Security Operations Management

From the Datacenter to the Public Cloud

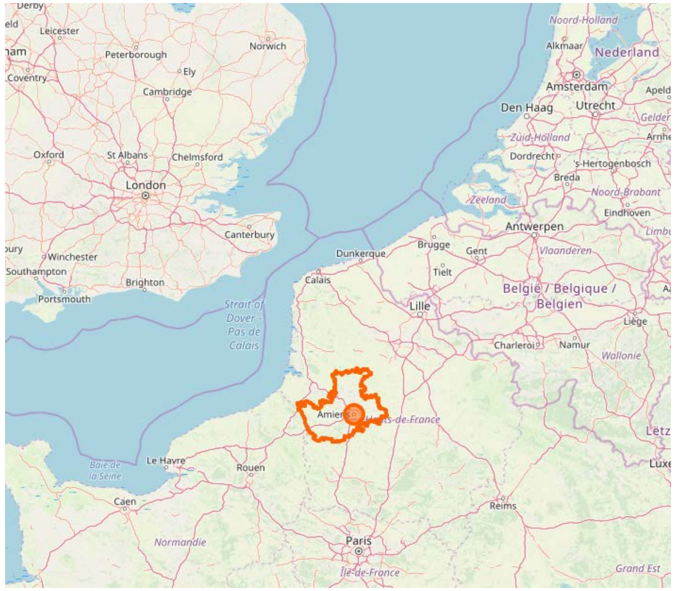
A Technical Focus

Aristide Bouix
18/10/2019

Agenda

1. About me
2. The basis of account and data management
3. What change in the Cloud?
4. Remediation management

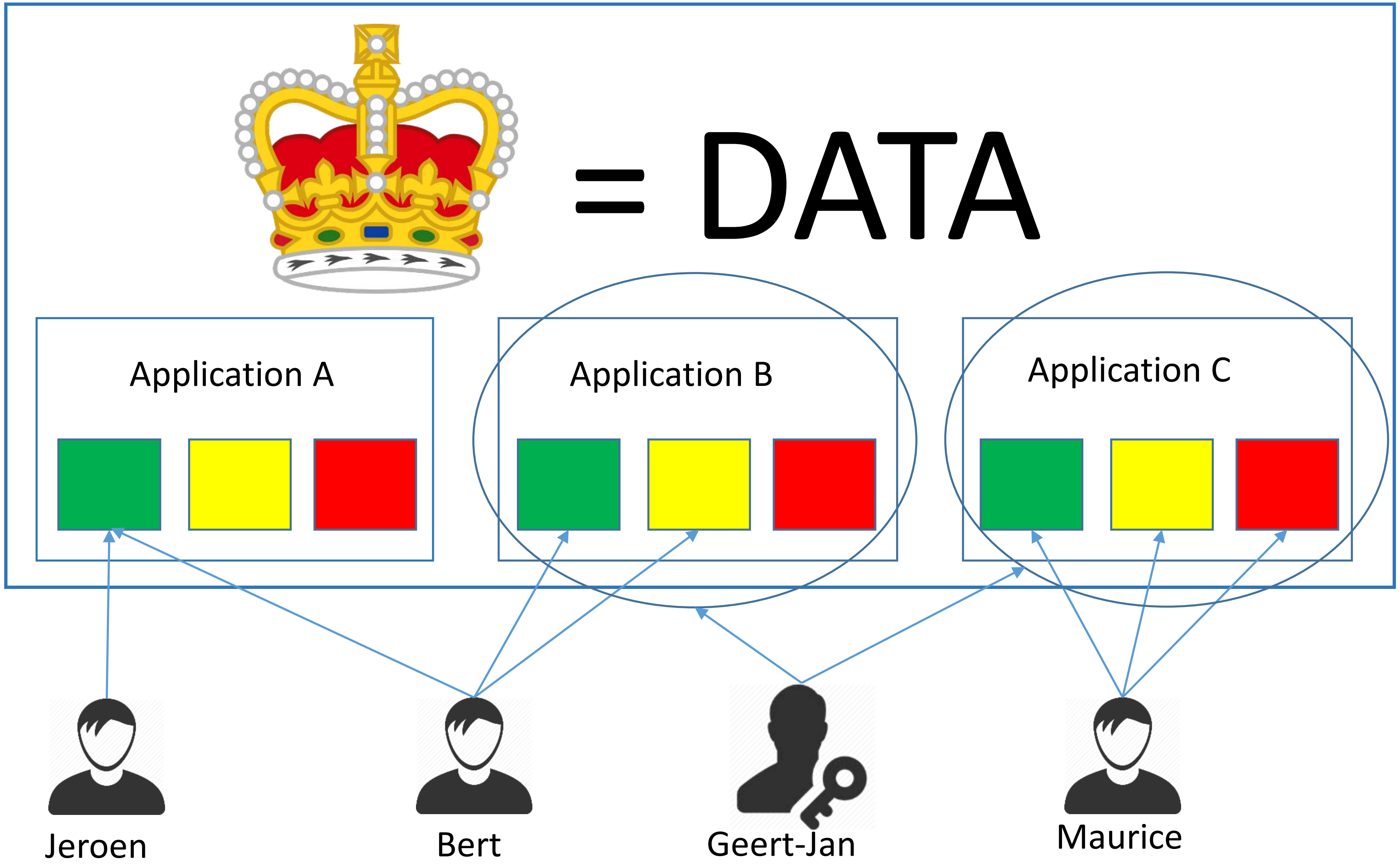
About me



- Senior Consultant, Cybersecurity, DevSecOps lead
  - Certification: 5 AWS certifications, CCSK, Itilv3
- Focus on security operations and secure IT architecture
  - Actively working on Cloud security automation and DevOps security

- Prior worked at an MSSP at Atos and consulting at Devoteam/D2SI
  - MSC in Telecommunication Engineering, major in Network and System security
  - BSC in Electrical Engineering
- Like: Korean food, Metal, Hiking, HomeLabs, Gaming, …
- Dislike: Parsley, Writing security policies, …

Accounts and Data Management



Accounts and Data Management

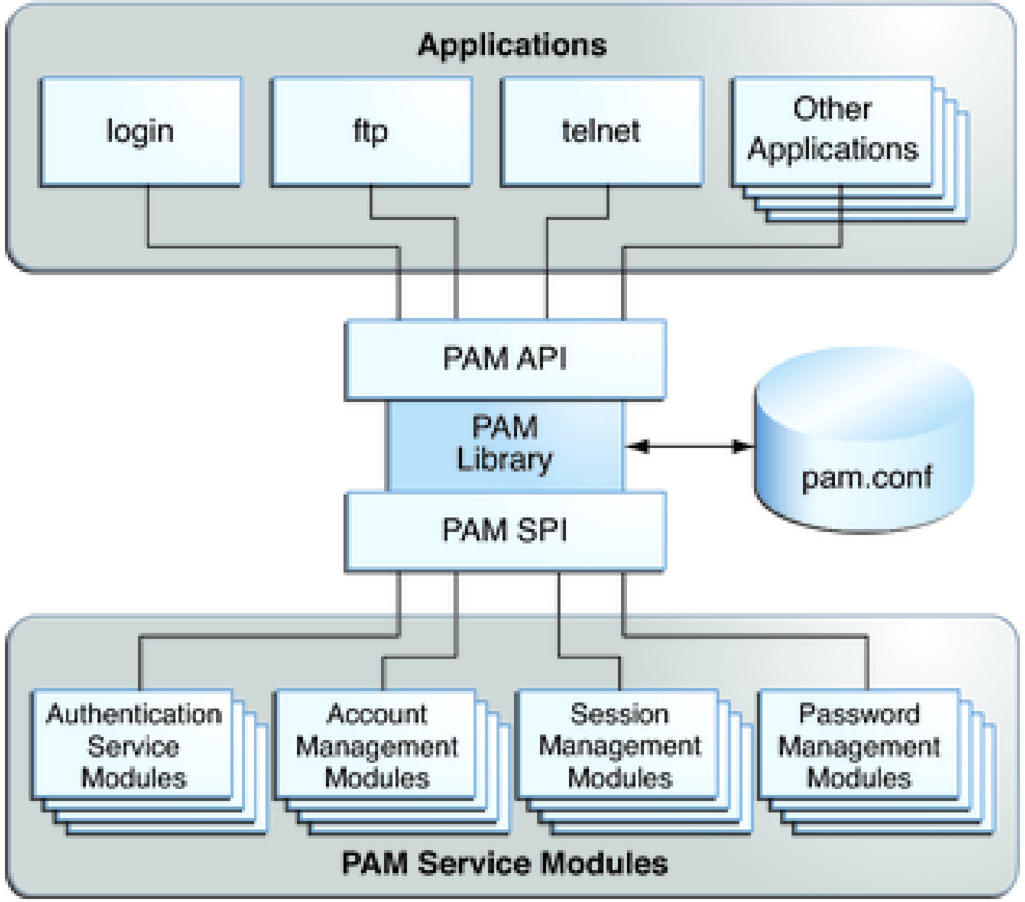
- **A user use an application to perform a Business Function**
  - A core Business Function aims to the production of final goods or services intended for the market or for third parties.

- **An administrator operates an application to make sure it can be used to perform a Business Function**

Accounts are local to each computer, operating system. An application is made of multiple operating systems, software and middleware

➔ We need a centralized database of accounts (Name, password, permissions) = A DIRECTORY

PAM


Applications
login
ftp
telnet
Other Applications
PAM API
PAM Library
PAM SPI
pam.conf
Authentication Service Modules
Account Management Modules
Session Management Modules
Password Management Modules
PAM Service Modules

QUALITY APPROVED CYBERARK®

Source: https://docs.oracle.com/cd/E26505_01/html/E27224/pam-2.html

The different types of outsourced services

Infrastructure management: An external company is contracted to ensure the maintenance of the infrastructure or provide an external service (ex SOC as MSSP)..

Application management: An external company is contracted to ensure the maintenance and availability of an internal application.

Hosting Services

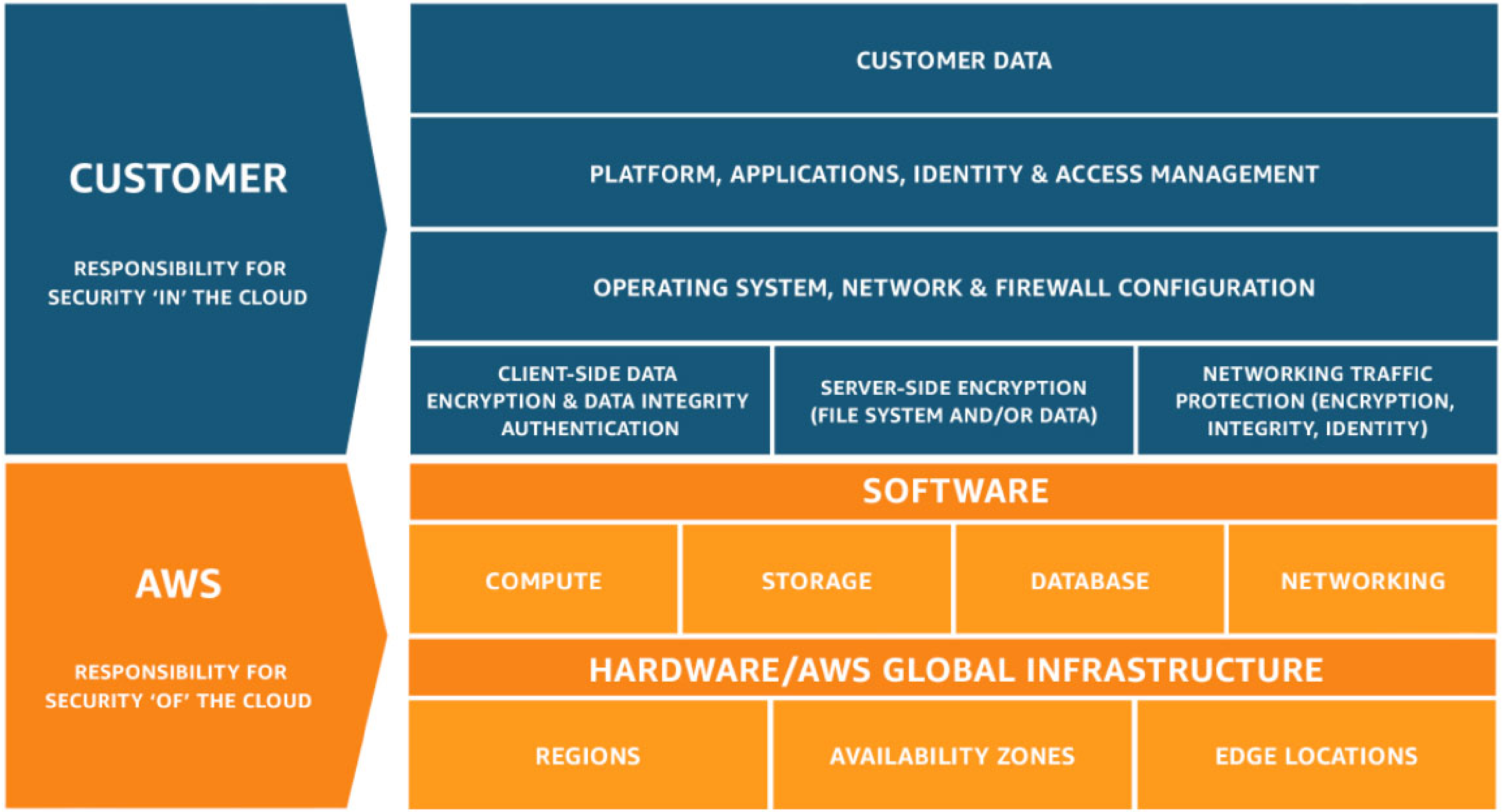
Infrastructure as a Service (IaaS): Provisioning of virtual machines and virtual components allowing to emulate the way of functioning of a traditional Data Centers without having to worry about the physical hardware (and most of the time virtualization hypervisor)

Platform as a Service (PaaS): Web platform allowing to deploy company API and services without any system or network management tasks.

Software as a Service (SaaS): Applications that can be directly used remotely

The Shared Responsibility Model

The provider is accountable for security **OF** the Cloud while client is accountable for security **IN** the Cloud



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

Source: https://aws.amazon.com/compliance/shared-responsibility-model/

Main risks

CONFIDENTIALITY INTEGRITY AVAILABILITY (CIA) TRACEABILITY

General risks of outsourcing: A contractor may have neither technical nor financial ability to provide the service.
MAKE SURE YOUR CONTRACT HAS A REVERSIBILITY CLAUSE

Risks relative to data location:

Often the contractor will ask to store your data in multiple locations for a better Availability; however, by doing so, it may increase the risk on confidentiality:

- Uncontrolled data location can limit company ability to check contractor activities
- May make an infrastructure audit of the contractor more difficult
- May give him an opportunity to escape to local justice (relative to taxes for instance)
- Extradition of personal data outside of the EU borders falls under GDPR legislation and control.

Risks relative to contractor technological choices:

They can try to save on security for financial reasons, for that reason the client should keep a validation right before any new technical decision.
Proprietary or uncommon solutions should generally be avoided as they usually favored vendor lock-in
Data should be recoverable at any time in a standardized format for operability reason with another contractor in case of disagreement.

Risks depending of the outsourced service type

CONFIDENTIALITY INTEGRITY AVAILABILITY (CIA) TRACEABILITY

Risks relative to remote access:

Threats:

- Permanent access from the outside (contractor site)
- Default or weak password
- No logging of contractor activities on client side
- Access to sensitive systems over the Internet

Associated risks:

- Access to managed systems by an unauthorized person (attacker) and attempt to C I A of the service
- Privilege abuse from the contractor technician during a maintenance operation

Risks specific to Cloud computing:

Data can be moved from continent to continent very easily

Most providers don’t allow external audit when asked for, they usually have their own program with affiliate companies and keep results private. All that the client knows is if their proposed services compliant or not with corresponding security standard (FIPS, PCI-DSS, SOCI/II/III, HIPAA ....)

Physical host is usually shared, and VM isolation may be a concern for some companies.

No guarantee that data is fully deleted outside of the word of the provider.

Outside of huge customers, very difficult to get particular conditions out of their standard offers.

Cloud is about Software Defined Architecture and Automation

Restriction are at the API level and you can actively monitor API use to achieve least privilege to your users and applications.

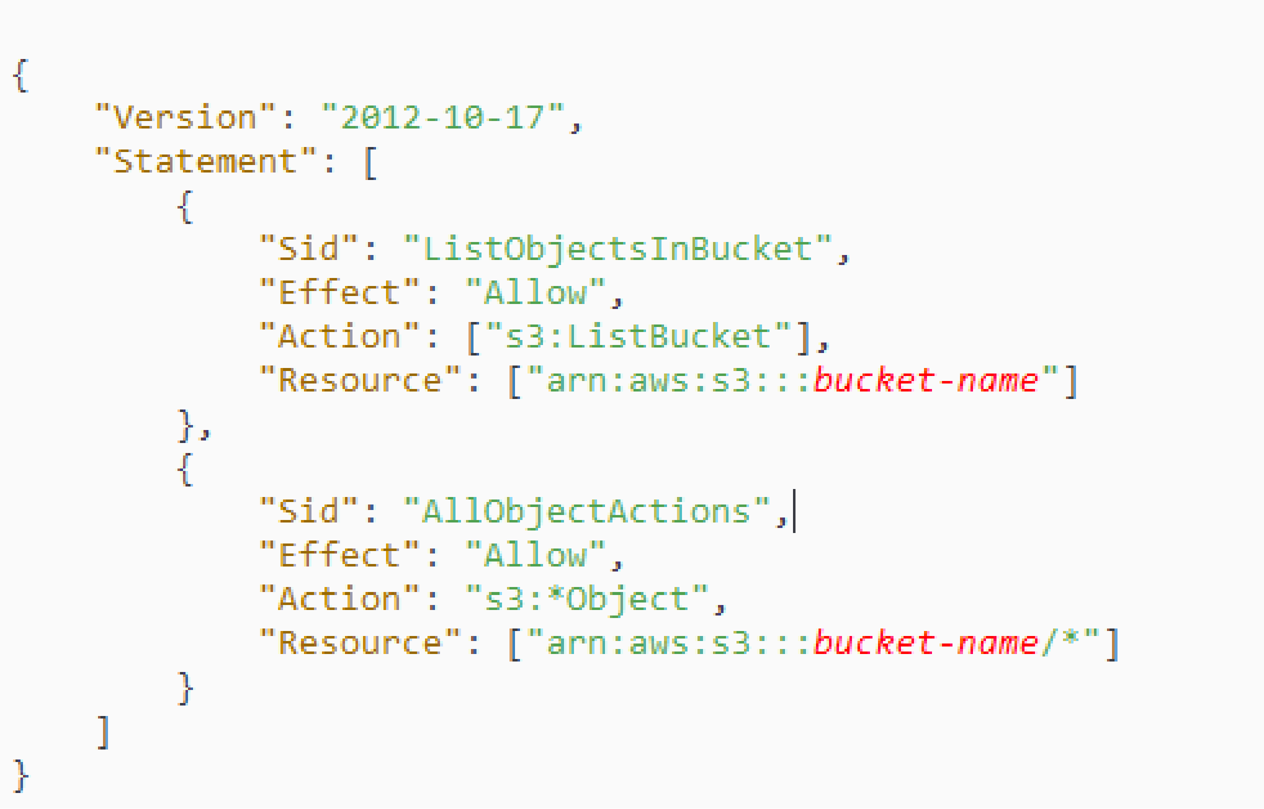
Traditional Network Directory service

- Can be query with LDAP
- Use Kerberos for authentication
- Has an organization (or LDAP Namespace) structure (e.g. "CN=Dev,OU=Distribution Groups, DC=google,DC=com")

Cloud IAM (Identity and Access Management) engine

- Use REST API's over HTTP or HTTPS for communication
- Use protocol built on HTTP(S) such as Security Assertion Markup Language (SAML) or OpenID Connect for authentication (and OAuth for authorization)
- Has a flat file structure

Example: Allows Read and Write Access to Objects in an S3 Bucket

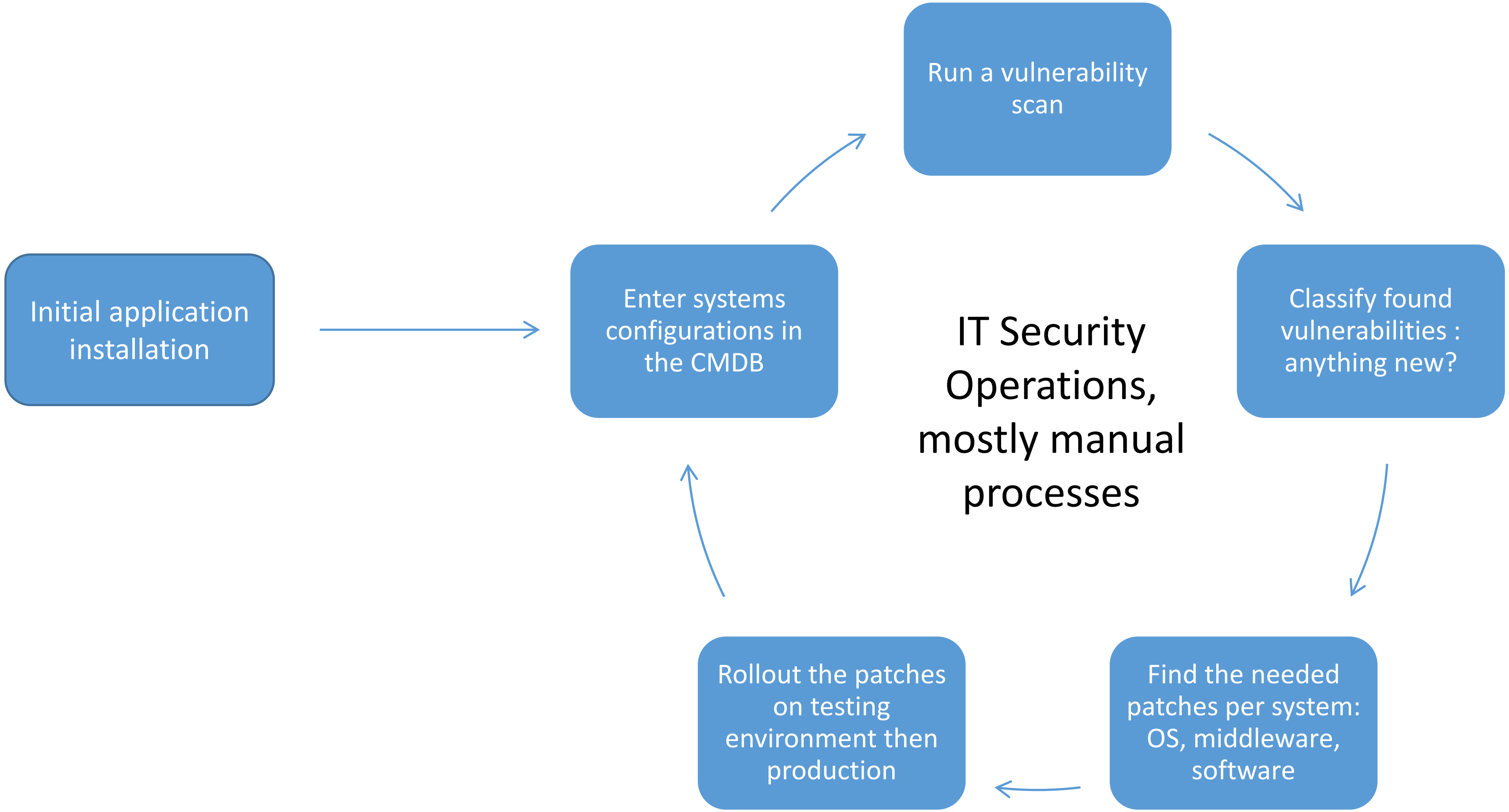


```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ListObjectsInBucket",
            "Effect": "Allow",
            "Action": ["s3:ListBucket"],
            "Resource": ["arn:aws:s3:::bucket-name"]
        },
        {
            "Sid": "AllObjectActions",
            "Effect": "Allow",
            "Action": "s3:*Object",
            "Resource": ["arn:aws:s3:::bucket-name/*"]
        }
    ]
}
```

Source: https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_s3_rw-bucket.html

NB: The wildcard in the *AllObjectActions* statement allows the *GetObject*, *DeleteObject*, *PutObject*, and any other Amazon S3 action that ends with the word "Object".

Remediation management: The OLD Way



Initial application installation

Enter systems configurations in the CMDB

Run a vulnerability scan

Classify found vulnerabilities : anything new?

Find the needed patches per system: OS, middleware, software

Rollout the patches on testing environment then production

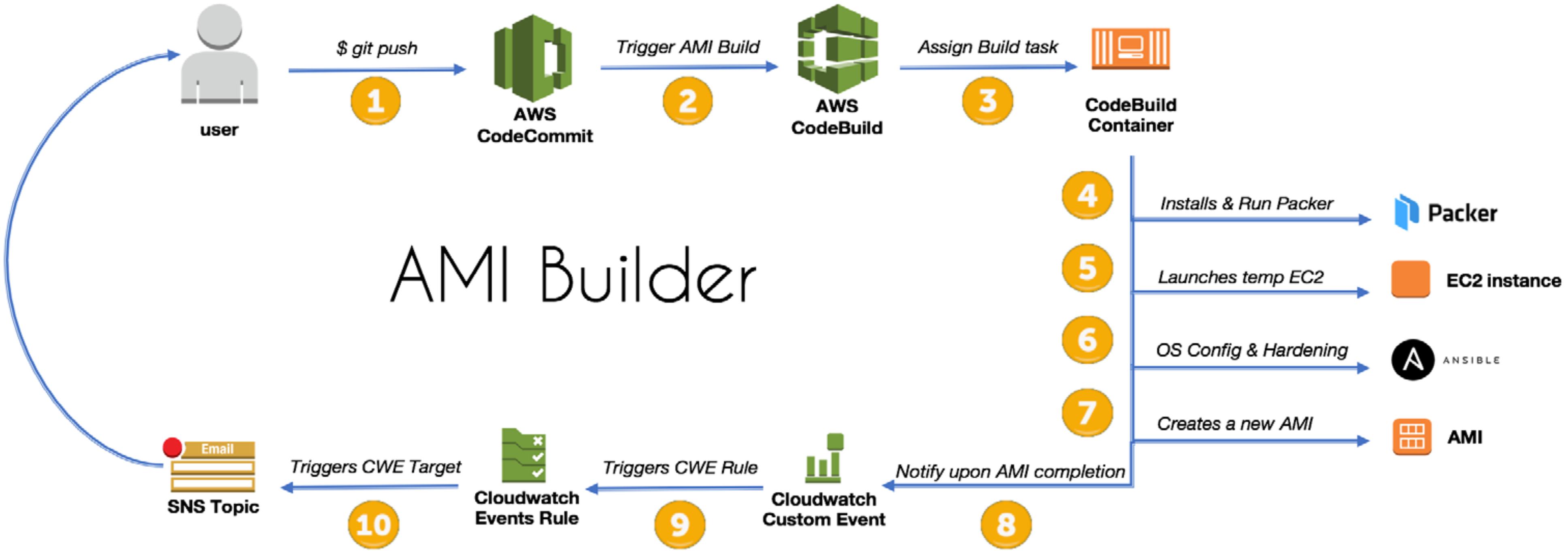
IT Security Operations, mostly manual processes

Remediation management: The NEW Way

Continual Integration and Security Assessment

SAAS & PAAS = Managed by the Cloud Service Provider

IAAS =



Source: https://aws.amazon.com/blogs/devops/how-to-create-an-ami-builder-with-aws-codebuild-and-hashicorp-packer-part-2/

Exercise

- Create two Ubuntu Virtual Machines on the same network
- On one machine, install and configure OpenLDAP:
  - https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-a-basic-ldap-server-on-an-ubuntu-12-04-vps
- Configure the second machine to authenticate to the LDAP server:
  - https://www.digitalocean.com/community/tutorials/how-to-authenticate-client-computers-using-ldap-on-an-ubuntu-12-04-vps

Q: Can you login on the second machine with the account defined in LDAP?

- Delete the two virtual machines when completed.

Thank You!