Cloud Computing
Critical Areas of **Focus**

Meetup #4
IT Audit & Security
Sharing in the Cloud

PUBLIC
Public Release Authorized

ABOUT ME

herwonowr@indonesiancloud.com
linkedin.com/in/herwonowr
@HerwonoWr

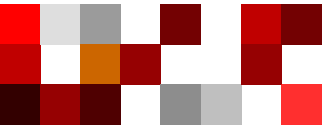
HERE IS A LITTLE BIT ABOUT ME

Herwono W. Wijaya

Head of Cyber Security Division

He started his career in IT industry for more than 10 years ago, started as a programmer and a Linux system engineer with experience in various IT projects both in Indonesia and outside Indonesia, while security (hacking) itself is his hobby.
Now he is more active as a security professional that focuses on the implementation of security as a business enabler for the organization and he also learn a lot about virtualization and cloud computing technology and sometimes still doing the programming in his spare times. He held certification of C | EH, VMware vExpert.

At IndonesianCloud he's responsible as a head of the cybersecurity division and cybersecurity business unit. He's responsible for all relevant compliance, and IT security in the organization and also to ensure target achievement of the cybersecurity business unit.



AGENDA

- OVERVIEW
- CLOUD COMPUTING INTRODUCTION
- CRITICAL AREAS IN CLOUD COMPUTING
- BONUS
  Taking over Docker host from Container
  (Portainer, Docker, & CoreOS)

OVERVIEW

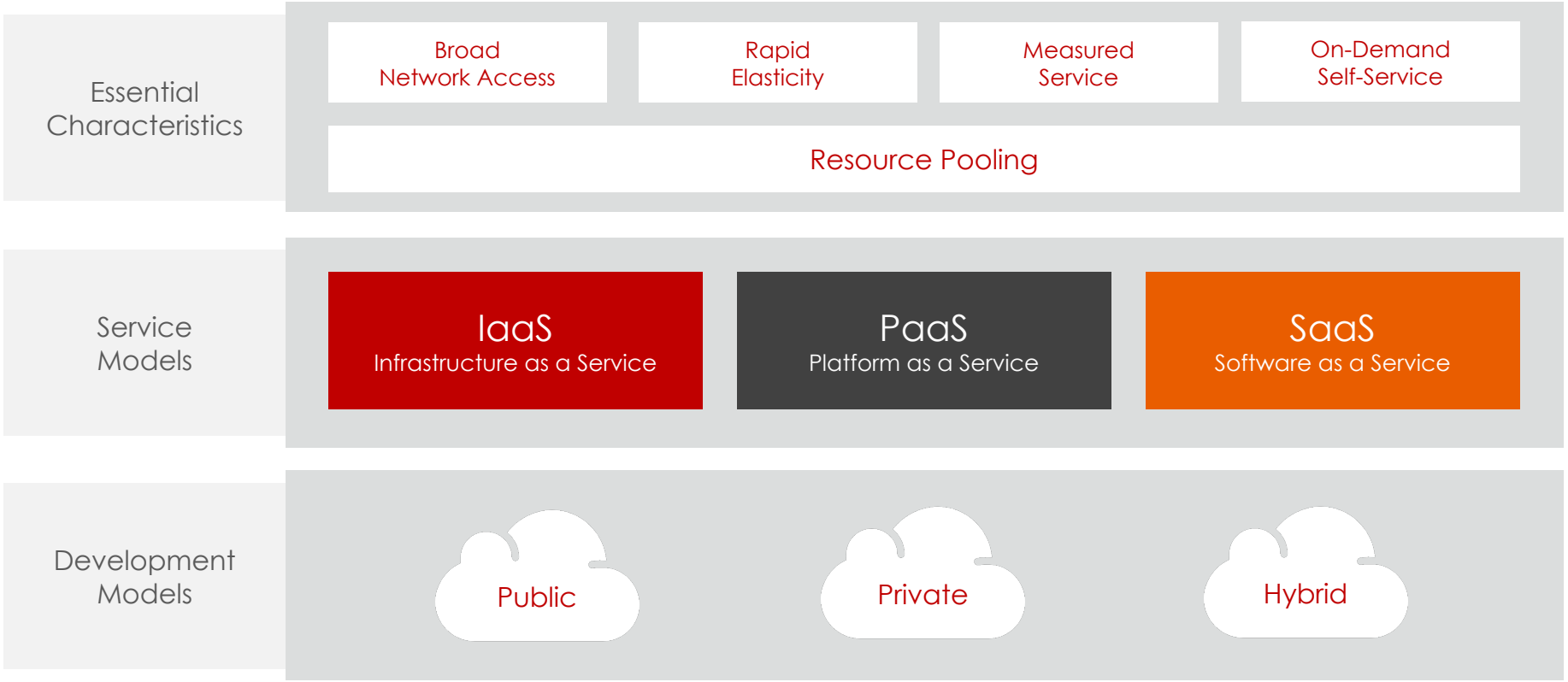
The rise of cloud computing as an ever evolving technology brings with it a number of opportunities and challenges.

We need to focus on
Critical areas of focus to mitigating the risks associated with the adoption of cloud computing technology.

CLOUD COMPUTING INTRODUCTION

Cloud Computing Definition

Cloud computing is a new operational model and set of technologies for managing shared pools of computing resources.



CLOUD COMPUTING INTRODUCTION con't

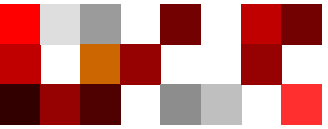
Cloud Computing Models

Who owns and manages?

	Infrastructure **Managed By**	Infrastructure **Located**	Accessible and **Consumed By**
Public	Third-Party Provider	Off-Premises	Untrusted
Private	Organization / Third-Party Provider	On-Premises / Off-Premises	Trusted
Hybrid	Both Organization & Third-Party Provider	Both On-Premises & Off-Premises	Trusted & Untrusted

CLOUD COMPUTING INTRODUCTION con't

Security Responsibilities



CRITICAL AREAS IN CLOUD COMPUTING

Critical Areas of Focus

DOMAIN 01 Governance and Enterprise Risk Management	**DOMAIN 02** Legal Issues, Contracts and Electronic Discovery	**DOMAIN 03** Compliance and Audit Management	**DOMAIN 04** Information Governance
DOMAIN 05 Management Plane and Business Continuity	**DOMAIN 06** Infrastructure Security	**DOMAIN 07** Virtualization and Containers	**DOMAIN 08** Incident Response, Notification and Remediation
DOMAIN 09 Application Security	**DOMAIN 10** Data Security and Encryption	**DOMAIN 11** Identity, Entitlement, and Access Management	

CRITICAL AREAS IN CLOUD COMPUTING con't

DOMAIN

01

Governance and Enterprise Risk Management

What we need to focus on

- Identify the shared responsibilities of security and risk management
- Understand how a contract affects your governance
- Develop a process for cloud provider assessments
- Align risk requirements to the specific assets
- Create a specific risk management and risk acceptance/mitigation methodology
- Use controls to manage residual risks
- Use tooling to track approved providers based on asset classification

CRITICAL AREAS IN CLOUD COMPUTING con't

DOMAIN

02

Legal Issues, Contracts and Electronic Discovery

What we need to focus on

- Understand the relevant legal and regulatory frameworks
- Understand the policies, requirements and capabilities
- Conduct a comprehensive evaluation of a proposed cloud service
- Understand how cloud provider physically operates and stores information

CRITICAL AREAS IN CLOUD COMPUTING con't

DOMAIN

03

Compliance and Audit Management

What we need to focus on

- Understand the compliance obligations
- Understand the scope of assessments and certifications, including both the controls and the features/services covered
- Select auditors with experience in cloud computing
- Keep a register of cloud providers used

CRITICAL AREAS IN CLOUD COMPUTING con't

DOMAIN

04

Information Governance

What we need to focus on

- Determine your governance requirements
- Ensure information governance policies and practices extend to the cloud
- Use the data security lifecycle to help model data handling and controls (Don't bring bad habits)

CRITICAL AREAS IN CLOUD COMPUTING con't

DOMAIN

05

Management Plane and Business Continuity

What we need to focus on

- Management plane (metastructure) security
  - E.g. Consistently implement least privilege accounts for metastructure access
- Business continuity
  - Take a risk-based approach to everything
  - Consider your DR plan

CRITICAL AREAS IN CLOUD COMPUTING con't

DOMAIN

06

Infrastructure Security

What we need to focus on

- Know the infrastructure security of your provider or platform
  - Make sure your provider is following cloud infrastructure best-practices and regulations
- Understand your network security
- Understand and comply with cloud provider limitations on vulnerability assessments and penetration testing

CRITICAL AREAS IN CLOUD COMPUTING con't

DOMAIN

07

Virtualization and Containers

What we need to focus on

- Understand Virtualization Security
  - Understand the capabilities offered by cloud providers as well as any security gaps
  - Properly configure virtualization services
- Understand Containers Security
  - Understand the security isolation capabilities
  - Ensure that only approved, known, and secure container images can be deployed

CRITICAL AREAS IN CLOUD COMPUTING con't

DOMAIN

08

Incident Response, Notification and Remediation

What we need to focus on

- Understand the SLAs and setting expectations around what the customer does versus what the provider does
- Set up proper communication paths with the provider
- Understand the content and format of data that the cloud provider will supply for analysis purposes
- Continuous monitoring
- Understand your incident response plan and how those change in the cloud

CRITICAL AREAS IN CLOUD COMPUTING con't

DOMAIN

09

Application Security

What we need to focus on

- Understand the new architectural options and requirements in the cloud
- Build security into the initial design process
- Reviewing SDLC basics and how those change in the cloud
- Understand the security capabilities of your cloud providers to leveraging cloud capabilities for more secure cloud applications

CRITICAL AREAS IN CLOUD COMPUTING con't

DOMAIN

10

Data Security and Encryption

What we need to focus on

- Understand the specific capabilities of the cloud platform you are using
- Don't dismiss cloud provider data security. In many cases it is more secure than building your own, and comes at a lower cost
- Create an entitlement matrix for determining access controls
- Use the appropriate encryption option based on the threat model for your data, business, and technical requirements
- Consider use of encryption and storage options
- Leverage architecture to improve data security
- Ensure both API and data-level monitoring are in place

CRITICAL AREAS IN CLOUD COMPUTING con't

DOMAIN

11

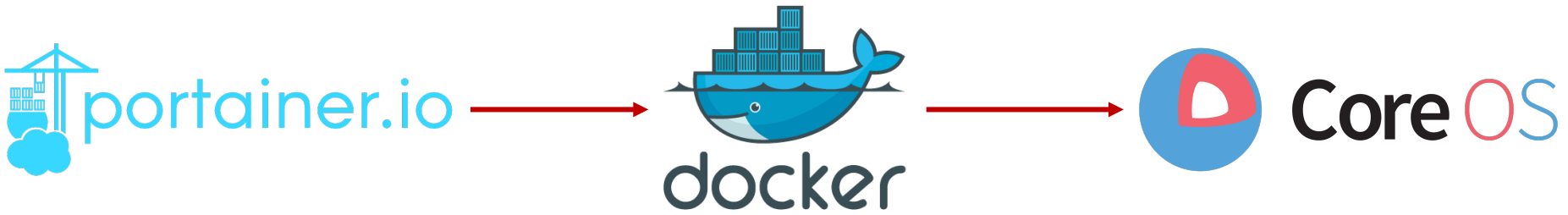
Identity, Entitlement, and Access Management

What we need to focus on

- Organizations should develop a comprehensive and formalized plan and processes for managing identities and authorizations with cloud services
- Develop an entitlement matrix for each cloud provider
- Prefer Attribute-based access control (ABAC) over Role-based access control (RBAC) for cloud computing

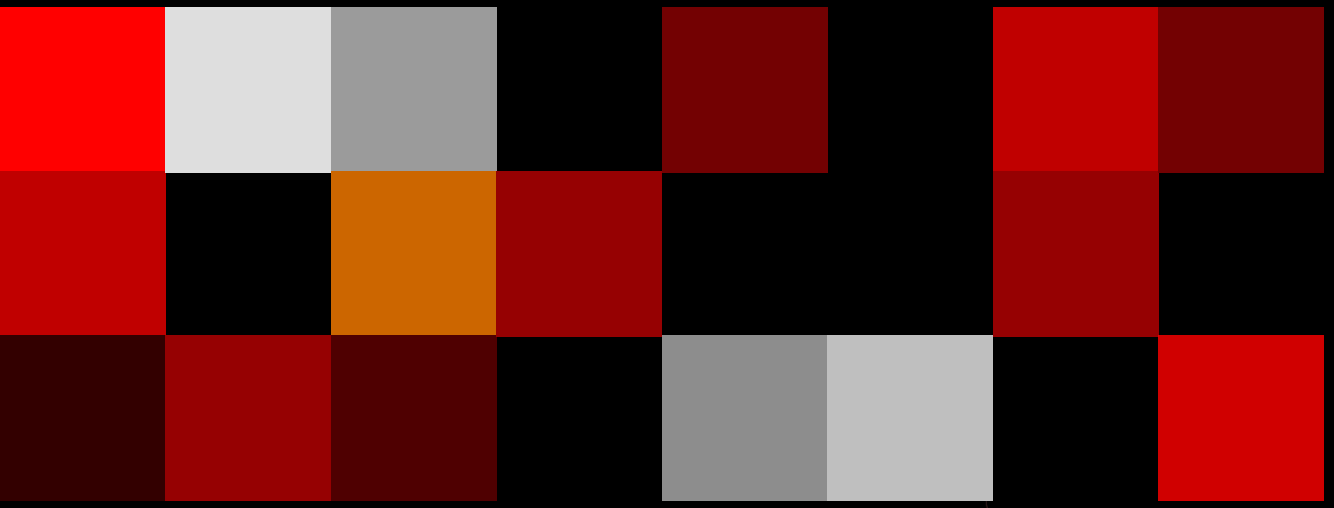
BONUS

Taking over Docker host from Container



Container Management | Docker Engine | Host Operating System

DEMO TIME



Thank You!