SEAS-8405

Week-1: Foundation of Cybersecurity Architecture

Dr. Mallarapu // 2025-03-22

Expectations

What to Expect in This Course

1. Case Study-Based Learning

- Defense in depth, MITRE frameworks, DevSecOps, and cloud-native security are crucial *but not foolproof.*
- Major corporations *still* suffer significant security incidents.
- Primary culprits: Zero-day exploits and Advanced Persistent Threats (APTs).
- We need a paradigm shift: Architecture-Centric Security
- This course will primarily focus on analyzing, learning, and designing architecture based on real-world case studies

2. Analyzing Major Cybersecurity Hacks

- We will examine **8-9 major cybersecurity breaches** over the last 15 years.

Expectations

What to Expect in This Course

4. Semester Activities & Praxis

- The class will engage in hands-on activities throughout the semester that will indirectly help with your **praxis.**

5. Homework

- Will be multiple-choice questions based on your understanding of the lectures and case studies.

6. Mid-terms and Finals

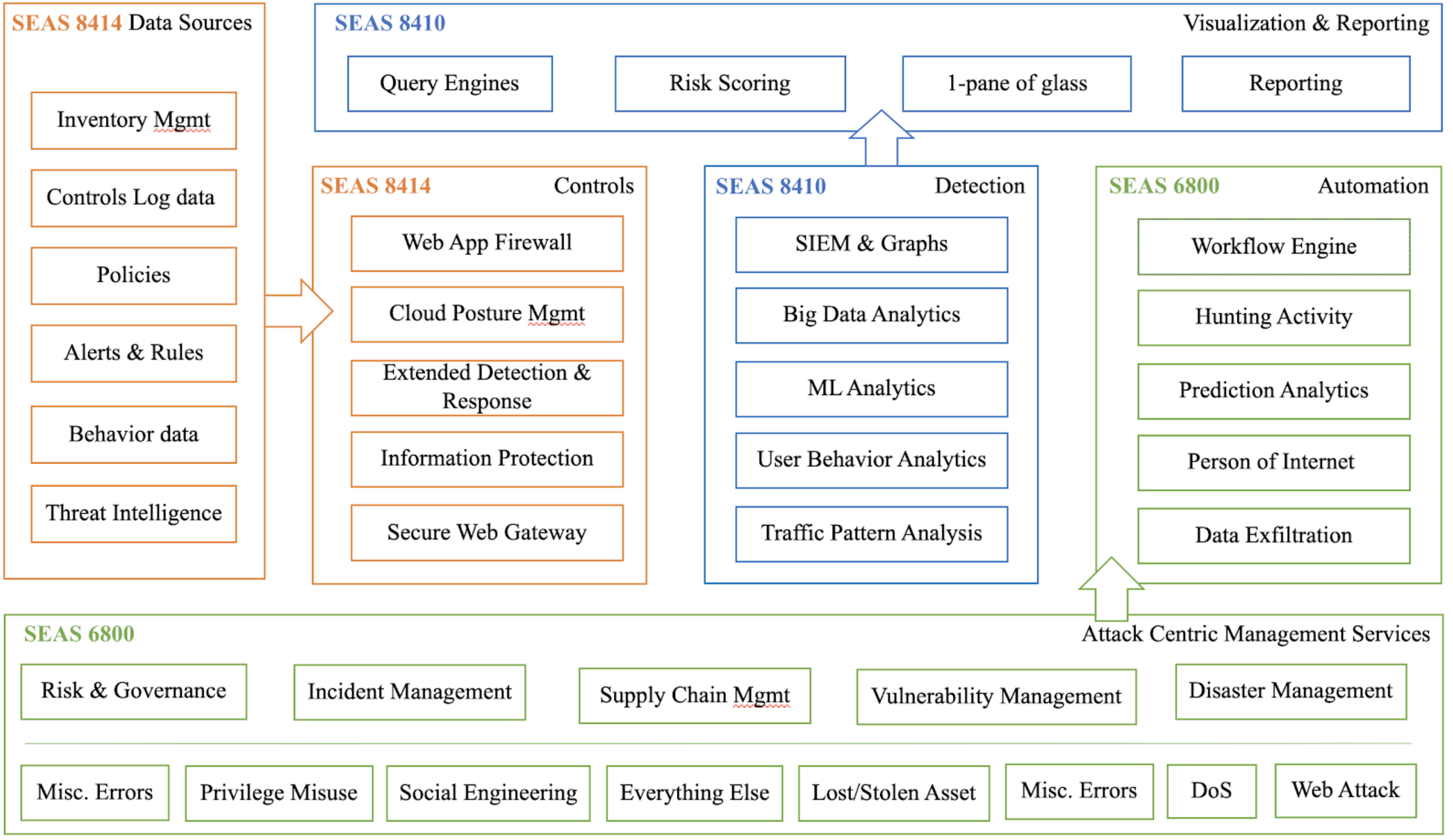
- Will be multiple-choice questions.

Logistics

Textbook & Online Access

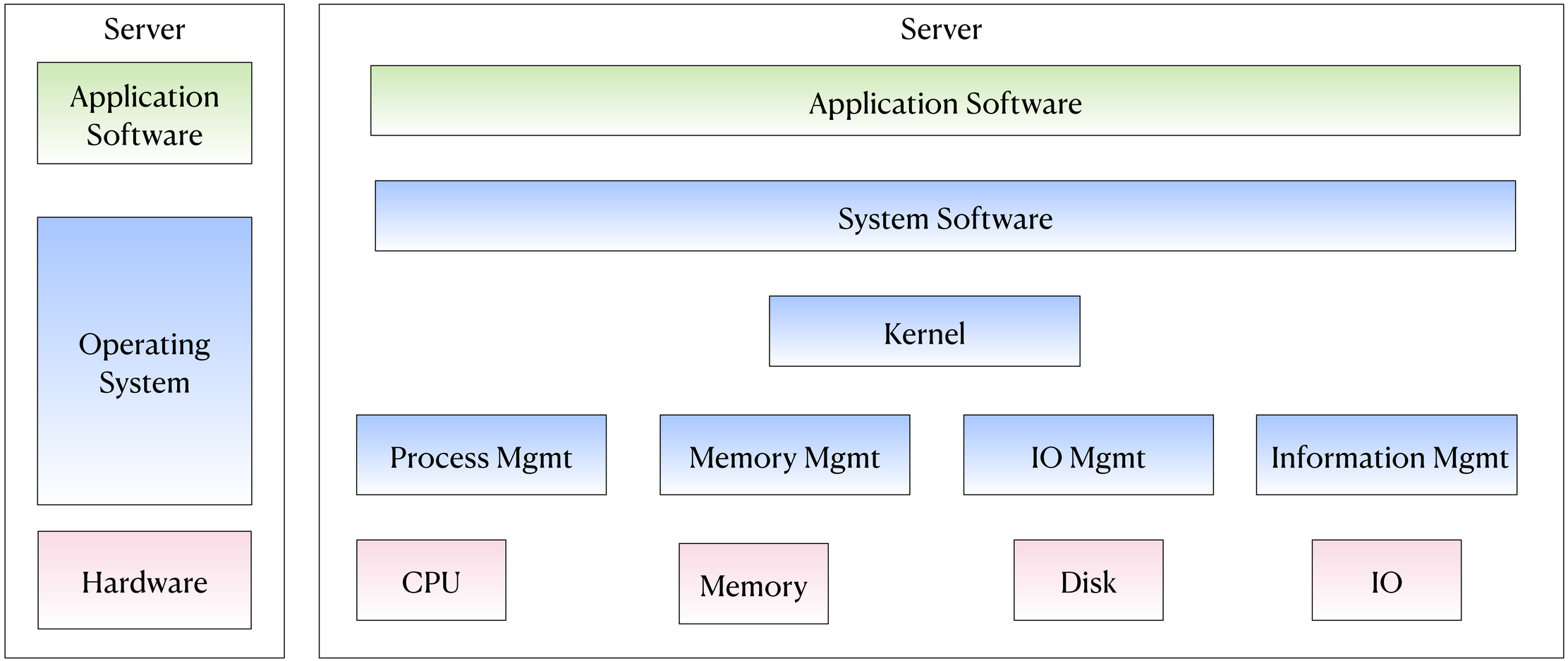
- **Textbook**: None
- **E-Textbook:** None
- **What is included in the exams?**
  - Everything that we talked about during the lectures
  - Homework assignments
  - Weekly reading material

Today’s Objectives

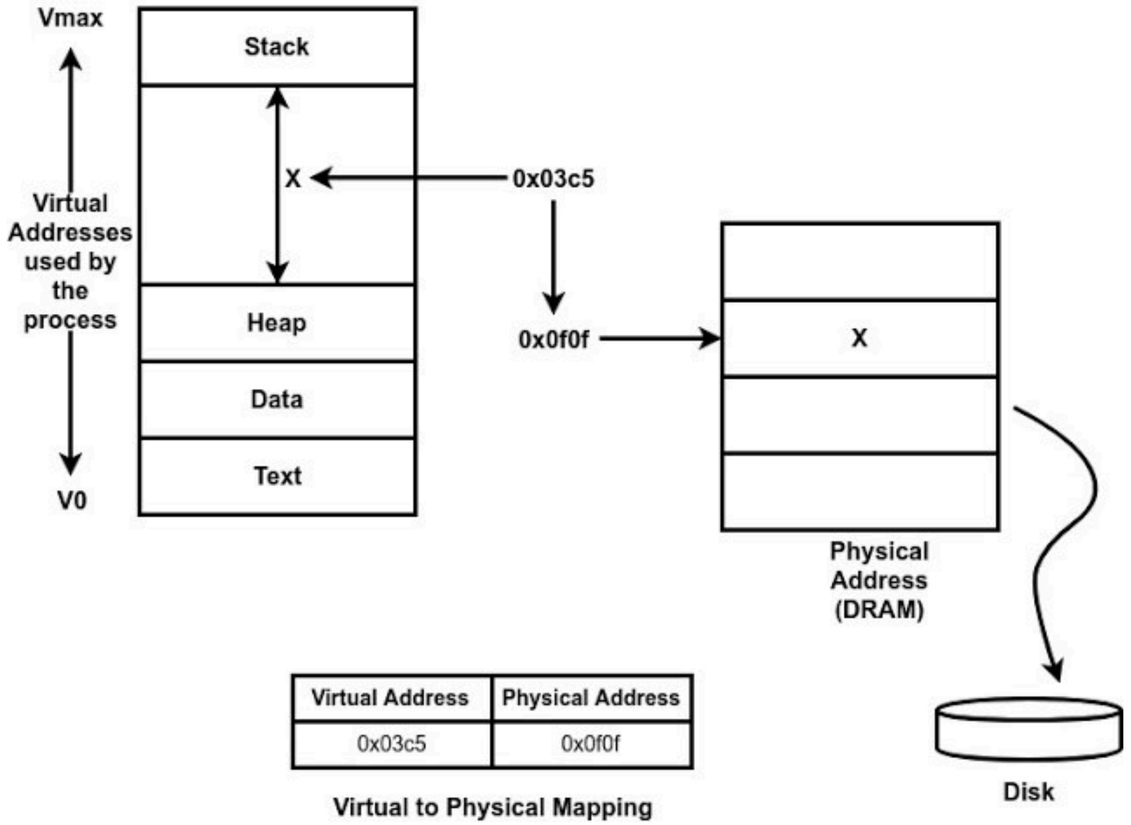

SEAS 8414 Data Sources
Inventory Mgmt
Controls Log data
Policies
Alerts & Rules
Behavior data
Threat Intelligence
SEAS 8410
Visualization & Reporting
Query Engines
Risk Scoring
1-pane of glass
Reporting
SEAS 8414
Controls
Web App Firewall
Cloud Posture Mgmt
Extended Detection & Response
Information Protection
Secure Web Gateway
SEAS 8410
Detection
SIEM & Graphs
Big Data Analytics
ML Analytics
User Behavior Analytics
Traffic Pattern Analysis
SEAS 6800
Automation
Workflow Engine
Hunting Activity
Prediction Analytics
Person of Internet
Data Exfiltration
SEAS 6800
Attack Centric Management Services
Risk & Governance
Incident Management
Supply Chain Mgmt
Vulnerability Management
Disaster Management
Misc. Errors
Privilege Misuse
Social Engineering
Everything Else
Lost/Stolen Asset
Misc. Errors
DoS
Web Attack

Operating System to Infrastructure

Operating System

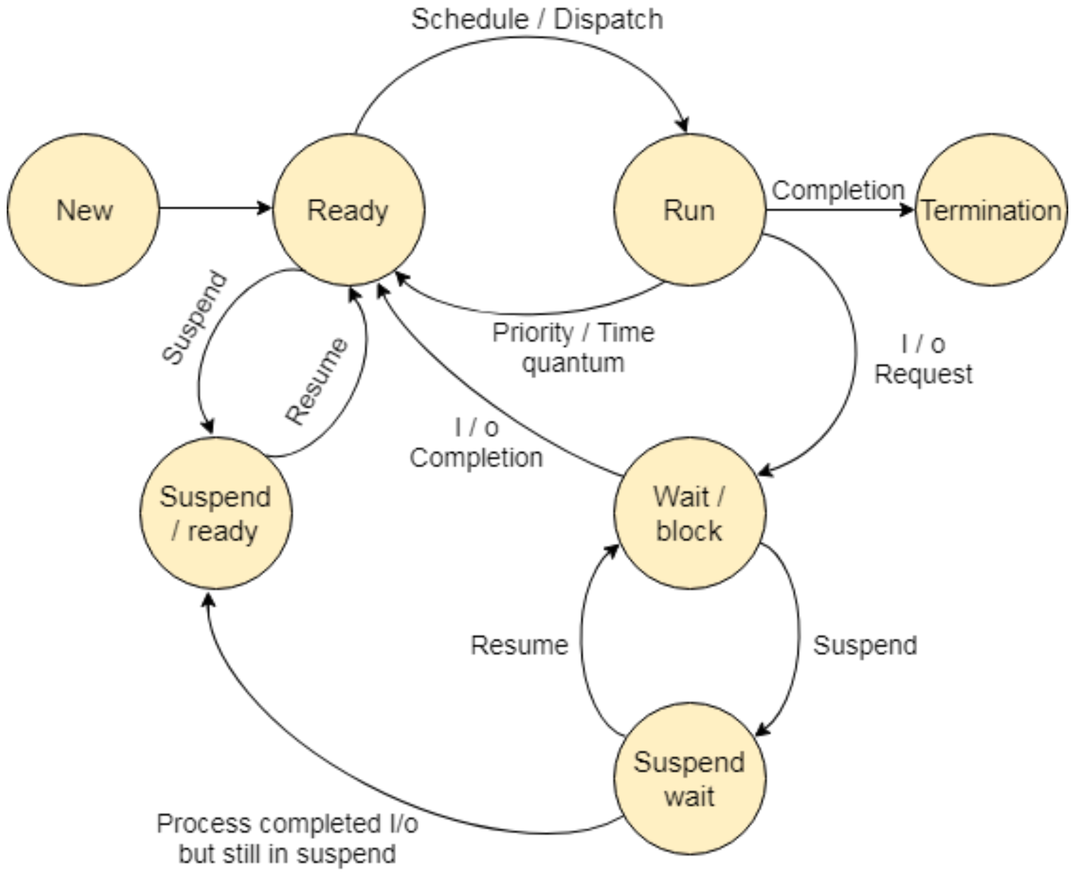


Process Management



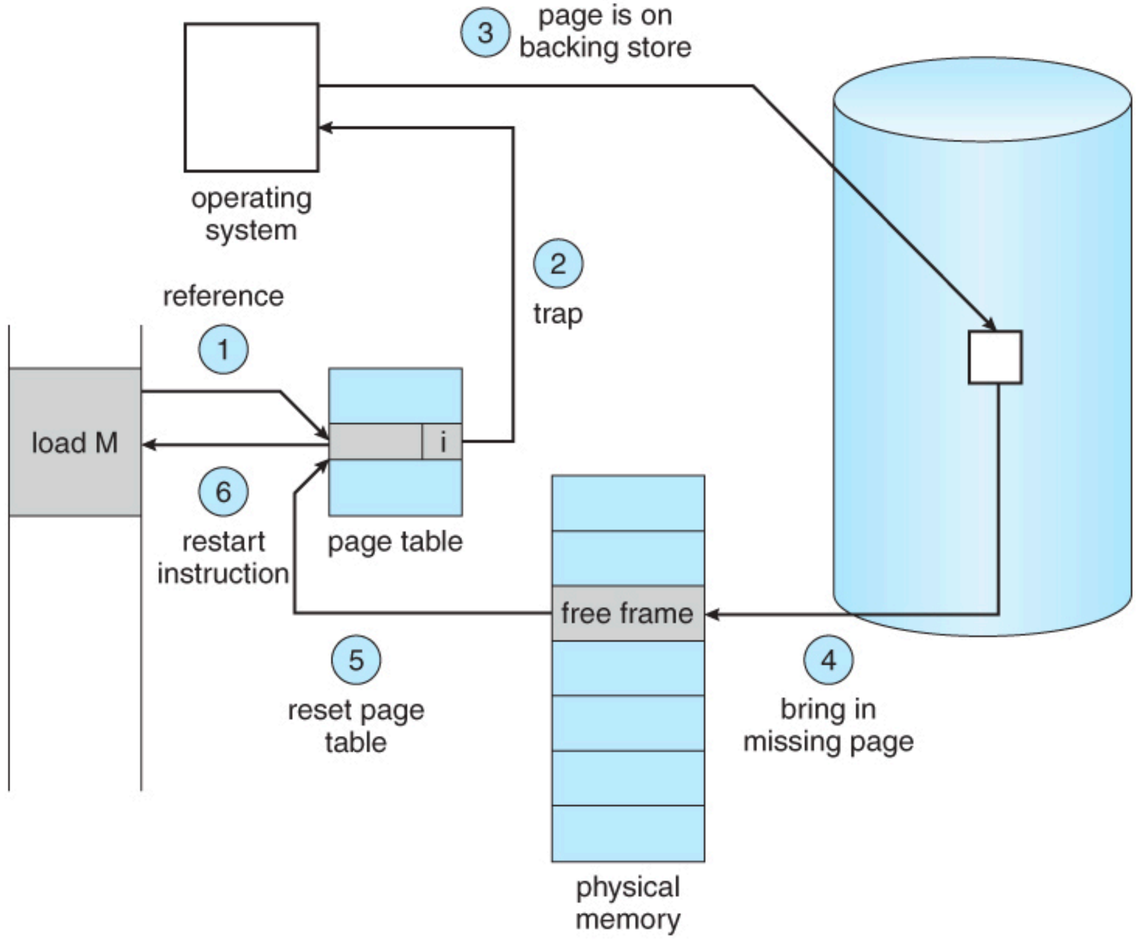
Virtual Address	Physical Address
0x03c5	0x0f0f

Virtual to Physical Mapping



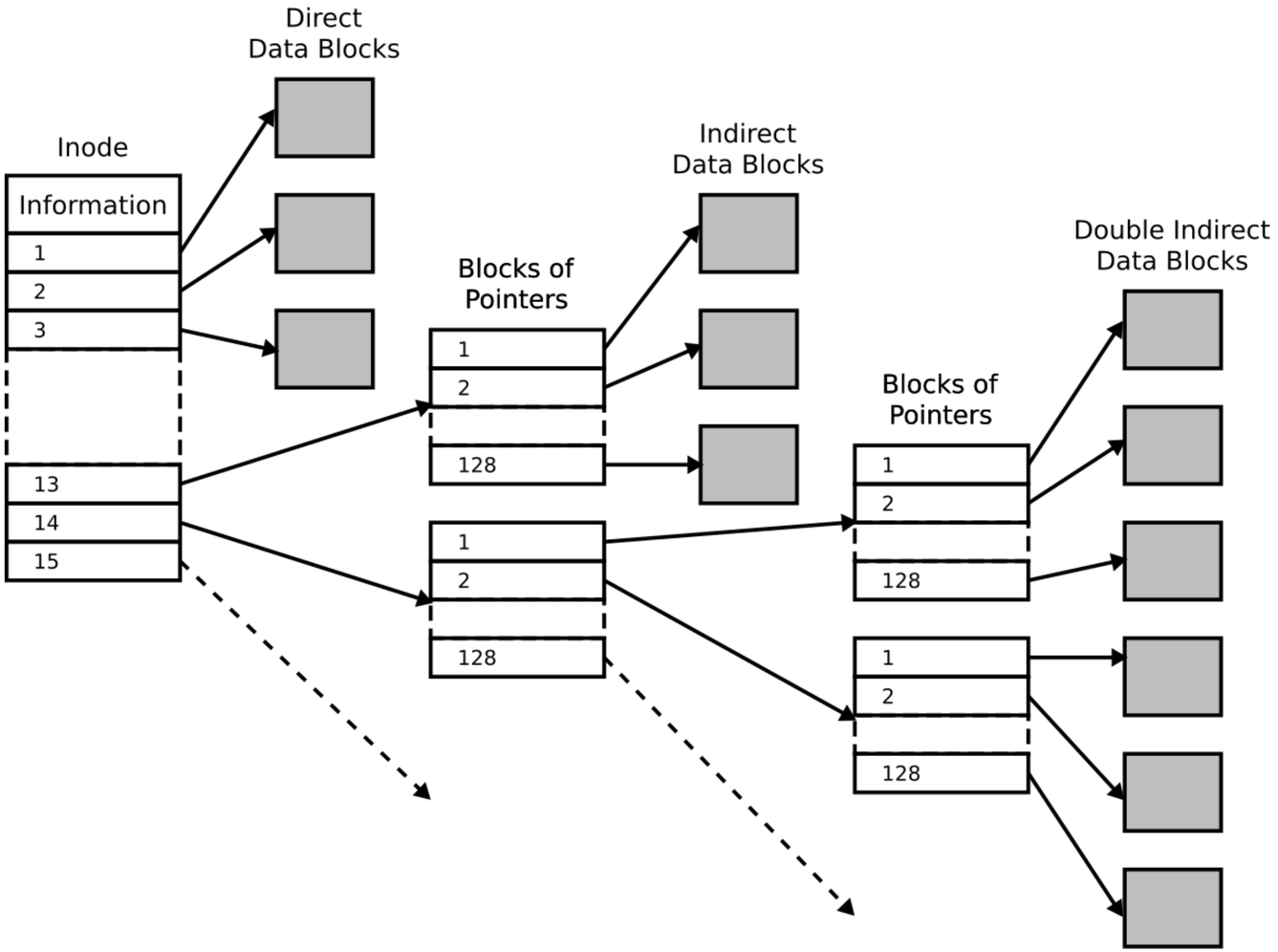
Source: Dias, Siddharth & Naik, Sidharth & Kotaguddam, Sreepraneeth & Raman, Sumedha & M., Namratha. (2017). A Machine Learning Approach for Improving Process Scheduling: A Survey. International Journal of Computer Trends and Technology. 43. 1-4. 10.14445/22312803/IJCTT-V43P101.

Memory Management



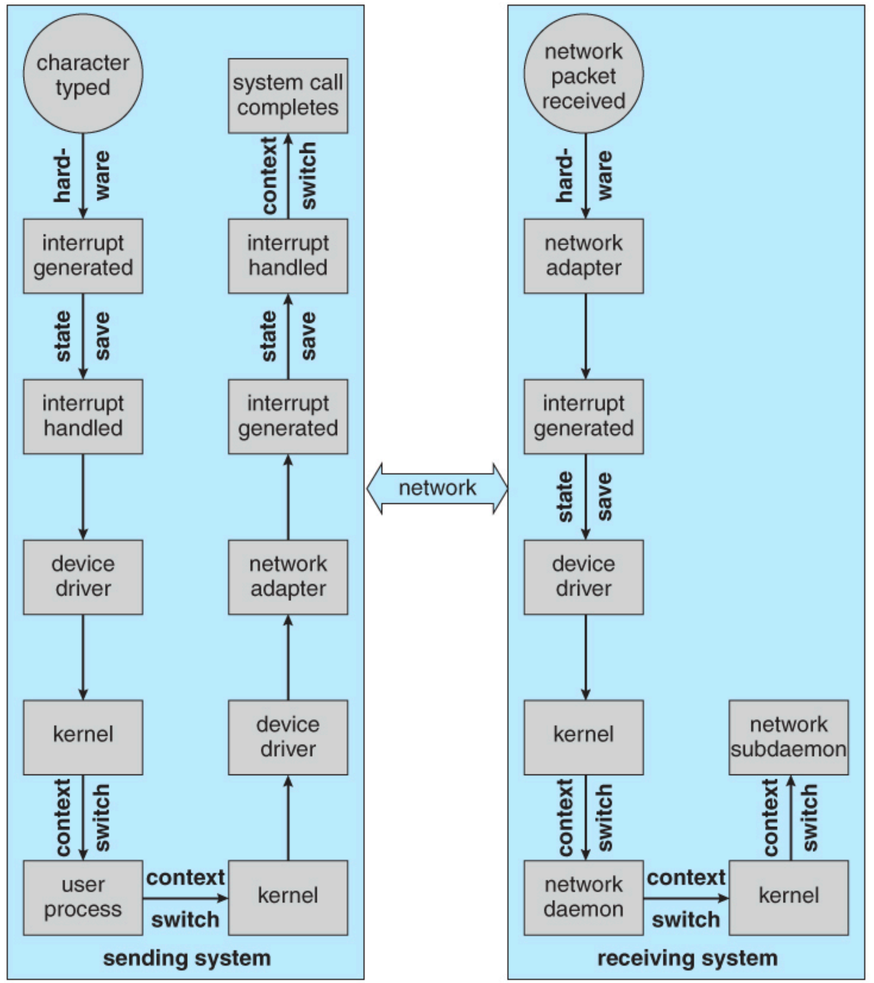
Source: https://www.cs.uic.edu/~jbell/CourseNotes/OperatingSystems/9_VirtualMemory.html

Information Management



Source: https://commons.wikimedia.org/wiki/File:Ext2-inode.svg

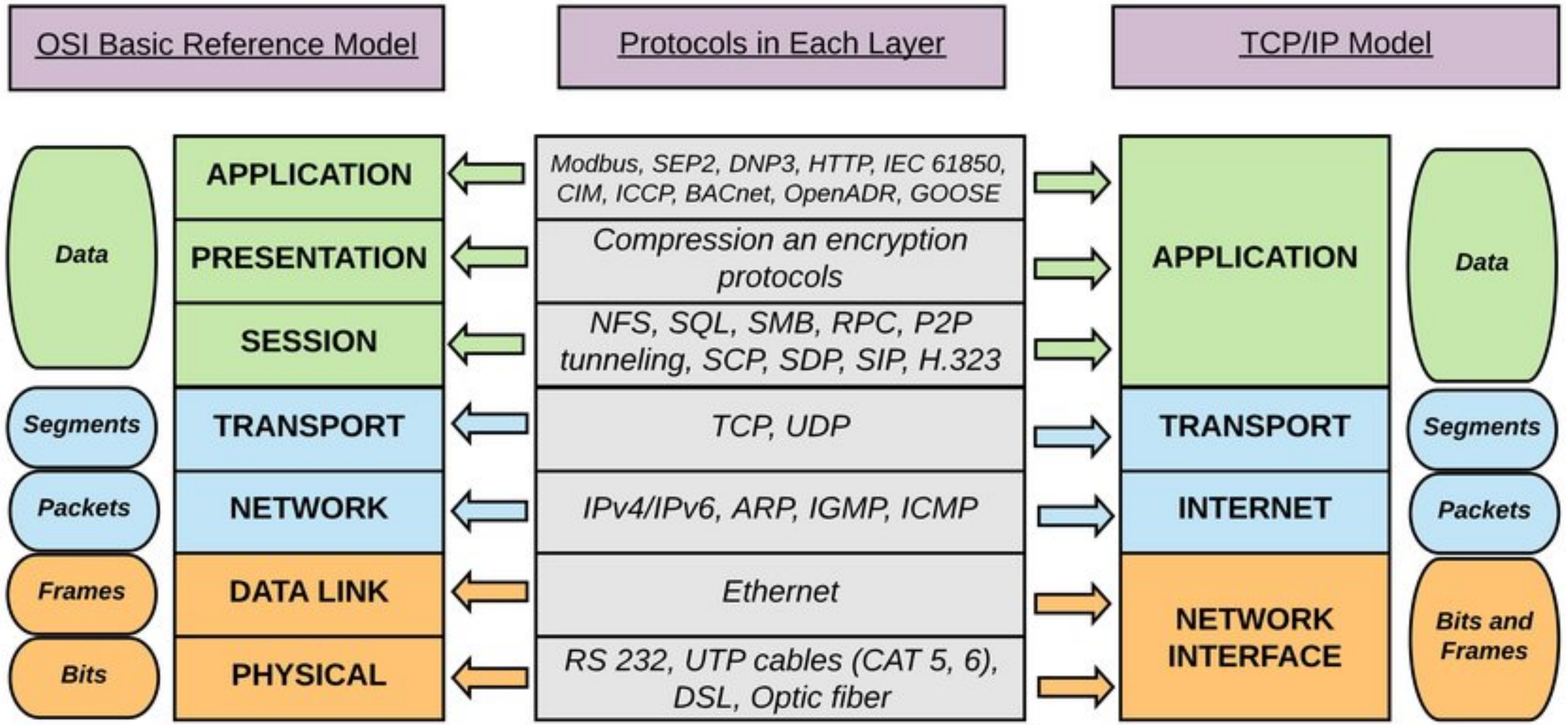
IO Management



Source: https://www.cs.uic.edu/~jbell/CourseNotes/OperatingSystems/13_IOSystems.html

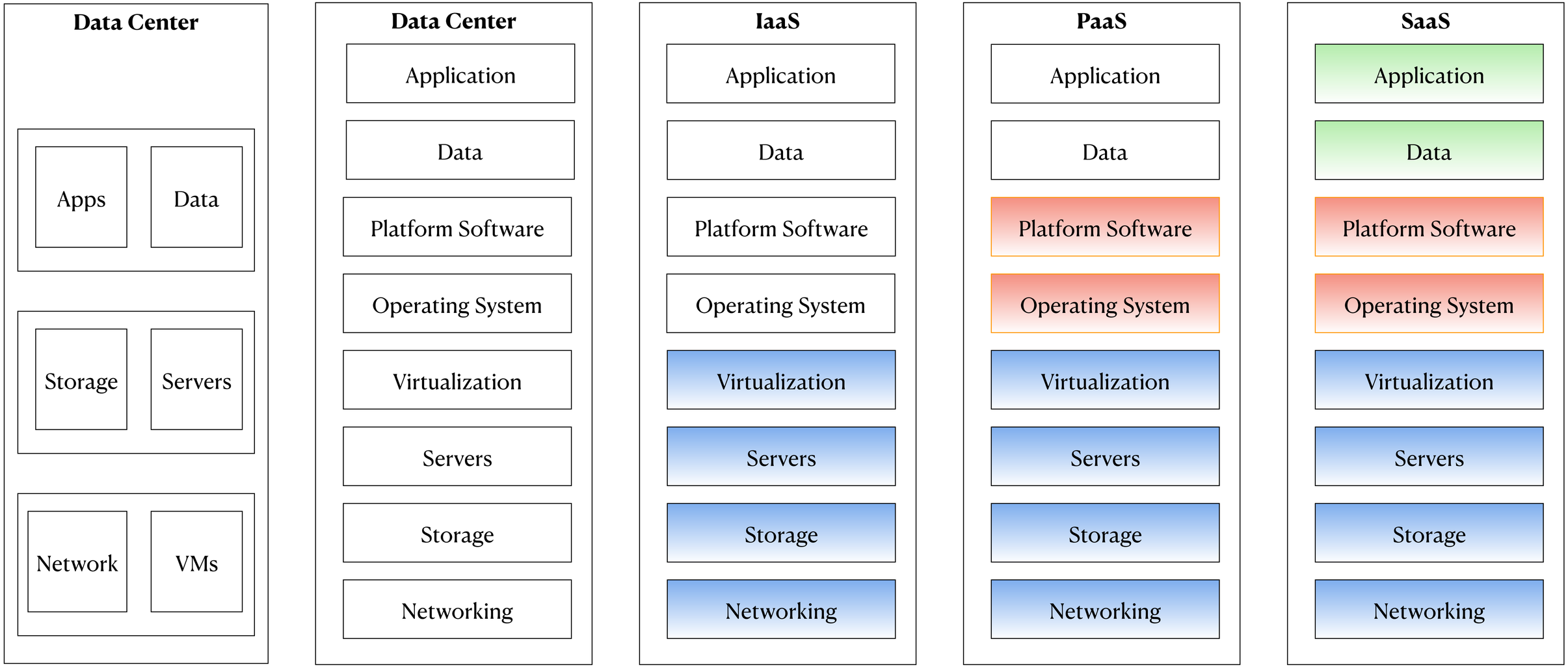
Network Management

OSI vs TCP/IP



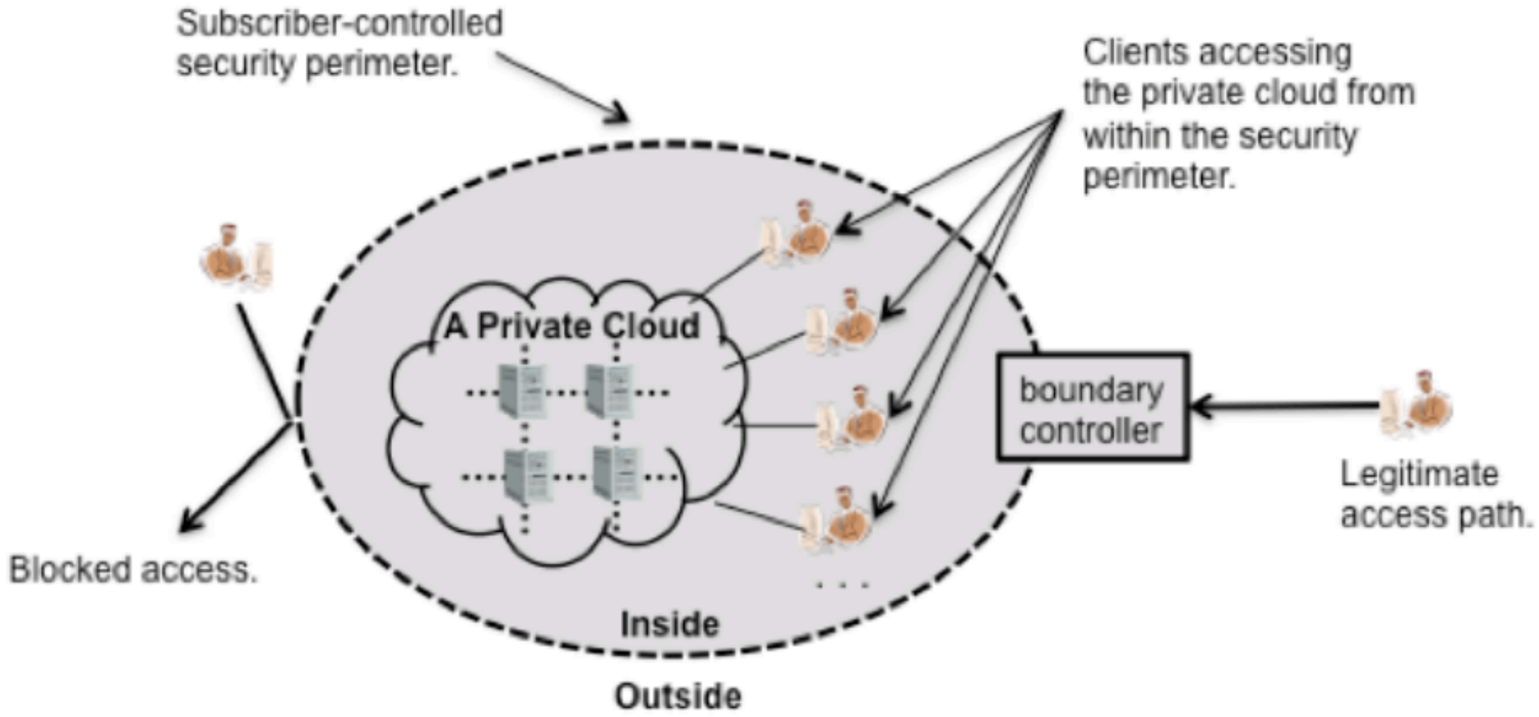
Source: https://www.researchgate.net/figure/The-logical-mapping-between-OSI-basic-reference-model-and-the-TCP-IP-stack_fig2_327483011

Data Center & Cloud Computing



Private Cloud

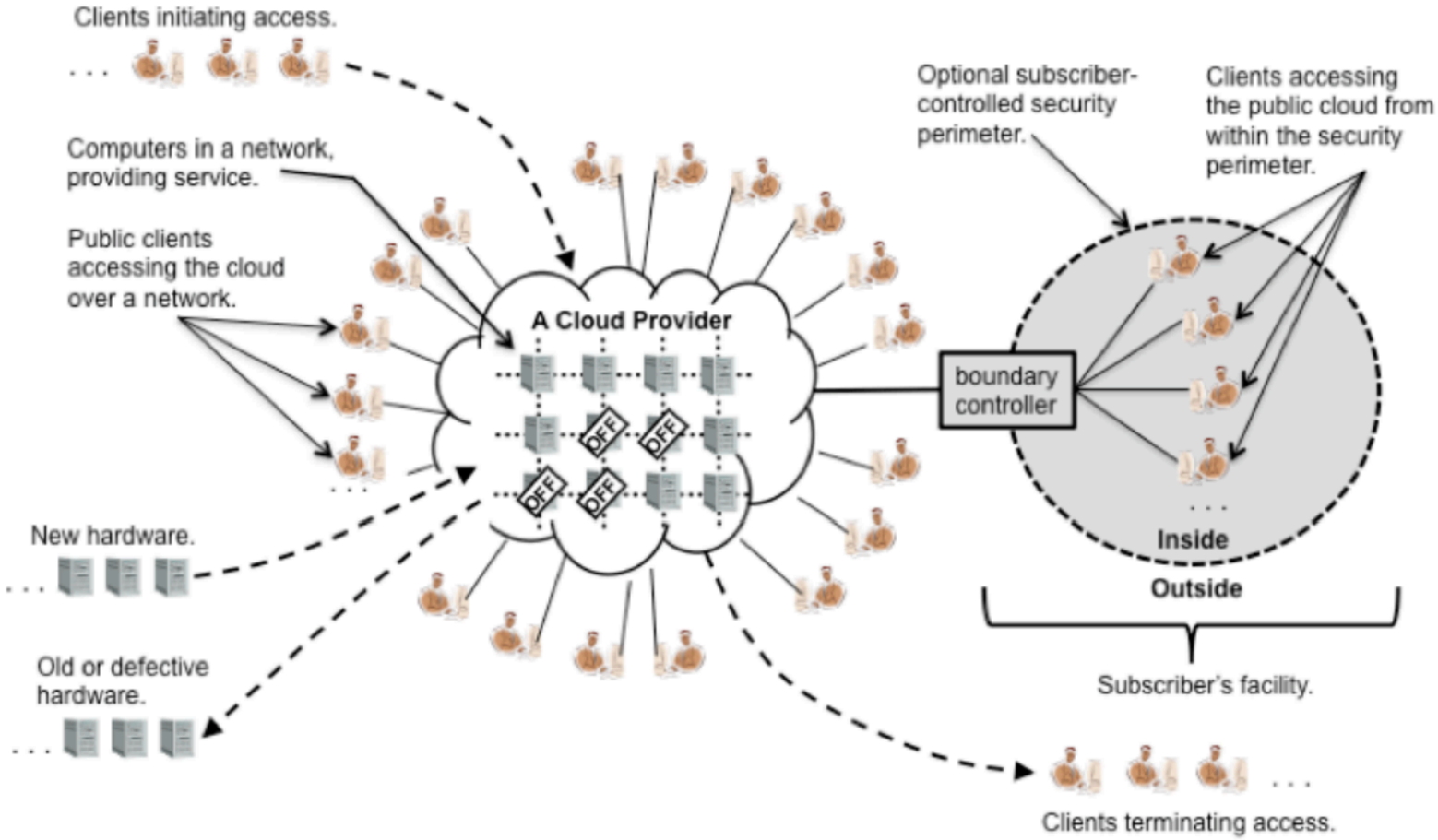
Security Posture in a Data Center



Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

Public Cloud

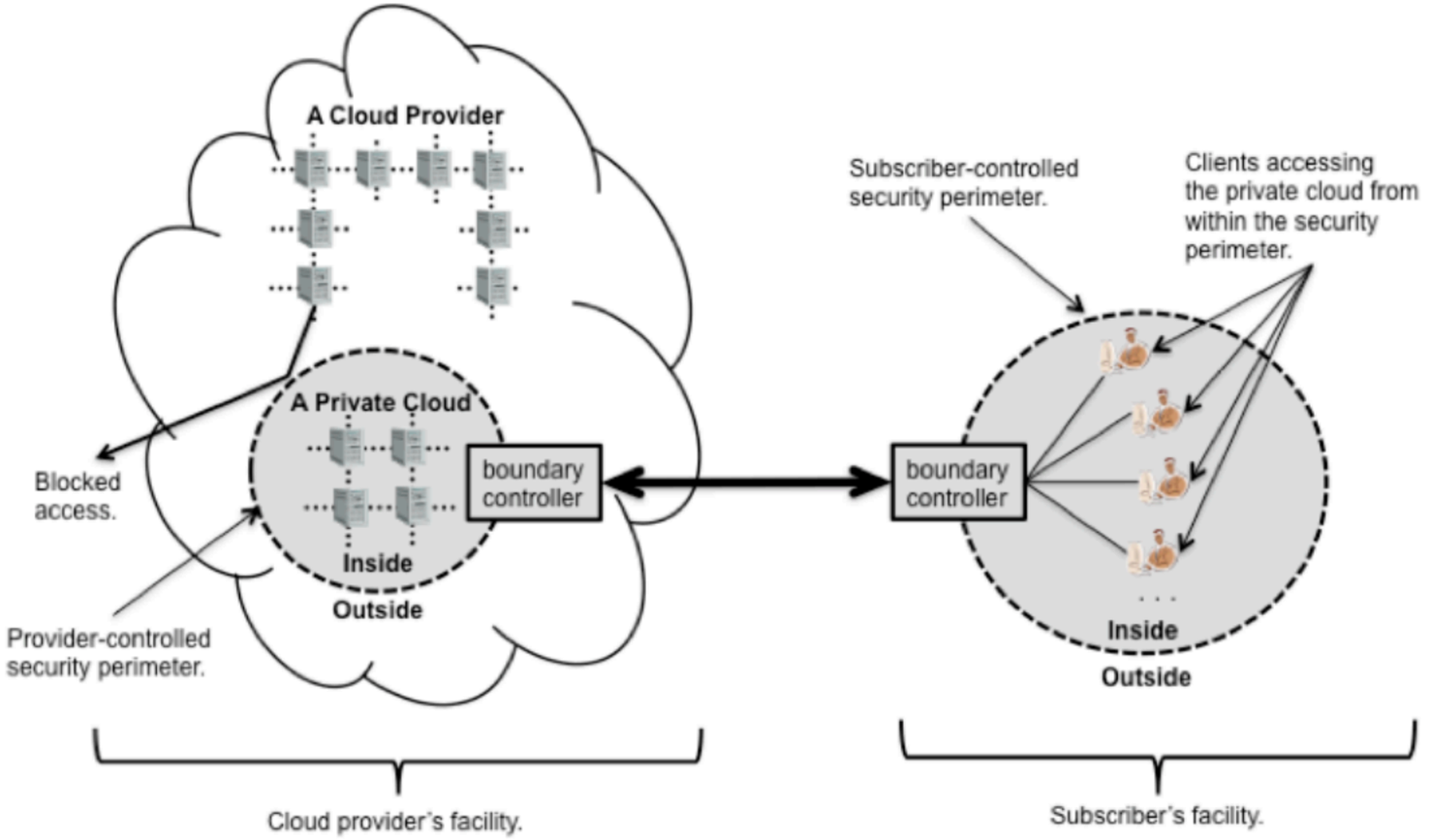
Security Posture



Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

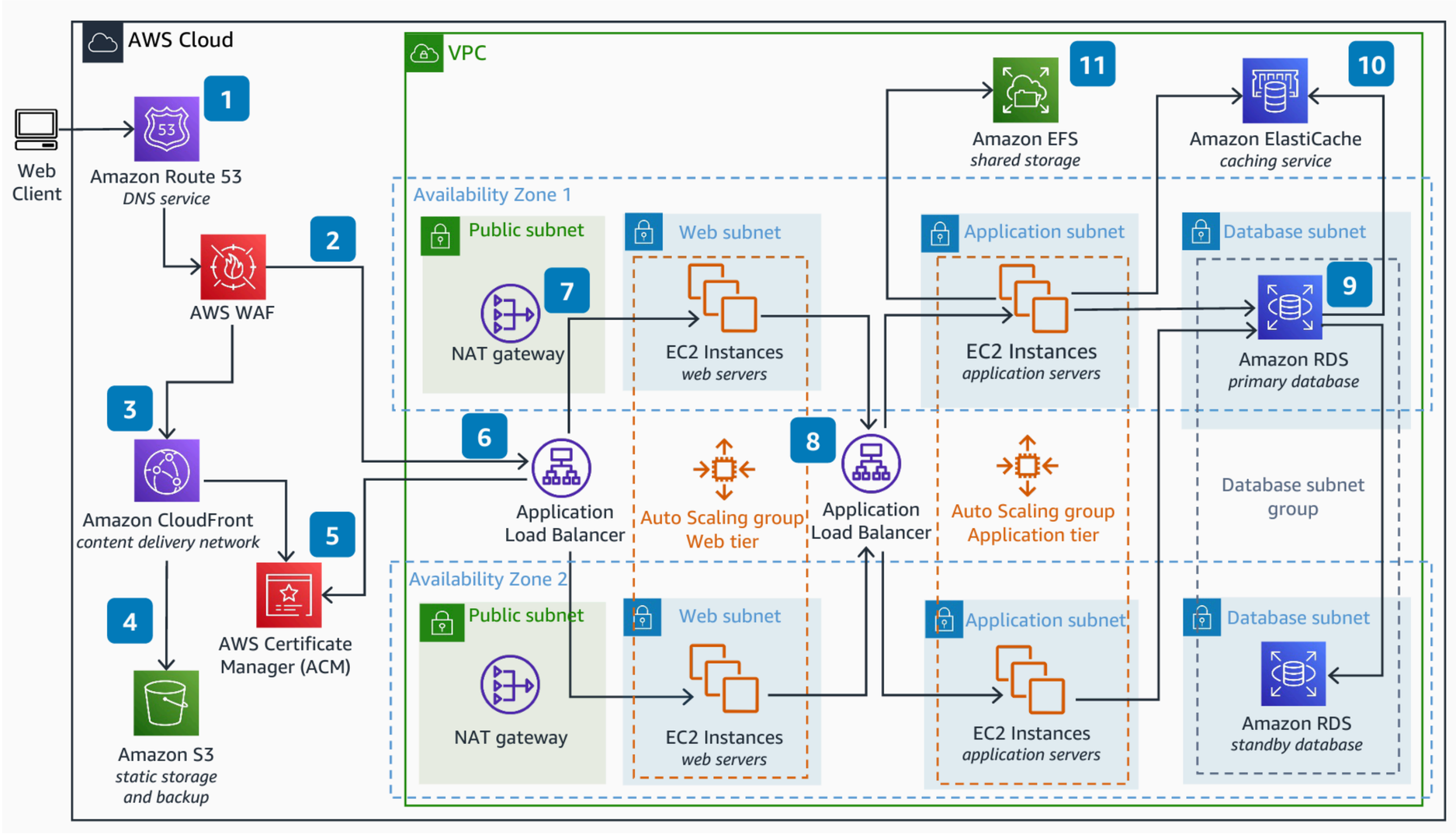
Hermetically Sealed Cloud

Practical Implementation - Private Cloud Security in a Public Cloud



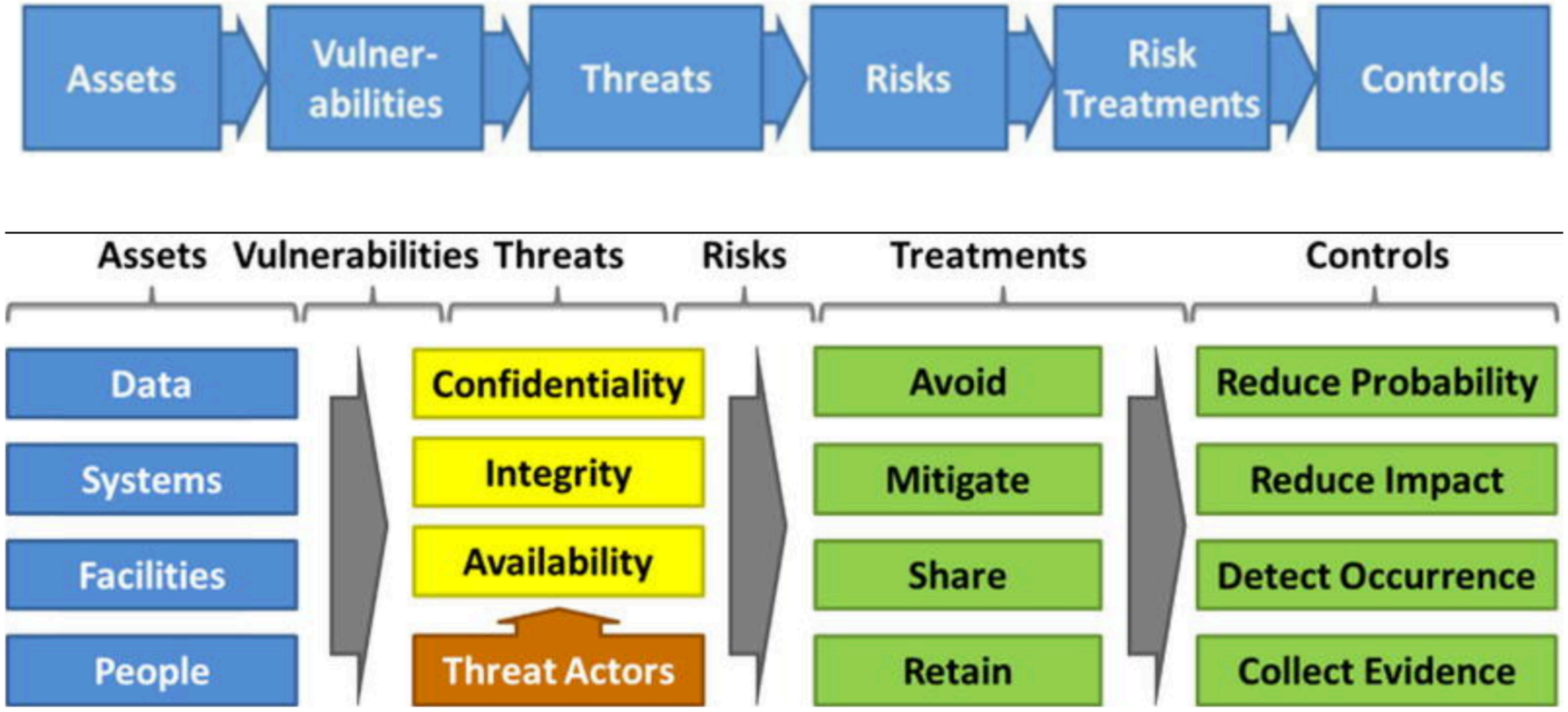
Source: https://csrc.nist.gov/csrc/media/publications/sp/800-146/final/documents/draft-nist-sp800-146.pdf

Traditional Web Application in the Cloud



Why do we need security architecture?

What are we protecting?



How do cyber attacks work?

Initial Access	Elevated Access	Expanded Access	Public Access
Phishing	Malware	Botnet	Exfiltration over Web
Watering hole	Keylogger	Command & control	Encrypted channels
Drive-by download	Pass-the-hash	Lateral movement	Non-web exfiltration

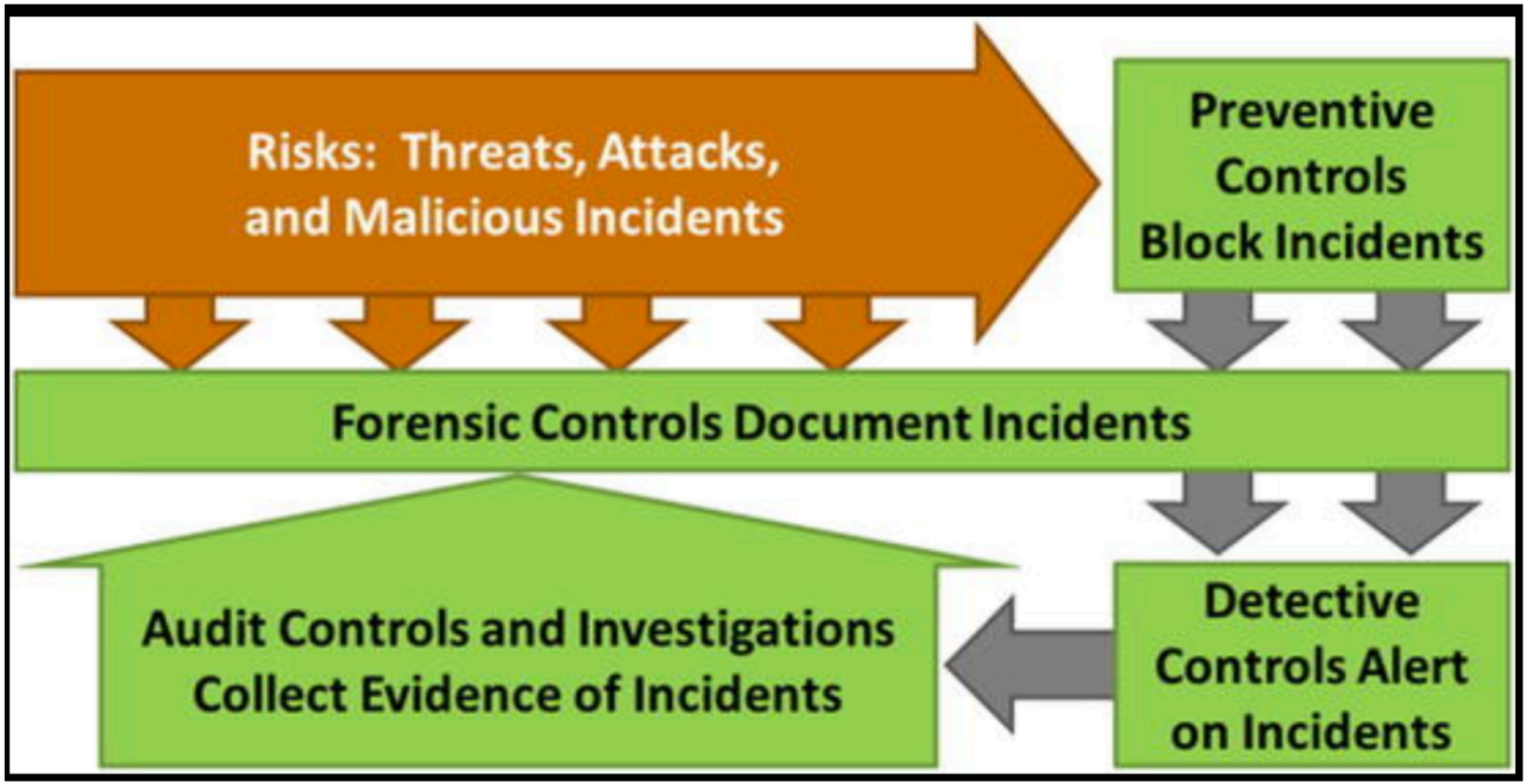
Technique	Relation to Internet Domain-based Exploitation
Phishing	The technique uses an Internet domain link to allure victims.
Watering hole	A frequently accessed domain is infected with malware.
Drive-by download	Unintentional download from a domain due to a vulnerability.
Botnet	A network of devices communicates using the Internet.
Command & Control	Communication with attacker-controlled Internet domain.
Exfiltration over Web	Send data to Internet domain using web and email
Encrypted channels	Send data to Internet domain using encryption protocols
Non-web exfiltration	Send data to Internet domain using applications and scripts

Real Life Cyber Incidents

Organization	Year	Initial Access	Elevated Access	Expanded Access	Public Access
Target	2013	Phishing	Malware	Botnet	Exfil over Web
Sony	2014	Spear Phishing	Pass the Hash	Command & Control	EoW
Yahoo	2014	Spear Phishing	Malware	Lateral Movement	EoW
Anthem	2014	Spear Phishing	Malware	Lateral Movement	EoW
U.S. OPM	2014	Phishing	Malware	Command & Control	EoW
RUAG	2015	Watering Hole	Malware	Botnet	EoW
MS	2015	Insider	NA	NA	EoW
Tesla	2018	Insider	NA	NA	EoW
Apple	2018	Insider	NA	NA	EoW
Capital One	2019	Insider	NA	NA	EoW
G.E.	2020	Insider	NA	NA	EoW
SolarWinds	2020	Vulnerability	NA	Command & Control	EoW

How do we think about Cyber architecture?

Controls by Type of Attack



Controls by Type of Attack

- **Preventive Controls** block the threat and prevent incidents from occurring altogether
- **Detective Controls** detect when the risk has transpired and generate alerts that can then be acted upon
- **Forensic Controls** collect records of activities related to the risk and can be used to produce artifacts to help the operation of detective controls, investigations of incidents, and audits of controls to verify their operation and effectiveness
- **Audit Controls** investigate for the presence of the risk, incidents associated with the risk, and the operation of controls that mitigate the risk

Impact of Controls

	Preventive	*Detective*	*Forensic*	*Audit*
Block Attacks?	Good	Medium	Poor	Poor
Detect Attacks?	Poor	Good	Poor	Medium
Operational Impact	High	Low	Low	Low
Investigate Attacks?	Poor	Medium	Good	Good
Cost to Implement	High	Medium	Medium	Low
Cost to Operate	Medium	High	Low	Medium
Flexibility	Poor	Poor	Medium	Good

Homework