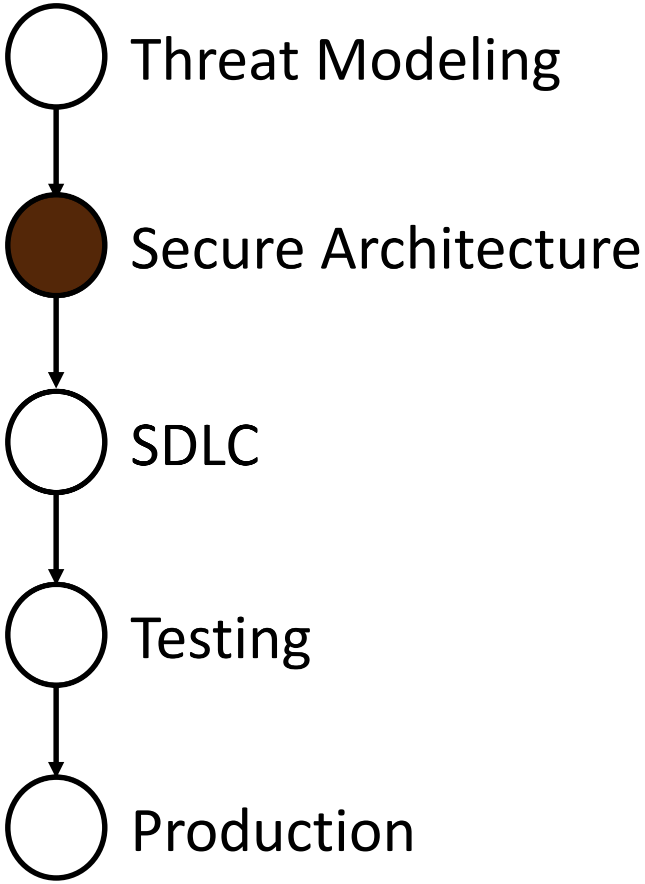
Secure Architecture

Memi Lavi
www.memilavi.com

Secure Architecture Process



Secure Architecture

Decide &
Design

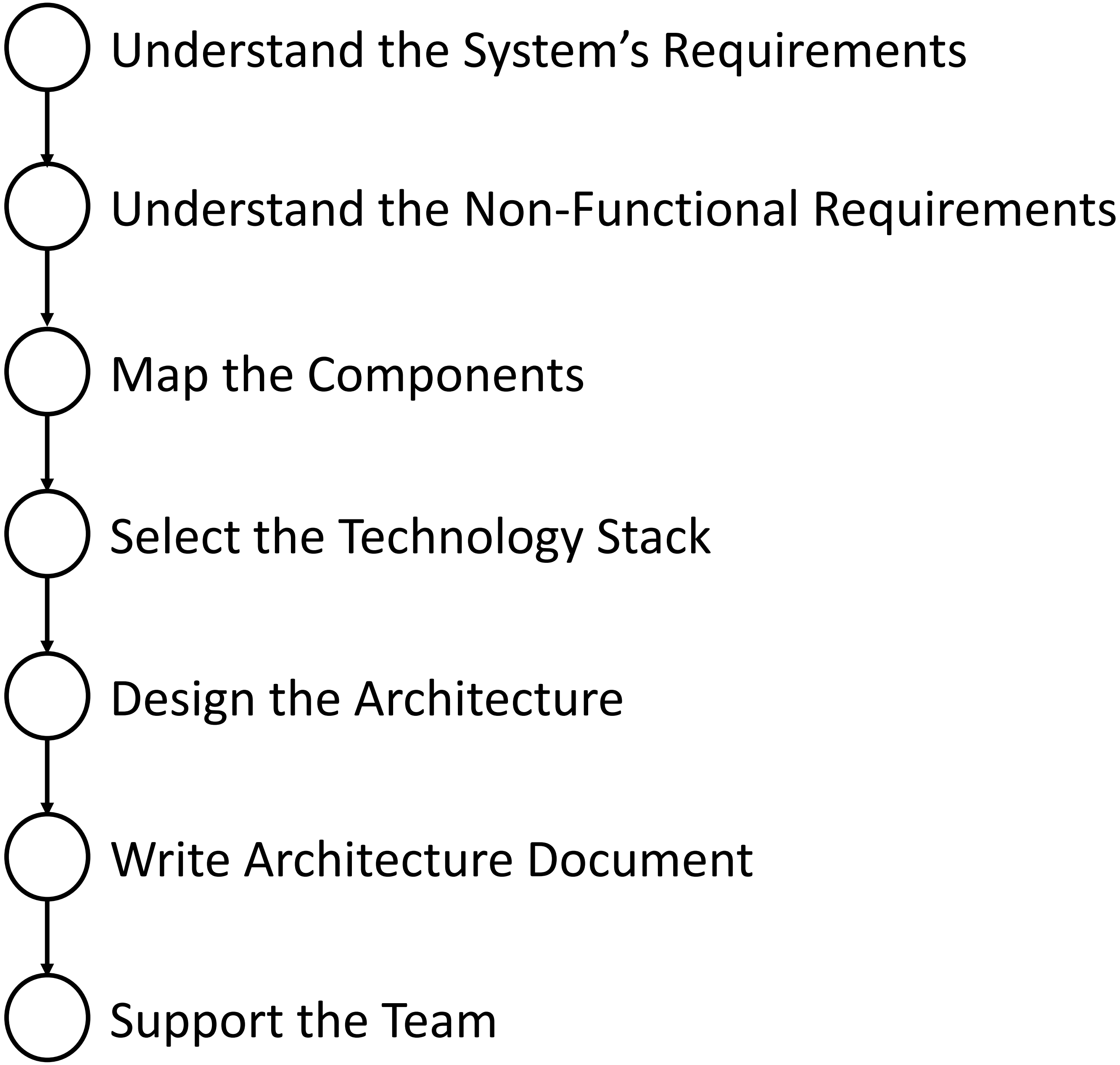
Goal: Design Secure Architecture based on the threats defined in the Threat Modeling

Participants:

- Architect
- Dev Manager (OP)
- System Analyst (OP)
- CISO (OP)
- IT (OP)
- Developers (OP)
- QA (OP)

(OP) = Optional

The Architecture Process



Understand the System’s Requirements

Understand the Non-Functional Requirements

Map the Components

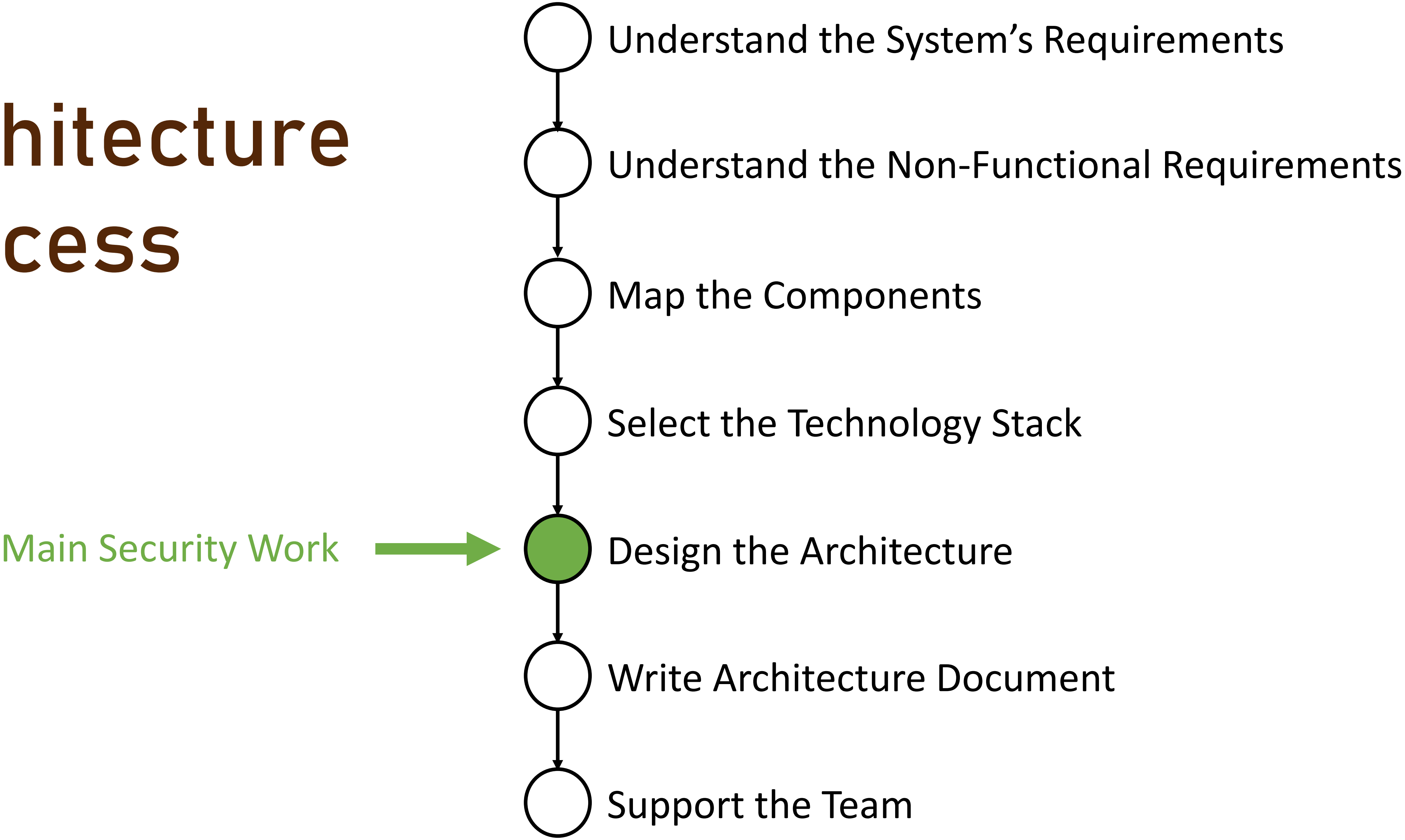
Select the Technology Stack

Design the Architecture

Write Architecture Document

Support the Team

The Architecture Process



Understand the System’s Requirements

Understand the Non-Functional Requirements

Map the Components

Select the Technology Stack

Main Security Work

Design the Architecture

Write Architecture Document

Support the Team

Result of This Stage

- Secure Architecture Document
- Part of the overall Architecture Document
- Takes into account the threats defined in the Threat Modeling Phase

But First…

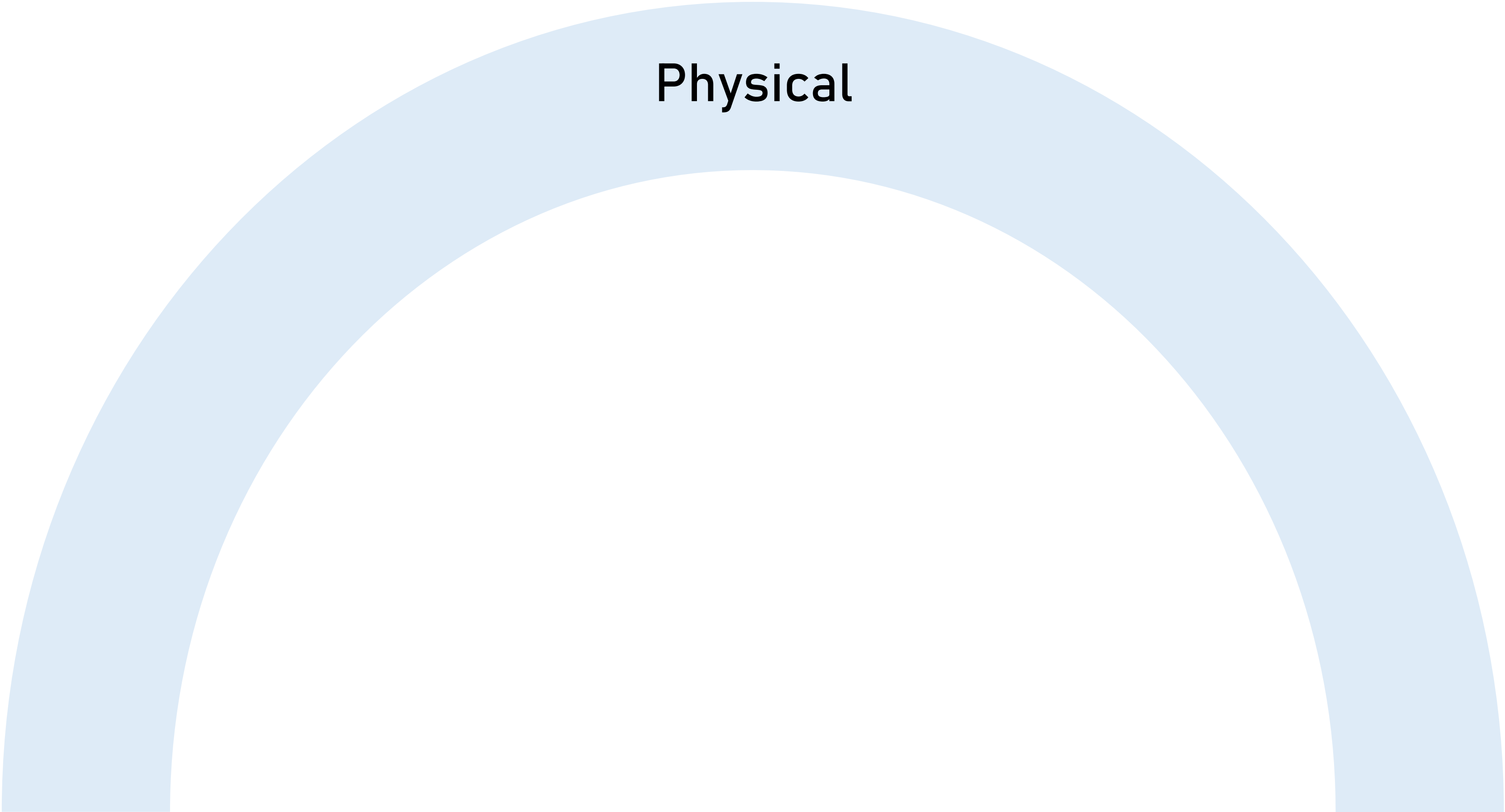
Let's have a review of

Software Security

Software Security 101

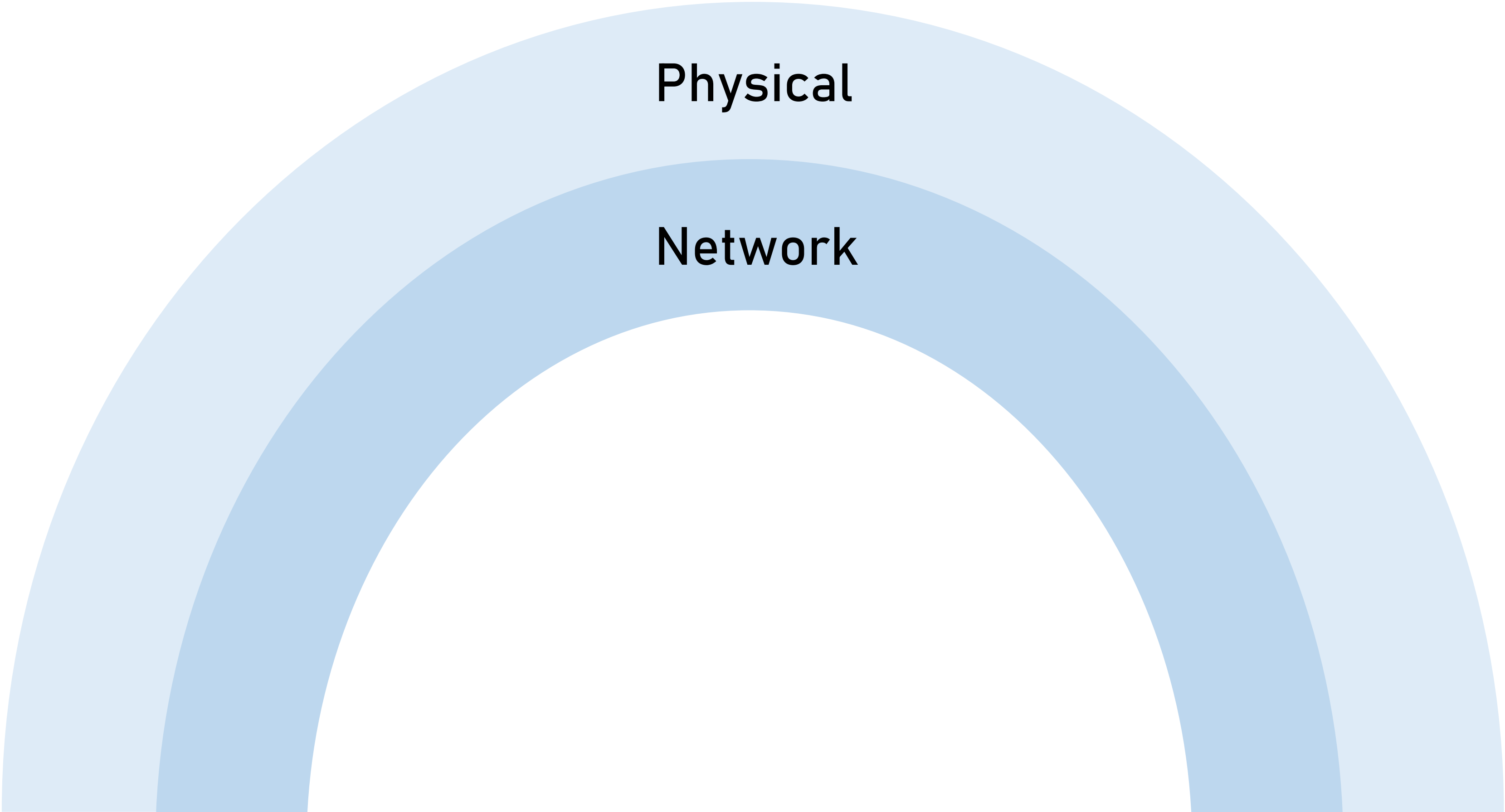
- Software Security is done using the Security Perimeters paradigm

Security Perimeters

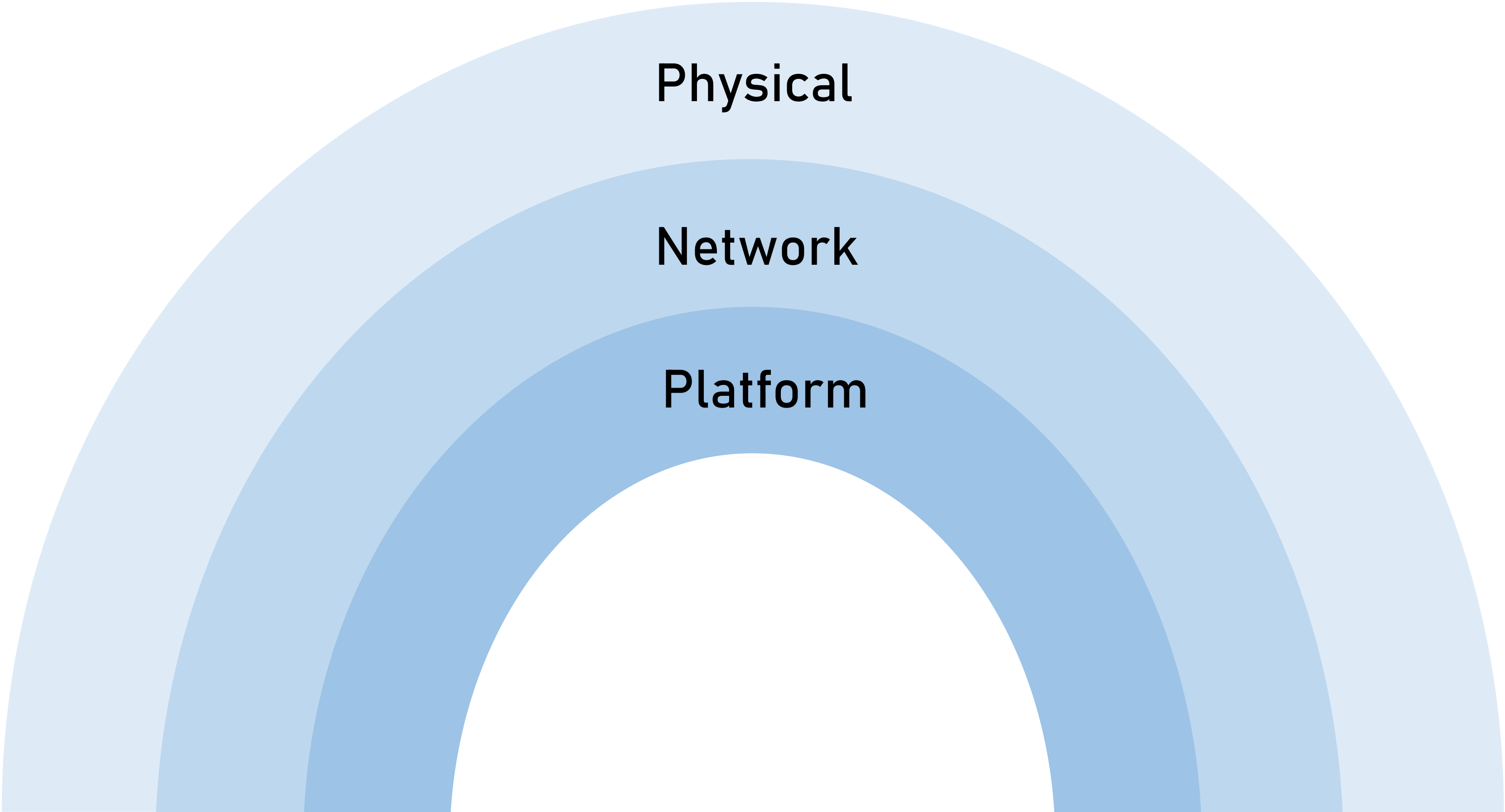


Physical

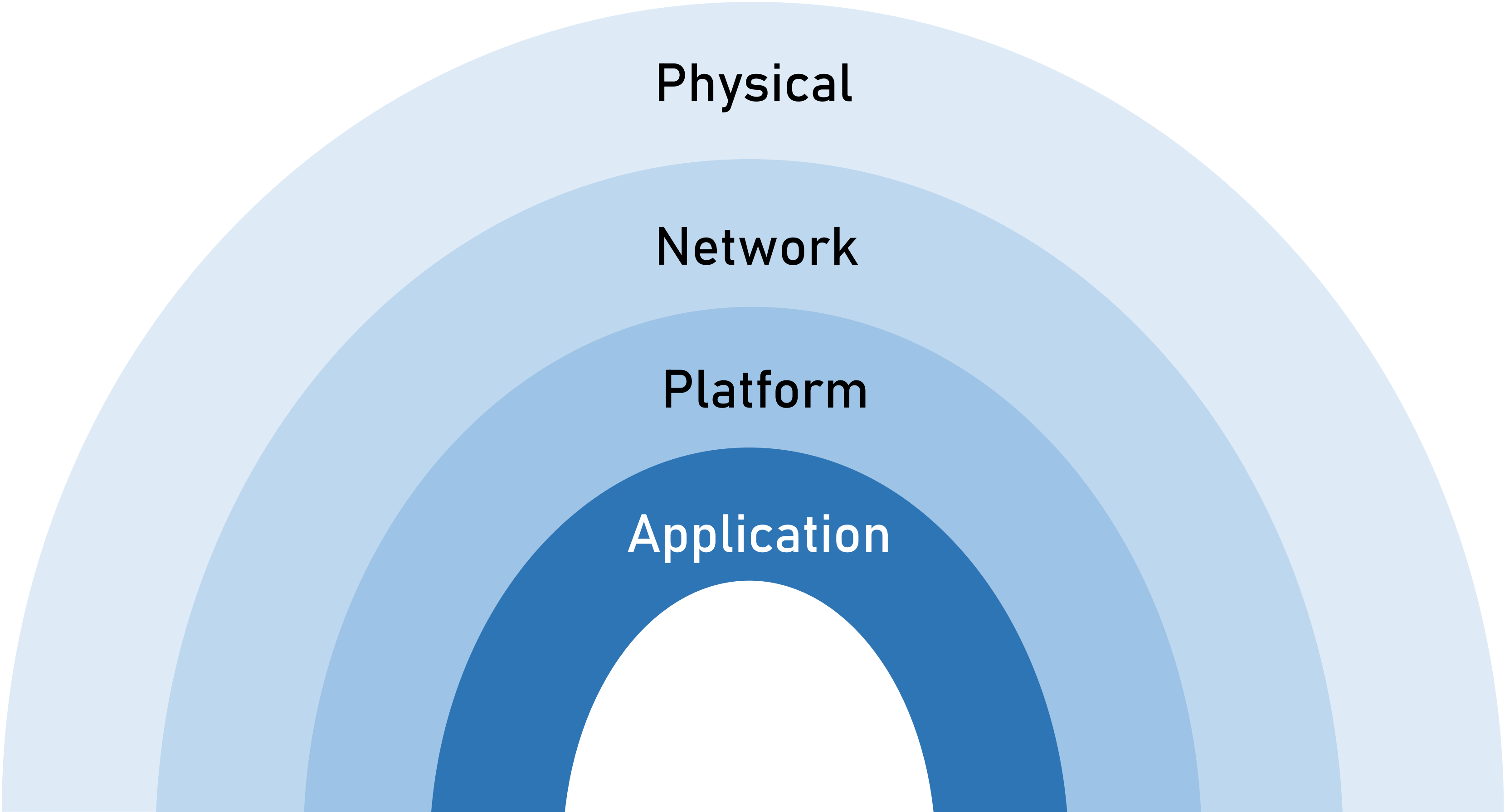
Security Perimeters



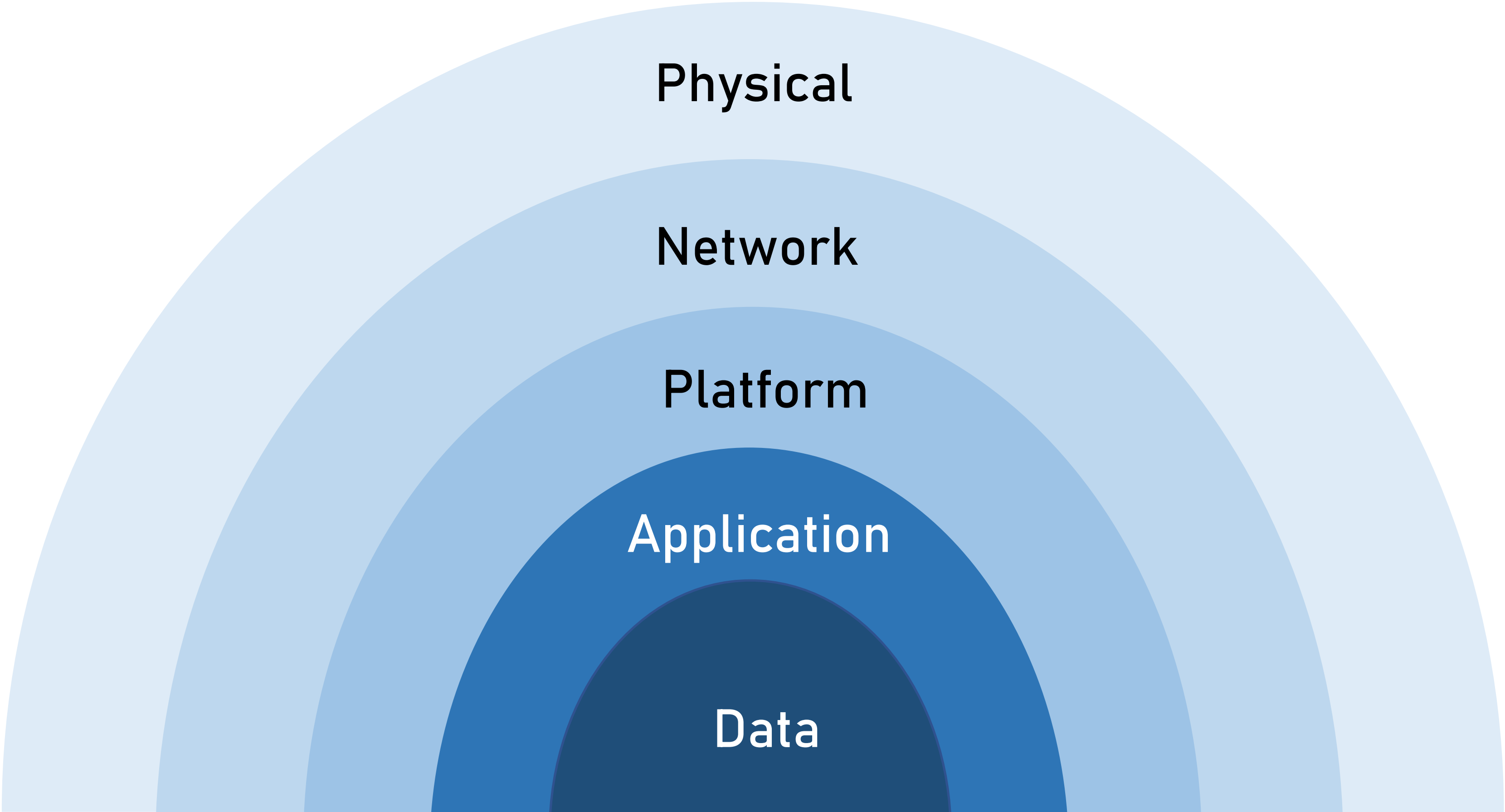
Security Perimeters



Security Perimeters

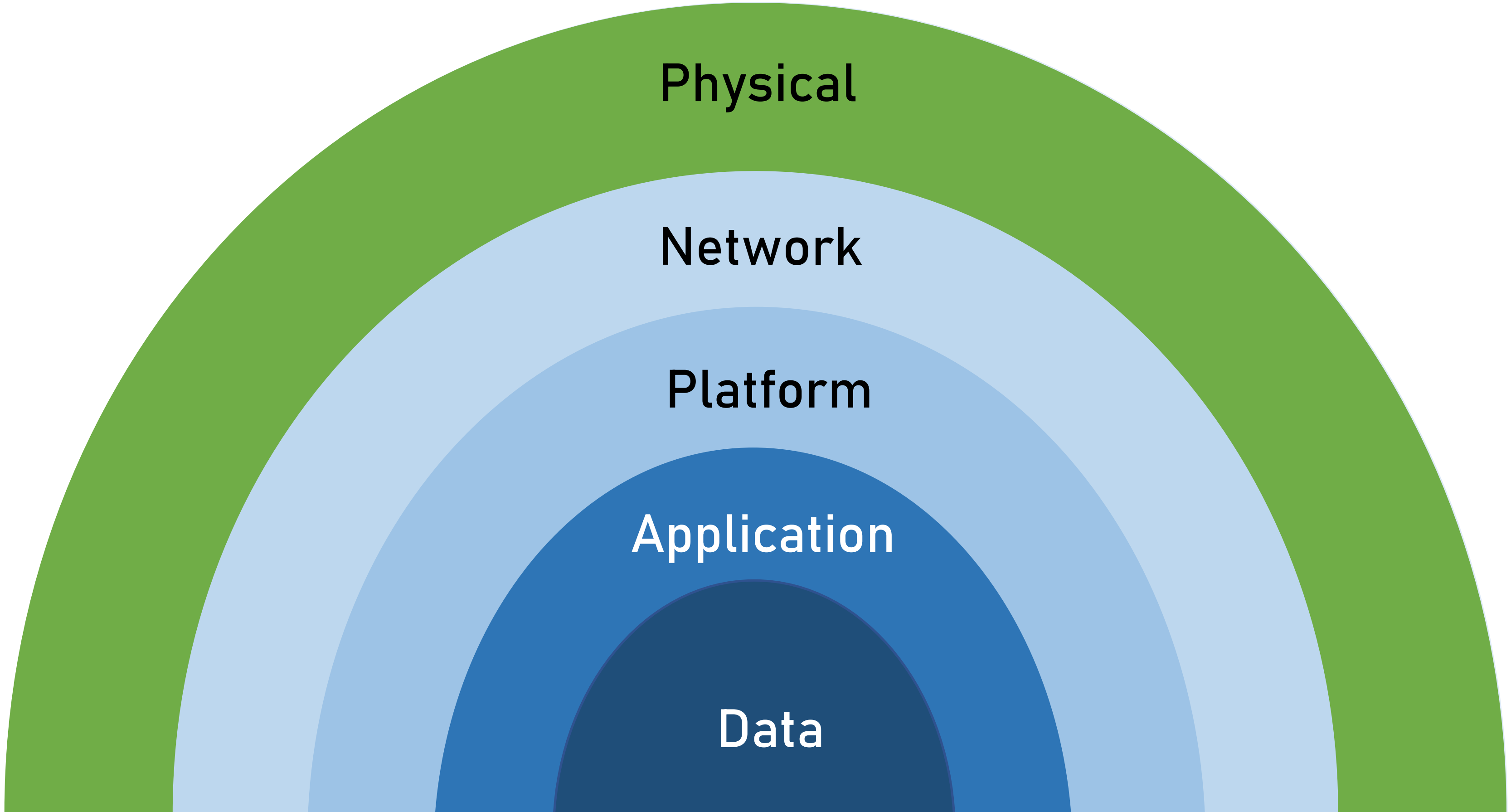


Security Perimeters



Physical Security

Ignore



Physical Security

- Controls the access to the physical hardware

- Usually using keycard, building control access, locks, etc.

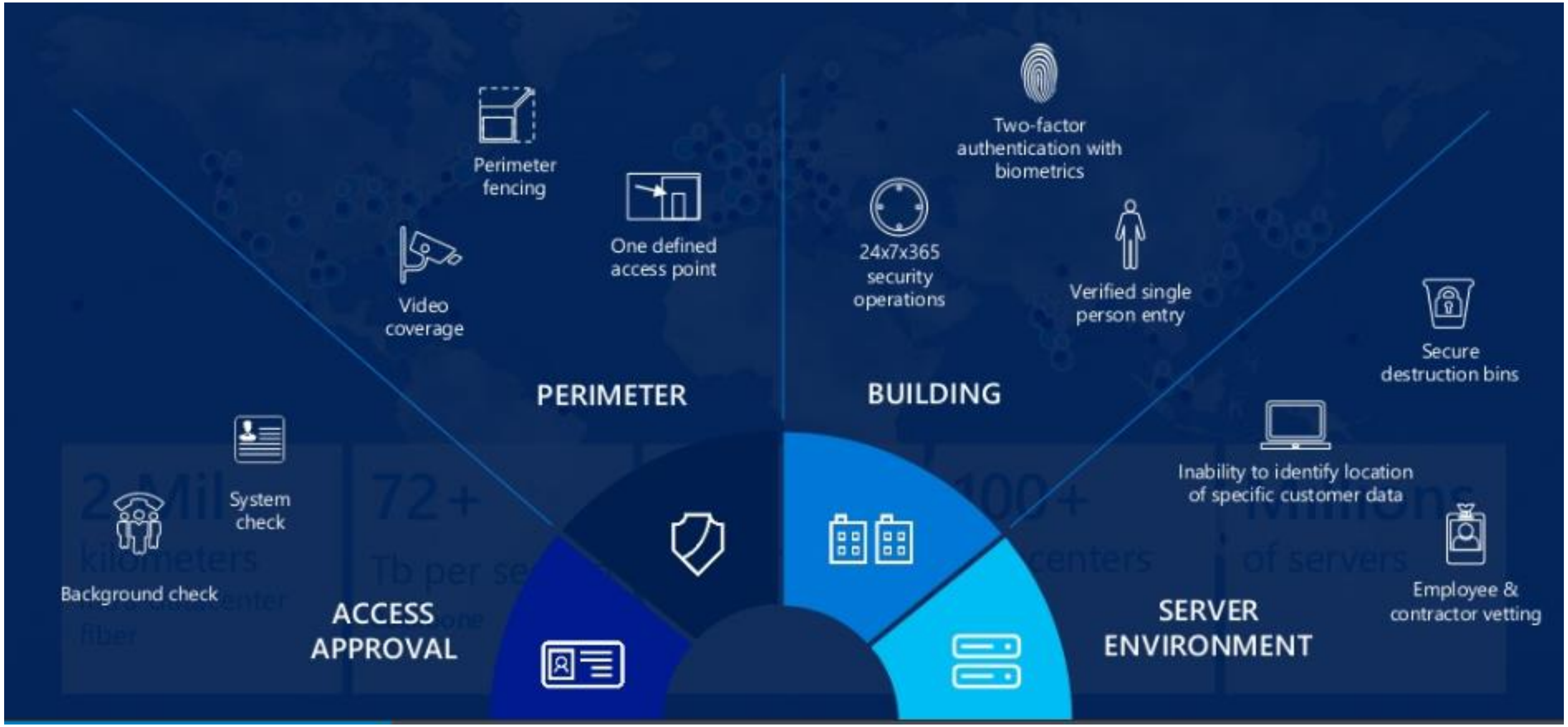
Physical Security - Example

Microsoft Azure's Datacenter

Source: https://www.youtube.com/watch?v=qNYf2Ox75gQ

Physical Security – Example

Microsoft Azure's Datacenter Physical Security


Perimeter fencing
One defined access point
Video coverage
PERIMETER
Two-factor authentication with biometrics
24x7x365 security operations
Verified single person entry
BUILDING
Secure destruction bins
System check
Background check
ACCESS APPROVAL
Inability to identify location of specific customer data
Employee & contractor vetting
SERVER ENVIRONMENT

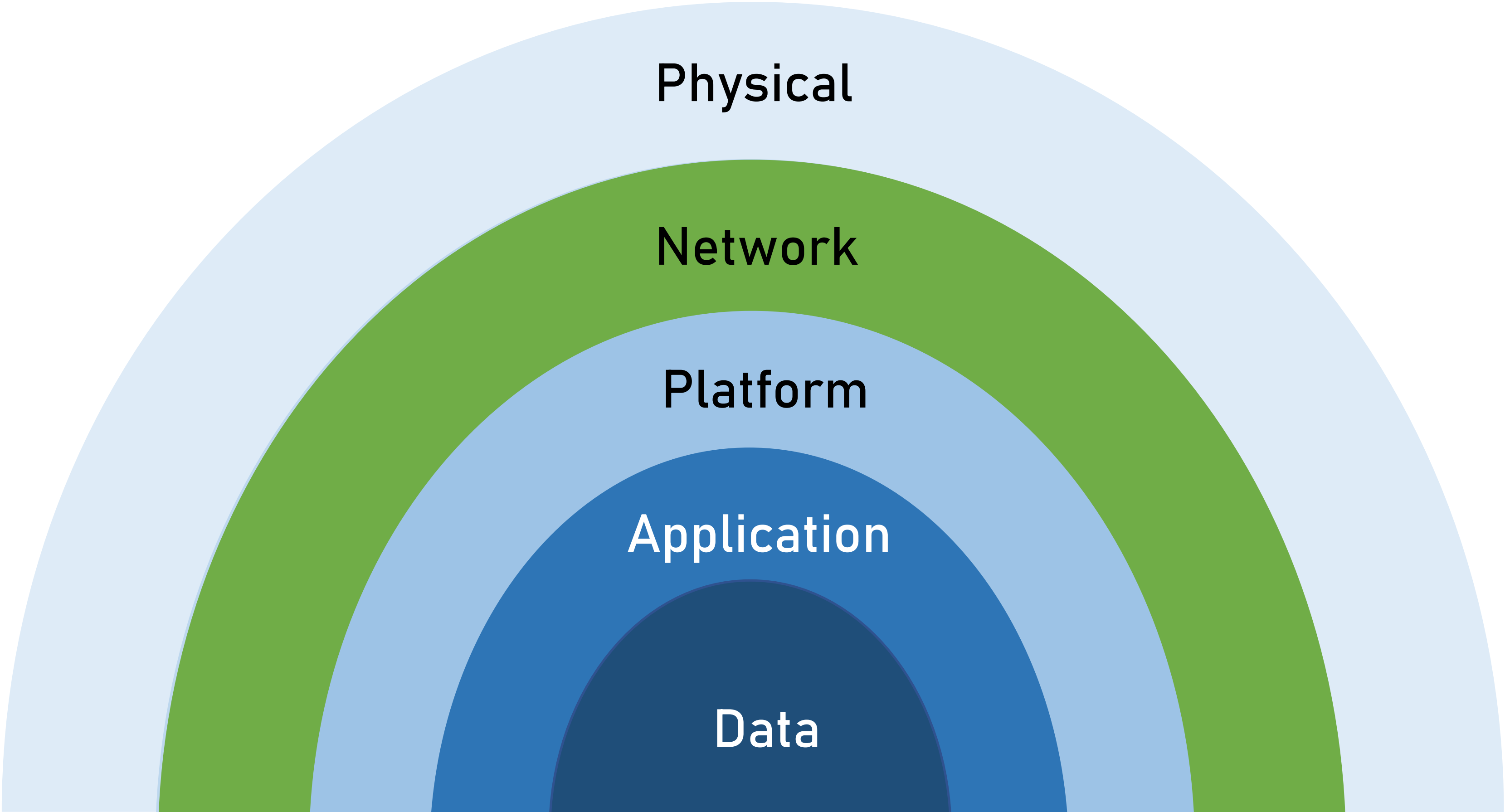
Source: https://www.slideshare.net/karlots/azure-security-architecture-88395266

Physical Security and the Architect

- The Architect usually not involved in physical security
- Usually it’s a given
- It’s good to be aware of it, nothing more

Network Security

Be Aware / Recommend



Network Security

- Controls the access to the organization’s network
- Makes sure the network stays up and running and reliable even under heavy attacks (DDoS…)
- Some more aspects we won’t discuss here

Network Security

- Access Control:
  - Usually performed by authentication engine
    - ie. Active Directory
  - Various types of authentication
    - User / Password, Biometric, Text, MFA

Network Security

- Reliability:
  - Firewall FORTINET f5 cisco
  - Segmentation
  - IPS – Intrusion Prevention System paloalto NETWORKS FIREEYE

Network Security and the Architect

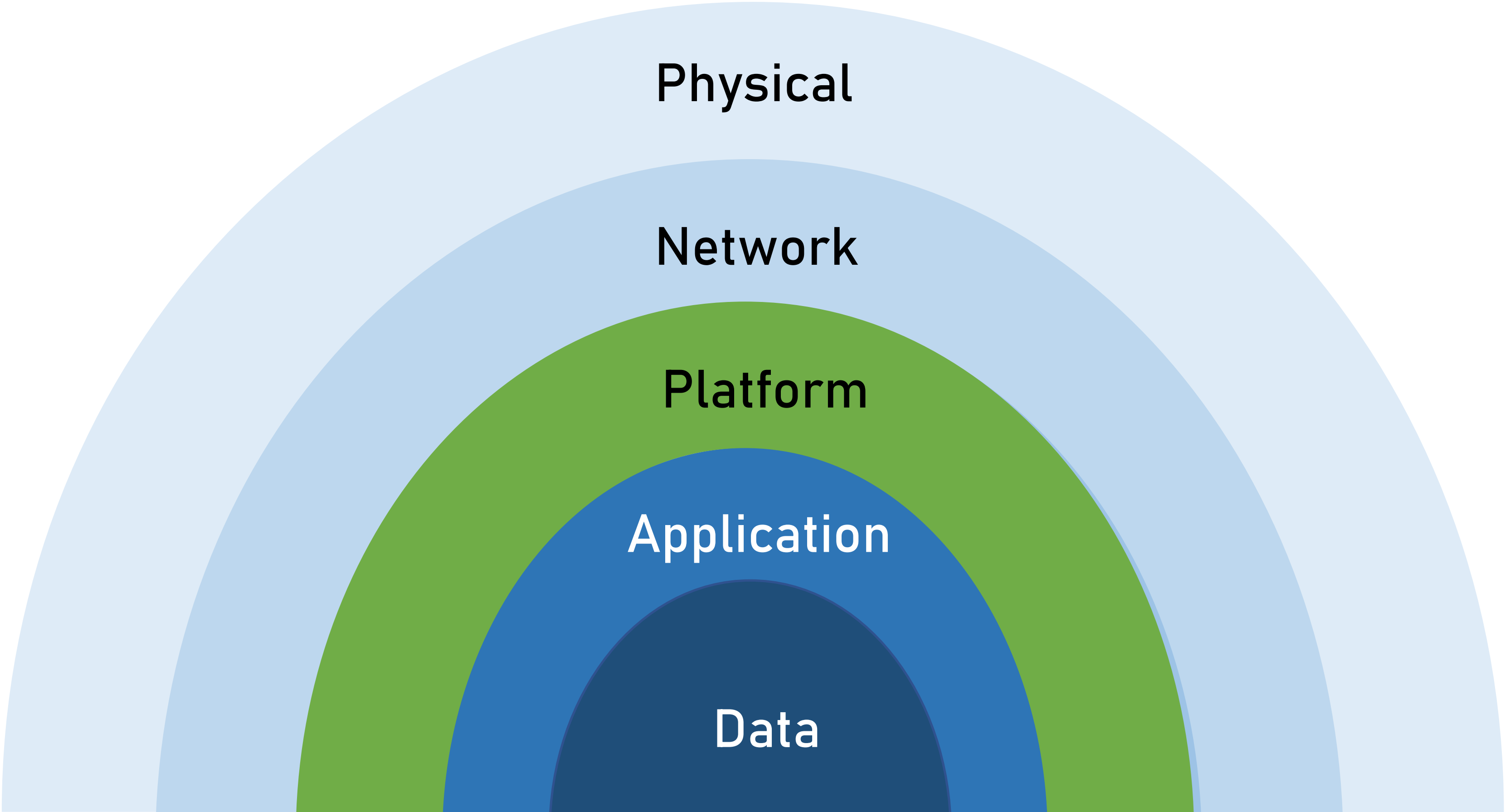
- The Architect should be aware of the network security
- Some components might affect the architecture
  - ie. Firewall that filters specific content, segmentation that prevents certain components from communicating

Network Security and the Architect

- The Architect might recommend some network security aspects:
  - Adding firewall in front of the system
  - Segmentation to protect sensitive data

Platform Security

Be Aware / Recommend



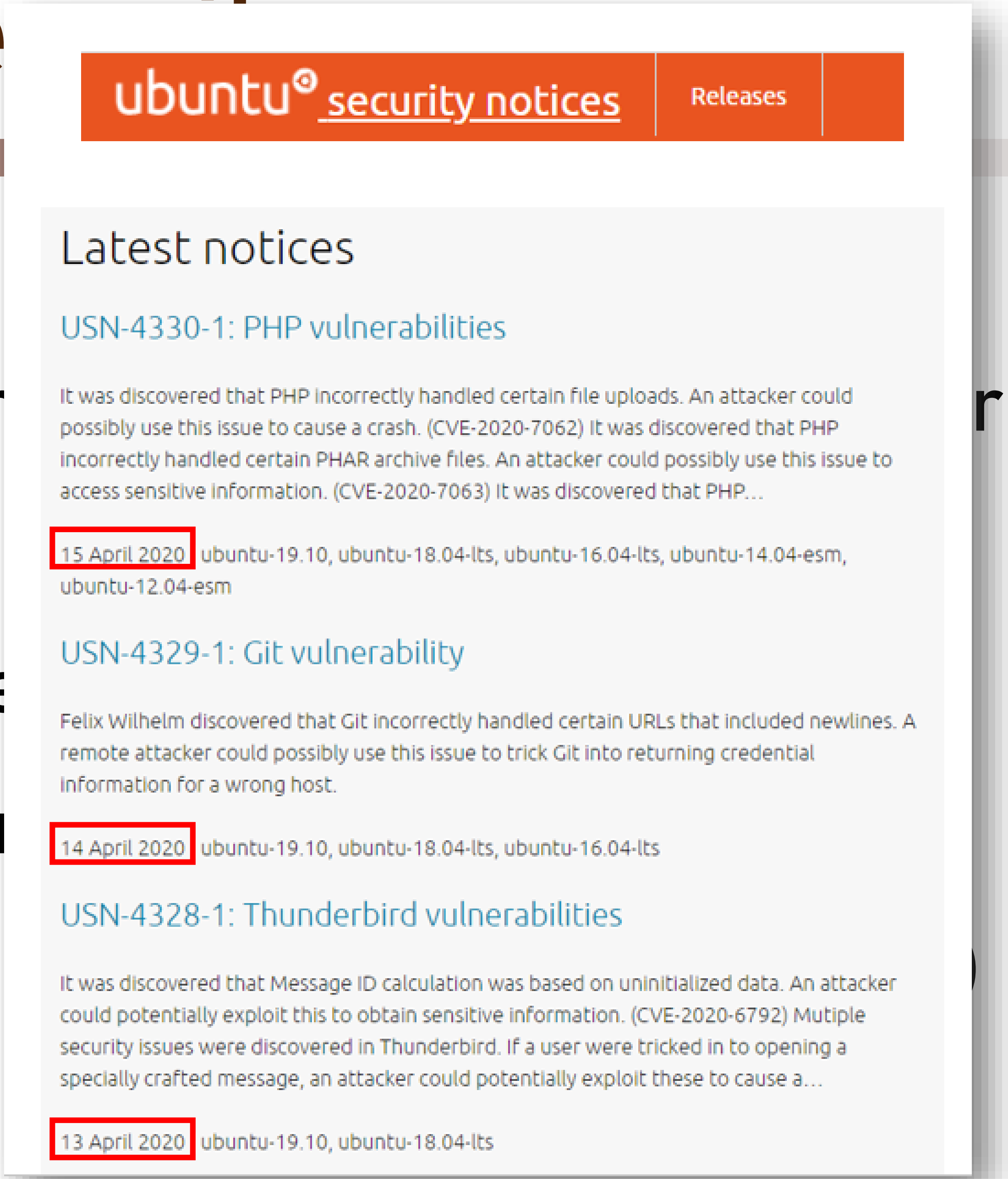
Platform Security

- Secures the computers, VMs, etc.

- Sometimes call Operations Security

Platform Se

- Done by:
  - Using modern re Windows 2003 / XP)
  - Patch Manage
  - Up-to-date A
  - Sometimes –)



ubuntu® security notices

Latest notices

USN-4330-1: PHP vulnerabilities

It was discovered that PHP incorrectly handled certain file uploads. An attacker could possibly use this issue to cause a crash. (CVE-2020-7062) It was discovered that PHP incorrectly handled certain PHAR archive files. An attacker could possibly use this issue to access sensitive information. (CVE-2020-7063) It was discovered that PHP...

15 April 2020 ubuntu-19.10, ubuntu-18.04-lts, ubuntu-16.04-lts, ubuntu-14.04-esm, ubuntu-12.04-esm

USN-4329-1: Git vulnerability

Felix Wilhelm discovered that Git incorrectly handled certain URLs that included newlines. A remote attacker could possibly use this issue to trick Git into returning credential information for a wrong host.

14 April 2020 ubuntu-19.10, ubuntu-18.04-lts, ubuntu-16.04-lts

USN-4328-1: Thunderbird vulnerabilities

It was discovered that Message ID calculation was based on uninitialized data. An attacker could potentially exploit this to obtain sensitive information. (CVE-2020-6792) Mutiple security issues were discovered in Thunderbird. If a user were tricked in to opening a specially crafted message, an attacker could potentially exploit these to cause a...

13 April 2020 ubuntu-19.10, ubuntu-18.04-lts

https://usn.ubuntu.com/

Platform Security and the Architect

- The Architect should be aware of the platform security
- The OS version is often part of the architecture
- Need to make sure it’s supported and protected (patched, Anti-Virus)