

# 专科文凭 防御型网络安全



**tech** 科学技术大学

## 专科文凭 防御型网络安全

- » 模式:在线
- » 时长: 6个月
- » 学位: TECH 科技大学
- » 课程表:自由安排时间
- » 考试模式:在线

网页链接: [www.techtitute.com/cn/school-of-business/postgraduate-diploma/postgraduate-diploma-defensive-cybersecurity](http://www.techtitute.com/cn/school-of-business/postgraduate-diploma/postgraduate-diploma-defensive-cybersecurity)

# 目录

01	02	03	04
欢迎	为什么在TECH学习?	为什么选择我们的课程?	目标
4	6	10	14
	05	06	07
	结构和内容	方法	我们学生的特质
	20	28	36
	08	09	10
	课程管理	对你事业的影响	对你公司的好处
	40	46	50
			11
			学位
			54

# 01 欢迎

在大多数发达社会，互联网是日常生活的一部分。它们的日常使用意味着公民越来越习惯于使用数字工具，并将其用于任何日常行动。它们也导致了重大的商业突破。然而，犯罪分子已经找到了一种新的在线操作方式，使几乎所有的公司都面临风险。在这种情况下，公司高管和中层管理人员需要获得卓越的知识，使他们能够在面对可能的攻击时采取防御行动，采取预防措施，避免其数字基础设施受到攻击。为了满足企业专业人员的这种专业化需求，TECH设计了这个关于防御性网络安全的专门学术课程，这对保护你的企业非常有用。



预防性网络安全专科文凭。  
TECH 科技大学



“

得益于情报、网络安全和颠覆性技术专家教授的大师班, 专注于防御性网络安全”

02

# 为什么在TECH学习?

TECH是世界上最大的100%在线商业学校。它是一所精英商学院，具有最大的学术需求模式。一个国际高绩效和管理技能强化培训的中心。



“

TECH是一所站在技术前沿的  
大学, 它将所有资源交给学生支  
配, 以帮助他们取得商业成功”

## TECH科技大学



### 创新

该大学提供一种在线学习模式,将最新的教育科技与最大的教学严谨性相结合。一种具有最高国际认可度的独特方法,将为学生提供在不断变化的世界中发展的钥匙,在这个世界上,创新必须是所有企业家的基本承诺。

“由于在节目中加入了创新的互动式多视频系统,被评为“微软欧洲成功案例”。



### 最高要求

TECH的录取标准不是经济方面的。在这所大学学习没有必要进行大量投资。然而,为了从TECH毕业,学生的智力和能力的极限将受到考验。该机构的学术标准非常高。

**95%** | TECH学院的学生成功完成学业



### 联网

来自世界各地的专业人员参加TECH,因此,学生将能够建立一个庞大的联系网络,对他们的未来很有帮助。

**+100,000**

每年培训的管理人员

**+200**

不同国籍的人



### 赋权

学生将与最好的公司和具有巨大声望和影响力的专业人士携手成长。TECH已经与7大洲的主要经济参与者建立了战略联盟和宝贵的联系网络。

**+500**

| 与最佳公司的合作协议



### 人才

该计划是一个独特的建议,旨在发挥学生在商业领域的才能。这是一个机会,你可以利用它来表达你的关切和商业愿景。

TECH帮助学生在这个课程结束后向世界展示他们的才华。



### 多文化背景

通过在TECH学习,学生将享受到独特的体验。你将在一个多文化背景下学习。在一个具有全球视野的项目中,由于该项目,你将能够了解世界不同地区的工作方式,收集最适合你的商业理念的创新信息。

TECH的学生来自200多个国家。

TECH追求卓越,为此,有一系列的特点,使其成为一所独特的大学:



### 分析报告

TECH探索学生批判性的一面,他们质疑事物的能力,他们解决问题的能力和他们的人际交往能力。



### 优秀的学术成果

TECH为学生提供最好的在线学习方法。大学将再学习方法(国际公认的研究生学习方法)与哈佛大学商学院的案例研究相结合。传统和前卫在一个艰难的平衡中,在最苛刻的学术行程中。



### 规模经济

TECH是世界上最大的网上大学。它拥有超过10,000个大学研究生课程的组合。而在新经济中,数量+技术=颠覆性价格。这确保了学习费用不像在其他大学那样昂贵。



### 向最好的人学习

TECH教学团队在课堂上解释了导致他们在其公司取得成功的原因,在一个真实、活泼和动态的环境中工作。全力以赴提供优质专业的教师,使学生在事业上有所发展,在商业世界中脱颖而出。

来自20个不同国籍的教师。



在TECH,你将有机会接触到学术界最严格和最新的案例研究"

03

# 为什么选择我们的课程？

完成科技课程意味着在高级商业管理领域取得职业成功的可能性倍增。

这是一个需要努力和奉献的挑战，但它为我们打开了通往美好未来的大门。学生将从最好的教学团队和最灵活、最创新的教育方法中学习。



“

我们拥有最著名的教师队伍和市场上最完整的教学大纲, 这使我们能够为您提供最高学术水平的培训”

该方案将提供众多的就业和个人利益,包括以下内容。

01

### 对学生的职业生涯给予明确的推动

通过在TECH学习,学生将能够掌握自己的未来,并充分开发自己的潜力。完成该课程后,你将获得必要的技能,在短期内对你的职业生涯作出积极的改变。

本专业70%的学员在不到2年的时间内实现了职业的积极转变。

02

### 制定公司的战略和全球愿景

TECH提供了一般管理的深刻视野,以了解每个决定如何影响公司的不同职能领域。

我们对公司的全球视野将提高你的战略眼光。

03

### 巩固高级商业管理的学生

在TECH学习,为学生打开了一扇通往非常重要的专业全景的大门,使他们能够将自己定位为高级管理人员,对国际环境有一个广阔的视野。

你将在100多个高层管理的真实案例中工作。

04

### 承担新的责任

在该课程中,将介绍最新的趋势、进展和战略,以便学生能够在不断变化的环境中开展专业工作。

45%的参训人员在内部得到晋升。

05

### 进入一个强大的联系网络

TECH将其学生联系起来,以最大限度地增加机会。有同样关注和渴望成长的学生。你将能够分享合作伙伴、客户或供应商。

你会发现一个对你的职业发展至关重要的联系网络。

06

### 以严格的方式开发公司项目

学生将获得深刻的战略眼光,这将有助于他们在考虑到公司不同领域的情况下开发自己的项目。

我们20%的学生发展自己的商业理念。

07

### 提高软技能和管理技能

TECH帮助学生应用和发展他们所获得的知识,并提高他们的人际交往能力,使他们成为有所作为的领导者。

提高你的沟通和领导能力,为你的职业注入活力。

08

### 成为一个独特社区的一部分

学生将成为由精英经理人、大公司、著名机构和来自世界上最著名大学的合格教授组成的社区的一部分:TECH科技大学社区。

我们给你机会与国际知名的教授团队一起进行专业学习。

# 04 目标

TECH的这个大学预防网络安全专家是为了加强希望在网络安全方面获得更高专业性的公司经理的专业技能。在这种特殊情况下,这个课程的重点是防御型网络安全以便学生获得必要的技能,在一个在商业领域越来越受欢迎的部门成功地进行管理。毫无疑问,这项工作在当今社会具有重要意义。





培养你管理企业数字安全所需的技能"

你的目标就是我们的目标  
我们一起工作,帮助你实现这些目标。  
防御性网络安全专科文凭学生培训在:

01

指定个人和专业数据的备份策略

04

扫描你的计算机以查找入侵者

02

评估不同的工具,为特定的安全问题提供解决方案

03

建立机制以更新系统

05

确定系统访问规则



06

检查和分类电子邮件以防止欺诈

08

分析当前的网络架构以确定我们必须保护的边界

09

开发具体的防火墙和 Linux 配置以减轻最常见的攻击

07

发展允许的软件列表

10

检查下一代防火墙提供的不同附加层以及云环境的网络功能



11

确定网络保护工具并展示它们为何对多层防御至关重要

14

指定在 iOS 平台和 Android 平台上执行渗透测试的主要步骤

12

确定移动设备用户面临的主要攻击和恶意软件类型

13

分析最新设备以在配置中建立更高的安全性



15

发展有关不同保护和安全工具的专业知识

16

分析主要的物联网架构

17

开发核心应用协议

18

评估风险级别和已知漏洞



# 05

## 结构和内容

这个TECH课程的设计是为了满足那些希望拓宽IT安全知识的商业专业人士的专业需求，这是一个基础的领域，以便能够控制可能对公司构成巨大风险的潜在威胁。通过这种方式，大学防御性网络安全专科文凭将使他们能够获得具体的知识，并将其应用于工作实践，以防止可能的网络攻击。



“

以有利于你在网络安全过程中的培训为导向的教学大纲”

## 教学大纲

TECH - 科技大学的专科文凭网络安全防御课程是一项密集的计划,旨在为学生在信息安全领域面对挑战和企业决策做好准备。

在 600 个学时的学习中,学生将通过个人工作学习大量的实际案例,从而掌握必要的技能,在日常实践中取得成功。因此,它是一个真正的沉浸在真实的商业环境中。

这个课程深入处理商业的不同领域,旨在让管理人员从战略、国际和创新的角度理解教育管理。

此外,TECH 为学生提供完整且独家的大师班,出自具有丰富专业经验和国际威望的专家教师之手。

因此,毕业生将深入研究网络安全防御,涉及诸如主机安全、网络安全、智能手机安全和物联网等重要概念。

一个为学生设计的计划,专注于你的专业提高,为他们在环境和能源管理领域取得优异成绩做准备。一个通过基于最新趋势的创新内容了解你和你公司需求的课程,并得到最佳教育方法和杰出师资的支持,这将使你获得创造性和高效地解决关键情况的技能。

模块 1

主机的安全

模块 2

网络安全(周边)

模块 3

智能手机的安全

模块 4

物联网安全



### 何时,何地,如何授课?

TECH提供了以完全在线的方式发展这种防御性网络安全专科文凭的可能性。在培训持续的6个月中,学生可以将能够访问这个课程的所有内容,这将使你能够自我管理你的学习。

一个独特的、关键的、决定性的教育经历,以促进你的专业发展,实现明确的飞跃。

## 模块 1.主机的安全

### 1.1. 备份副这个

- 1.1.1. 备份策略
- 1.1.2. 适用于 Windows 的工具
- 1.1.3. Linux 的工具
- 1.1.4. macOS 的工具

### 1.2. 用户的防毒软件

- 1.2.1. 防毒软件的类型
- 1.2.2. 适用于 Windows 的防毒软件
- 1.2.3. linux 的防毒软件
- 1.2.4. MacOS的防毒软件
- 1.2.5. 智能手机的防毒软件

### 1.3. 入侵探测器 - HIDS

- 1.3.1. 入侵探测方法
- 1.3.2. Sagan
- 1.3.3. Aide
- 1.3.4. Rkhunter

### 1.4. 这个地防火墙

- 1.4.1. Windows 防火墙
- 1.4.2. Linux 的防火墙
- 1.4.3. MacOS 防火墙

### 1.5. 密码管理器

- 1.5.1. Password
- 1.5.2. LastPass
- 1.5.3. KeePass
- 1.5.4. 粘性密码
- 1.5.5. RoboForm

### 1.6. 网络钓鱼检测器

- 1.6.1. 手动 钓鱼 检测器
- 1.6.2. 网络 钓鱼 工具

### 1.7. 间谍软件

- 1.7.1. 回避机制
- 1.7.2. 反间谍软件工具

### 1.8. 追踪器

- 1.8.1. 系统保护措施
- 1.8.2. 反追踪工具

### 1.9. EDR- 端点检测和响应

- 1.9.1. EDR 系统行为
- 1.9.2. EDR 和防病毒软件的区别
- 1.9.3. EDR系统的未来

### 1.10. 控制安装 software 软件

- 1.10.1. 存储库和软件商店
- 1.10.2. 允许或禁止的软件列表
- 1.10.3. 更新标准
- 1.10.4. 安装软件的权限

**模块 2. 网络安全(周边)****2.1. 威胁检测和预防系统**

- 2.1.1. 安全事件的总体框架
- 2.1.2. 目前的防御系统: 纵深防御和 SOC
- 2.1.3. 当前的网络架构
- 2.1.4. 用于检测和预防事故的工具类型
  - 2.1.4.1. 基于网络的系统
  - 2.1.4.2. 基于主机的Host系统
  - 2.1.4.3. 集中式系统
- 2.1.5. 阶段/主机、容器和无服务器的通信和检测

**2.2. 防火墙**

- 2.2.1. 防火墙的类型
- 2.2.2. 攻击和缓解
- 2.2.3. Linux 内核的常用防火墙 防火墙
  - 2.2.3.1. UFW
  - 2.2.3.2. Nftables 和 iptables
  - 2.2.3.3. 防火墙(Firewalld)
- 2.2.4. 基于系统日志的检测系统
  - 2.2.4.1. TCP 包装器
  - 2.2.4.2. BlockHosts 和 DenyHosts
  - 2.2.4.3. Fai2ban

**2.3. 入侵检测和预防系统(IDS/IPS)**

- 2.3.1. 对 IDS/IPS 的攻击
- 2.3.2. IDS/IPS 系统
  - 2.3.2.1. Snort
  - 2.3.2.2. Suricata

**2.4. 下一代防火墙(NGFW)**

- 2.4.1. NGFW与传统防火墙的区别
- 2.4.2. 核心能力
- 2.4.3. 商务解决方案
- 2.4.4. cloud防火墙
  - 2.4.4.1. 云 VPC 架构
  - 2.4.4.2. 云ACLs
  - 2.4.4.3. 安全组

**2.5. 代理服务器**

- 2.5.1. 类型 Proxy
- 2.5.2. Proxy.使用优缺点

**2.6. 防毒引擎**

- 2.6.1. 恶意软件和 IOC 的背景
- 2.6.2. 防毒引擎的问题

**2.7. 邮件保护系统**

- 2.7.1. 反垃圾邮件
  - 2.7.1.1. 黑白名单
  - 2.7.1.2. 贝叶斯过滤器
- 2.7.2. 邮件网关 (MGW)

**2.8. SIEM**

- 2.8.1. 组件和架构
- 2.8.2. 关联规则和用例
- 2.8.3. SIEM 系统的当前挑战

**2.9. SOAR**

- 2.9.1. SOAR和SIEM: 敌人或盟友
- 2.9.2. SOAR系统的未来

**2.10. 其他基于网络的系统**

- 2.10.1. WAF
- 2.10.2. NAC
- 2.10.3. 蜜罐和蜜网
- 2.10.4. CASB

## 模块 3. 智能手机的安全

### 3.1. 移动设备的世界

- 3.1.1. 移动平台类型
- 3.1.2. 设备
- 3.1.3. 安卓设备

### 3.2. 移动安全管理

- 3.2.1. OWASP 移动安全项目
  - 3.2.1.1. 十大漏洞
- 3.2.2. 通信、网络 and 连接模式

### 3.3. 商业环境的移动设备

- 3.3.1. 风险
- 3.3.2. 安全政策
- 3.3.3. 设备监控
- 3.3.4. 移动设备管理 (MDM)

### 3.4. 用户隐私和数据安全

- 3.4.1. 信息状态
- 3.4.2. 数据保护和保密
  - 3.4.2.1. 许可权
  - 3.4.2.2. 加密
- 3.4.3. 安全数据存储
  - 3.4.3.1. iOS 的安全存储
  - 3.4.3.2. 安卓的安全存储
- 3.4.4. 应用程序开发中的正确做法

### 3.5. 漏洞和攻击媒介

- 3.5.1. 漏洞
- 3.5.2. 攻击向量
  - 3.5.2.1. 恶意软件
  - 3.5.2.2. 泄露数据
  - 3.5.2.3. 操作数据

### 3.6. 主要威胁

- 3.6.1. 用户未强制
- 3.6.2. 恶意软件
  - 3.6.2.1. 恶意软件的类型
- 3.6.3. 社会工程学
- 3.6.4. 数据泄露
- 3.6.5. 信息盗窃
- 3.6.6. 不安全的 Wi-Fi 网络

- 3.6.7. 过时的软件
- 3.6.8. 恶意应用程序
- 3.6.9. 弱密码
- 3.6.10. 安全设置薄弱或不正确
- 3.6.11. 物理访问
- 3.6.12. 丢失或被盗的设备
- 3.6.13. 身份冒充 (诚信)
- 3.6.14. 弱或损坏的密码学
- 3.6.15. 拒绝服务 (DoS)

### 3.7. 主要攻击

- 3.7.1. 网络钓鱼攻击
- 3.7.2. 与通信模式相关的攻击
- 3.7.3. 网络钓鱼攻击
- 3.7.4. Criptojacking 攻击
- 3.7.5. 中间人攻击

### 3.8. 黑客攻击

- 3.8.1. Rooting 和 Jailbreaking
- 3.8.2. 移动攻击剖析
  - 3.8.2.1. 威胁传播
  - 3.8.2.2. 在设备上安装恶意软件
  - 3.8.2.3. 持久性
  - 3.8.2.4. 有效载荷执行和信息提取
- 3.8.3. 入侵 iOS 设备: 机制和工具
- 3.8.4. 入侵 Android 设备: 机制和工具

### 3.9. 渗透测试

- 3.9.1. iOS 渗透测试
- 3.9.2. 安卓 渗透测试
- 3.9.3. 工具

### 3.10. 保护和安全的

- 3.10.1. 安全设定
  - 3.10.1.1. iOS 设备
  - 3.10.1.2. 安卓设备
- 3.10.2. 安防措施
- 3.10.3. 保护工具

**模块 4. 物联网安全****4.1. 设备**

- 4.1.1. 设备类型
- 4.1.2. 标准化架构
  - 4.1.2.1. ONEM2M
  - 4.1.2.2. IoTWF
- 4.1.3. 应用协议
- 4.1.4. 连接技术

**4.2. 物联网设备应用领域**

- 4.2.1. 智能家居
- 4.2.2. 智慧城市
- 4.2.3. 运输
- 4.2.4. 可穿戴设备
- 4.2.5. 卫生部门
- 4.2.6. IIoT

**4.3. 通讯协议**

- 4.3.1. MQTT
- 4.3.2. LWM2M
- 4.3.3. OMA-DM
- 4.3.4. TR-069

**4.4. 智能家居**

- 4.4.1. 家庭自动化
- 4.4.2. 网络
- 4.4.3. 家用电器
- 4.4.4. 警惕和安全

**4.5. 智慧城市**

- 4.5.1. 照明
- 4.5.2. 气象
- 4.5.3. 安全

**4.6. 运输**

- 4.6.1. 地点
- 4.6.2. 付款和获得服务
- 4.6.3. 连接性

**4.7. 可穿戴设备**

- 4.7.1. 智能衣服
- 4.7.2. 智能首饰
- 4.7.3. 智能手表

**4.8. 卫生部门**

- 4.8.1. 运动/心率监测
- 4.8.2. 监测患者和老年人
- 4.8.3. 可植入的
- 4.8.4. 手术机器人

**4.9. 连接性**

- 4.9.1. WiFi/网关
- 4.9.2. 蓝牙
- 4.9.3. 内置连接

**4.10. 证券化**

- 4.10.1. 专用网络
- 4.10.2. 密码管理器
- 4.10.3. 使用加密协议
- 4.10.4. 使用提示

# 06 方法

这个培训计划提供了一种不同的学习方式。我们的方法是通过循环的学习模式发展起来的: **Re-learning**。

这个教学系统被世界上一些最著名的医学院所采用,并被**新英格兰医学杂志**等权威出版物认为是最有效的教学系统之一。





“

发现 Re-learning, 这个系统放弃了传统的线性学习, 带你体验循环教学系统: 这种学习方式已经证明了其巨大的有效性, 尤其是在需要记忆的科目中”



## TECH商学院使用案例研究来确定所有内容的背景

我们的方案提供了一种革命性的技能和知识发展方法。我们的目标是在一个不断变化, 竞争激烈和高要求的环境中加强能力建设。

“

和TECH,你可以体验到一种正在动摇  
世界各地传统大学基础的学习方式”



该课程使你准备好在不确定的环境中  
面对商业挑战, 使你的企业获得成功。



我们的课程使你准备好在不确定的环境中面对新的挑战,并取得事业上的成功。

## 一种创新并不同的学习方法

该技术课程是一个密集的培训课程,从头开始创建,为国内和国际最高水平的管理人员提供挑战和商业决策。由于这种方法,个人和职业成长得到了促进,向成功迈出了决定性的一步。案例法是构成这一内容的基础的技术,确保遵循最新的经济,社会和商业现实。



你将通过合作活动和真实案例,学习如何解决真实商业环境中的复杂情况”

在世界顶级商学院存在的时间里,案例法一直是最广泛使用的学习系统。1912年开发的案例法是为了让法律学生不仅在理论内容的基础上学习法律,案例法向他们展示真实的复杂情况,让他们就如何解决这些问题作出明智的决定和价值判断。1924年,它被确立为哈佛大学的一种标准教学方法。

在特定情况下,专业人士应该怎么做?这就是我们在案例法中面临的问题,这是一种以行动为导向的学习方法。在整个课程中,学生将面对多个真实案例。他们必须整合所有的知识,研究,论证和捍卫他们的想法和决定。

## Re-learning 方法

TECH有效地将案例研究方法与基于循环的100%在线学习系统相结合, 在每节课中结合了个不同的教学元素。

我们用最好的100%在线教学方法加强案例研究: Re-learning。

我们的在线系统将允许你组织你的时间和学习节奏, 使其适应你的时间表。你将能够从任何有互联网连接的固定或移动设备上获取容。

在TECH, 你将用一种旨在培训未来管理人员的尖端方法进行学习。这种处于世界教育学前沿的方法被称为 Re-learning。

我们的商学院是唯一获准采用这种成功方法的西班牙语学校。2019年, 我们成功地提高了学生的整体满意度 (教学质量, 材料质量, 课程结构, 目标.....), 与西班牙语最佳在线大学的指标相匹配。





在我们的方案中,学习不是一个线性的过程,而是以螺旋式的方式发生(学习,解除学习,忘记和重新学习)。因此,我们将这些元素中的每一个都结合起来。这种方法已经培养了超过65万名大学毕业生,在生物化学,遗传学,外科,国际法,管理技能,体育科学,哲学,法律,工程,新闻,历史,金融市场和工具等不同领域取得了前所未有的成功。所有这些都是在一个高要求的环境中进行的,大学学生的社会经济状况很好,平均年龄为43.5岁。

Re-learning 将使你的学习事半功倍,表现更出色,使你更多地参与到训练中,培养批判精神,捍卫论点和对比意见:直接等同于成功。

从神经科学领域的最新科学证据来看,我们不仅知道如何组织信息,想法,图像y记忆,而且知道我们学到东西的地方和背景,这是我们记住它并将其储存在海马体的根本原因,并能将其保留在长期记忆中。

通过这种方式,在所谓的神经认知背景依赖的电子学习中,我们课程的不同元素与学员发展其专业实践的背景相联系。

该方案提供了最好的教育材料,为专业人士做了充分准备:



### 学习材料

所有的教学内容都是由教授该课程的专家专门为该课程创作的,因此,教学的发展是具体的。

然后,这些内容被应用于视听格式,创造了TECH在线工作方法。所有这些,都是用最新的技术,提供最高质量的材料,供学生使用。



### 大师课程

有科学证据表明第三方专家观察的有用性。

向专家学习可以加强知识和记忆,并为未来的困难决策建立信心。



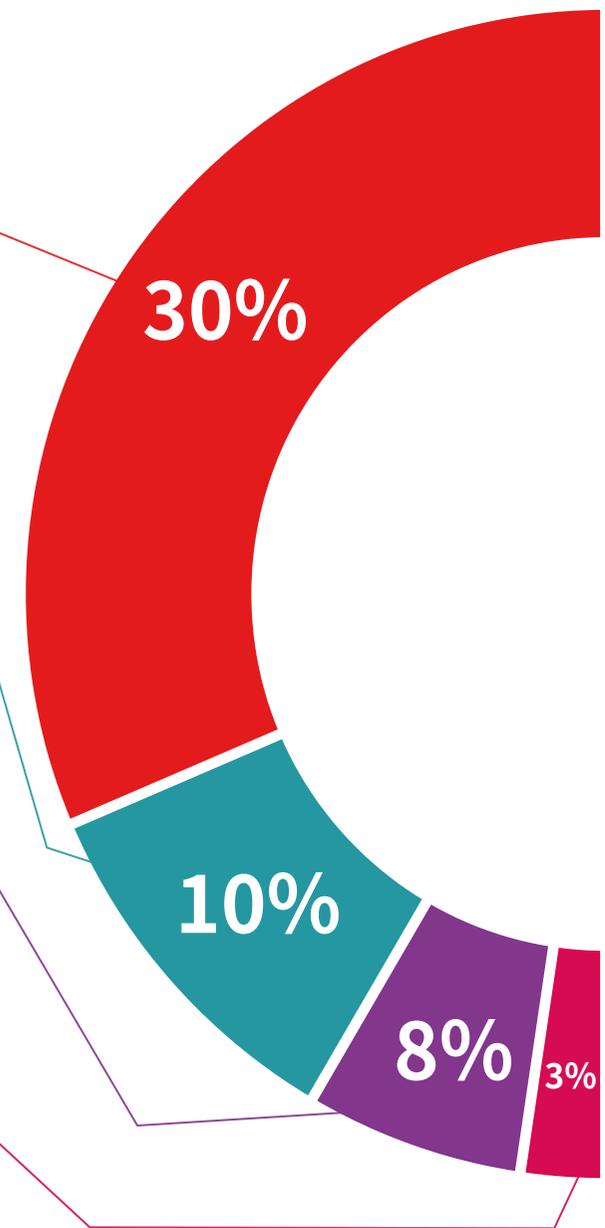
### 管理技能实习

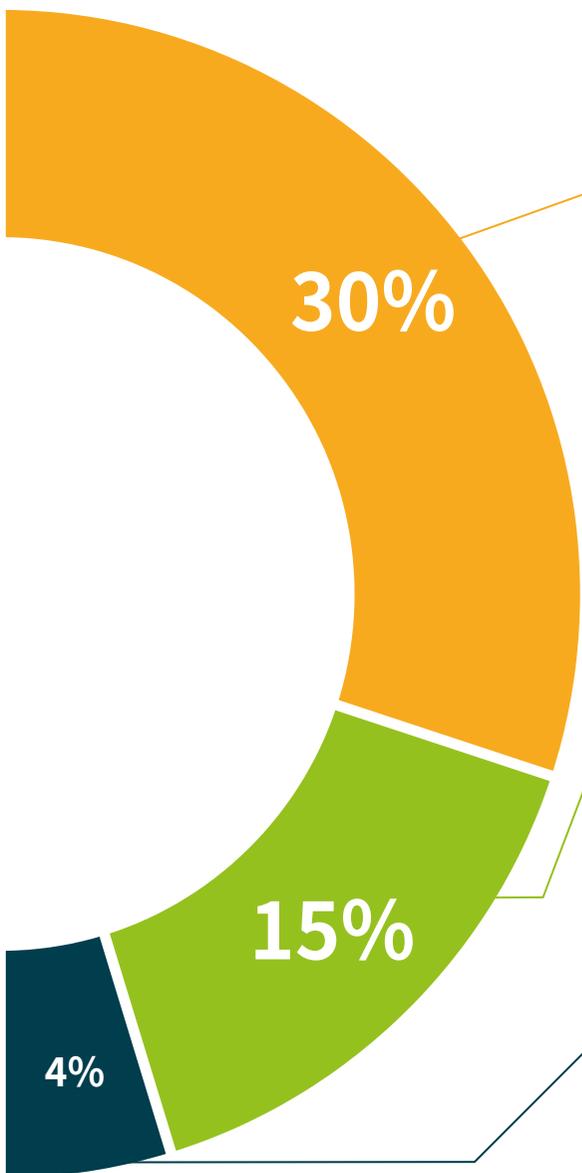
他们将在每个学科领域开展具体的管理能力发展活动。获得和培训高级管理人员在我们所处的全球化框架内所需的技能和能力的做法和新情况。



### 延伸阅读

最近的文章,共识文件和国际准则等。在TECH的虚拟图书馆里,学生可以获得他们完成培训所需的一切。





### 案例研究

他们将完成专门为这个学位选择的最佳案例研究。由国际上最好的高级管理专家介绍,分析和辅导的案例。



### 互动式总结

TECH团队以有吸引力和动态的方式将内容呈现在多媒体中,其中包括音频,视频,图像,图表和概念图,以强化知识。这个用于展示多媒体内容的独特教育系统被微软授予“欧洲成功案例”称号。



### 测试和循环测试

在整个课程中,通过评估和自我评估活动和练习,定期评估和重新评估学习者的知识:通过这种方式,学习者可以看到他/她是如何实现其目标的。



07

# 我们学生的特质

防御性网络安全专科文凭是一个高学术水平的课程, 针对希望通过优质教育提高培训水平的企业经理或中层管理人员。21世纪的学生, 意识到互联网对公司的危险, 希望在任何部门的相关领域拓宽自己的知识, 为了保护他们的企业和他们工作的公司, 决定获得计算机安全方面的更高专业。





“

这个课程的学生是经验丰富的专业人员, 希望在复杂的网络安全领域扩展他们的知识”

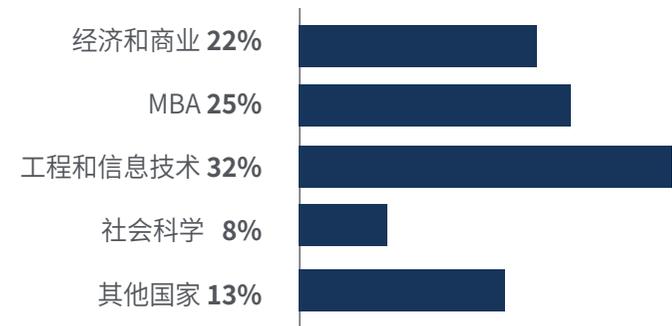
### 平均年龄

**35**岁至**45**岁之间

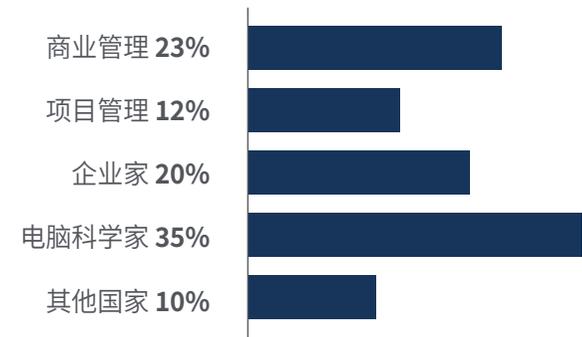
### 经验年限



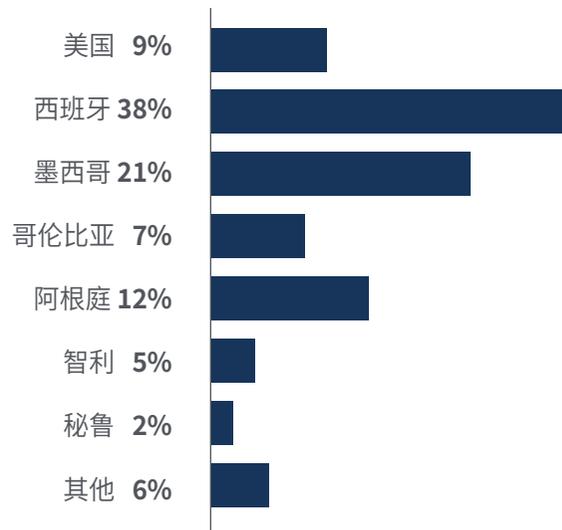
### 教育



### 学术概况



## 地域分布



## Jaime Díaz

首席收入官

“完成这个课程使我能够提高我在防御性网络安全方面的培训,这是IT安全的一个相关方面,对我的职业发展非常有用,因为在一个明显的数字时代,能够防止数字攻击是任何专业人士的附加价值。”

08

# 课程管理

这个大学防御性网络安全专科文凭的教师是在这个领域具有丰富经验的专业人士,无论是在专业方面还是在教育方面。他们在这一领域的专业性使他们拥有必要的资格,为学生提供完整和高质量的学习科目,这些科目对他们在商业世界的日常工作很有帮助。他们当然是相信高等教育是推动其专业发展和提高企业竞争力的途径的人。





“

经验丰富的教师,帮助你在  
网络安全方面的专业性”

## 国际客座董事

Frederic Lemieux 博士是国际公认的创新专家和鼓舞人心的领导者 智力, 国土安全部, 内部安全, 网络安全 和 颠覆性技术。他在研究和教育方面的不懈努力和贡献, 使他成为促进安全和了解当今新兴技术的关键人物。在他的职业生涯中, 他曾在 蒙特利尔大学、乔治-华盛顿大学 和 乔治城大学等多所知名院校构思和指导尖端学术课程。

在他的广泛背景中, 他出版了许多重要著作, 所有这些著作都与犯罪情报、警务、网络威胁和国际安全有关。刑事情报、警务、网络威胁和国际安全。他还在学术期刊上发表了大量文章, 研究重大灾害期间的犯罪控制、反恐、情报机构和警务合作等问题, 为网络安全领域做出了重大贡献。此外, 他还在各种国家和国际会议上担任小组成员和主旨发言人, 在学术和专业领域树立了自己的典范。

莱米厄博士曾在各种学术、私人 and 政府组织中担任编辑和评估职务, 这反映了他在其专业领域的影响力和追求卓越的决心。他卓越的学术生涯使他担任乔治城大学MPS应用智能、网络安全风险管理、技术管理以及信息技术管理项目的实践教授和学院主任。



## Lemieux, Frederic 博士

---

- 美国华盛顿州乔治敦网络安全风险管理硕士主任
- 乔治城大学技术管理硕士课程主任
- 乔治敦大学应用情报学硕士课程主任
- 乔治敦大学实习教授
- 他还获得了蒙特利尔大学犯罪学学院的犯罪学博士学位
- 拉瓦尔大学社会学硕士和心理学辅修学位
- 成员: 乔治城大学新项目圆桌委员会

“

感谢 TECH, 你将能够与世界上最优秀的专业人士一起学习”

## 管理人员



### Fernández Sapena, Sonia 女士

- 马德里赫塔菲的国家计算机和电信参考中心的计算机安全和道德黑客培训师
- 认证的电子理事会讲师
- 获得以下认证的培训师: EXIN 道德 黑客基金会 以及 EXIN 网络和 IT 安全基金会。马德里
- 获得以下专业证书的CAM专家认证培训师: 计算机安全 (IFCT0190)、语音和数据网络管理 (IFCM0310)、部门网络管理 (IFCT0410)、电信网络警报管理 (IFCM0410)、语音和数据网络运营商 (IFCM0110) 和互联网服务管理 (IFCT0509)
- 巴利阿里群岛大学外部合作者CSO/SSA (首席安全官/高级安全架构师)
- 马德里毕业于阿尔卡拉德埃纳雷斯大学的生物学专业
- DevOps领域的大师: Docker 和 KubernetesCas-培训
- 微软 Azure 安全技术。E-Council

## 教师

### Jiménez Ramos, Álvaro 先生

- ◆ 网络安全分析师
- ◆ The Workshop 高级安全分析师
- ◆ Axians 网络安全分析师 L1
- ◆ Axians 网络安全分析师 L2
- ◆ SACYR S.A. 的网络安全分析师
- ◆ 马德里理工大学远程信息处理工程学士
- ◆ CICE 网络安全和道德黑客硕士
- ◆ Deusto Training 的高级网络安全课程

### Peralta Alonso, Jon 先生

- ◆ 阿尔蒂亚高级数据保护和网络安全顾问
- ◆ Arriaga Asociados Asesoramiento Jurídico y Económico S.L. 律师/法律顾问
- ◆ 专业公司的法律顾问/实习生: Óscar Padura
- ◆ 巴斯克公立大学法律学位
- ◆ EIS 创新学校数据保护硕士课程代表
- ◆ 巴斯克公立大学宣传硕士学位
- ◆ 卡斯蒂利亚伊莎贝尔一世国际大学民事诉讼实践专业硕士学位
- ◆ 个人数据保护、网络安全和信息通信技术法硕士学位讲师

### Marcos Sbarbaro, Victoria Alicia 女士

- ◆ B60 的原生 Android 移动应用程序开发人员UK (英国)
- ◆ 负责管理、协调和记录虚拟化安全警报环境的分析程序员
- ◆ 自动取款机 Java 应用程序分析员
- ◆ 签名验证和文件管理 应用软件 开发专业人员
- ◆ 系统技术人员负责设备迁移和PDA移动设备的管理、维护和培训
- ◆ 加泰罗尼亚奥伯塔大学计算机系统技术工程师
- ◆ 新技术专业学院 CICE 的官方 EC-Council 和 CompTIA 计算机安全和道德黑客硕士课程

### Catalá Barba, José Francisco 先生

- ◆ 电子技术员 网络安全专家
- ◆ 移动应用程序开发人员
- ◆ 西班牙国防部中级指挥部电子技术员
- ◆ 巴伦西亚福特 Sita 工厂的电子技术员

09

# 对你事业的影响

完成这一课程将为商业专业人员的资格增加一个质量加分项,因为它提供了一个外部领域的深入知识,对于需要控制那些可能藏有影响整个组织的有害外部因素的IT流程的商业专业人员来说,是非常有用的。因此,这门专科文凭将成为最高级管理人员培训的增值。



“

一个高水平的计划,可以让你彻底改变你的职业”

## 你准备好飞跃了吗？ 卓越的职业提升在等着你

TECH Global University大学防御网络安全专家是一个密集且高价值的项目，旨在提高学生在广泛能力领域的工作技能。这无疑是一个独特的机会，可以提高专业水平，也可以提高个人水平，因为这涉及到努力和奉献。

提高自己学生专业水平上实现积极的变化，并与最好的人交流，这里就是你的地方在TECH。

完成这个课程后，你将能够更好地控制数字流程的安全。

一个独特的个人和职业改进方案。

### 改变的时候到



### 改变的类型



## 工资提高

---

完成这个课程后, 我们学生的工资会增长超过**25.22%**



# 10

## 对你公司的好处

防御性网络安全专科文凭、通过培训高级领导人,帮助最大限度地发挥组织的人才潜力通过这种方式,商业专业人士将能够通过掌握必要的技能,自己控制网络安全进程,为公司带来更多的质量。一个适合学生获得必要工具的计划,他们随后可以在日常实践中应用这些工具,为他们的公司带来巨大利益。





“

对于希望监测和管理潜在的网络安全问题的商业专业人员来说, 这是一个必备的方案”

培养和留住公司的人才是最好的长期投资。

01

### 人才和智力资本的增长知识资本

该专业人员将为公司带来新的概念、战略和观点,可以为组织带来相关的变化。

---

02

### 留住高潜力的管理人员,避免人才流失

这个计划加强了公司和经理人之间的联系,并为公司内部的职业发展开辟了新的途径。

03

### 培养变革的推动者

你将能够在不确定和危机的时候做出决定,帮助组织克服障碍。

---

04

### 增加国际扩张的可能性

由于这一计划,该公司将与世界经济的主要市场接触。



05

### 开发自己的项目

可以在一个真实的项目上工作, 或在其公司的研发或业务发展领域开发新。

---

06

### 提高竞争力

该课程将使具备接受新挑战的技能, 从而促进组织的发展。

# 11 学位

防御型网络安全专科文凭除了保证最严格和最新的培训外,还可以获得由TECH科技大学颁发的专科文凭学位证书。



“

成功地完成这一培训,并获得你的大学学历,没有旅行或行政文书的麻烦”

这个**防御型网络安全专科文凭**包含了市场上最完整和最新的科学课程。

评估通过后, 学生将通过邮寄收到**TECH科技大学**颁发的相应的**专科文凭**学位。

**TECH科技大学**颁发的证书将表达在专科文凭获得的资格, 并将满足工作交流, 竞争性考试和专业职业评估委员会的普遍要求。

学位: **防御型网络安全专科文凭**

模式: **在线**

时长: **6个月**





## 专科文凭 防御型网络安全

- » 模式:在线
- » 时长: 6个月
- » 学位: TECH 科技大学
- » 课程表:自由安排时间
- » 考试模式:在线

# 专科文凭 防御型网络安全

