

# SECURITY FUNDAMENTALS AND DEVELOPMENT

WEEK 8: SECURITY FRAMEWORKS AND POLICIES

# **AGENDA**

- Activities:
  - Quiz
  - Work on your CA
  - Work on CIS Control Case Study (answers to be discussed next week)

# CASE STUDY

**CIS CONTROLS** 

## Activity: CIS Controls Case Study

This is a group activity

- I. Open the file entitled: "Week 08 -Activity (CIS Controls Case study v7")
- 2. Read the security incident described in the case study and analyze the situation:
  - a) What security issues do you detect in the scenario?
  - b) What CIS v7 controls could have been implemented to reduce the impact to the company?
- 3. Add your answer to the paddlet:

https://padlet.com/rohitvexp/cis-controls-v7-case-study-7rhrlqggnodjs6sd

- Resources on Moodle
  - PDF with CIS v7 Controls
  - CIS Control Navigator & Mapping to other cybersec frameworks - https://www.cisecurity.org/ controls/cis-controls-navigator/v7-I
  - Other case studies

#### Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

#### **Foundational**

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
  - 13 Data Protection
  - 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- and Control

### **Organizational**

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises