80021927	X	134alkdfjalkdjfa	UPS	UPS		1	LB	Atlanta	GA	30328	US	000001	FOB	01/06/2011
	80021929	X	134alkdfjalkdjfa	UPS	UPS		1	LB	Atlanta	GA	30328	US	000001	FOB	01/06/2011
2180	80021909	X	716941816	CNWY	Con-Way Freight		2	LB	Atlanta	GA	30328	US	000001	FOB	01/03/2011
	80021910	X	716941816	CNWY	Con-Way Freight		1	LB	Atlanta	GA	30328	US	000001	FOB	01/03/2011
	80021917	X	716941816	CNWY	Con-Way Freight		2	LB	Atlanta	GA	30328	US	000001	FOB	01/03/2011
2162	80021895		716941746	CNWY	Con-Way Freight		1	LB	Atlanta	GA	30328	US	000001	FOB	12/30/2010
2158	80021890		716941735	CNWY	Con-Way Freight		1	LB	Atlanta	GA	30328	US	000001	FOB	12/30/2010
2156	80021885		716941702	CNWY	Con-Way Freight		2	LB	Atlanta	GA	30328	US	000001	FOB	12/28/2010



Labs Canada
Main Locations:
Vancouver/Montreal
(2010)

2

Labs Ireland
Main Location:
Dublin
(2008)

Labs DE "Walldorf"
Main Locations:
Walldorf/Rot
(1972)

5

Labs in Germany
Main Locations:
Markdorf (2010)/
Berlin (2016)

Labs CIS
Main Location:
Moscow
(2012)

Labs US
Main Location:
„Silicon Valley"
(1993)

Labs China
Main Location:
Shanghai
(2003)

Labs in France
Main Locations:
Sophia-Antipolis (1996) /
Paris (2009)

Labs India
Main Location:
Bangalore
(1998)

16

Labs Czech Republic
One Location:
Brno
(2016)

Labs Vietnam
One Location:
Ho-Chi-Minh-City
(2015)

Labs Latin America
One Location:
Sao Leopoldo
(2008)

Labs Israel
Main Location:
Ra'anana
(1998)

Labs Poland
One Location:
Gliwice
(2016)

Labs Slovakia
One Location:
Bratislava
(2016)

Labs Hungary
One Location:
Budapest
(2005)

Labs Bulgaria
One Location:
Sofia
(2000)

Purpose and Agenda

Purpose

- Share observations and host a dialog on the impact of cloud to PSIRT
- Focus on **operations**, not concept…the actual workings of handling vulnerabilities in real organizations
- Consider the future role of PSIRT in the Cloud (and perhaps extend to IoT?)

Proposed Agenda

- 30 minutes of presentation and sharing observations
- 15 minutes of panel discussion, share observation (solution?) where appropriate

References (just to put some structure to the discussion…without bias)

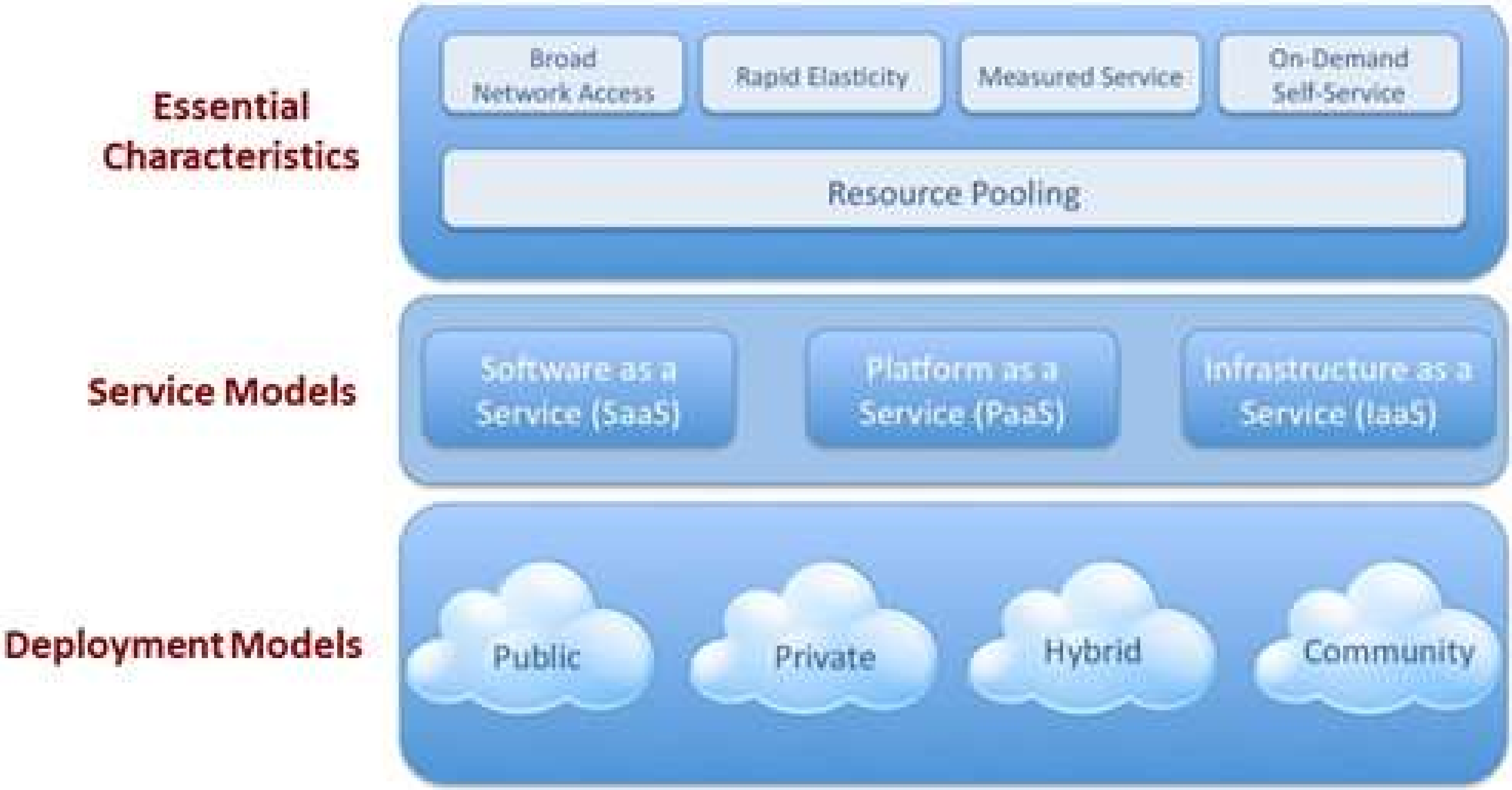
- Cloud Security Alliance
  - Security Guidance for Critical Areas of Focus in Cloud Computing v3.0
  - NIST definition of cloud (secondary reference)
  - ISO 270XX (secondary reference)

Expected outcome

So…the cloud

I know you know all about it, but just to make sure everyone is on the same page

- *The NIST definition of Cloud Computing*



Essential Characteristics

Broad Network Access

Rapid Elasticity

Measured Service

On-Demand Self-Service

Resource Pooling

Service Models

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

Deployment Models

Public

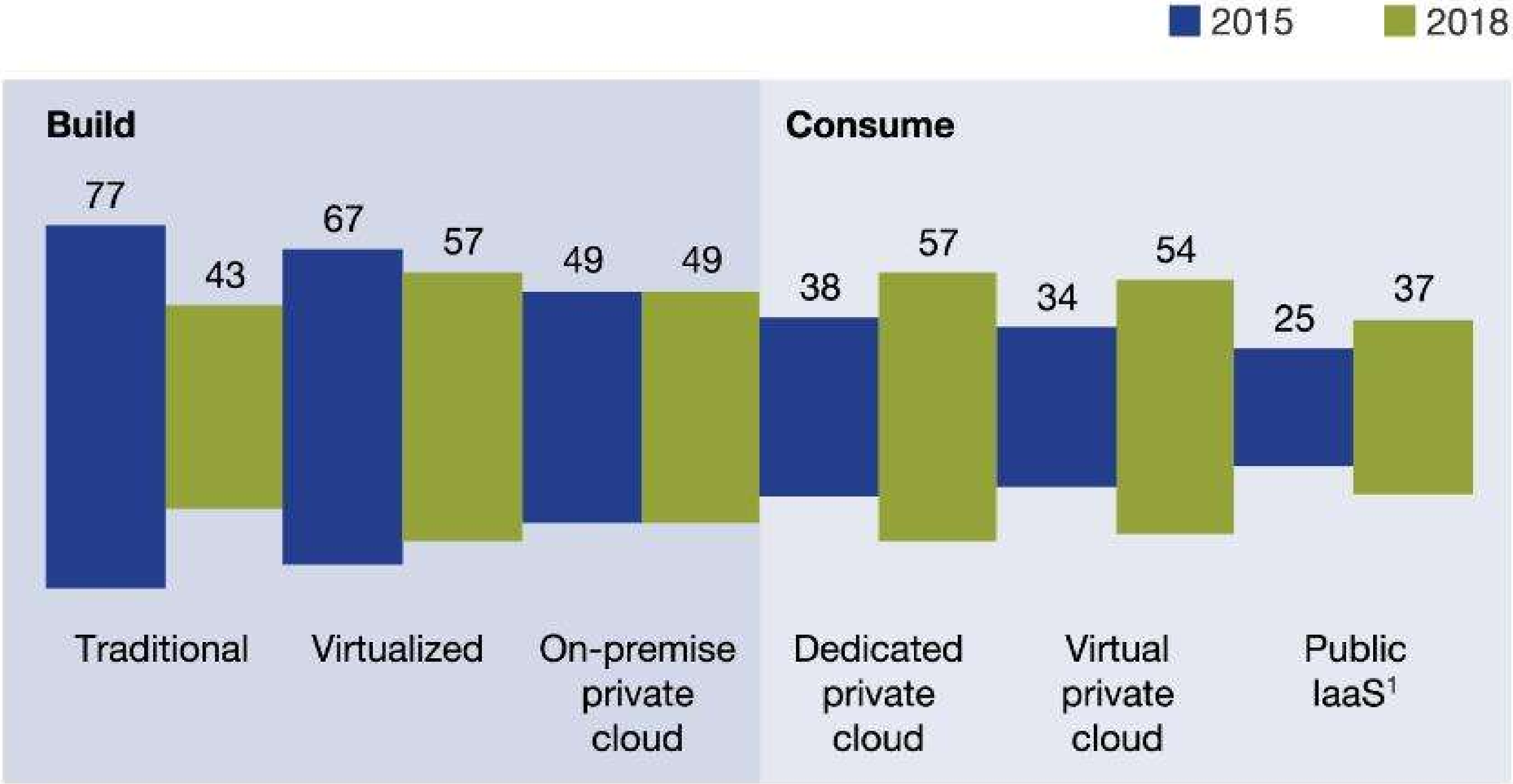
Private

Hybrid

Community

A fundamental shift is under way from a 'build' to 'consume' model for IT workloads.

% of companies planning to have following environments as primary environment for at least 1 workload type in 2015 and 2018



[1] Infrastructure as a service.

McKinsey&Company | Source: McKinsey IT-as-a-Service (ITaaS) Cloud Survey

The ‘cloud’

1. ‘Orchestrated’, ‘provisioned’, ‘implemented’, ‘decommissioned’, ‘scaled up and down’ – an on demand utility-like model of allocation and consumption
2. The ‘perimeter’
3. Supplier/Contractor problem – SLA, agreement-based

A cloud product position depends on its go-to-market strategy:

1. simple – fit in to one of the ‘cloud’ bucket
2. Or complex – with a product available in every imaginable service models and deployment models

Some standards to cloud security…

ISO/IEC 27017: Cloud Computing Security and Privacy Management System-Security Controls

ISO/IEC 27036-x: Multipart standard for the information security of supplier relationship management that is planned to include a part relevant to the cloud supply chain

ITU-T X.ccsec: Security guideline for cloud computing in telecommunication area

ITU-T X.srfcts: Security requirements and framework of cloud-based telecommunication service environment(X.srfcts)

ISO/IEC 30111:2013 gives guidelines for how to process and resolve potential vulnerability information in a product or online service.

ISO/IEC 29147:2014 gives guidelines for the disclosure of potential vulnerabilities in products and online services.

Product in the Cyber Space

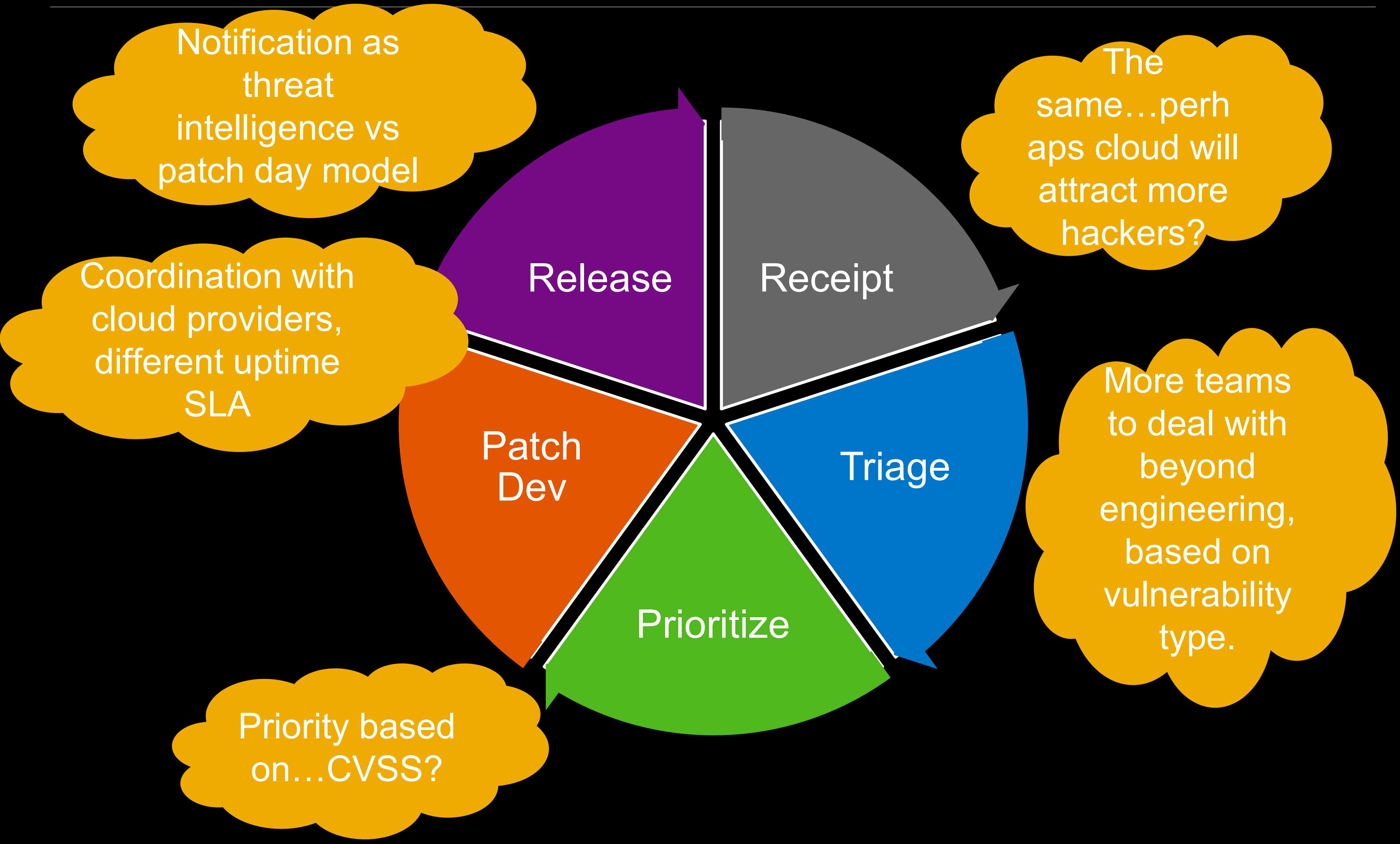
Product Incident Response – Computer (‘Cyber’) Incident Response

The pursuit of no down-time

99.99% = 4 minutes per month

99.9% = 43 minutes per month

PSIRT process abstraction



Notification as threat intelligence vs patch day model

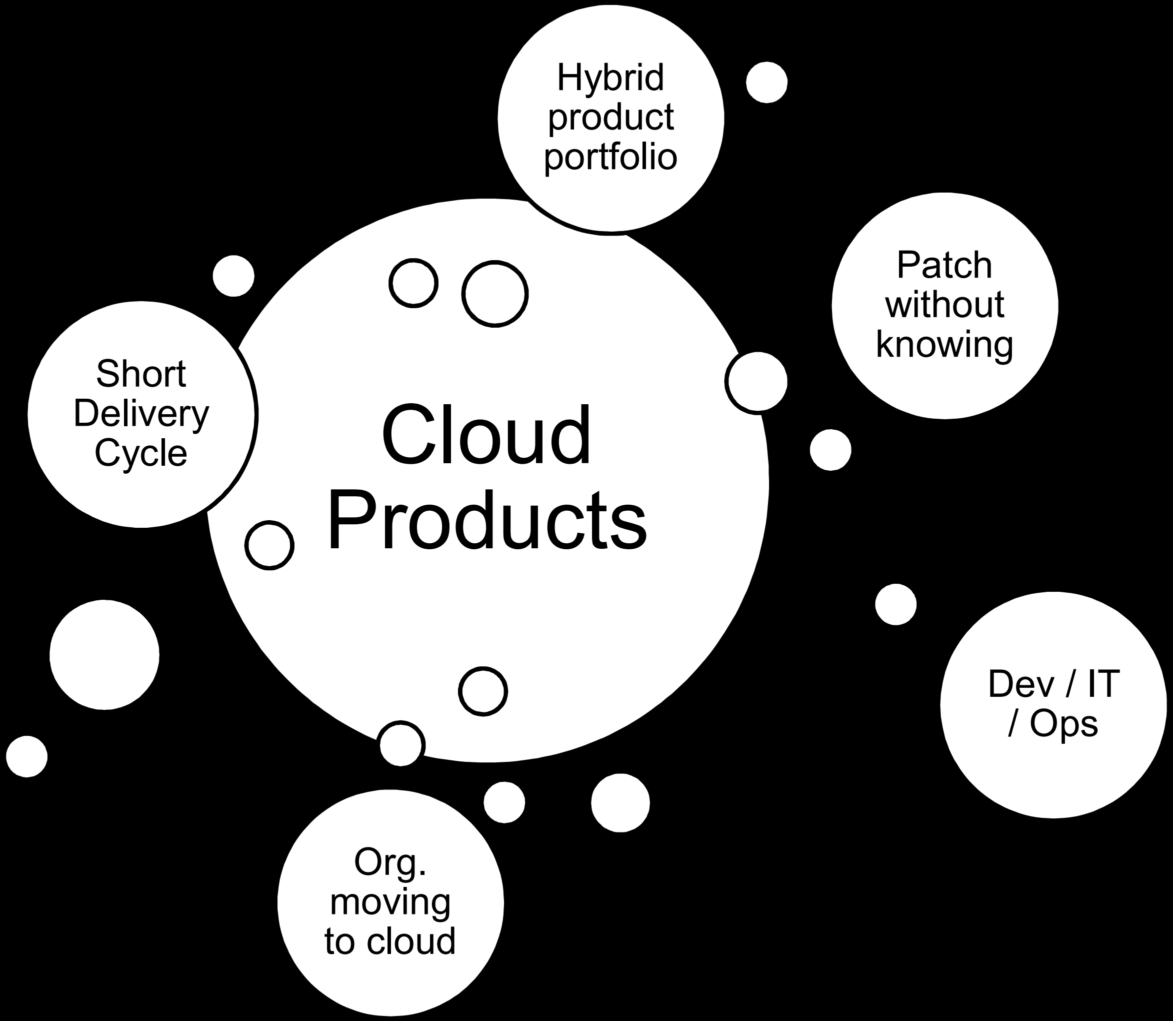
The same…perh aps cloud will attract more hackers?

Coordination with cloud providers, different uptime SLA

More teams to deal with beyond engineering, based on vulnerability type.

Priority based on…CVSS?

Transition to cloud



PSIRT as a sub-culture

Communications

Project Management

Security Knowledge

Our ‘real’ organization – organic growth

Context of each organization moving to the cloud is very dynamic

- Old business model (on-premise) and new business model (cloud, IoT) often co-exist
- On-premise products are converted to the cloud (or simply ‘load’ on to the cloud)
- Hybrid of models: S/P/IaaS wherever $$ is
- Internal politics, power struggle, and defined processes
- Customers demand are different – cloud customers (esp. SaaS) expect trouble-free operations and care-less of how it is managed.
- Complex partner ecosystem in the supply-chain – vulnerability notification is even more difficult

Our ‘real’ organization – M&A

Acquisition-based innovation is not new, but is very fierce among companies to race to the cloud. Does your organization face challenges when the new clashes with the old?

My Observations and Experience

1) Cloud is very agile…release management time-frame is really quick.
2) Need to patch all DC, need to make sure all DC are account for
3) Vulnerabilities discovered via institutionalized pen-test contract
4) New colleagues from M&A perceive traditional vulnerability management as history and refuse to integrate – above typical M&A resistance
5) App Sec team needs to bridge among engineering and IT, they don't usually get along
6) How do we notify our customers of fixed vulnerabilities? There is no patch to apply…this is not easy, especially when there is a mix of cloud deployment models and simultaneous on premise/cloud product offering
7) Security Issues vs. vulnerability
8) Administration of bounty, acknowledgements

Thank you

Contact information:

Vic Chung
Product Security Architect

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.