From 0 to Secure in 1 Minute

DEFCON 23

Nir Valtman & Moshe Ferber

CSAIL cloud security alliance ISRAEL

NCR

About Us

Nir Valtman | **Moshe Ferber**

Passionate about information security

Involved in numerous startups and initiatives – sometimes with success, sometimes not…

Industry speakers and lecturers – that's why we are here

- ✓ CISO Retail in NCR Corporation.
  - We own a private cloud & offering SaaS
  - Yes… we do security!
- ✓ Instructor for Cloud Security (CCSK) – that's what I really like doing

I like non-sweating sports!



I don't like sport!

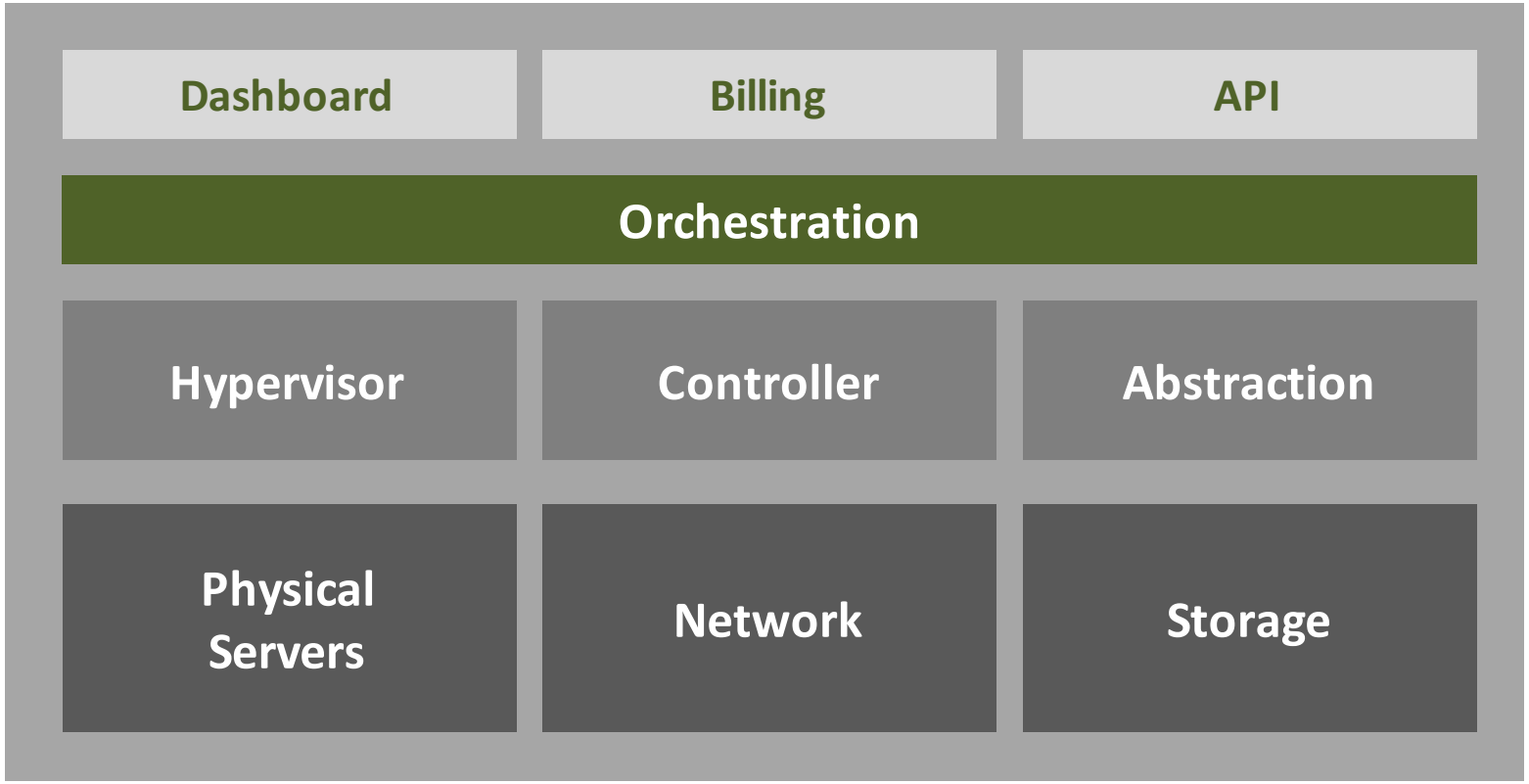
CSAIL cloud security ISRAEL alliance

NCR

About the talk

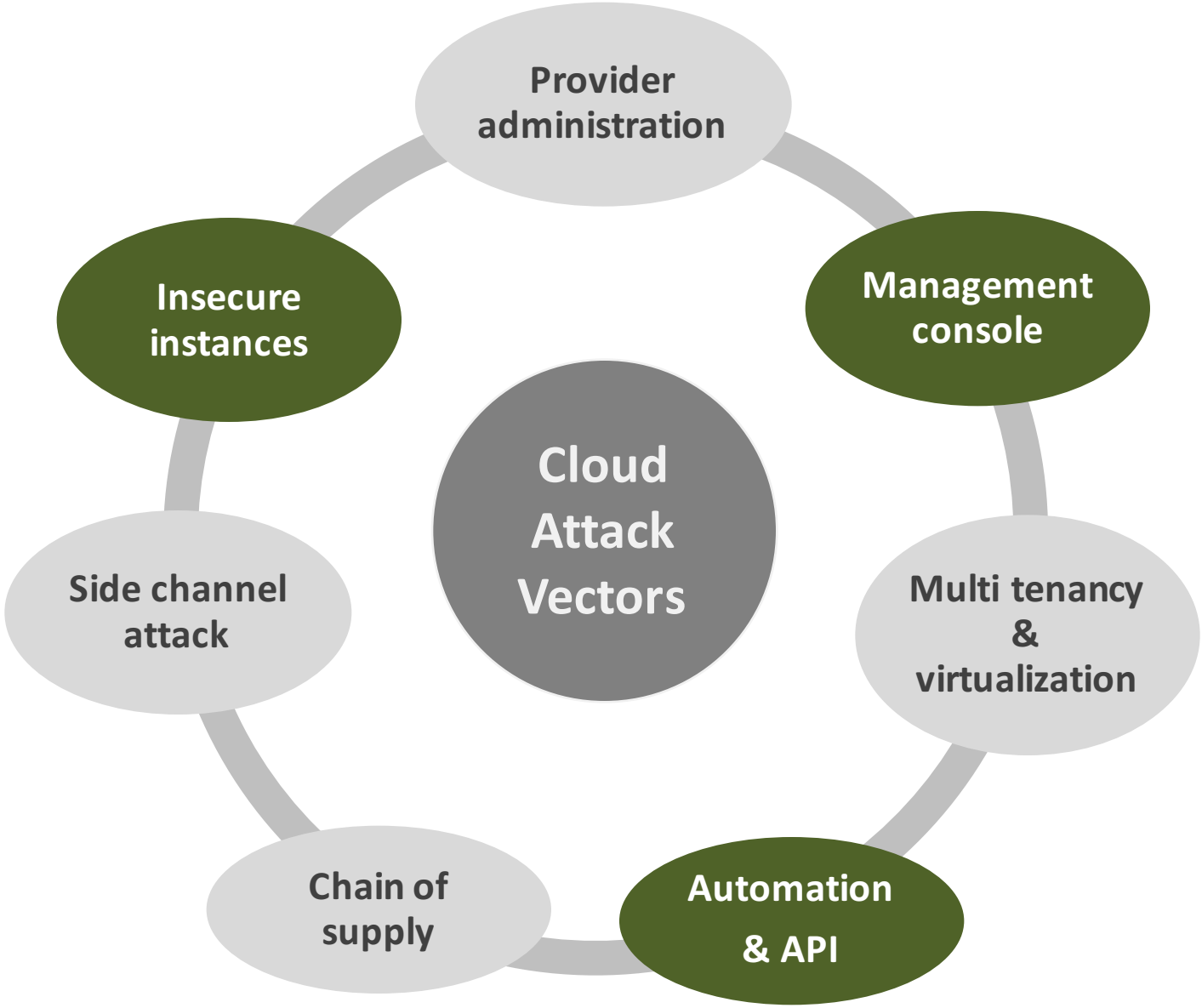
Cloud security challenges and benefits

And more specifically, using IaaS automation and orchestration features for increasing the security



CSAIL cloud security ISRAEL alliance

NCR


Provider administration
Management console
Multi tenancy & virtualization
Automation & API
Chain of supply
Side channel attack
Insecure instances
Cloud Attack Vectors

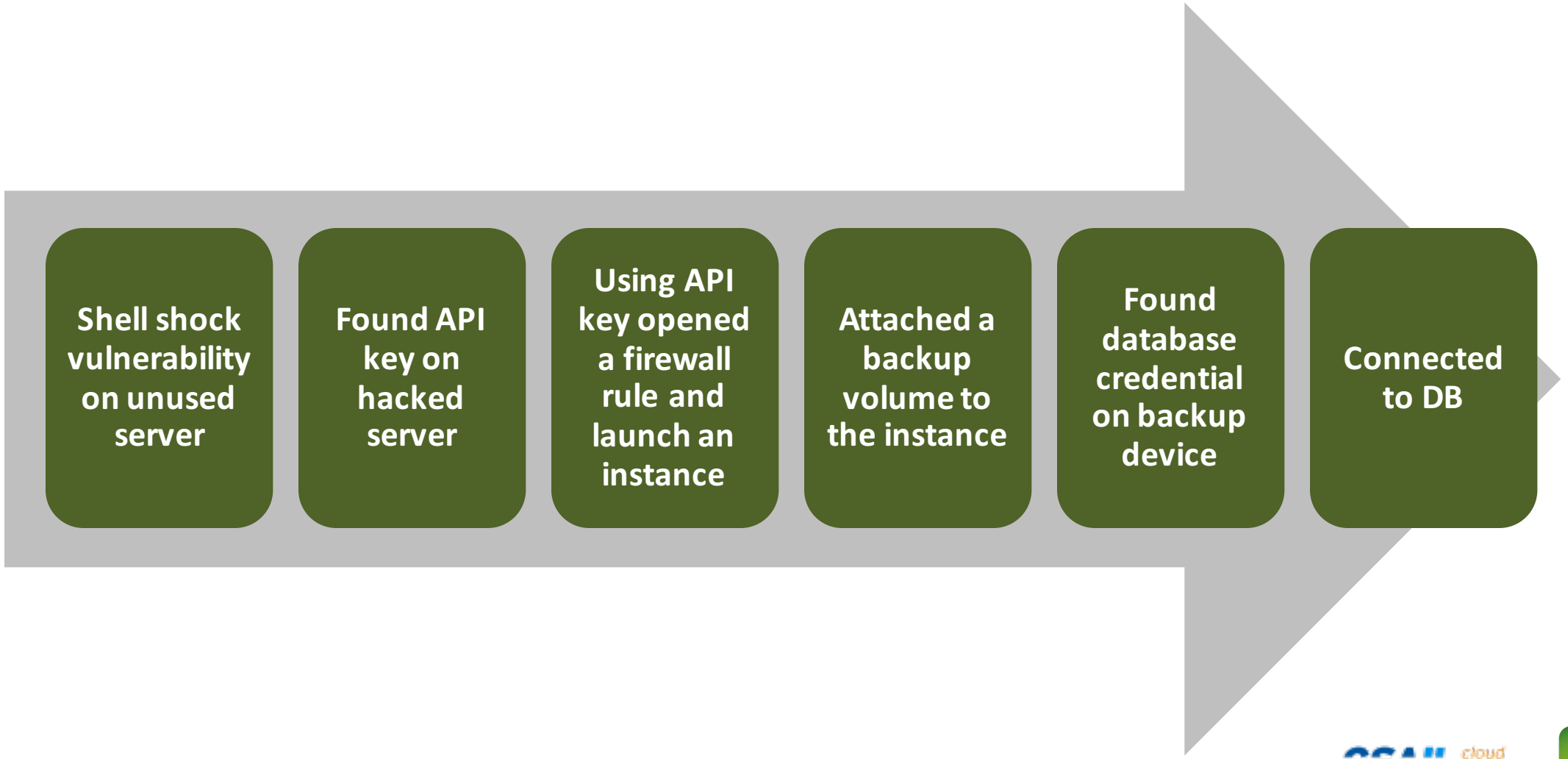
Anatomy of a cloud hack



CSAIL cloud security ISRAEL alliance

NCR

Anatomy of a cloud hack – the BrowserStack story



SOURCE: https://www.browserstack.com/attack-and-downtime-on-9-November

CSAIL cloud security ISRAEL alliance

NCR

Do we have the right tools?



Source: http://ifail.info/wp-content/uploads/2010/04/street_dentist_thumb.jpg?98bbf9

Architecture & Deployments is changing

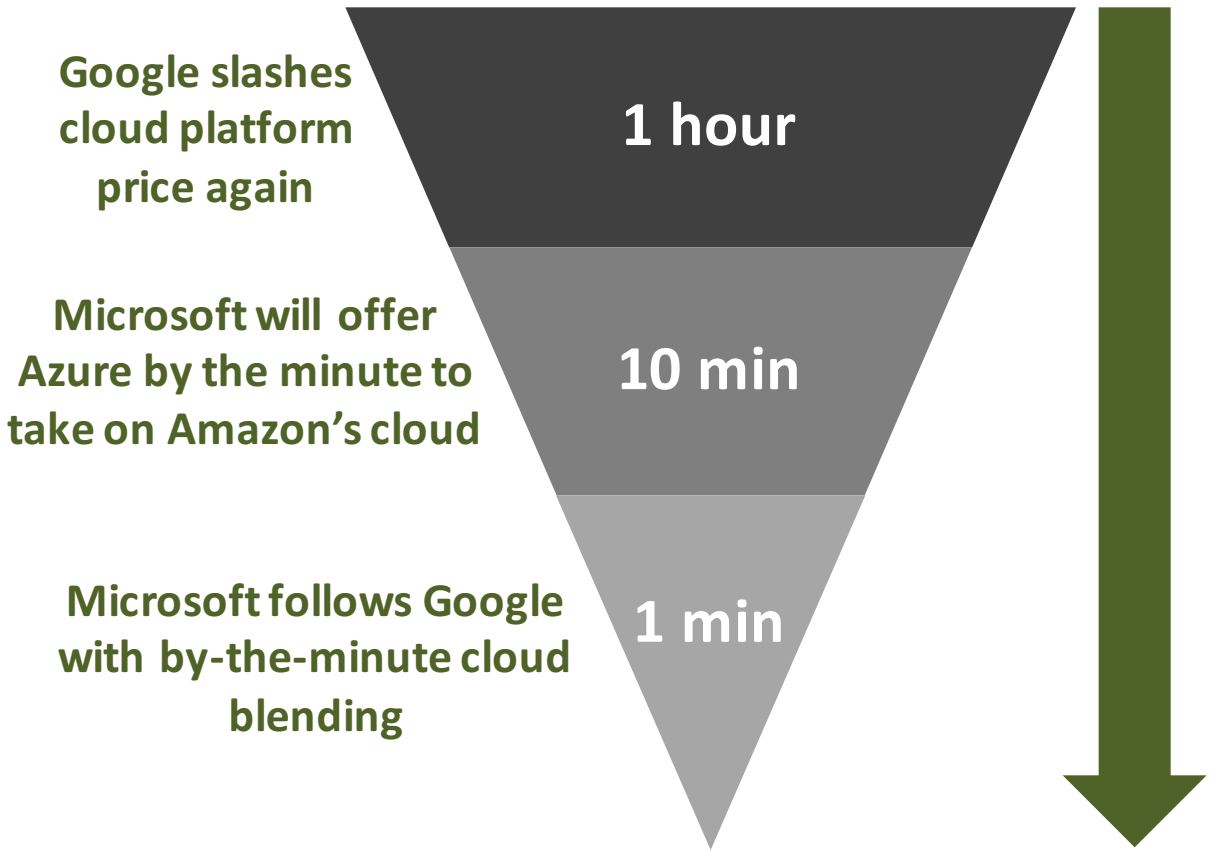
AUTO SCALING

Micro-Services Architecture

DEV OPS

Continuous Delivery

The billing cycle is reducing



CSAIL cloud security ISRAEL alliance

NCR

How to do security when servers alive for 10 minutes?

Patch management

Maintenance windows

Periodic vulnerability scanning

Hardening

CSAIL cloud security ISRAEL alliance

NCR

DON’T LET SECURITY HOLD YOU DOWN



Source: www.avon-barrier.co.uk

Introducing



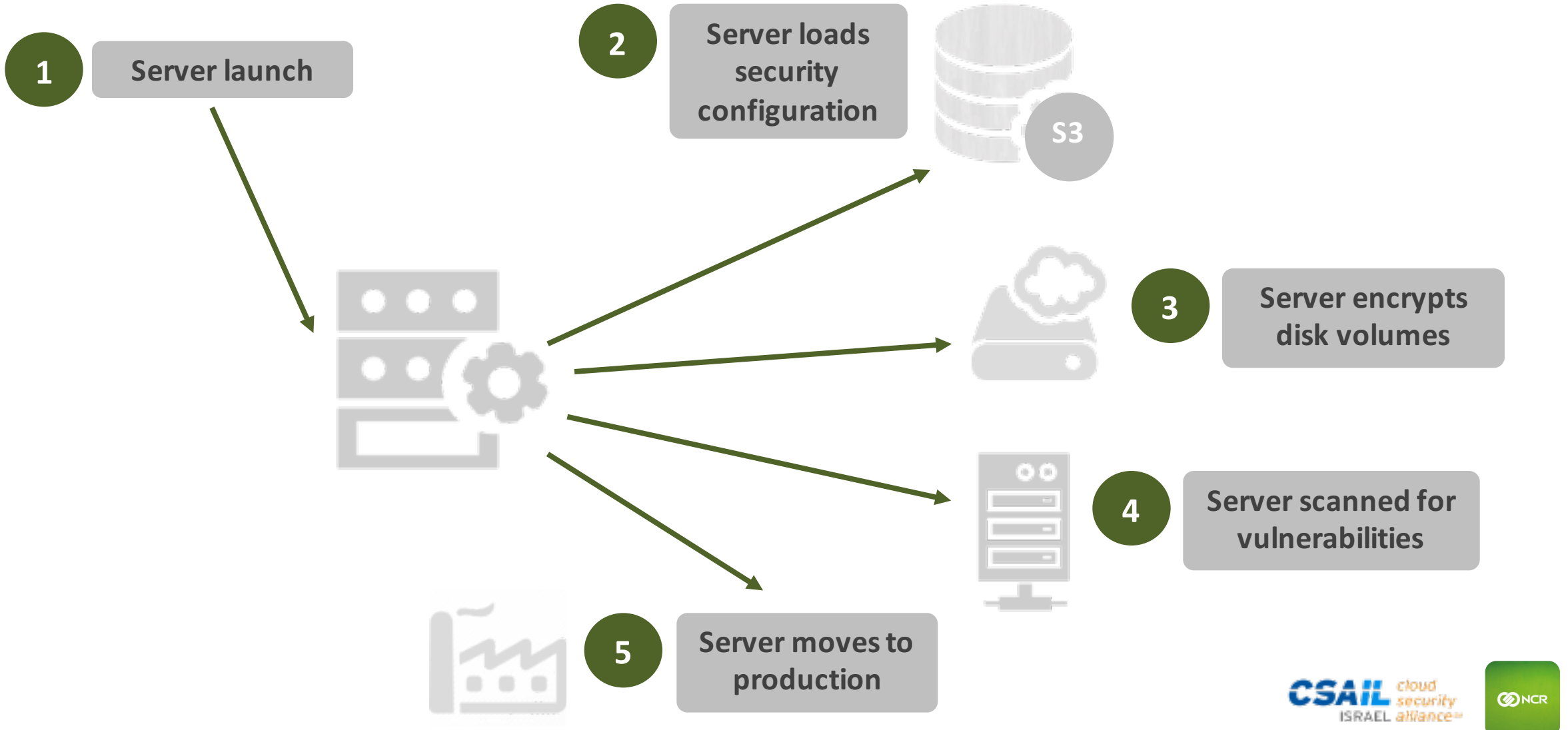
SOURCE: http://www.cloudefigo.org/

Based on the work made by Rich Mogull from Securosis
https://github.com/securosis

CSAIL cloud security ISRAEL alliance

NCR

Cloudefigo Lifecycle



Components

Object Storage



Vulnerability Scanner



Cloud-Init



Configuration Management



IAM Roles



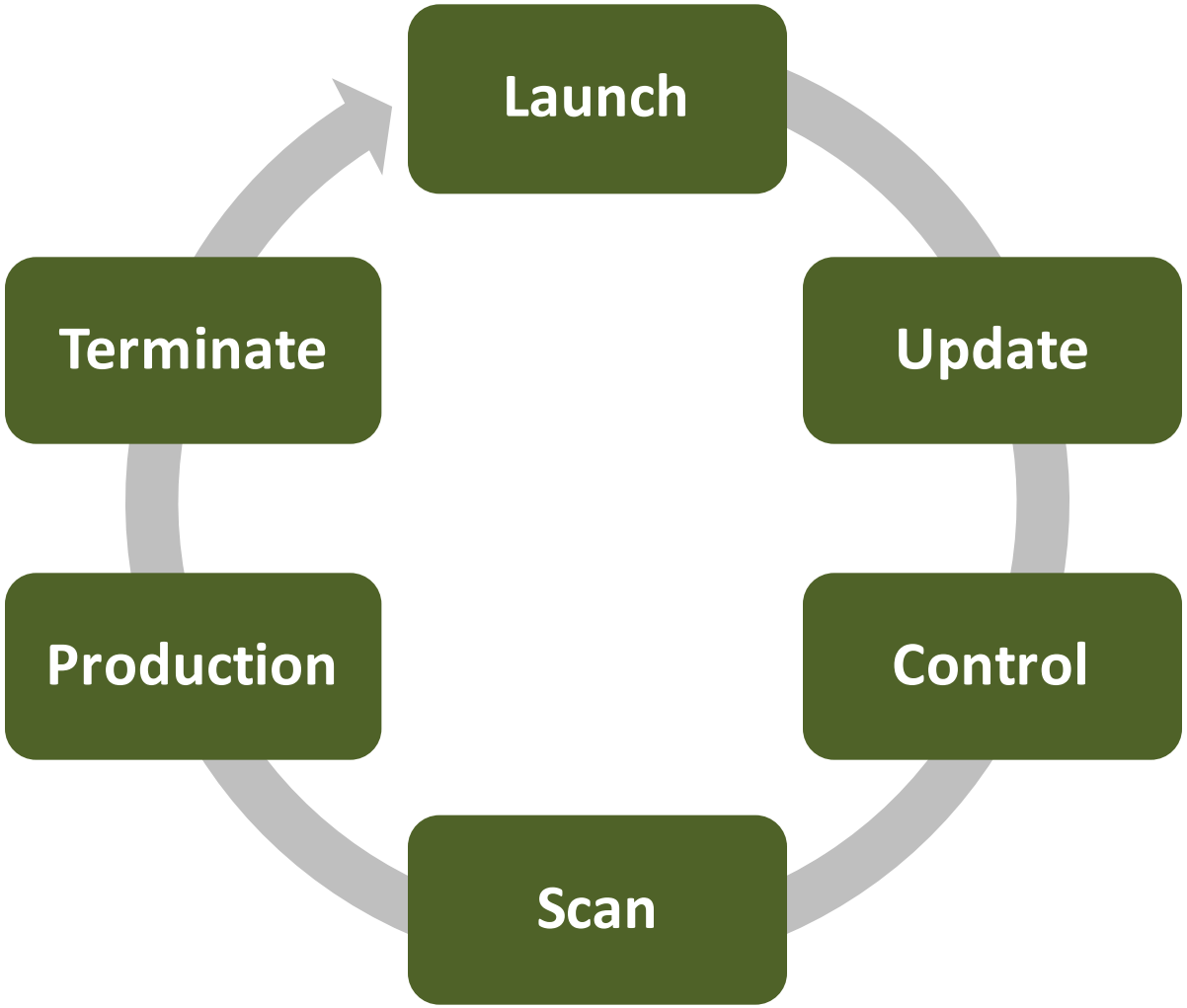
Volume Encryption



CSAIL cloud security ISRAEL alliance

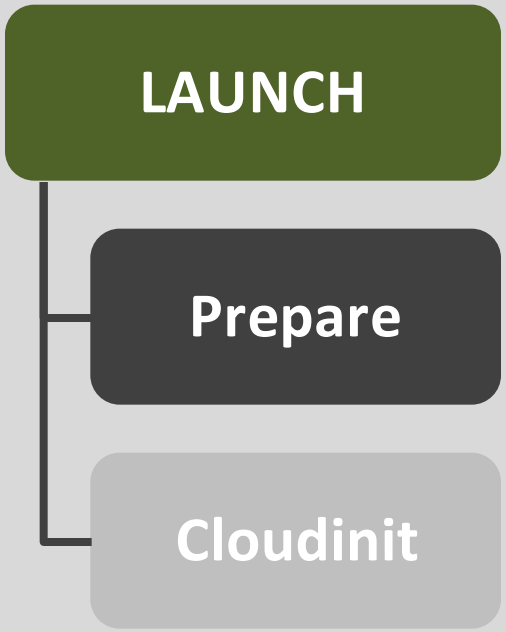
NCR

Instant Lifecycle



CSAIL cloud security ISRAEL alliance

NCR



- ✓ **Each machine manage its own attributes**
  - Encryption keys
  - Remediation vs production groups
- ✓ **Management of these attributes require permissions**
- ✓ **Permissions during launch > production**
- ✓ **Thus, a dynamic IAM role is required**

LAUNCH

Prepare

Cloudinit

IAMBasicPolicy.config

File Path : ~/PycharmProjects/CloudInit/AWS/IAMBasicPolicy.config

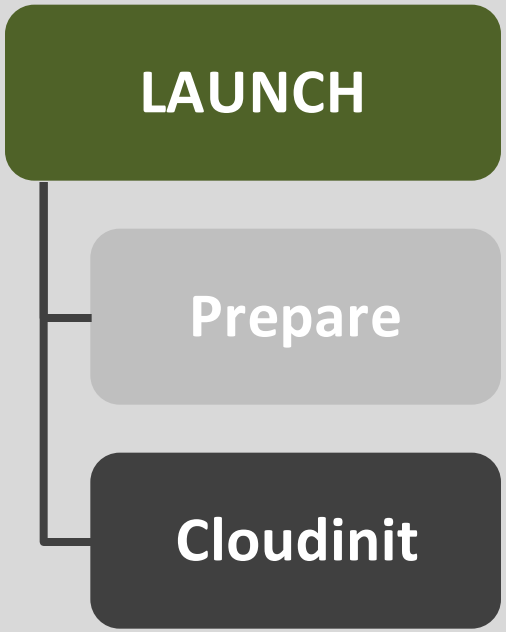
IAMBasicPolicy.config

```
{
  "Sid": "Stmt1413488885000",
  "Effect": "Allow",
  "Action": [
    "s3:CreateBucket",
    "s3:DeleteBucket",
    "s3:GetObject",
    "s3:ListBucket",
    "s3:PutBucketPolicy",
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::BUCKETNAME"
  ]
},
{
  "Sid": "Stmt1413489080000",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource": [
    "arn:aws:s3:::config-cloudsec"
  ]
},
{
  "Sid": "Stmt1413548658000",
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstances",
    "ec2:DescribeSecurityGroups",
    "ec2:ModifyInstanceAttribute",
    "ec2:RunInstances",
    "ec2:CreateTags"
  ],
  "Resource": [
    "*"
  ]
},
```

Line 2 Col 27 (none) Unicode (UTF-8) Unix (LF) 1,301 / 82 / 64

CSAIL cloud security ISRAEL alliance

NCR



- ✓ Executed in root permissions when image is launching.
- ✓ Responsible for building the infrastructure for the following steps.

- **LAUNCH**
  - Prepare
  - Cloudinit



UPDATE

- OS update
- Pre-requisites

- ✓ CloudInit to update & upgrade software packages
- ✓ Primary goal is to make sure the cloud instance is secure once upgraded

UPDATE

OS update

Pre-requisites

- ✓ **CloudInit to install the software packages required to operate:**
  - Python + pip + wheel
  - AWS SDK (Boto)
  - Chef Client + Chef SDK (PyChef)
- ✓ **Download configurations and scripts from S3:**
  - Cloudefigo script
  - Chef client initialization files
- ✓ **Cloudinit to create and attach a volume for application files and data.**

CSAIL cloud security ISRAEL alliance

NCR

UPDATE

- OS update
- Pre-requisites



CONTROL

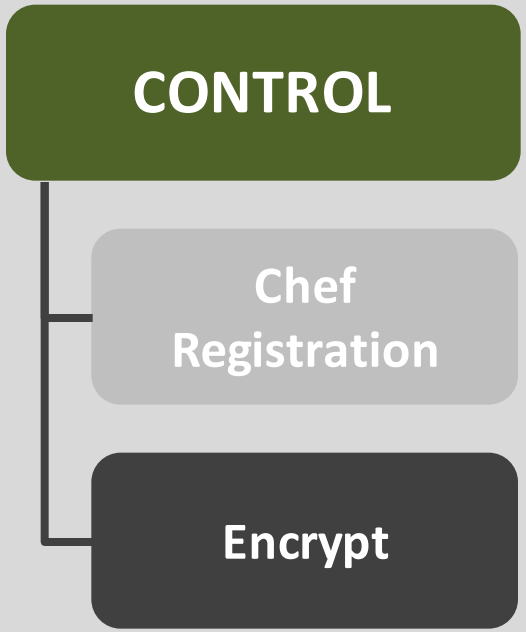
- Chef Registration
- Encrypt

- ✓ The Chef clients register to the Chef Management server using the initialization files loaded from S3.
- ✓ Once the client is registered, a policy is loaded and enforced on the instance.

CSAIL cloud security ISRAEL alliance

NCR

Where should you keep your keys?

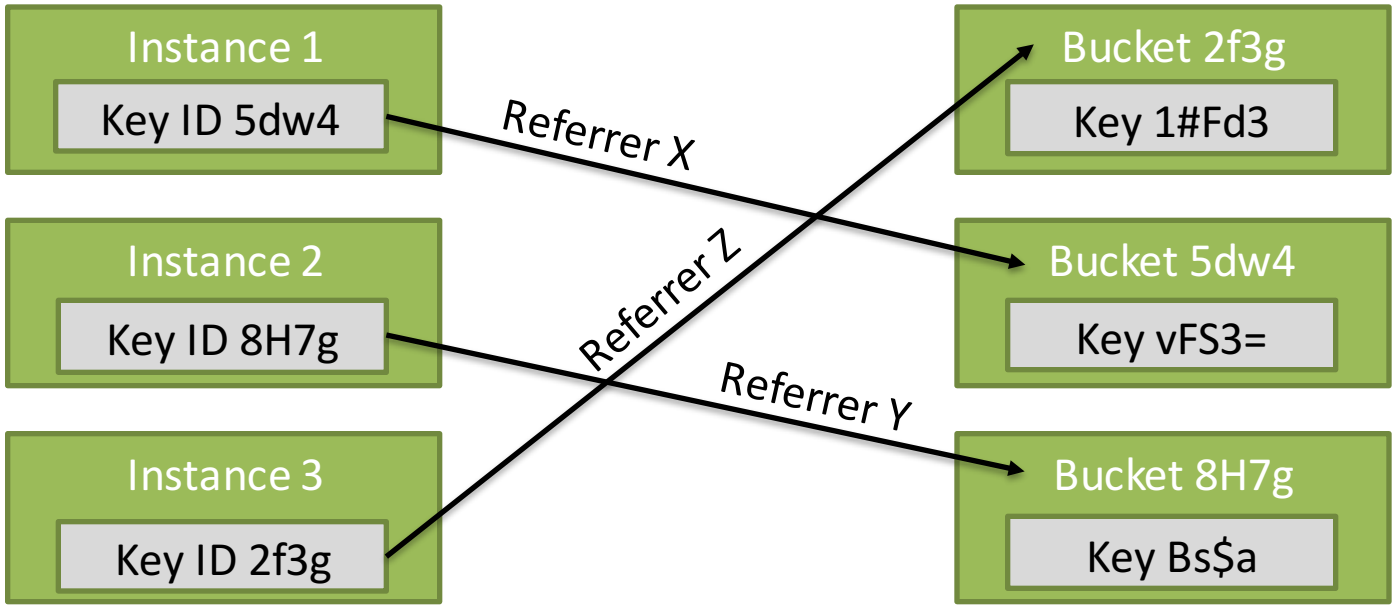


	Cloud Provider	On Premise	3rd Party
Protected	Snapshots and backups	Snapshots, backups, subpoena and malicious insiders	Snapshots, backups and cloud provider's malicious insiders
Vulnerable	Malicious insider attacks and subpoena	Key exchange attacks	Key exchange attacks and subpoena (partial)

CONTROL

- Chef Registration
- Encrypt

- ✓ **The volume to be encrypted using randomly generated key.**
  - The key is stored on S3 for later use.
- ✓ **The application database to be installed in the encrypted volume.**



CSAIL cloud security ISRAEL alliance

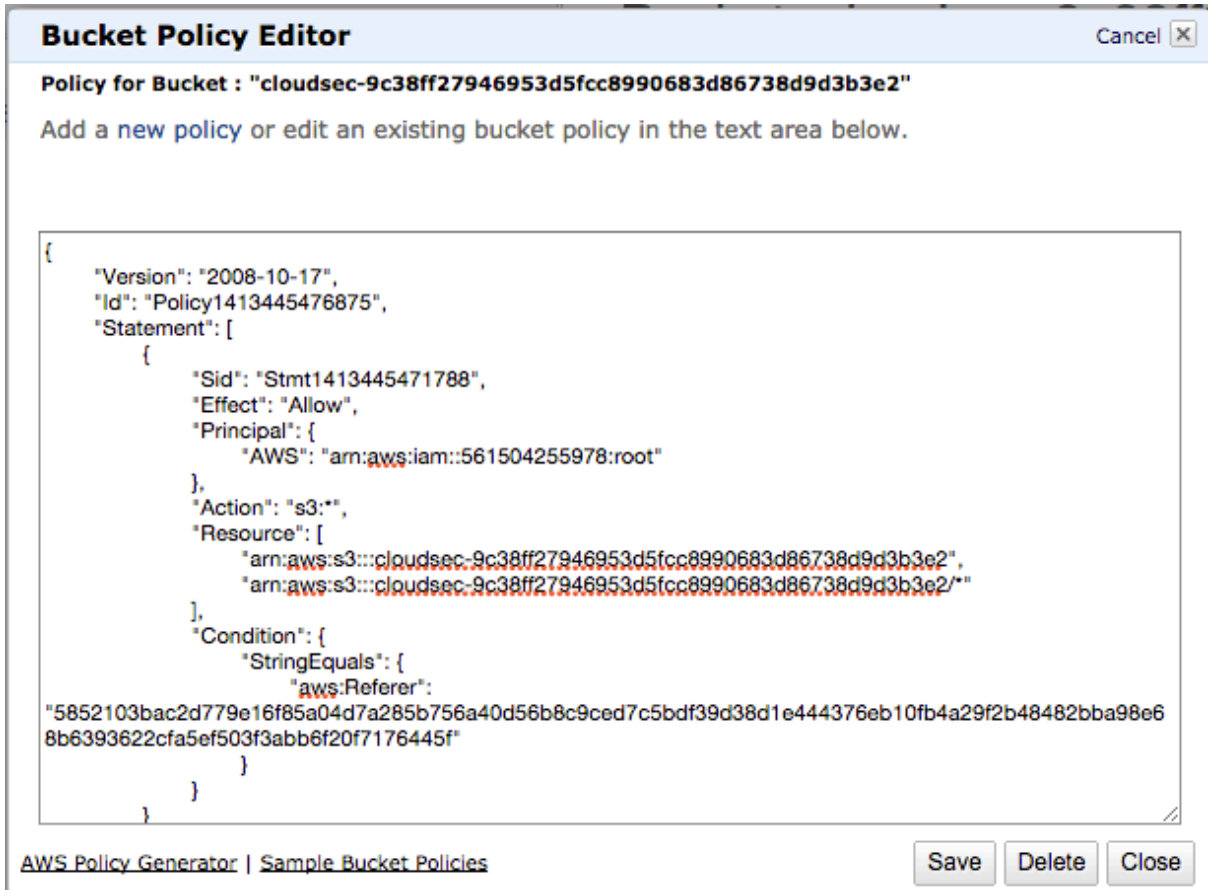
NCR

CONTROL

Chef Registration

Encrypt

- ✓ Dynamic S3 policy: access to key require a referrer header that is generated based on attributes from the instance.



CONTROL

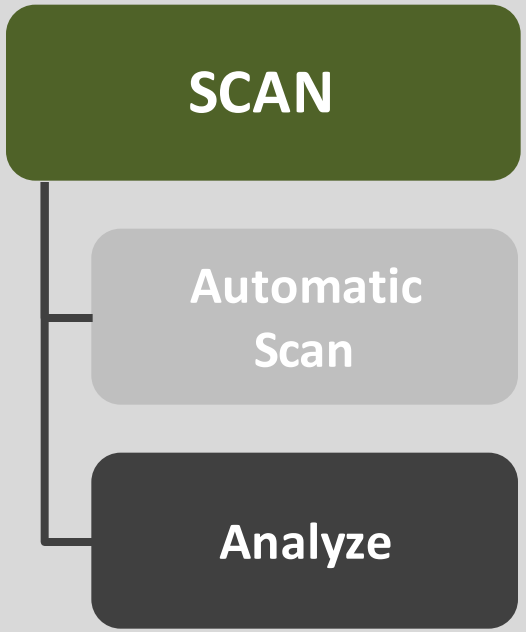
- Chef Registration
- Encrypt



SCAN

- Automatic Scan
- Analyze

- ✓ A vulnerability scan to be launched automatically by CloudInit script.
- ✓ The deeper the scan, the longer it takes to move to production.



- ✓ The results of the scan are analyzed by the Cloudefigo script.
- ✓ Based on scan results – the instance to move to production or remain in the remediation group.
- ✓ The lowest security risk severity can be defined.

SCAN

- Automatic Scan
- Analyze



CSAIL cloud security ISRAEL alliance

NCR

PRODUCTION

- Least privileged role
- Manage

- ✓ Reminder: Permissions in launch > production
- ✓ IAM role permissions reduced dynamically - contains read only access

IAMStrictPolicy.config

File Path : ~/PycharmProjects/SecureCloudInit/AWS/IAMStrictPolicy.config

IAMStrictPolicy.config

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1413489080000",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::BUCKETNAME"
      ]
    }
  ]
}
```

Line 12 Col 34 (none) Unicode (UTF-8) Unix (LF) Last saved: 10/23/14, 12:29:49 AM 260 / 19 / 17

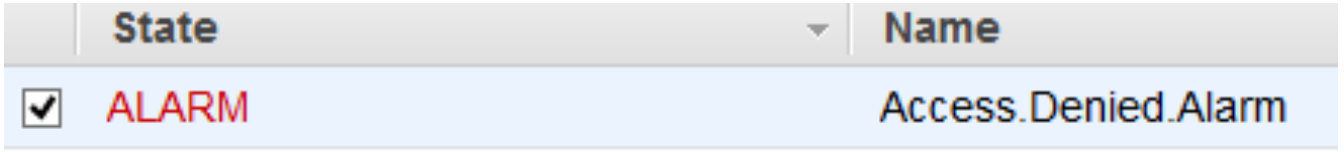
CSAIL cloud security ISRAEL alliance

NCR

PRODUCTION

- Least privileged role
- Manage

- ✓ For the ongoing operations – a compensating controls are required.
- ✓ Cloudefigo management script lists cloud instances and validates they are managed by Chef
- ✓ Cloudefigo will set alert when someone will try to use access keys.



	State	Name
☑	ALARM	Access.Denied.Alarm

CSAIL cloud security ISRAEL alliance

NCR

Setting a CloudWatch alarm

PRODUCTION

- Least privileged role
- Manage

	State	Name
☑	ALARM	Access.Denied.Alarm

Filter Pattern

```
{ ($.errorCode="AccessDenied") }
```

Filter Pattern

```
{ ($.errorCode="Client.UnauthorizedOperation") }
```

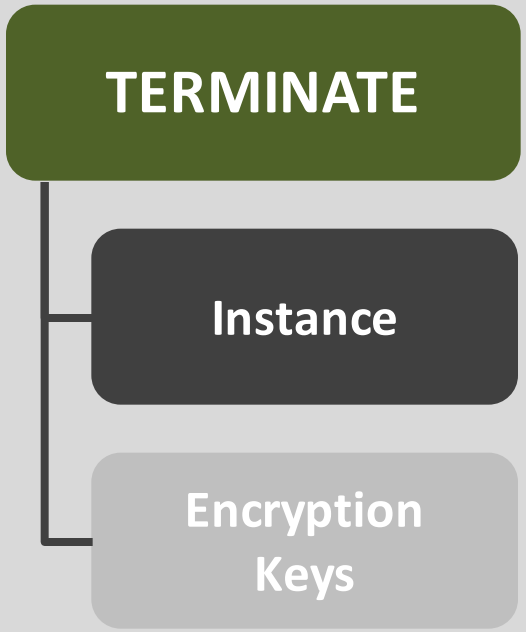
CSAIL cloud security ISRAEL alliance

NCR

PRODUCTION

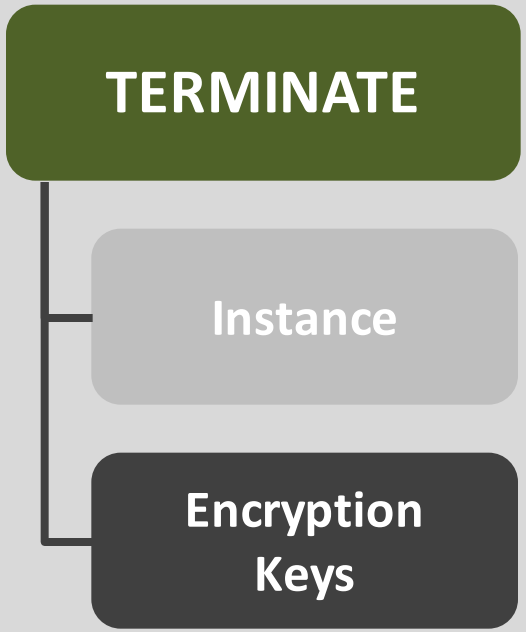
- Least privileged role
- Manage





- ✓ **The life cycle ends once a server is terminated along with:**
  - Attached volumes
  - IAM role

CSAIL cloud security ISRAEL alliance
NCR



- ✓ The instance data still exist in backups/snapshots or provider storage
- ✓ Encryption keys to be deleted with instance in order to make sure the backup data remain inaccessible (not implemented in this version)

Wrapping Up

The new software architecture and applications delivery in cloud module disrupts traditional correctives controls

We need to adopt new thinking to automate security

Think how security automation can help you in moving your infrastructure forward. Faster.

CSAIL cloud security ISRAEL alliance

NCR

Questions

Moshe Ferber

@: moshe (at) onlinecloudsec.com
w: www.onlinecloudsec.com
in: www.linkedin.com/in/MosheFerber
t: @FerberMoshe

Nir Valtman

@: nir.valtman (at) ncr.com
w: www.ncr.com | www.valtman.org
in: www.linkedin.com/in/valtmanir
t: @ValtmaNir



www.cloudefigo.org

CSAIL cloud security ISRAEL alliance

NCR