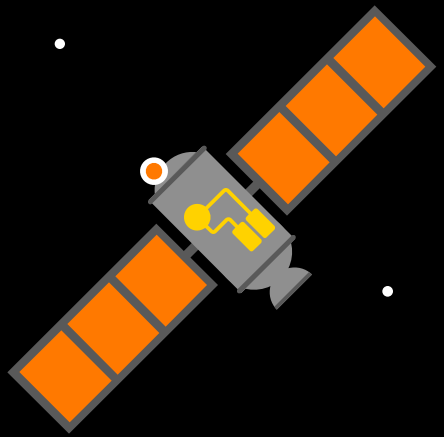
Cloud Cyber Security

Introduction to

Ioan Constantin,
Orange Romania

orange™

Smart, witty and insightful quote



Some smart lady / man

Agenda

1

Concepts & Definitions

Moving infrastructure to the cloud

Vulnerabilities in the cloud

2

Security Perimeters

Cyber Security perimeters
Physical Security Perimeters
IaaS & SaaS vs Datacenters and Hard Iron

3

Scaling Cyber Security

Virtualization and its impact on Cyber Security

Future Networks Security

IoT and 5G

4

Public versus Private Clouds

Securing the access points

Securing the infrastructure

5

Q and A

orange™

Concepts Definitions

Cloud ?

the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Moving infrastructure from datacenters to cloud – widening the security perimeter

Vulnerabilities

A computer vulnerability refers to a defect in a system that can leave it open to attack. It could also refer to any type of weakness present in a computer itself, in a set of procedures, or in anything that allows information security to be exposed to a threat.

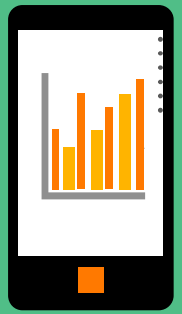
orange™

Security Perimeters

Physical Perimeter

Cyber Security Perimeter

Mobility



Datacenters

Software as a Service

Infrastructure as a Service

Hard Iron

Physical Perimeter

Assets

Sites

People

Specific vulnerabilities

Access control

Authentication

Redundancy

Availability

Monitoring

Resilience

Response

orange™

Cyber Perimeter

Assets

Cloud

People

Specific vulnerabilities

Software
Firmware
Middleware
People

Authentication
Encryption
Validation

Redundancy
Integrity
Availability

Monitor
Detect
Mitigate
Respond

Cloud security building blocks

IaaS

Infrastructure as a Service

‘Networks to go’, completely built around users specifications

SaaS

Software as a Service

Applications served from the cloud – most of the processing and data storage is done on remote servers

Datacenters

‘Data Factories’

Large, industrial-grade environments where data processing and storage is done for various IaaS / SaaS

Hard Iron

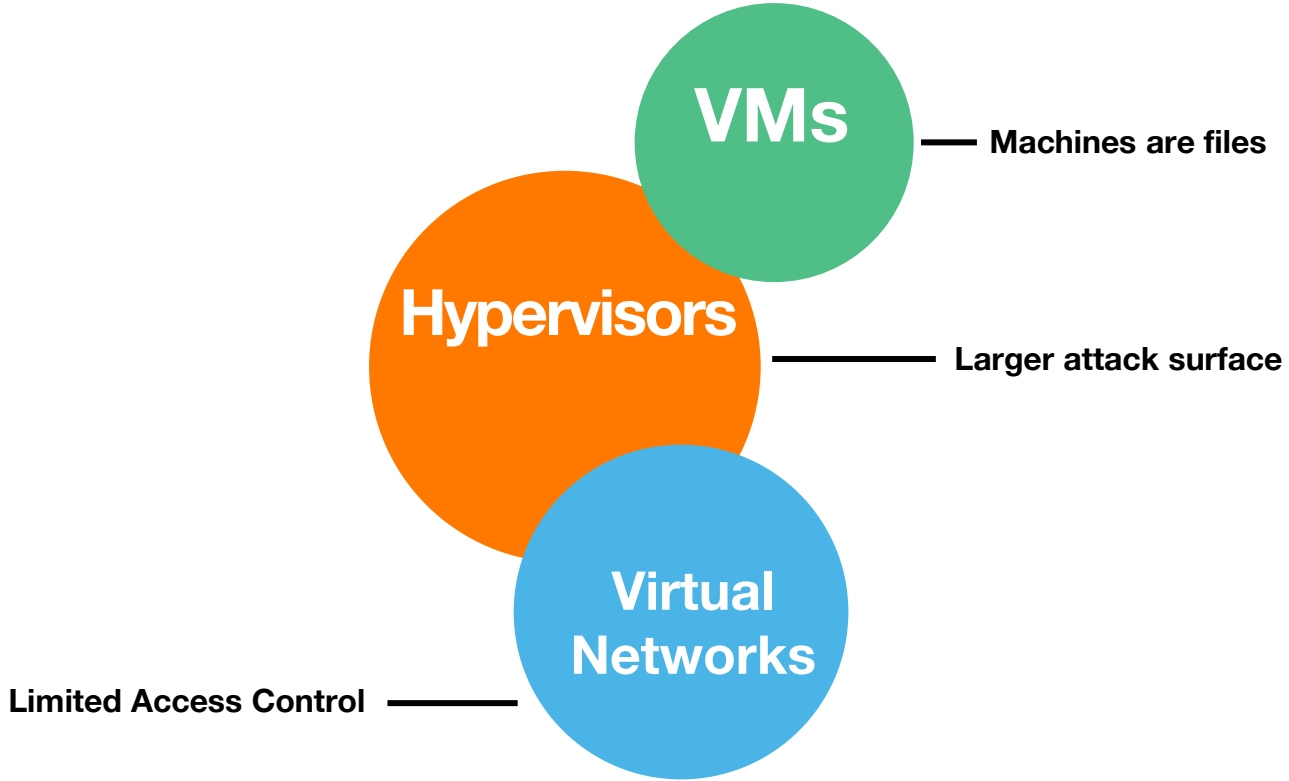
Hardware

Everything from servers, network equipment, storage units, security equipment

orange™

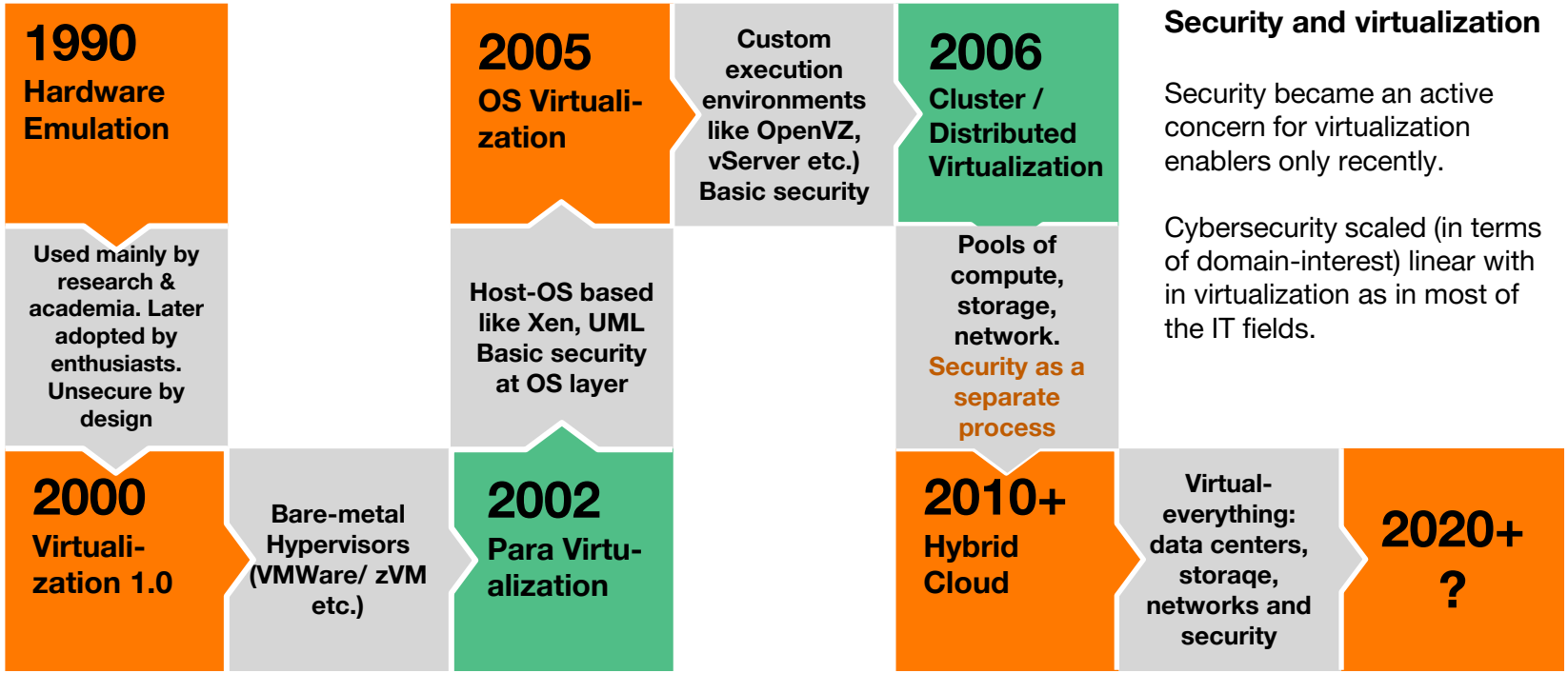
Virtualization

&challenges in cyber security



orange™

A pinch of History: Virtualization



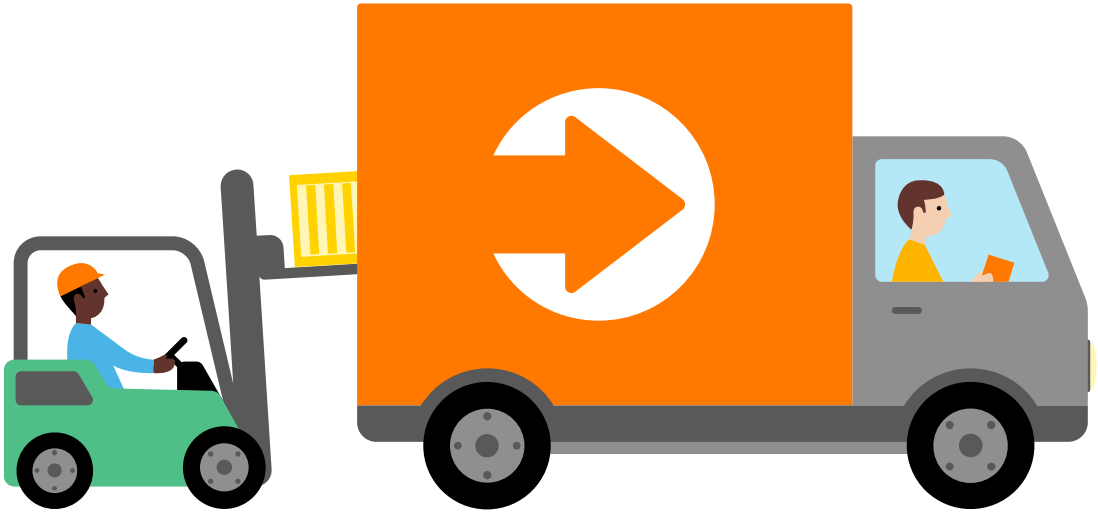
Security and virtualization

Security became an active concern for virtualization enablers only recently.

Cybersecurity scaled (in terms of domain-interest) linear with in virtualization as in most of the IT fields.

orange™

Hypervisor Vulnerabilities



A hypervisor is a software application that distributes computing resources (e.g., processing power, RAM, storage) into virtual machines (VMs), which can then be delivered to other computers in the network.

A hypervisor vulnerability can (in theory) expand the surface of attack (way) beyond the virtualization software itself to each and every VM and its respective data.

Hypervisor Security

Segregation
Separate VM & Management Networks

Cut down
on unnecessary services

Access
Set access privileges

Physical
Lock down server rooms!

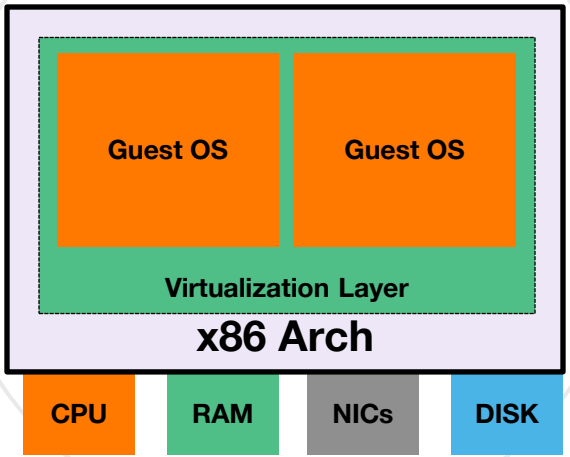
A hypervisor is a software application that distributes computing resources (e.g., processing power, RAM, storage) into virtual machines (VMs), which can then be delivered to other computers in the network.

A hypervisor vulnerability can (in theory) expand the surface of attack (way) beyond the virtualization software itself to each and every VM and its respective data.

VM Security

VMM
Most modern Virt Systems use Virtual Machine Monitoring for managing and controlling individual VMs

Isolation
VMMs usually provides isolation of several VMs running atop the same hypervisor



Trust chain
VM Security assumes that the underlying TCB (Trusted Computer Base) is also secure.

Robustness
Comes from isolation. If an attacker gains access to one VM the she or he shouldn't gain access to any other VMs

A Virtual Machine
Is a logical process (most often an operating system) that interfaces with emulated hardware and is managed by an underlying control program, i.e – a Hypervisor

orange™

Containers

?

At the most basic level, an container is a VM that virtualizes just the OS, not the underlying computer

How?

Several containers share the same underlying environment (i.e. – OS) and it's libraries while isolating apps and their spaces

Pros:

Scalability – a container deployment can host microservices

Efficiency – a container deployment translates into small overhead

LXC Docker

LXD CGManager

WSC

One thing in common:

They're all software. Software is inherently vulnerable.

Ephemereal

Multiple copies or instances of the same container can co-exist in any modern orchestration system

This diversifies attack surface

Cons:

No TCB – if the underlying OS is compromised, everything else can be compromise

OpenStack

Open-Source IaaS platform

Free & distributed

Platform for cloud computing

Modular

Compute
Networking **Storage**
Identity **Image**
Dashboard
Orchestration
Workflow **Database**
Messaging **DNS** **FS**
Search **RCA**

Compatibility

APIs

OpenStack can interact with EC2 and Google Compute Engine

Distribution

Public Cloud or On-Premises

IaaS or Appliance, Hosted or On-Premise

Security

OpenStack is secure

Because of large-scale adoption and large-enterprise deployments, OS is generally secure. There has been just one critical vulnerability reported in the past 8 years.

orange™

VMWare

Closed source Virtualization

Closed & Supported

VMWare is ubiquitous.

It is used everywhere from Desktop Virtualization to large-scale ‘clouds’

Hypervisors

Hypervisor-Based

Scales both horizontally and vertically

Cloud Deployment

vRealize

Dedicated Cloud Management Platform – VMWare Cloud Foundation that suports VDI (Virtual Desktop Infrastructure)

Distribution

Public Cloud or On-Premises

IaaS or Appliance, Hosted or On-Premise

Security

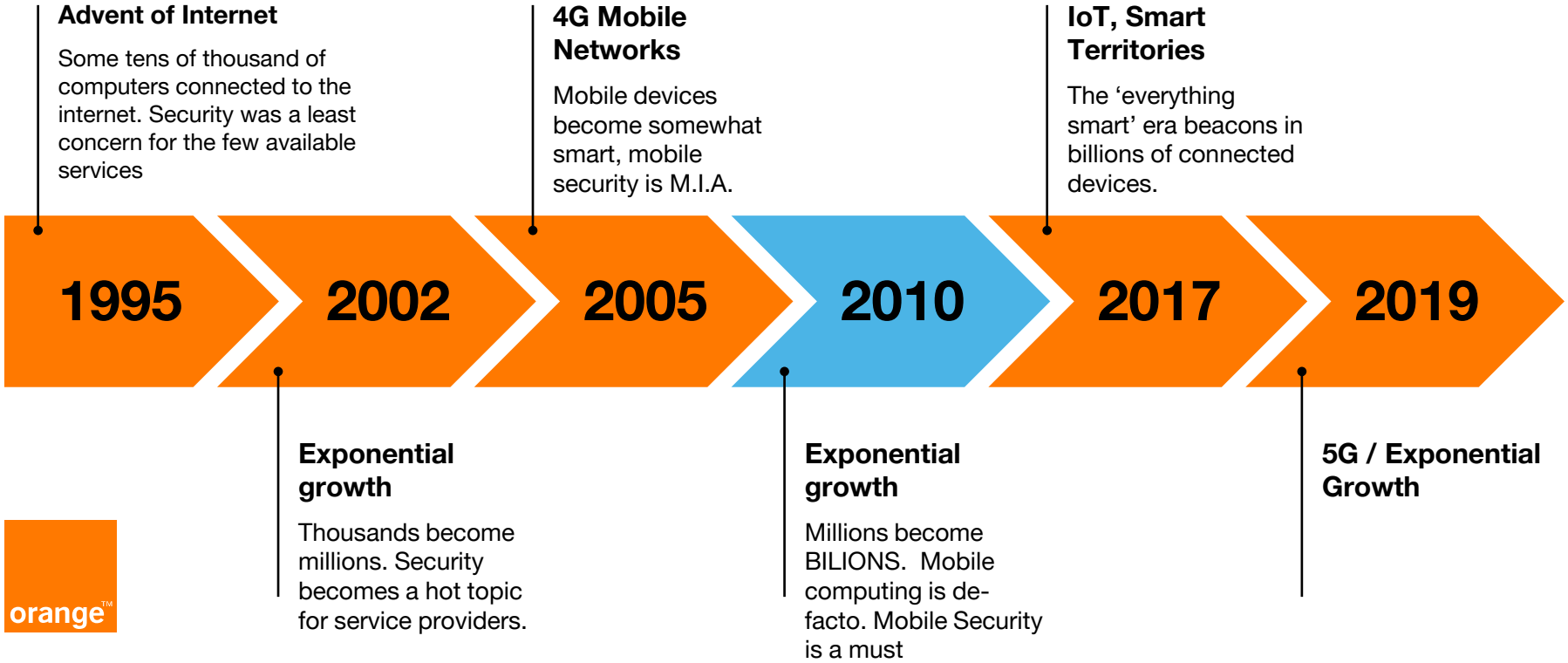
On-Stack NSX Security

VMWare uses custom SDN-type network virtualisation, secure-by-design

orange™

Expanding the perimeter

The attack surface is ever-expanding

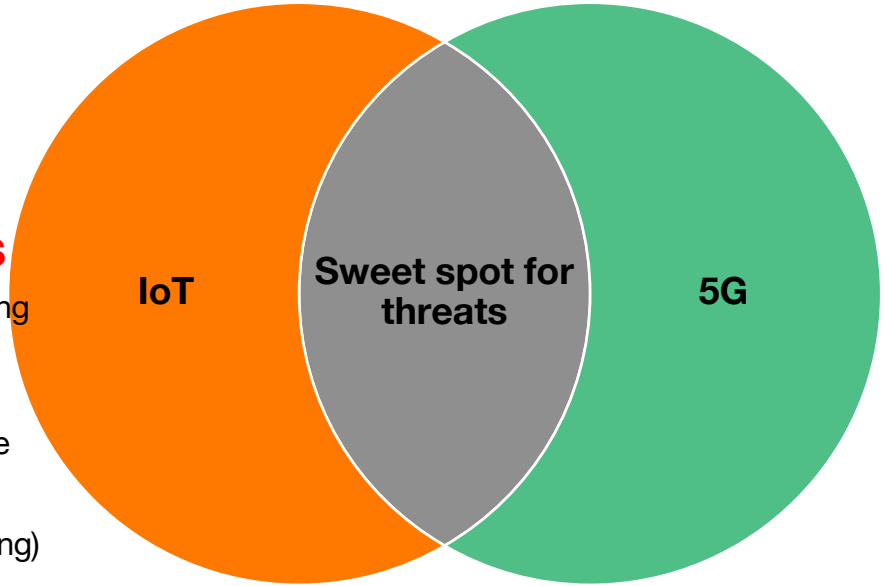


Future Technology Security

IoT is widespread. It will become ubiquitous in the near future

SECURITY CHALLENGES

- Insufficient testing & updating
- Brute forcing + default passwords
- IoT Malware + Ransomware
- IoT-based botnets
- Data security (data harvesting)
- A.I. and automation



5G is the next big thing to happen to societies and economies

SECURITY CHALLENGES

- New (and disruptive) business models
- SDN/NFV Architecture
- End2End security for Verticals
- Lack of uniformity of security management framework
- Lack of flexibility in security architecture (for different network slices)

orange™

Public versus Private Clouds

Is cyber security impacted by one main differentiator?

Spoilers: YES

Circling back to Perimeters

Private Cloud

On-Site

All components are hosted on-site, in the enterprise security perimeters

Private Perimeter

Limited attack surface

Access control, monitoring and response is performed in a defined, controlled and predictable environment

Public Cloud

Off-Site

All components and data are hosted on a 3rd party's services. The circle of trust must be expanded to encompass the provider

Public Perimeter

Large attack surface

One successful attack against a cloud provider (SaaS or IaaS) could lead to widespread compromise for any and all components and data hosted by them

orange™

Securing the infrastructure

Current-gen security

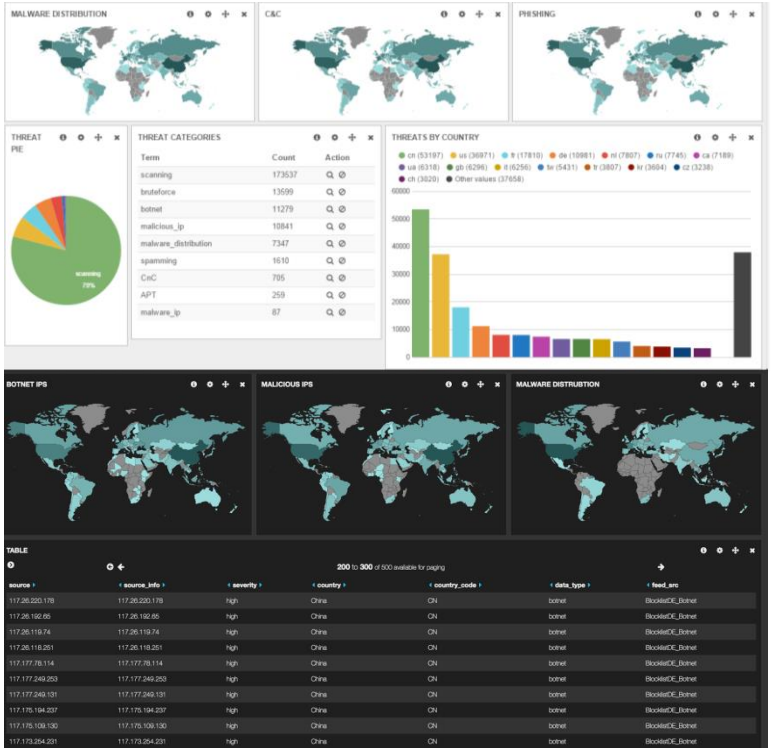
Firewalls, IPS/IDSs, Anti-DDoS, AV, AntiSpam, E-Mail Security, WAFs, URL Filters, et. all. They each play a very important part in providing a reasonable security level for large-scale cloud infrastructures

Next-gen security

A.I.-driven threat hunting, APT-hunting, Bot-net hunting, Phishing detection and prevention etc. The advent of 5G, IoT and widespread use of all-things-'smart' means that a cloud provider MUST use next-gen tools to protect against next-gen threats

Monitoring

Automation is great. A Security Operations Center is a MUST.



Thanks ☺