Section Introduction, Security Controls

This section of the Security Fundamentals domain will briefly cover security controls, as they will be covered in greater detail throughout the course. We will take a look at the following:

- **Physical Security Controls** (Deterrents, access controls, monitoring controls)
- **Network Security Controls** (Firewalls, NIPS, NIDS, SIEM, NAC)
- **Endpoint Security Controls** (HIPS, HIDS, EDR, Anti-Virus, SIEM)
- **Email Security Controls** (Spam filters, DLP, email scanning)

Although this lesson is looking at security controls grouped by where they are deployed (such as endpoints vs email systems), security controls are actually categorized into the below three groups. We have included a few examples in each.

TECHNICAL CONTROLS	ADMINISTRATIVE CONTROLS	PHYSICAL CONTROLS
Firewalls	Security Awareness Training	Security Guards
-	-	-
Intrusion Prevention Systems	Organisational Policies	Perimeter Fencing
-	-	-
Anti-Virus	Disciplinary Programs	Security Checkpoints
-		-
Endpoint Detection and Response		CCTV and Lighting

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Understand the basics of physical, network, host, and email security technologies.
- Explain what the different security controls do to reduce risk and protect the organization.
- Build a foundation of security controls that will be developed throughout the course.

Back to Lesson

● 5 Topics

○ DF2) Forensics Fundamentals

● 10 Topics | 5 Quizzes

‹ Previous Lesson

Back to Lesson

Next Topic ›

Privacy - Terms

Privacy & Cookies Policy