nviso

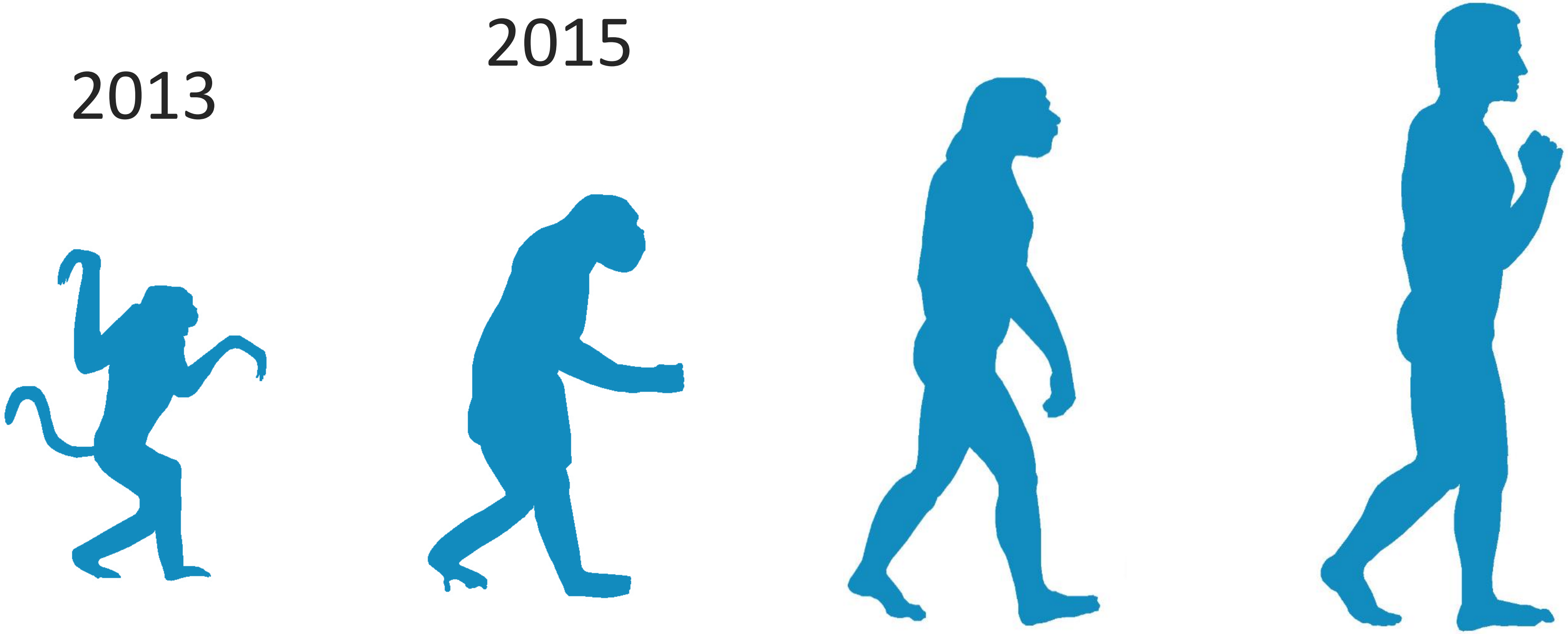
Du brouillard dans le nuage

Leçons tirées d'une migration complète vers Azure

Valentin Lecomte, 24/10/2019

How it all started

How it all started



2013 — *Google is our friend*

2015 — *Clouds, clouds, clouds*

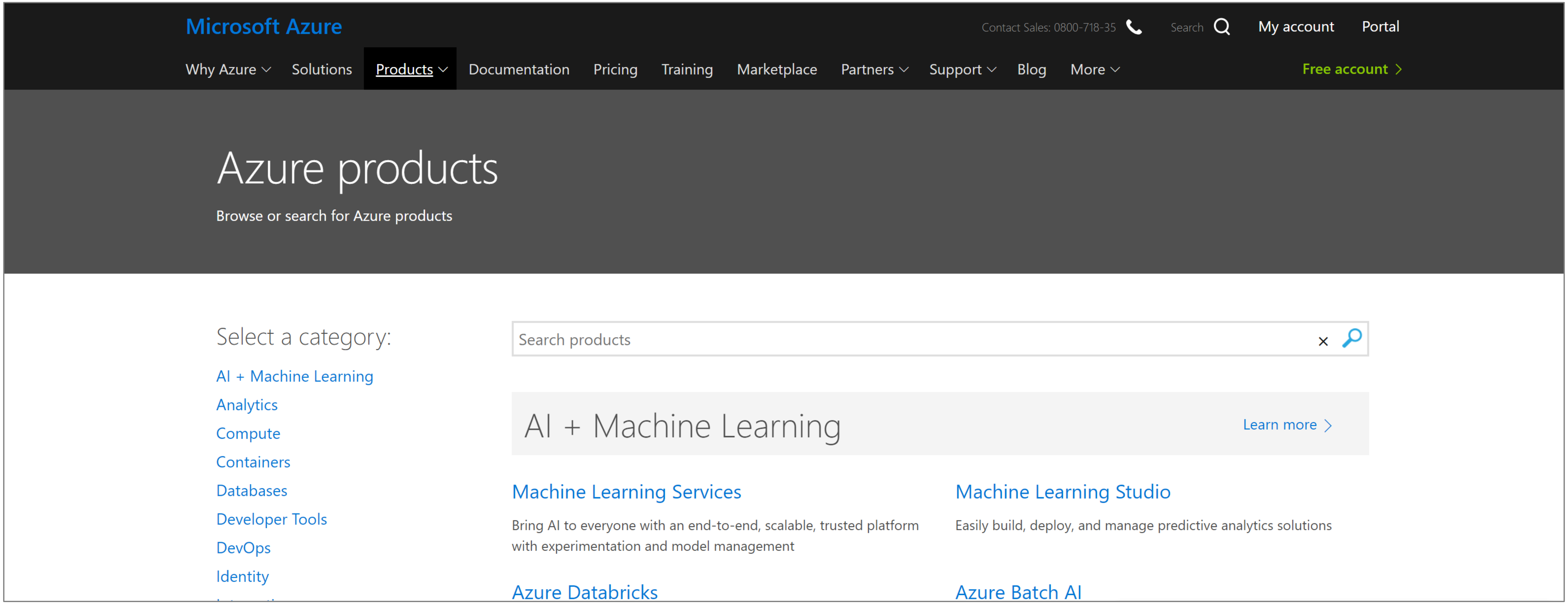
2016 — *25 users & a lot of documents*

2017 — *It’s complicated !*

User perspective

IT perspective

An impressive list of features



Microsoft Azure

Azure products

Browse or search for Azure products

Select a category:

- AI + Machine Learning
- Analytics
- Compute
- Containers
- Databases
- Developer Tools
- DevOps
- Identity

Search products

AI + Machine Learning

Learn more

Machine Learning Services

Bring AI to everyone with an end-to-end, scalable, trusted platform with experimentation and model management

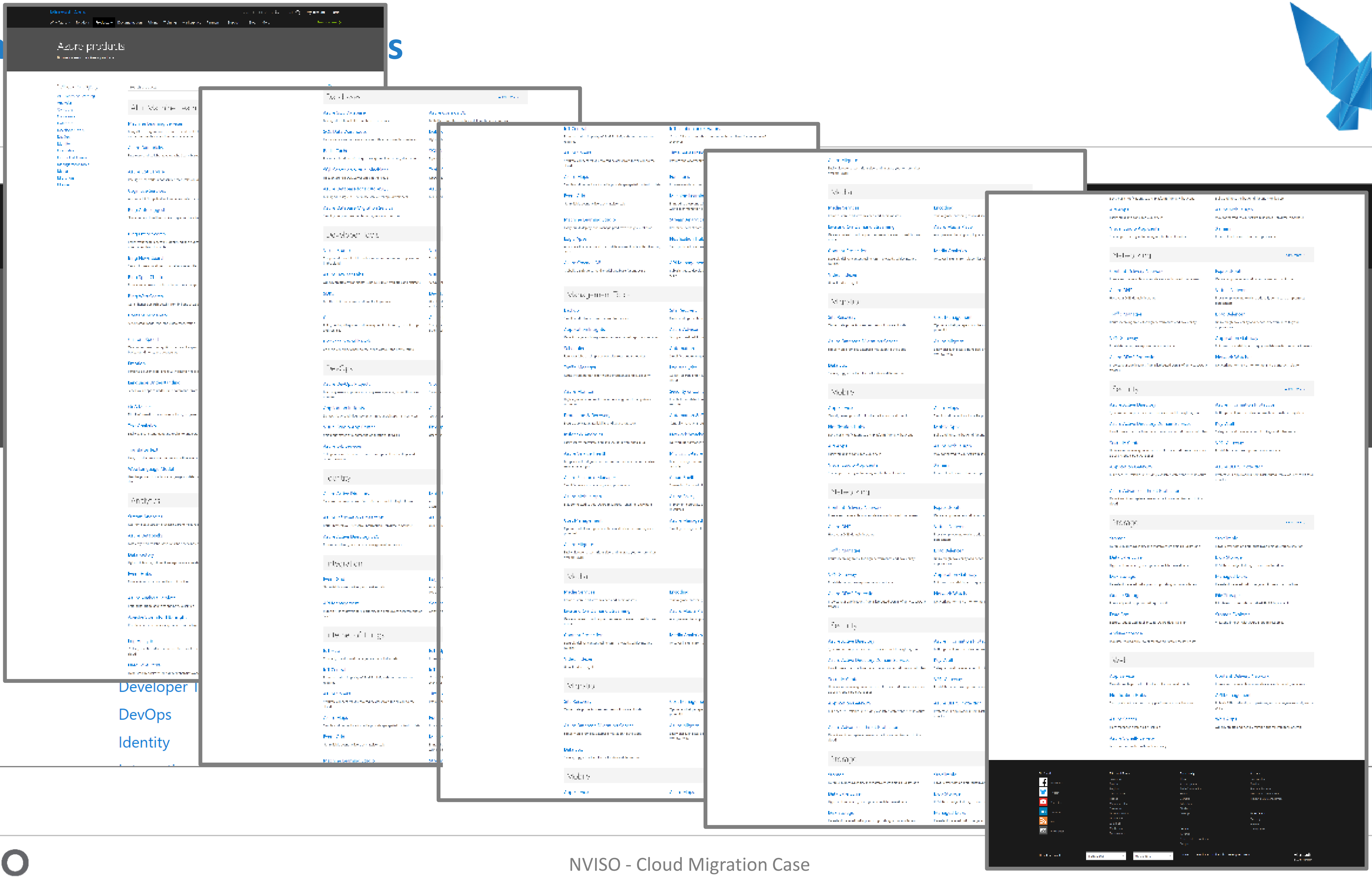
Machine Learning Studio

Easily build, deploy, and manage predictive analytics solutions

Azure Databricks

Azure Batch AI

An in s



Developer T

DevOps

Identity

Our IT needed a guide

Our experience in four chapters

Chapter 1

Define Cloud requirements

Chapter 2

Confront expectations to reality

Chapter 3

Prepare Cloud migration

Chapter 4

Operate the Cloud

Our experience in four chapters

Chapter 1

Define Cloud requirements

Chapter 2

Confront expectations to reality

Chapter 3

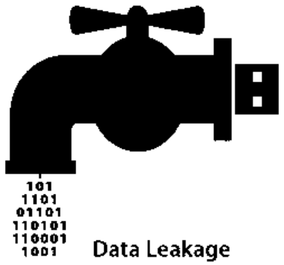
Prepare Cloud migration

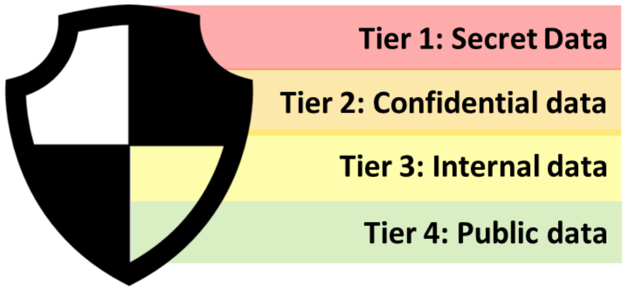
Chapter 4

Operate the Cloud

What do you need to know

Approaching the big move





1.1 Shift everyone’s mindset from perimeter to data-centric approach

1.2 Identify the main threats to our environment

1.3 Determine what we must protect

What do you need to know

Approaching the big move

1.4 Define our trust model

1.5 Define functional requirements

1.6 Define security & non-functional requirements

Our experience in four chapters

Chapter 1

Define Cloud requirements

Chapter 2

Confront expectations to reality

Chapter 3

Prepare Cloud migration

Chapter 4

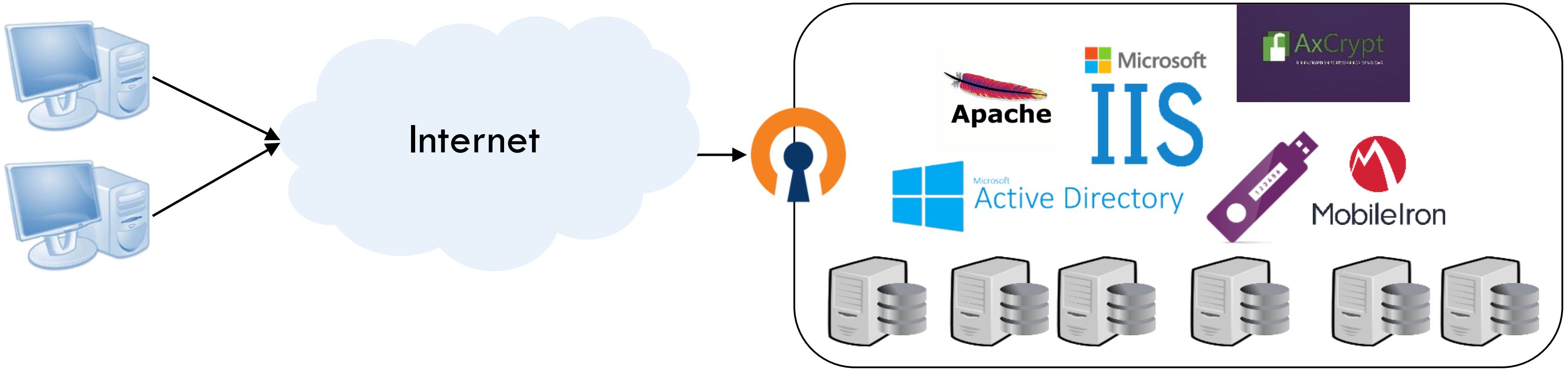
Operate the Cloud

Challenge 1 - Picking the cloud model that’s right for us

Cloud service model

2.1 Select our cloud service model and deployment

Option 1 : IaaS in private deployment

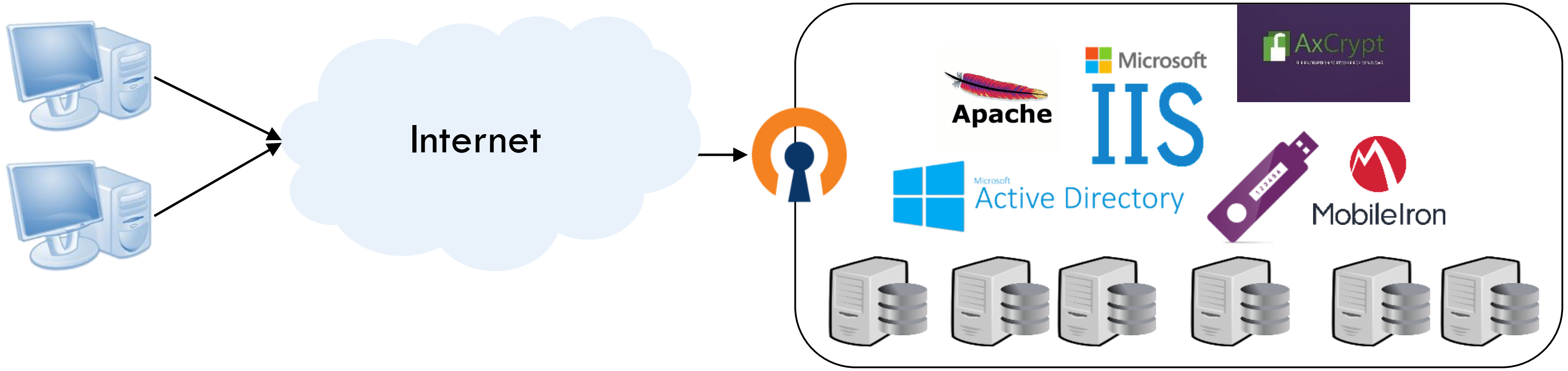


Challenge 1 - Picking the cloud model that’s right for us

Cloud service model

2.1 Select our cloud service model and deployment

Option 1 : IaaS in private deployment



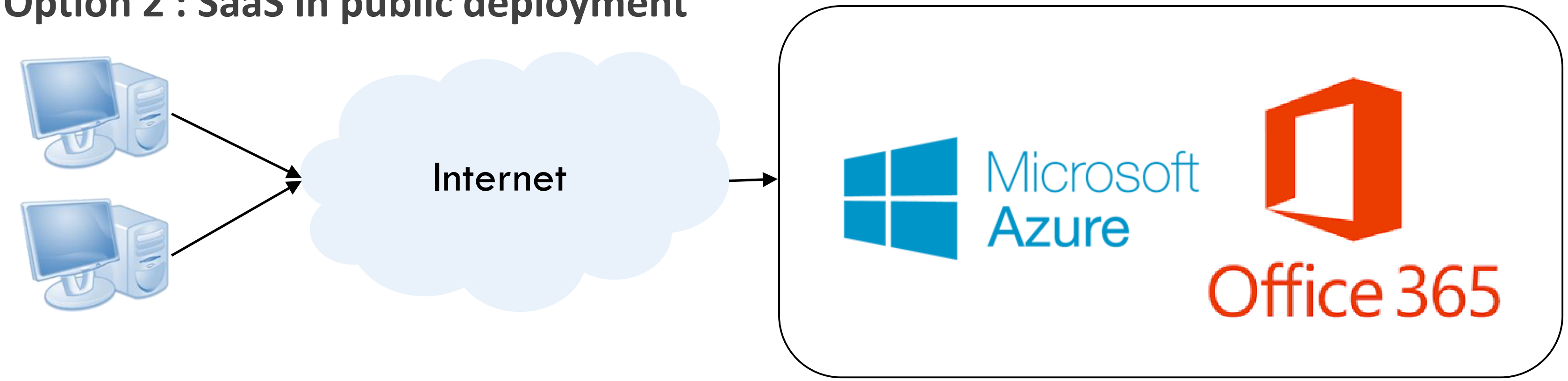
Requirements	Management	Security	Service Cost
79 %	⬇	⬆	⬆

Challenge 1 - Picking the cloud model that's right for us

Cloud service model

2.1 Select our cloud service model and deployment

Option 2 : SaaS in public deployment

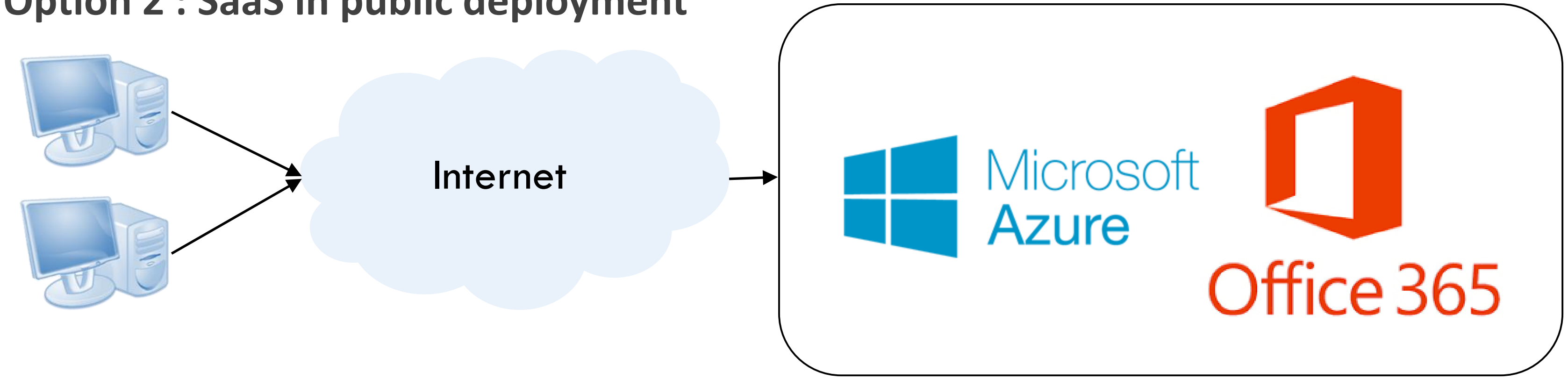


Challenge 1 - Picking the cloud model that’s right for us

Cloud service model

2.1 Select our cloud service model and deployment

Option 2 : SaaS in public deployment



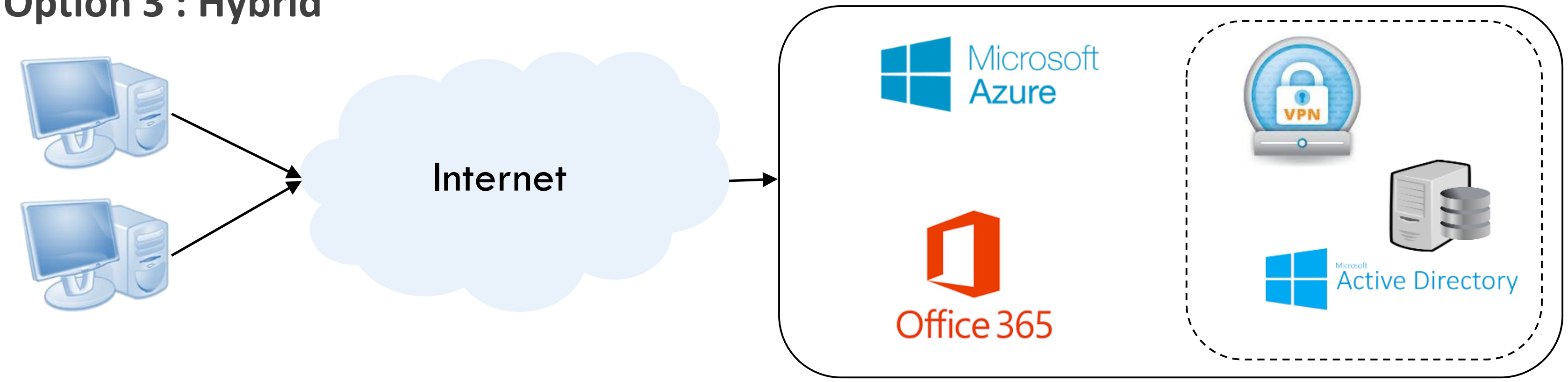
Requirements	Management	Security	Service Cost
29%	⬆	⬇	⬇

Challenge 1 - Picking the cloud model that’s right for us

Cloud service model

2.1 Select our cloud service model and deployment

Option 3 : Hybrid

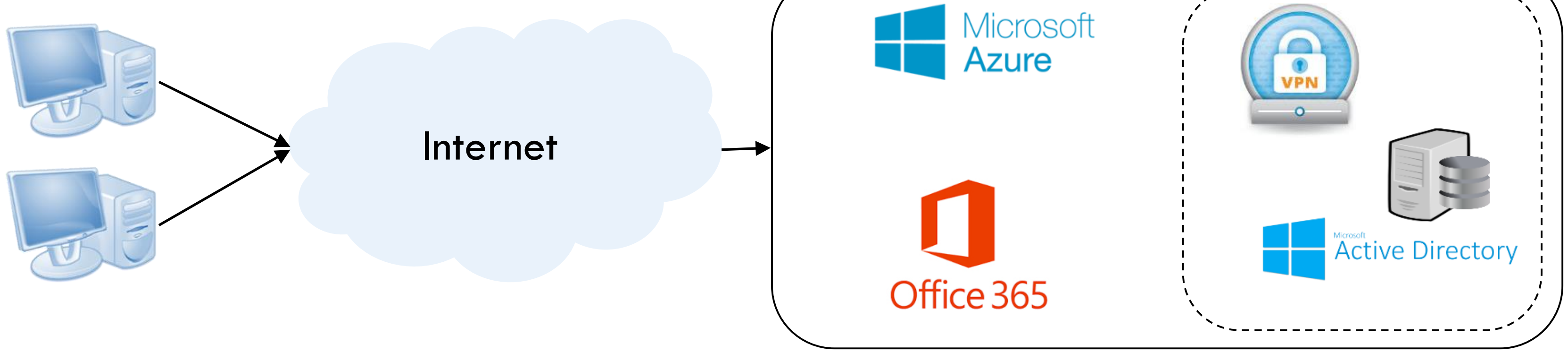


Challenge 1 - Picking the cloud model that's right for us

Cloud service model

2.1 Select our cloud service model and deployment

Option 3 : Hybrid



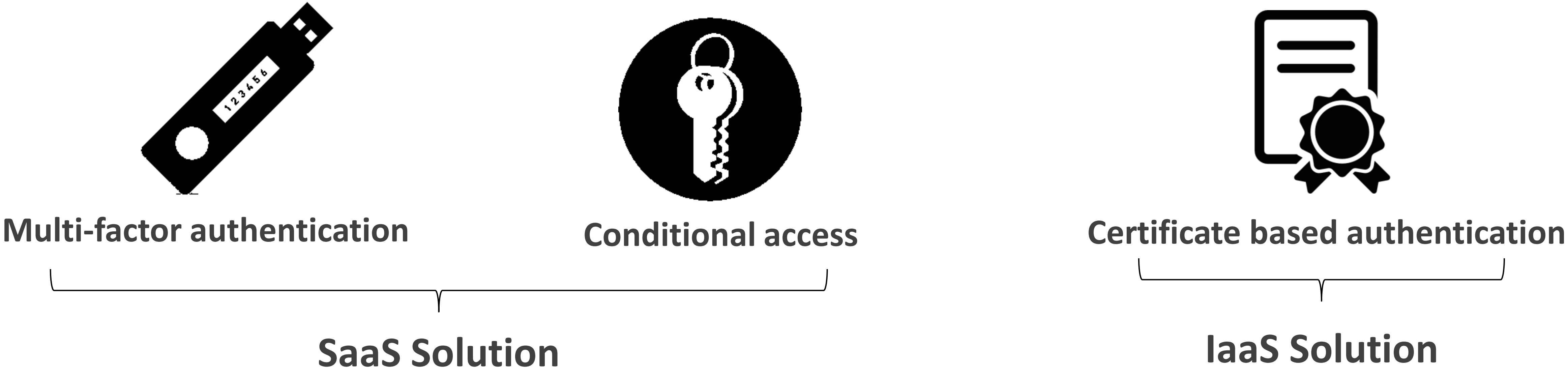
Requirements	Management	Security	Service Cost
55%	➡	⬆	⬇

Challenge 2- Cloud access controls

Access controls

2.2 Review our authentication model

There are virtually no limits to authentication solution, but re-using the Cloud-integrated authentication for all services can be challenging.



Multi-factor authentication

Conditional access

Certificate based authentication

SaaS Solution

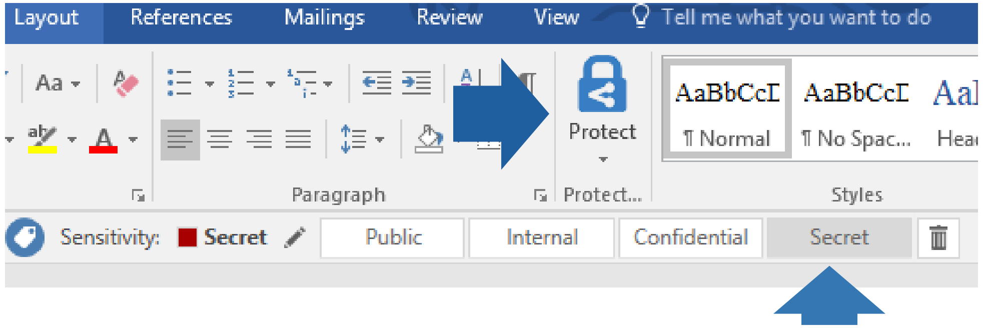
IaaS Solution

Challenge 3 – Data classification policy

Data classification toolset

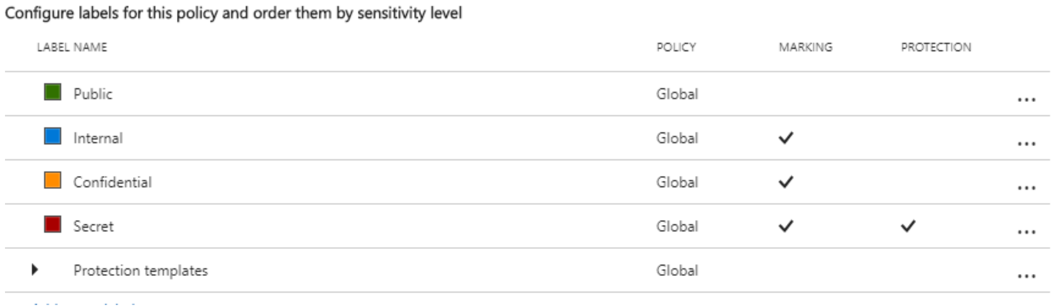
2.3 Enable data classification (Azure Information Protection)

Data protection is integrated in our cloud solution (Azure Information Protection), certificate management is done by the cloud provider.



Sensitivity: 🟥 Secret

Workstation application and plugin



Configure labels for this policy and order them by sensitivity level

LABEL NAME	POLICY	MARKING	PROTECTION	
🟩 Public	Global			...
🟦 Internal	Global	✓		...
🟧 Confidential	Global	✓		...
🟥 Secret	Global	✓	✓	...
▸ Protection templates	Global			...

Central configuration and enforcement

Challenge 4 - Data leakage

Security controls

2.4 Enable and configure data loss prevention rules

The Office 365 information protection policy provides de facto data loss prevention controls.

Labelling

File encryption based on user access

Exchange transaction rules

Challenge 5 - Device Management

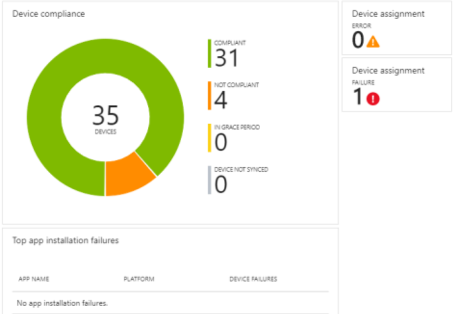
Trust vs non-trusted

2.5 Enforce Trust Model across all devices

Mobile Device Management functionalities are usually included out of the box and embed the ‘trust model’ principle we defined.

Mobile Device Management

Mail on BYOD



Device compliance

35 DEVICES

COMPLIANT 31

NOT COMPLIANT 4

IN GRACE PERIOD 0

DEVICE NOT SYNCED 0

Device assignment

ERROR

0 ⚠

Device assignment

FAILURE

1 ❗

Top app installation failures

APP NAME	PLATFORM	DEVICE FAILURES
No app installation failures.		

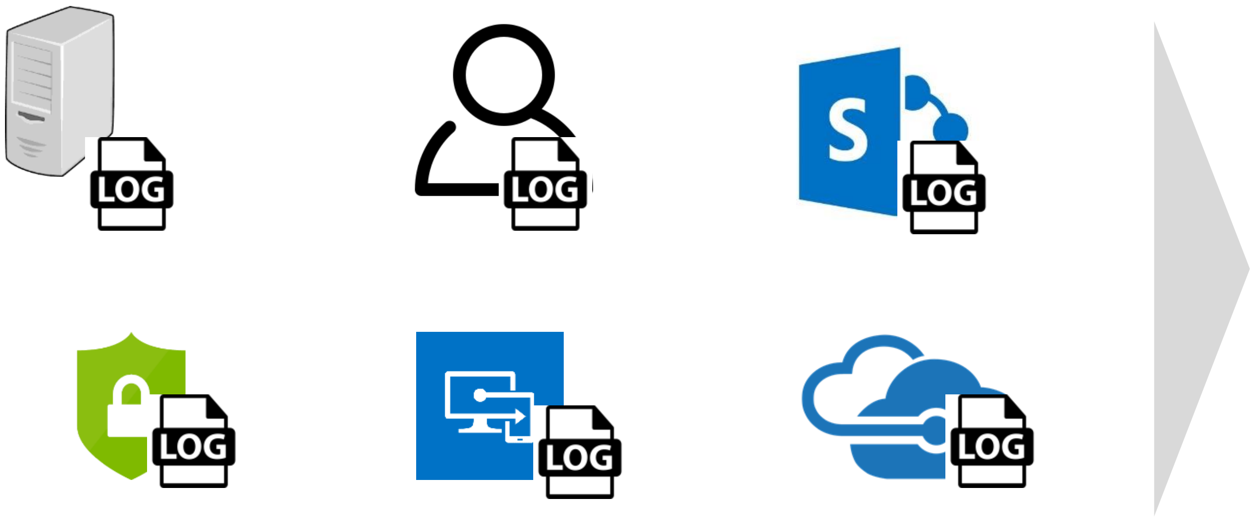
Compliance checks

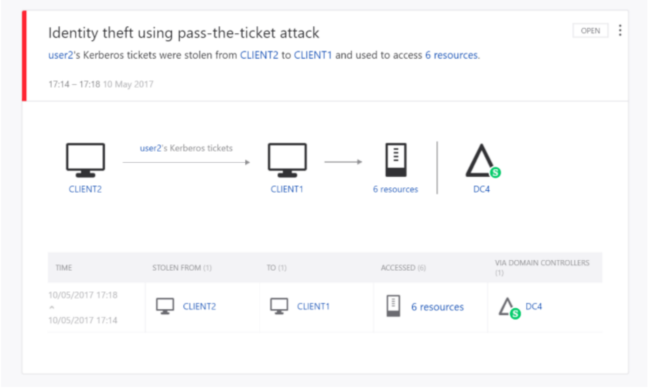
Challenge 6 - Continous security monitoring

Centralized logs

2.6 Collect logs to support monitoring

Dealing with multiple Azure technologies … and our own: Azure dashboards do not yet offer a sufficiently rich, integrated dashboard.




Identity theft using pass-the-ticket attack

user2's Kerberos tickets were stolen from CLIENT2 to CLIENT1 and used to access 6 resources.

17:14 – 17:18 10 May 2017

TIME	STOLEN FROM (1)	TO (1)	ACCESSED (6)	VIA DOMAIN CONTROLLERS (1)
10/05/2017 17:18 - 10/05/2017 17:14	CLIENT2	CLIENT1	6 resources	DC4

Azure Security Center

Our experience in four chapters

Chapter 1

Define Cloud requirements

Chapter 2

Confront expectations to reality

Chapter 3

Prepare Cloud migration

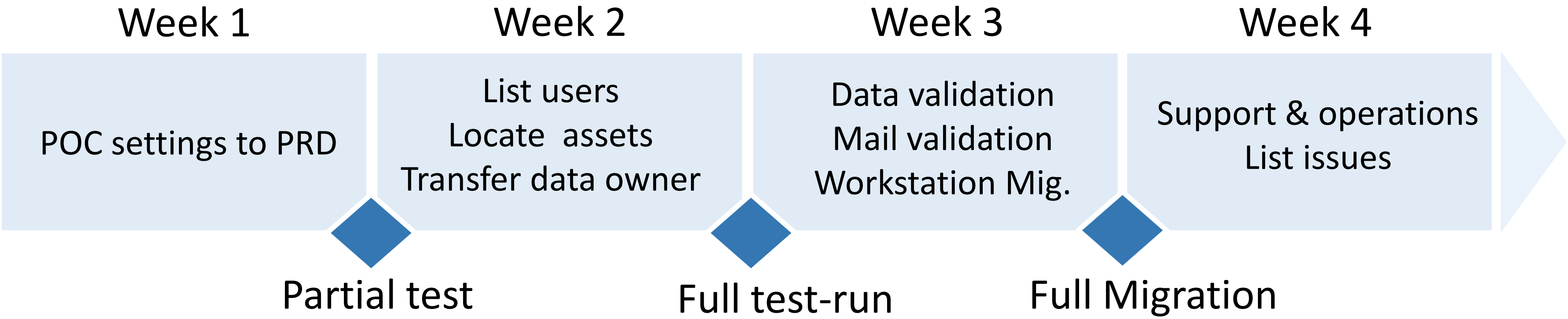
Chapter 4

Operate the Cloud

Moving towards the cloud

A man with a plan !

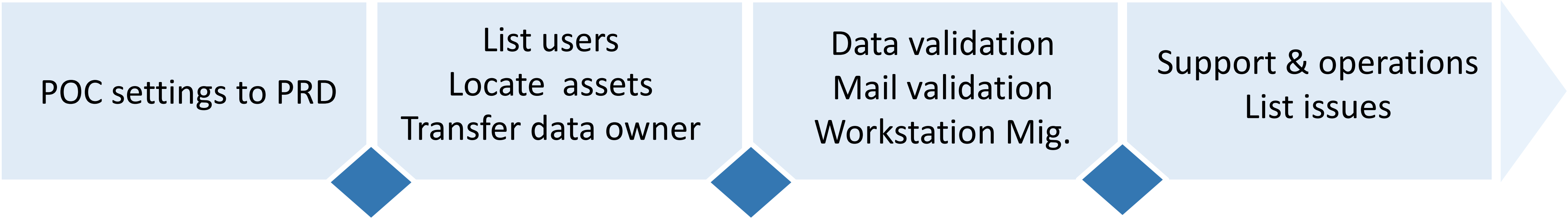
3.1 Define Migration plan



Moving towards the cloud

A man with a plan !

3.2 Migration process



POC settings to PRD

List users
Locate assets
Transfer data owner

Data validation
Mail validation
Workstation Mig.

Support & operations
List issues

- ⚠ Data ownership changed
- ⚠ Mail throttling
- ⚠ Data throttling

- ⚠ Folder path < 255 characters
- ⚠ Conditional access issues
- ⚠ Immature products (e.g. Microsoft Teams)

Our experience in four chapters

Chapter 1

Define Cloud requirements

Chapter 2

Confront expectations to reality

Chapter 3

Prepare Cloud migration

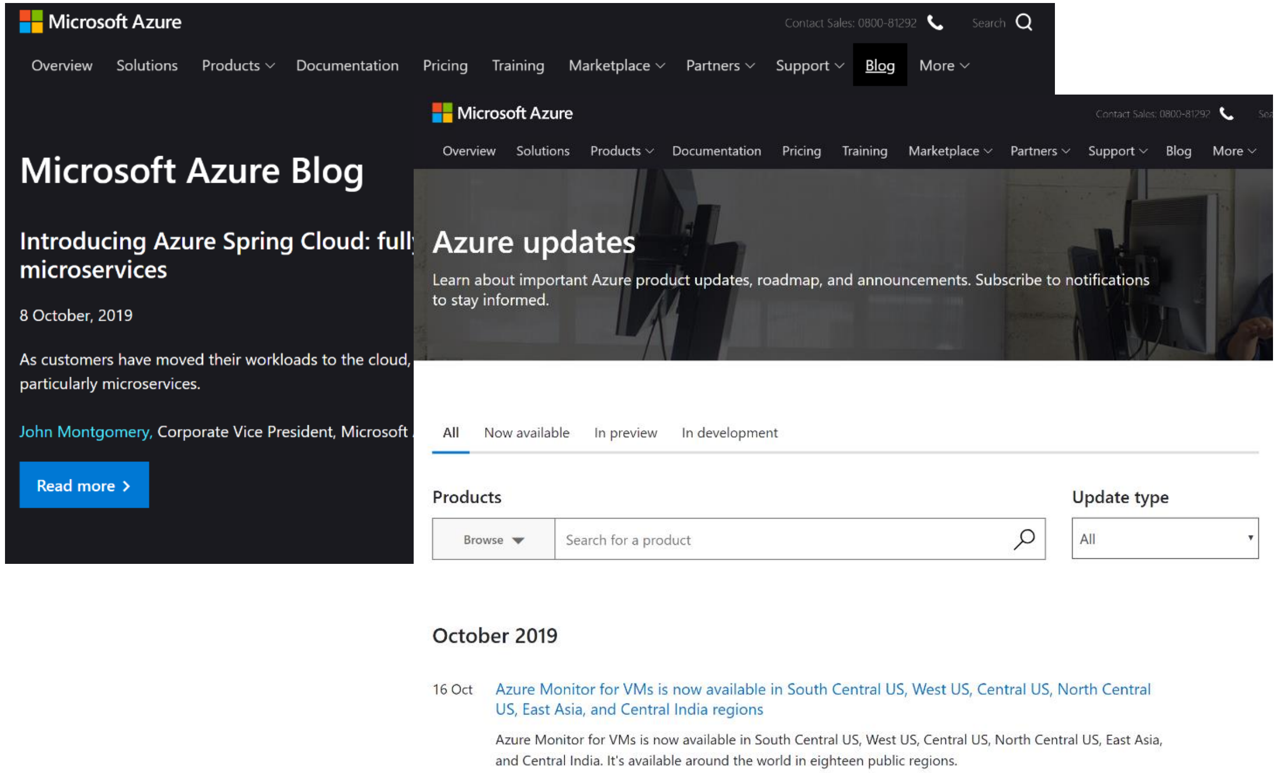
Chapter 4

Operate the Cloud

Cloud Operational model

Support and management

4.1 Keep up with the change, stay up to date !


Microsoft Azure

Contact Sales: 0800-81292 Search

Overview Solutions Products Documentation Pricing Training Marketplace Partners Support Blog More

Microsoft Azure Blog

Introducing Azure Spring Cloud: full microservices

8 October, 2019

As customers have moved their workloads to the cloud, particularly microservices.

John Montgomery, Corporate Vice President, Microsoft

Read more ›

Microsoft Azure

Contact Sales: 0800-81292

Overview Solutions Products Documentation Pricing Training Marketplace Partners Support Blog More

Azure updates

Learn about important Azure product updates, roadmap, and announcements. Subscribe to notifications to stay informed.

All Now available In preview In development

Products: Browse ▾ | Search for a product

Update type: All ▾

October 2019

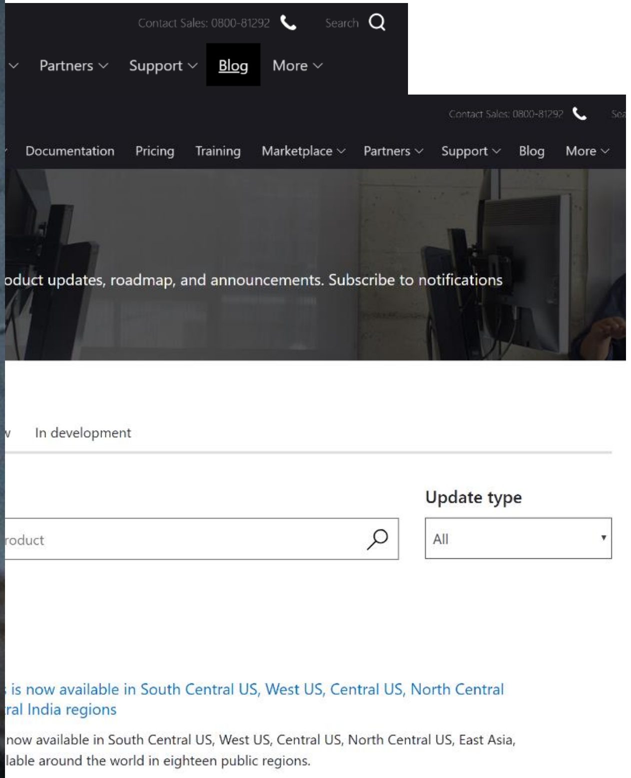
16 Oct Azure Monitor for VMs is now available in South Central US, West US, Central US, North Central US, East Asia, and Central India regions

Azure Monitor for VMs is now available in South Central US, West US, Central US, North Central US, East Asia, and Central India. It's available around the world in eighteen public regions.

Cloud Operational model

Support and management

4.1 Keep up with the change, stay up to date !



oduct updates, roadmap, and announcements. Subscribe to notifications

In development

Update type

roduct

All

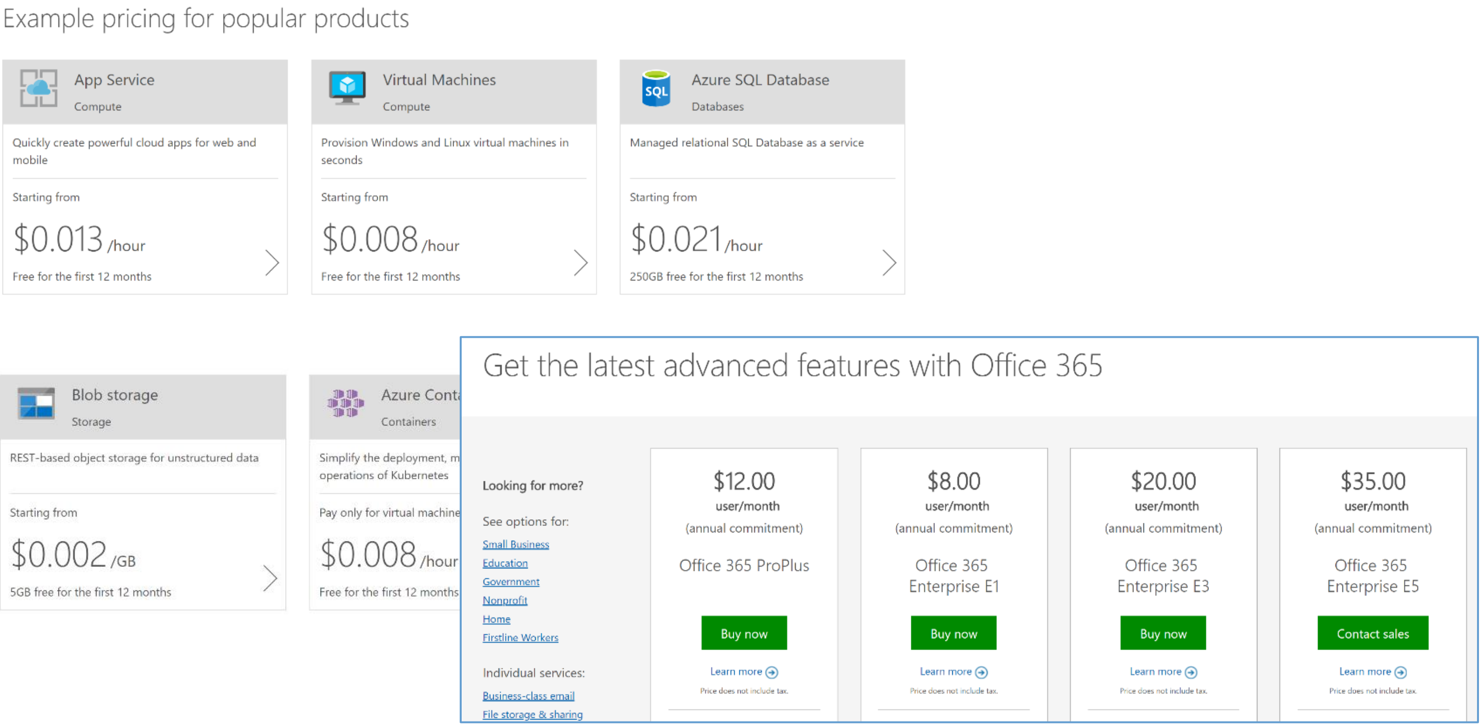
is now available in South Central US, West US, Central US, North Central ral India regions

now available in South Central US, West US, Central US, North Central US, East Asia, lable around the world in eighteen public regions.

Cloud Operational model

Support and management

4.2 Monitor usage, as it drives cost: financial control is not as easy as we thought.



Example pricing for popular products

App Service
Compute
Quickly create powerful cloud apps for web and mobile
Starting from
$0.013 /hour
Free for the first 12 months

Virtual Machines
Compute
Provision Windows and Linux virtual machines in seconds
Starting from
$0.008 /hour
Free for the first 12 months

Azure SQL Database
Databases
Managed relational SQL Database as a service
Starting from
$0.021 /hour
250GB free for the first 12 months

Blob storage
Storage
REST-based object storage for unstructured data
Starting from
$0.002 /GB
5GB free for the first 12 months

Azure Conta
Containers
Simplify the deployment, m
operations of Kubernetes
Pay only for virtual machine
$0.008 /hour
Free for the first 12 months

Get the latest advanced features with Office 365

Looking for more?

See options for:
Small Business
Education
Government
Nonprofit
Home
Firstline Workers

Individual services:
Business-class email
File storage & sharing

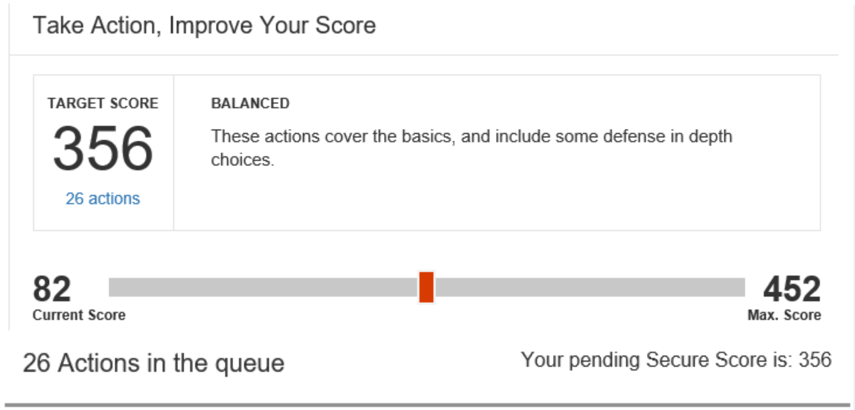
$12.00 user/month (annual commitment)	$8.00 user/month (annual commitment)	$20.00 user/month (annual commitment)	$35.00 user/month (annual commitment)
Office 365 ProPlus	Office 365 Enterprise E1	Office 365 Enterprise E3	Office 365 Enterprise E5
Buy now	Buy now	Buy now	Contact sales
Learn more	Learn more	Learn more	Learn more
Price does not include tax.	Price does not include tax.	Price does not include tax.	Price does not include tax.

Risk and security monitoring

Detect vulnerabilities and incidents

4.3 Continuously monitor security… across all dashboards.

O365 - Risk Monitor



Take Action, Improve Your Score

TARGET SCORE
356
26 actions

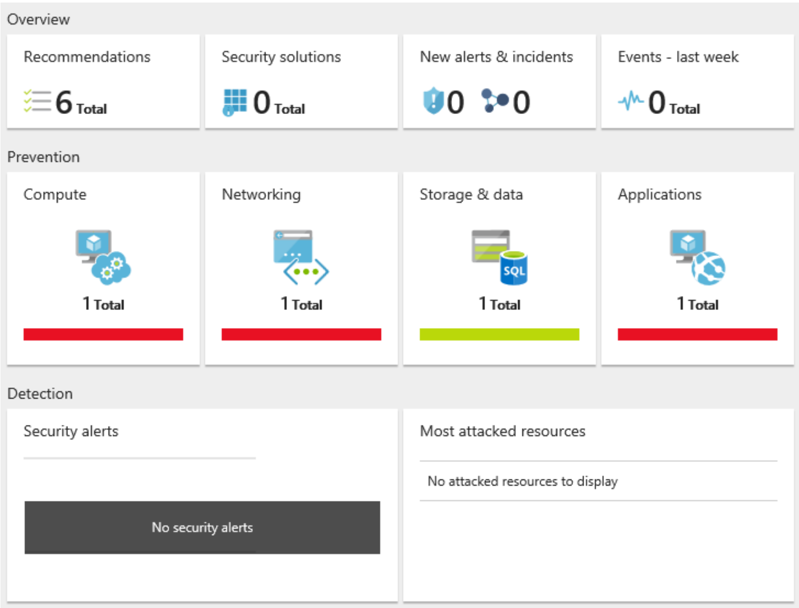
BALANCED
These actions cover the basics, and include some defense in depth choices.

82 Current Score — 452 Max. Score

26 Actions in the queue

Your pending Secure Score is: 356

Vulnerability Management



Overview

Recommendations	Security solutions	New alerts & incidents	Events - last week
6 Total	0 Total	0 0	0 Total

Prevention

Compute	Networking	Storage & data	Applications
1 Total	1 Total	1 Total	1 Total

Detection

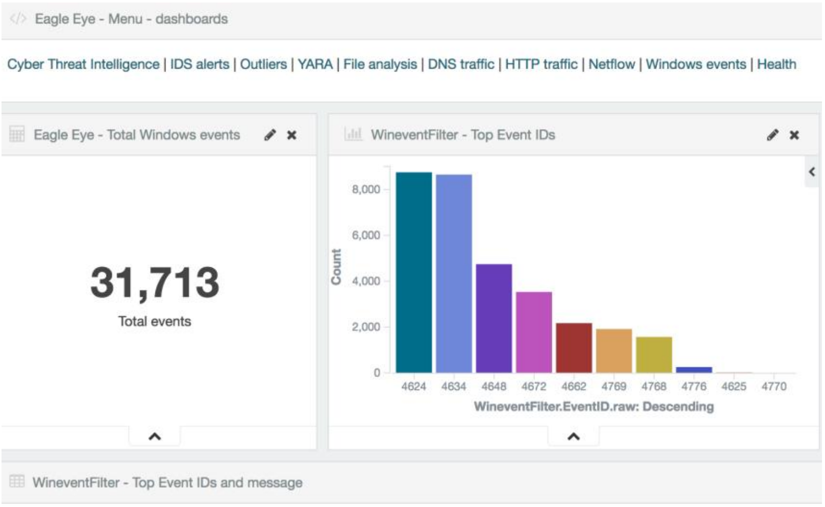
Security alerts

No security alerts

Most attacked resources

No attacked resources to display

Security Monitoring



Eagle Eye - Menu - dashboards

Cyber Threat Intelligence | IDS alerts | Outliers | YARA | File analysis | DNS traffic | HTTP traffic | Netflow | Windows events | Health

Eagle Eye - Total Windows events

31,713
Total events

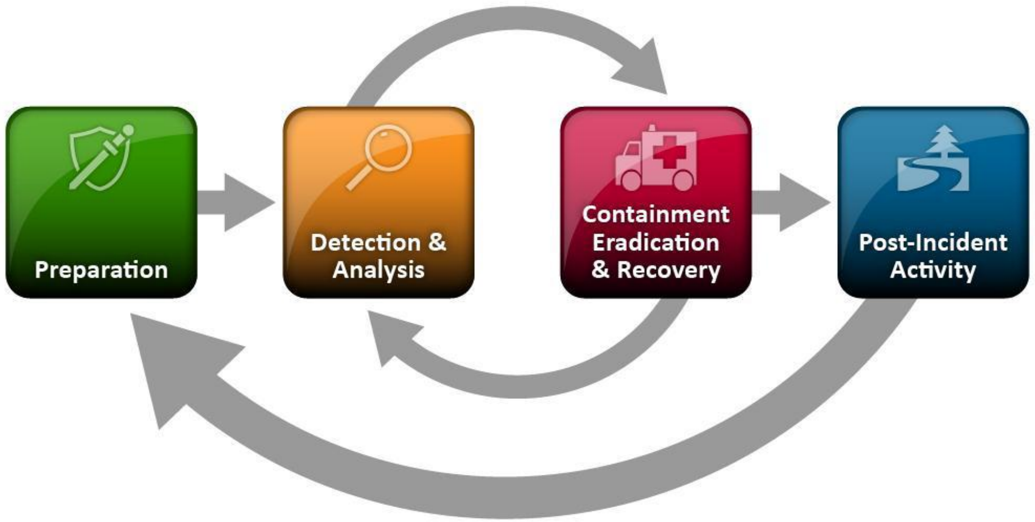
WineventFilter - Top Event IDs

WineventFilter - Top Event IDs and message

Incident response

How to do incident response in cloud environments

4.4 Prepare for incidents and challenge regularly based on new features



Understand our service provider
Shared responsibility model

Validate acquisition procedure
in our cloud model

Create an incident response plan
for cloud environments

Validate new features
(e.g Azure Security Center investigate incidents in Preview)

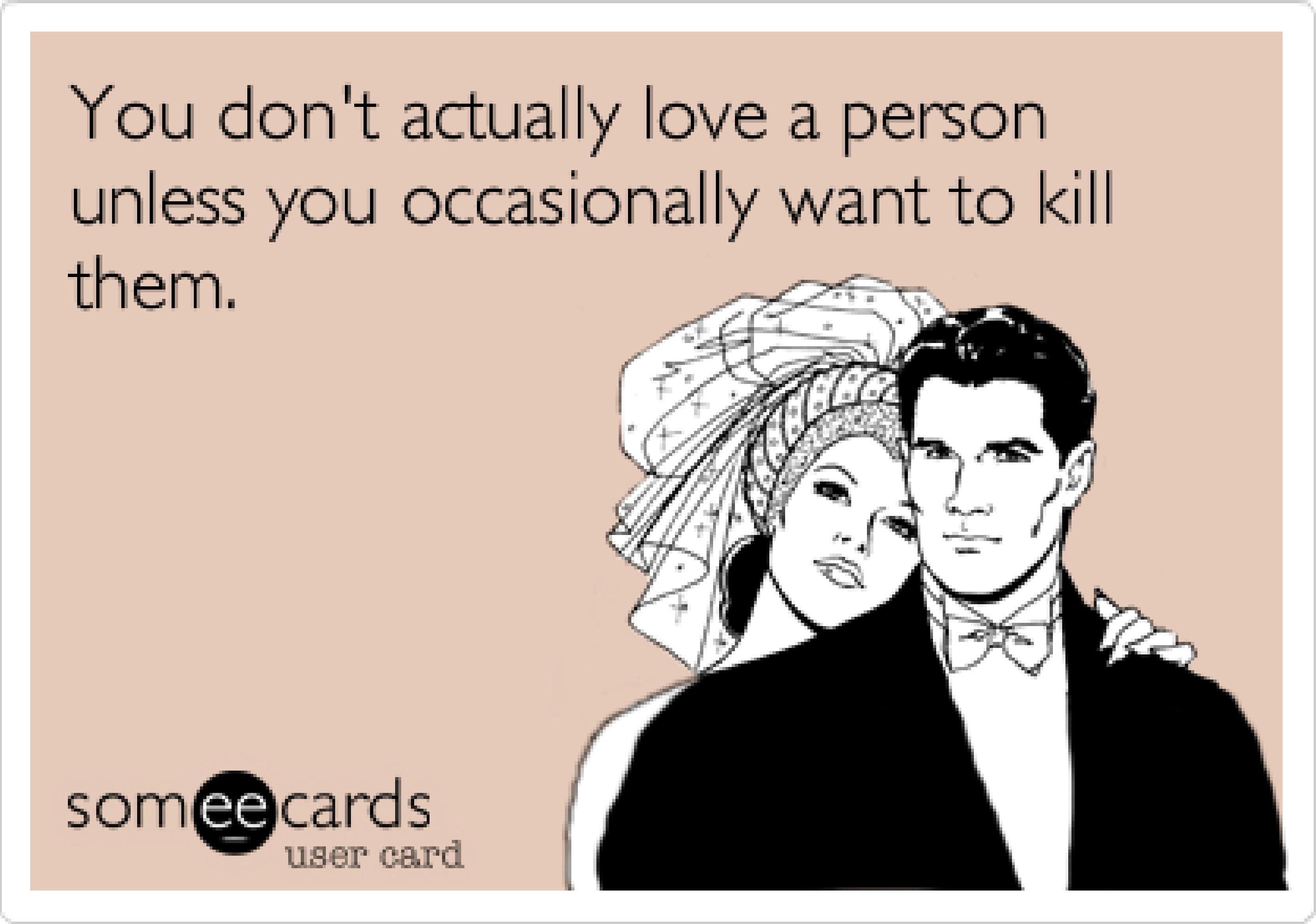
https://docs.microsoft.com/en-us/azure/security-center/security-center-investigation

LESSONS
LEARNED

Lessons learned

1. Talk to your industry peers
2. Go for a solid POC with diverse users
3. Anticipate changes in an IT admin job
4. Read weekly updates & newsletters

My personal conclusion


You don't actually love a person unless you occasionally want to kill them.
someecards
user card

Merci pour votre attention.

Hacked? Malware? Need urgent support?

Call us *+32 (0)2 588 43 80*

Mail us *csirt@nviso.be*