UNIVERSITATEA LUCIAN BLAGA DIN SIBIU

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

CLUJ IT

Sibiu IT Cluster

SID 2024
Sibiu Innovation Days
24-25 October, Sibiu - RO

THE EMERGING TECHNOLOGIES: the drivers for digital transformation in business and education

Architecting Cybersecurity

Planning and Designing the Cybersecurity Program

Cybersecurity at Continental

› Importance of cybersecurity in Continental locations and environments
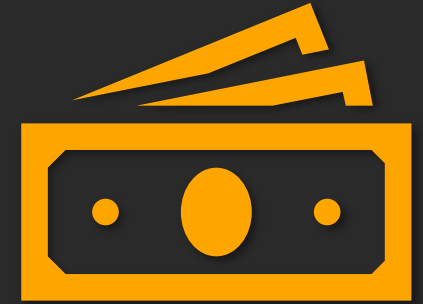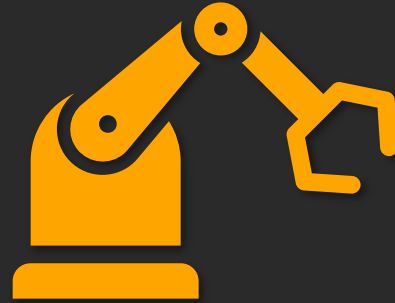› Key goals: regulation compliance, best practices, and quality standards

Approach and End Goals

› Integrate cybersecurity from the ground up into all development phases
› Compliance with industry standards (ISO/SAE 21434, IEC 62443)
› Enhancing interoperability between Continental entities
› Ensuring secure locations and production environments

Sec[Prod]

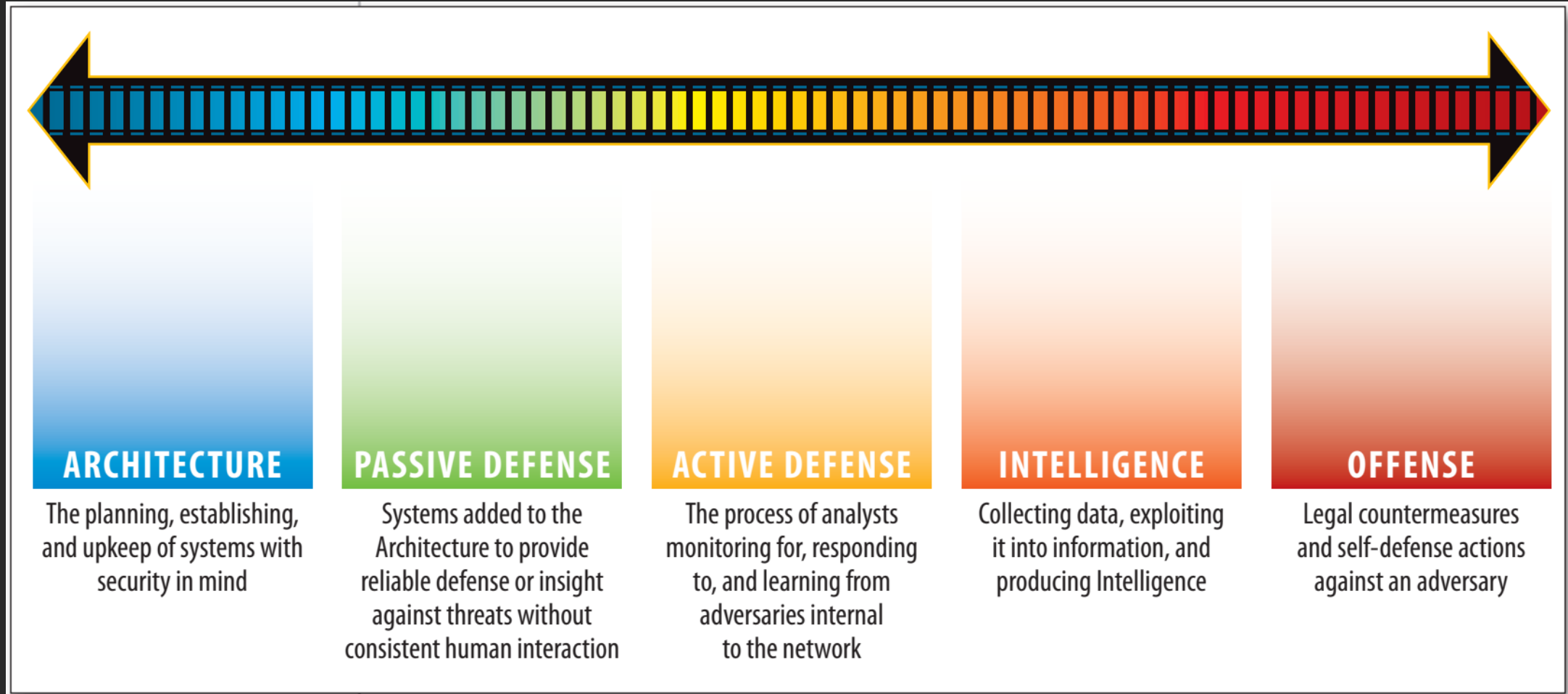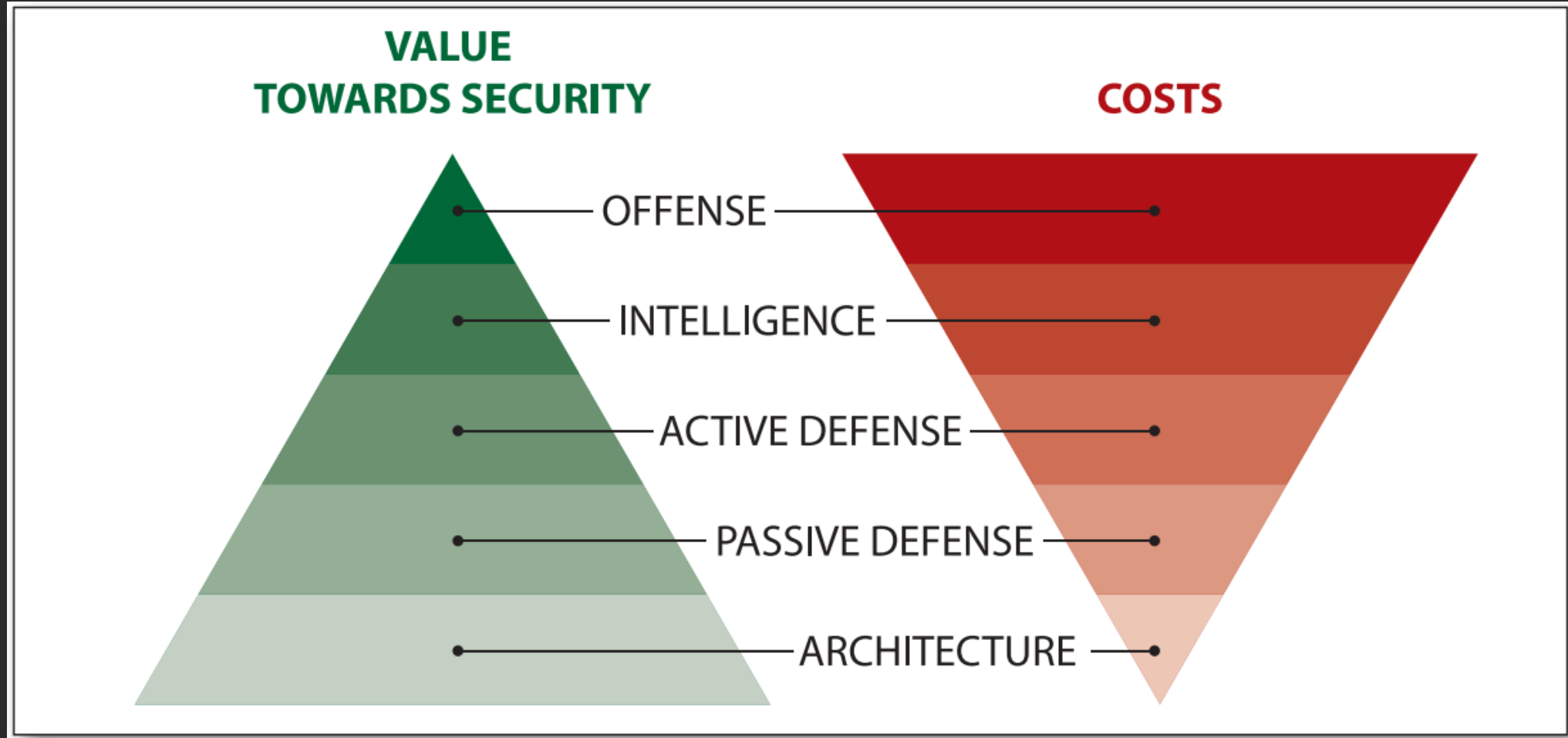# Cybersecurity Challenges

› Managing evolving threats in OT environments

› Effective integration of cybersecurity in the manufacturing processes

› Security throughout the lifecycle

› Balancing cost versus security effectiveness

The Sliding Scale of Cyber Security

ARCHITECTURE — The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE — Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

ACTIVE DEFENSE — The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

INTELLIGENCE — Collecting data, exploiting it into information, and producing Intelligence

OFFENSE — Legal countermeasures and self-defense actions against an adversary

Internal

Value Towards Security vs. Cost

Internal

Defense-in-Depth Architecture

Anti-Malware and Whitelisting

Patchmanagement

Network Separation

Access Control

Secure Settings
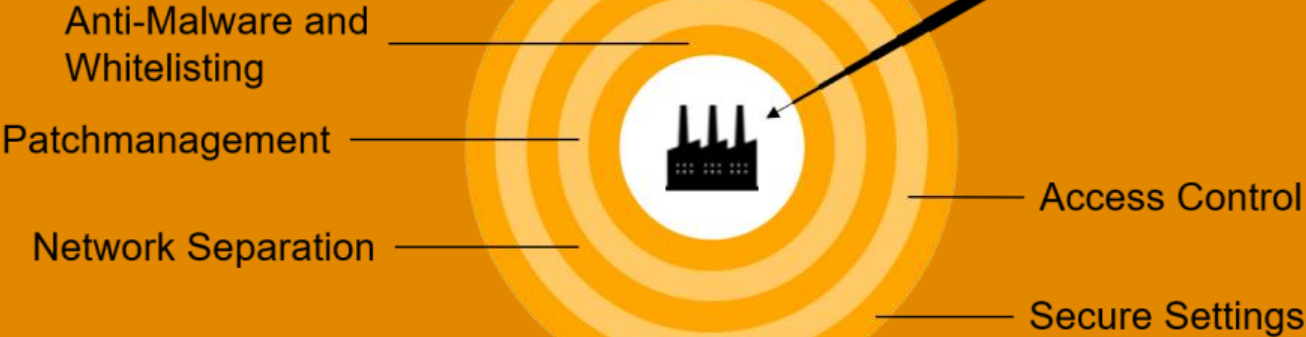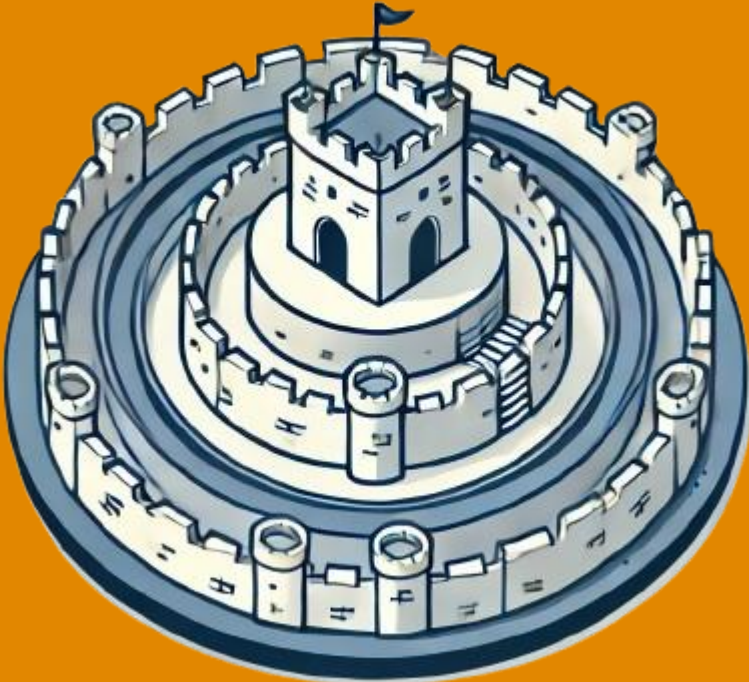
Roadmap
NIST Cybersecurity Framework

Identify

What type of protection do our assets and processes need?

Asset & Risk Management

Protect

Implement appropriate safeguards to ensure protection of the enterprise's assets

Preventive Measures

Detect

Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents

Scans & Analysis

Respond

Develop techniques to contain the impact of cybersecurity events

Response & Remediation

Recover

Implement processes to restore capabilities and services impaired by security events

Resiliency & Recovery

Internal

Core & Functions
NIST Cybersecurity Framework

Functions	ID//identify 1	PR//protect 2	DE//detect 3	RS//respond 4	RC//recover 5
Categories	**AM//** (1.1) asset management	**AC//** (2.1) identity management and access control	**AE//** (3.1) anomalies and events	**RP//** (4.1) response planning	**RP//** (5.1) recovery planning
	BE// (1.2) business environment	**AT//** (2.2) awareness and training	**CM//** (3.2) continuous monitoring	**CO//** (4.2) communications	**IM//** (5.2) improvements
	GV// (1.3) governance	**DS//** (2.3) data security	**DP//** (3.3) detection processes	**AN//** (4.3) analysis	**CO//** (5.3) communications
	RA// (1.4) risk assessment	**IP//** (2.4) information protection		**MI//** (4.4) mitigation	
	RM// (1.5) risk management strategy	**MA//** (2.5) maintenance		**IM//** (4.5) improvements	
	SC// (1.6) supply chain risk management	**PT//** (2.6) protective technology			

Risk Management

Systematic approach to identifying and managing cybersecurity risks

Thank you!

For questions or further discussion, feel free to reach out.

roland-paul.moraru@continental-corporation.com

Internal