高级硕士

网络安全高级管理 (CIS O, Chief Information Security Officer)

tech 科学技术大学

tech 科学技术大学

高级硕士
网络安全高级管理 (CISO, Chief Information Security Officer)

- 模式:**在线**
- 时长: **2年**
- 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/information-technology/advanced-master-degre/advanced-master-degree-senior-cybersecurity-management-ciso-chief-information-security-officer

目录

01

课程介绍

如今，网络安全已成为保护个人和企业免受日益增加的数字威胁的关键支柱。这一学科不仅专注于保护组织的技术系统和关键信息，还在领导安全策略的规划、实施和监督方面发挥重要作用。因此，其主要目标是降低风险并有效应对网络攻击和事件。网络安全总监的主要职责包括设计安全政策、管理技术风险以及领导专业团队。面对技术进步和数字化带来的挑战，专门为解决这些问题而设计的课程应运而生。TECH不仅专注于确保信息保护的效率，还在于识别和管理新的漏洞。这使得CISO成为任何组织恢复力最重要的因素。

通过 TECH，你可以专攻 IT 领域最重要的领域之一，并成为该领域的领导者”

网络安全高级管理在数字化和高度互联的世界中，保障组织的稳定性和连续性至关重要。通过实施强有力的安全战略和采用先进的技术，风险得到了降低，并且防止了灾难性后果的攻击。在银行、医疗保健和公共基础设施等关键领域，在这些领域专业人士的推动下，治理和监管合规使得安全性得到加强。

这一纪律使组织能够建立更加安全的数字工作环境，从而增强了客户、合作伙伴和用户的信任。成功的结果大大节省了数百万美元的潜在经济损失，同时促进了以安全为共同优先事项的组织文化。此外，事实证明，在不断变化的环境中，对于保护组织的创新，声誉和可持续性至关重要。

TECH 的高级硕士旨在培养专业人员领导有效的安全策略。在整个课程中，学生将按照自己的节奏学习，重点培养管理技能和战略商业眼光。此外，您还将获得尖端的专业技术，为您在全球市场上高度需求的职业中脱颖而出做好准备。由于采用 100% 在线模式，参与者能够将学习与工作职责结合起来，从而让他们能够在不影响专业活动的情况下取得进步。

这个**网络安全高级管理（CISO，Chief Information Security Officer）高级硕士**包含了市场上最完整又最新的科学课程。主要特点是：

- 由计算机专家提出的实际案例的发展
- 内容图文并茂,示意性强,实用性强,为那些视专业实践至关重要的学科提供了科学和实用的信息
- 进行自我评估以改善学习的实践练习
- 特别强调高级网络安全管理(CISO, Chief Information Security Officer)的创新方法
- 理论知识,专家预论,争议主题讨论论坛和个人反思工作
- 可以通过任何连接互联网的固定或便携设备访问课程内容

> 本高级硕士将让您站在行业的最前沿，并为您打开无尽的工作机会”

培养应对未来挑战所需的技能，同时不忽视当前的活动”

通过适应您的学习进度的Relearning方法成为技术基础设施的保护者。

成为世界上最大的数字大学的一部分，并在世界任何地方进行专业化。

教学人员包括来自新闻领域的专业人士，他们将自己的工作经验带到这个课程中，还有来自领先公司和著名大学的公认专家。

通过采用最新的教育技术制作的多媒体内容，专业人士将能够进行情境化学习，即通过模拟环境进行沉浸式培训，以应对真实情况。

这个课程的设计重点是基于问题的学习，通过这种方式，学生必须尝试解决整个学术课程中提出的不同专业实践情况。为此，职业人士将得到由著名专家开发的创新互动视频系统的协助。

02

为什么在TECH学习?

TECH 是世界上最大的数字大学。拥有超过14,000个大学课程的令人印象深刻的目录，涵盖11种语言，我们以就业率99%的领先地位跻身行业前列。此外，超过6,000名享有国际声誉的顶尖教授团队。

在世界上最大的数字大学学习并确保您的职业成功。未来始于TECH”

福布斯评选的全球最佳在线大学

著名的商业和金融杂志福布斯将泰晤士河科技大学评为《世界上最好的在线大学》。他们在数字版最近的一篇文章中提到了这一点，并在文中重复了这所学校的成功故事，«这要归功于它提供的学术课程，精选的师资队伍以及旨在培养未来专业人员的创新学习方法»

最好的国际教学团队

TECH 的教学人员由 6,000 多名具有最高国际声望的教授组成。教授、研究人员和跨国公司高层管理人员，其中包括：Isaiah Covington，波士顿凯尔特人队的表现教练；Magda Romanska，哈佛MetaLAB的首席研究员；Ignacio Wistumba，MD安德森癌症中心转化分子病理学部门的主席；以及D.W Pine，TIME杂志的创意总监等。

世界上最大的数字化大学

TECH 是世界上最大的数字大学。我们是最大的教育机构，拥有最好，最广泛的数字课程目录，100%在线且涵盖绝大多数知识领域。我们提供世界上最多的自主学位、官方研究生学位和本科学位。总共有超过 14,000 个大学学位，涵盖十种不同的语言，使我们成为世界上最大的教育机构。

大学里最全面的学习计划

TECH 提供大学中最全面的课程，其主题涵盖基本概念以及特定科学领域的主要科学进步。这些课程也不断更新，以确保学生拥有最先进的学术技能和最需要的专业技能。通过这种方式，大学学位为毕业生在职业成功道路上提供了显著的优势。

独特的学习方法

TECH 是第一所在所有学位中采用Relearning的大学。这是最好的在线学习方法，获得著名教育机构提供的国际教学质量认证。并且，这一颠覆性的学术模式与“案例教学法”相辅相成，构成了独特的在线教学策略。还提供创新的教料，包括详细的视频，信息图表和交互式摘要。

NBA 官方在线大学

TECH是NBA的官方在线大学。由于与主要篮球联盟达成协议，该校为学生提供独家大学课程，以及专注于联盟业务和体育产业其他领域的各种教料。每个课程都有独特设计的课程设置，并邀请了杰出的演讲嘉宾：这些职业运动员具有卓越的运动经历，将分享他们在相关主题上的经验。

就业率领先者

TECH 已成功成为就业能力领先的大学。99%的学生在完成大学课程后不到一年时间，就能在所学专业领域找到工作。同样多的人也成功地立即提升了自己的职业生涯。这一切都归功于一种学习方法，该方法的有效性基于掌握专业发展所必需的实践技能。

Google Partner Premier

北美科技巨头已授予TECH Google Partner Premier 徽章。该奖项仅授予全球 3% 的公司，凸显了该大学为学生提供的有效，灵活和定制的体验。这一认可不仅认可了 TECH 数字基础设施的最高严谨性，性能和投资，而且还使该大学成为世界上最前沿的科技公司之一。

被学生评价为最佳大学

主要的评价网站已将TECH评为全球学生评分最高的大学。这些评价平台因其可靠性和声誉而受到认可，得益于对每条评论真实性的严格验证和确认，它们给予了TECH高度正面的评价。这些数据表明，TECH 是国际上绝对的大学参考。

03

教学大纲

网络安全高级管理（CIS O，Chief Information Security Officer）高级硕士旨在培养能够管理全球组织信息安全的战略领导者。该课程采用全面，最新的方法，涵盖了网络安全治理和风险管理等关键领域。通过这种方式，学生将培养领导高绩效团队和实施安全政策的管理技能。此外，在了解最新趋势和新兴技术的同时，毕业生将学会应对数字环境的挑战并引领未来的安全。

TECH 让您成为在全球商业环境中预防、检测和缓解网络威胁的战略家”

模块 1. 网络情报与网络安全

1.1. 网络情报
- 1.1.1. 网络情报
  - 1.1.1.1.智能
    - 1.1.1.1.1.情报周期
  - 1.1.1.2.网络情报
  - 1.1.1.3.网络情报与网络安全
- 1.1.2. 情报分析员
  - 1.1.2.1.情报分析师的角色
  - 1.1.2.2.情报分析员在评估活动中的偏见

1.2. 网络安全
- 1.2.1. 安全层
- 1.2.2. 识别网络威胁
  - 1.2.2.1.外部威胁
  - 1.2.2.2.内部威胁
- 1.2.3. 不利的行动
  - 1.2.3.1.社会工程学
  - 1.2.3.2.常用方法

1.3. 智能技术和工具
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. HUMIT
- 1.3.4. Linux 发行和工具
- 1.3.5. OWISAM
- 1.3.6. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTM

1.4. 评估方法
- 1.4.1. 情报分析
- 1.4.2. 组织获取信息的技术
- 1.4.3. 信息来源的可靠性和可信度
- 1.4.4. 分析方法
- 1.4.5. 情报结果展示

1.5. 审计和文件
- 1.5.1. IT安全审计
- 1.5.2. 审计文件和许可证
- 1.5.3. 审计的类型
- 1.5.4. 可交付的成果
  - 1.5.4.1.技术报告
  - 1.5.4.2.执行报告

1.6. 网络匿名
- 1.6.1. 使用匿名
- 1.6.2. 匿名技术（Proxy，VPN）
- 1.6.3. TOR、Freenet 和 IP2 网络

1.7. 威胁和安全类型
- 1.7.1. 威胁类型
- 1.7.2. 实体安全
- 1.7.3. 网络安全
- 1.7.4. 逻辑安全
- 1.7.5. Web 应用程序的安全性
- 1.7.6. 移动设备的安全

1.8. 法规和合规性
- 1.8.1. RGPD
- 1.8.2. 2019 年国家网络安全战略
- 1.8.3. ISO 27000 系列
- 1.8.4. NIST 网络安全框架
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. 云法规
- 1.8.8. SOX
- 1.8.9. PCI

1.9. 风险分析和指标
- 1.9.1. 风险范围
- 1.9.2. 资产
- 1.9.3. 威胁

1.9.4. 漏洞
1.9.5. 风险评估
1.9.6. 风险处理
1.10. 网络安全领域的重要组织
1.10.1. NIST
1.10.2. ENISA
1.10.3. INCIBE
1.10.4. OEA
1.10.5. UNASUR - PROSUR

模块 2. 主机的安全

2.1. 备份副本
2.1.1. 备份策略
2.1.2. 适用于 Windows 的工具
2.1.3. Linux 的工具
2.1.4. macOS 的工具
2.2. 用户的防毒软件
2.2.1. 防毒软件的类型
2.2.2. 适用于 Windows 的防毒软件
2.2.3. linux 的防毒软件
2.2.4. MacOS的防毒软件
2.2.5. 智能手机的防毒软件
2.3. 入侵探测器 - HIDS
2.3.1. 入侵探测方法
2.3.2. Sagan
2.3.3. Aide
2.3.4. Rkhunter
2.4. 本地防火墙
2.4.1. Windows 防火墙
2.4.2. Linux 的防火墙
2.4.3. MacOS 防火墙
2.5. 密码管理器
2.5.1. Password
2.5.2. LastPass
2.5.3. KeePass
2.5.4. StickyPassword
2.5.5. RoboForm
2.6. 网络钓鱼检测器
2.6.1. 动手钓鱼 检测器
2.6.2. 网络 钓鱼工具
2.7. 间谍软件
2.7.1. 回避机制
2.7.2. 反间谍软件工具
2.8. 追踪器
2.8.1. 系统保护措施
2.8.2. 反追踪工具
2.9. EDR- End Point Detection and Response
2.9.1. EDR 系统行为
2.9.2. EDR 和防病毒软件的区别
2.9.3. EDR系统的未来
2.10. 控制安装软件
2.10.1. 存储库和软件商店
2.10.2. 允许或禁止的软件列表
2.10.3. 更新标准
2.10.4. 安装软件的权限

模块 3. 网络安全（周边）

3.1. 威胁检测和预防系统
3.1.1. 安全事件的总体框架
3.1.2. 目前的防御系统. Defense in Depth 和 SOC
3.1.3. 当前的网络架构

3.1.4. 用于检测和预防事故的工具类型
3.1.4.1.基于网络的系统
3.1.4.2.基于主机的系统
3.1.4.3.集中式系统
3.1.5. 阶段/主机、容器和无服务器的通信和检测
3.2. 防火墙
3.2.1. 防火墙的类型
3.2.2. 攻击和缓解
3.2.3. Linux 内核的常用防火墙 防火墙
3.2.3.1.UFW
3.2.3.2.Nftables 和 iptables
3.2.3.3. Firewalld
3.2.4. 基于系统日志的检测系统
3.2.4.1. TCP Wrappers
3.2.4.2.BlockHosts 和 DenyHosts
3.2.4.3.Fai2ban
3.3. 入侵检测和预防系统(IDS/IPS)
3.3.1. 对 IDS/IPS 的攻击
3.3.2. IDS/IPS 系统
3.3.2.1.Snort
3.3.2.2.Suricata
3.4. 下一代防火墙(NGFW)
3.4.1. NGFW与传统防火墙的区别
3.4.2. 核心能力
3.4.3. 商务解决方案
3.4.4. cloud防火墙
3.4.4.1.云 VPC 架构
3.4.4.2.云ACLs
3.4.4.3.Security Group
3.5. Proxy
3.5.1. proxy类型
3.5.2. proxy使用代理优点与缺点
3.6. 防毒引擎
3.6.1. 恶意软件和 IOC 的背景
3.6.2. 防毒引擎的问题
3.7. 邮件保护系统
3.7.1. 反垃圾邮件
3.7.1.1.黑白名单
3.7.1.2.贝叶斯过滤器
3.7.2. Mail Gateway (MGW)
3.8. SIEM
3.8.1. 组件和架构
3.8.2. 关联规则和用例
3.8.3. SIEM 系统的当前挑战
3.9. SOAR
3.9.1. SOAR 和 SIEM：敌人或盟友
3.9.2. SOAR系统的未来
3.10. 其他基于网络的系统
3.10.1. WAF
3.10.2. NAC
3.10.3. HoneyPots 和 HoneyNets
3.10.4. CASB

模块 4. 智能手机的安全

4.1. 移动设备的世界
4.1.1. 移动平台类型
4.1.2. Ios备
4.1.3. 安卓设备
4.2. 移动安全管理
4.2.1. OWASP 移动安全项目
4.2.1.1.十大漏洞
4.2.2. 通信、网络和连接模式

4.3. 商业环境的移动设备
- 4.3.1. 风险
- 4.3.2. 安全策略
- 4.3.3. 设备监控
- 4.3.4. 移动设备管理 (MDM)

4.4. 用户隐私和数据安全
- 4.4.1. 信息状态
- 4.4.2. 数据保护和保密
  - 4.4.2.1.许可权
  - 4.4.2.2.加密
- 4.4.3. 安全数据存储
  - 4.4.3.1.iOS 的安全存储
  - 4.4.3.2.安卓的安全存储
- 4.4.4. 应用程序开发中的正确做法

4.5. 漏洞和攻击媒介
- 4.5.1. 漏洞
- 4.5.2. 攻击向量
  - 4.5.2.1.恶意软件
  - 4.5.2.2.泄露数据
  - 4.5.2.3.操作数据

4.6. 主要威胁
- 4.6.1. 用户未强制
- 4.6.2. 恶意软件
  - 4.6.2.1.恶意软件的类型
- 4.6.3. 社会工程学
- 4.6.4. 数据泄露
- 4.6.5. 信息盗窃
- 4.6.6. 不安全的 Wi-Fi 网络
- 4.6.7. 过时的软件
- 4.6.8. 恶意应用程序
- 4.6.9. 弱密码
- 4.6.10. 安全设置薄弱或不存在
- 4.6.11. 物理访问
- 4.6.12. 丢失或被盗的设备
- 4.6.13. 身份冒充(诚信)
- 4.6.14. 弱或损坏的密码学
- 4.6.15. 拒绝服务 (DoS)

4.7. 主要攻击
- 4.7.1. 网络钓鱼攻击
- 4.7.2. 与通信模式相关的攻击
- 4.7.3. smishing攻击
- 4.7.4. 加密劫持攻击
- 4.7.5. Man in The Middle

4.8. 黑客攻击
- 4.8.1. Rooting 和Jailbreaking
- 4.8.2. 移动攻击剖析
  - 4.8.2.1.威胁传播
  - 4.8.2.2.在设备上安装恶意软件
  - 4.8.2.3.持久性
  - 4.8.2.4.有效载荷执行和信息提取
- 4.8.3. 黑客入侵 iOS 设备 :机制和工具
- 4.8.4. 黑客入侵安卓 设备 :机制和工具

4.9. 渗透测试
- 4.9.1. iOS 渗透测试
- 4.9.2. 安卓 渗透测试
- 4.9.3. 工具

4.10. 保护和安全
- 4.10.1. 安全设定
  - 4.10.1.1.iOS 设备
  - 4.10.1.2.安卓设备
- 4.10.2. 安防措施
- 4.10.3. 保护工具

模块 5. IoT安全

5.1. 设备
- 5.1.1. 设备类型
- 5.1.2. 标准化架构
  - 5.1.2.1.ONEM2M
  - 5.1.2.2.IoTWF
- 5.1.3. 应用协议
- 5.1.4. 连接技术

5.2. 物联网设备。应用领域
- 5.2.1. 智能家居
- 5.2.2. 智慧城市
- 5.2.3. 运输
- 5.2.4. 可穿戴设备
- 5.2.5. 健康领域
- 5.2.6. IioT

5.3. 通讯协议
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. 智能家居
- 5.4.1. 家庭自动化
- 5.4.2. 网络
- 5.4.3. 家用电器
- 5.4.4. 警惕和安全

5.5. 智慧城市
- 5.5.1. 照明
- 5.5.2. 气象
- 5.5.3. 安全

5.6. 运输
- 5.6.1. 地点
- 5.6.2. 付款和获得服务
- 5.6.3. 连接性

5.7. 可穿戴设备
- 5.7.1. 智能衣服
- 5.7.2. 智能首饰
- 5.7.3. 智能手表

5.8. 健康领域
- 5.8.1. 运动/心率监测
- 5.8.2. 监测患者和老年人
- 5.8.3. 植入它们
- 5.8.4. 手术机器人

5.9. 连接性
- 5.9.1. WiFi/网关
- 5.9.2. 蓝牙
- 5.9.3. 内置连接

5.10. 证券化
- 5.10.1. 专用网络
- 5.10.2. 密码管理器
- 5.10.3. 使用加密协议
- 5.10.4. 使用提示

模块 6. 道德黑客

6.1. 工作环境
- 6.1.1. Linux 发行版
  - 6.1.1.1.Kali Linux - 进攻性安全
  - 6.1.1.2. Parrot OS
  - 6.1.1.3.Ubuntu
- 6.1.2. 虚拟化系统
- 6.1.3. Sandbox
- 6.1.4. 实验室部署

6.2. 方法
- 6.2.1. OSSTM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. Footprinting
- 6.3.1. 开源情报 (OSINT)
- 6.3.2. 搜索数据泄露和漏洞
- 6.3.3. 使用被动工具

6.4. 网络扫描
- 6.4.1. 扫描工具
  - 6.4.1.1.Nmap
  - 6.4.1.2.Hping3
  - 6.4.1.3.其他扫描工具
- 6.4.2. 扫描技术
- 6.4.3. 防火墙和 IDS 规避技术
- 6.4.4. Banner Grabbing
- 6.4.5. 网络图

6.5. 枚举
- 6.5.1. SMTP 枚举
- 6.5.2. DNS 枚举
- 6.5.3. NetBIOS 和 Samba 枚举
- 6.5.4. LDAP 枚举
- 6.5.5. SNMP 枚举
- 6.5.6. 其他枚举技术

6.6. 漏洞扫描
- 6.6.1. 漏洞分析解决方案
  - 6.6.1.1.Qualys
  - 6.6.1.2.Nessus
  - 6.6.1.3.CFI LanGuard
- 6.6.2. 漏洞评分系统
  - 6.6.2.1.CVSS
  - 6.6.2.2.CVE
  - 6.6.2.3.NVD

6.7. 无线网络攻击
- 6.7.1. 无线网络黑客攻击方法
  - 6.7.1.1. Wi-Fi Discovery
  - 6.7.1.2.流量分析
  - 6.7.1.3.aircrack攻击
    - 6.7.1.3.1.WEP攻击
    - 6.7.1.3.2.WPA/WPA2攻击
  - 6.7.1.4.Evil Twin攻击
  - 6.7.1.5.WPS攻击
  - 6.7.1.6.干扰
- 6.7.2. 无线安全工具

6.8. 入侵网络服务器
- 6.8.1. Cross Site Scripting
- 6.8.2. CSRF
- 6.8.3. 会话Hijacking
- 6.8.4. SQLinjection

6.9. 利用漏洞
- 6.9.1. 使用已知漏洞
- 6.9.2. 使用metasploit
- 6.9.3. 使用恶意软件
  - 6.9.3.1.定义和范围
  - 6.9.3.2.生成恶意软件
  - 6.9.3.3.绕过防病毒解决方案

6.10. 持久性
- 6.10.1. Rootkit 的安装
- 6.10.2. ncat 的使用
- 6.10.3. 为后门使用计划任务
- 6.10.4. 用户创建
- 6.10.5. HIDS 检测

模块 7. 逆向工程

7.1. 编译器
- 7.1.1. 代码类型
- 7.1.2. 编译器的阶段
- 7.1.3. 符号表
- 7.1.4. 错误的处理程序
- 7.1.5. GCC 编译器

7.2. 编译器中的解析类型
- 7.2.1. 词法分析
  - 7.2.1.1.术语
  - 7.2.1.2.词汇成分
  - 7.2.1.3.LEX 词法分析器
- 7.2.2. 句法分析
  - 7.2.2.1.文法无上下文
  - 7.2.2.2.解析类型
    - 7.2.2.2.1.自上向下分析
    - 7.2.2.2.2.自下而上分析
  - 7.2.2.3.语法树和派生
  - 7.2.2.4.解析器的类型
    - 7.2.2.4.1.LR（从左到右）解析器
    - 7.2.2.4.2.LALR 解析器
- 7.2.3. 语义分析
  - 7.2.3.1.文法的属性
  - 7.2.3.2.S-属性
  - 7.2.3.3.L-属性

7.3. 汇编器数据结构
- 7.3.1. 变数
- 7.3.2. 数组
- 7.3.3. 指引
- 7.3.4. 结构
- 7.3.5. 物品

7.4. 汇编代码结构
- 7.4.1. 选择结构
  - 7.4.1.1.如果，否则 如果，否则
  - 7.4.1.2.转变
- 7.4.2. 迭代结构
  - 7.4.2.1.For
  - 7.4.2.2.While
  - 7.4.2.3.休息时间的使用
- 7.4.3. 功能

7.5. x86硬件架构
- 7.5.1. x86 处理器架构
- 7.5.2. x86 数据结构
- 7.5.3. x86 代码结构
- 7.5.3. x86 代码结构

7.6. ARM硬件架构
- 7.6.1. ARM 处理器架构
- 7.6.2. ARM 数据结构
- 7.6.3. ARM 代码结构

7.7. 静态代码分析
- 7.7.1. 反汇编程序
- 7.7.2. IDA
- 7.7.3. 代码重建器

7.8. 动态代码分析
- 7.8.1. 行为分析
  - 7.8.1.1.工业电子通讯
  - 7.8.1.2.监测
- 7.8.2. Linux 代码调试器
- 7.8.3. Windows 的代码调试器

7.9. Sandbox
- 7.9.1. sandbox架构
- 7.9.2. 避免 sandbox
- 7.9.3. 检测技术

7.9.4. 躲避技巧
7.9.5. 反措施
7.9.6. Linux 的Sandbox
7.9.7. Windows中的沙盒
7.9.8. MacOS中的sandbox
7.9.9. 安卓上的sandbox
7.10. 恶意软件分析
7.10.1. 恶意软件分析方法
7.10.2. 恶意软件混淆技术
7.10.2.1.可执行的混淆
7.10.2.2.执行环境的限制
7.10.3. 恶意软件分析工具

模块 8. 安全发展

8.1. 安全发展
8.1.1. 质量、功能和安全
8.1.2. 保密性、完整性和可用性
8.1.3. 软件开发生命周期
8.2. 需求阶段
8.2.1. 认证控制
8.2.2. 控制角色和权限
8.2.3. 风险导向的要求
8.2.4. 特权批准
8.3. 分析和设计阶段
8.3.1. 访问组件和系统管理
8.3.2. 审计追踪
8.3.3. 会话管理
8.3.4. 历史数据
8.3.5. 正确的错误处理
8.3.6. 职责分开
8.4. 实施和编码阶段
8.4.1. 保护开发环境
8.4.2. 准备技术文件
8.4.3. 安全加密
8.4.4. 通讯安全
8.5. 安全编码最佳实践
8.5.1. 输入数据验证
8.5.2. 输出数据编码
8.5.3. 编程风格
8.5.4. 变更日志管理
8.5.5. 密码实践
8.5.6. 错误和日志管理
8.5.7. 文件管理
8.5.8. 管理。记忆
8.5.9. 安全功能的标准化和重用
8.6. 服务器准备和加固
8.6.1. 管理服务器上的用户、组别和角色
8.6.2. 软件安装
8.6.3. 服务器加固
8.6.4. 应用环境的配置
8.7. DB准备和硬化
8.7.1. 优化数据库引擎优化
8.7.2. 为应用程序创建自己的用户
8.7.3. 为用户分配精确的权限
8.7.4. 数据库加固加固
8.8. 测试阶段
8.8.1. 质安全控制的质量控制
8.8.2. 阶段性代码检查
8.8.3. 配置管理验证
8.8.4. 黑盒测试
8.9. 准备向生产过渡
8.9.1. 执行变更控制
8.9.2. 执行分步生产程序
8.9.3. 执行回滚过程
8.9.4. 预生产阶段的测试

8.10. 维护阶段
- 8.10.1. 基于风险的保险
- 8.10.2. 白盒安全维护测试
- 8.10.3. 黑盒安全维护测试

模块 9. 软件和硬件中安全策略的实际实施

9.1. 软件和硬件中安全策略的实际实施
- 9.1.1. 实施识别和授权
- 9.1.2. 识别技术的实施
- 9.1.3. 授权的技术措施

9.2. 识别和授权技术
- 9.2.1. 识别器和OTP
- 9.2.2. USB令牌或PKI智能卡
- 9.2.3. “机密防卫”钥匙
- 9.2.4. 有源RFID

9.3. 关于访问软件和系统的安全政策
- 9.3.1. 访问控制政策的实施
- 9.3.2. 通信访问政策的实施
- 9.3.3. 访问控制的安全工具类型

9.4. 用户访问管理
- 9.4.1. 访问权限管理
- 9.4.2. 访问角色和功能的隔离
- 9.4.3. 系统中访问权限的实施

9.5. 对系统和应用程序的访问控制
- 9.5.1. 最低访问规则
- 9.5.2. 安全登录技术
- 9.5.3. 密码安全政策

9.6. 识别系统技术
- 9.6.1. 活动目录
- 9.6.2. OTP
- 9.6.3. PAP, CHAP
- 9.6.4. KERBEROS, DIAMETER, NTLM

9.7. CIS 控制措施用于系统加固
- 9.7.1. 基本 CIS 控制措施
- 9.7.2. CIS 基本控制
- 9.7.3. 组织性的CIS控制

9.8. 运营安全
- 9.8.1. 对恶意代码的保护
- 9.8.2. 备份副本
- 9.8.3. 活动的记录和监测

9.9. 技术脆弱性的管理
- 9.9.1. 技术漏洞
- 9.9.2. 对技术脆弱性的管理
- 9.9.3. 软件安装的限制

9.10. 安全政策实践的实施
- 9.10.1. 逻辑上的漏洞
- 9.10.2. 防御政策的实施

模块 10. 法医分析

10.1. 数据采集和复制
- 10.1.1. 易失性数据采集
  - 10.1.1.1.系统信息
  - 10.1.1.2.网络信息
  - 10.1.1.3.波动率定律
- 10.1.2. 静态数据采集
  - 10.1.2.1.创建重复图像
  - 10.1.2.2.为监管链准备文件
- 10.1.3. 获取数据的验证方法
  - 10.1.3.1.适用于Linux 的方法
  - 10.1.3.2.适用于 Windows 的方法

10.2. 反取证技术的评估和失败
- 10.2.1. 反取证技术的目标
- 10.2.2. 删除数据
  - 10.2.2.1.删除数据和文件
  - 10.2.2.2.恢复文件
  - 10.2.2.3.恢复已删除的分区
- 10.2.3. 密码保护
- 10.2.4. 隐写术
- 10.2.5. 安全删除设备
- 10.2.6. 加密

10.3. 操作系统的取证分析
- 10.3.1. Windows 取证
- 10.3.2. Linux 取证
- 10.3.3. Mac 取证

10.4. 网络取证
- 10.4.1. 日志分析
- 10.4.2. 数据相关
- 10.4.3. 网络研究
- 10.4.4. 网络取证要遵循的步骤

10.5. 网络取证
- 10.5.1. 网络攻击调查
- 10.5.2. 攻击检测
- 10.5.3. IP 地址的位置

10.6. 数据库取证
- 10.6.1. MSSQL取证分析
- 10.6.2. MySQL取证分析
- 10.6.3. PostgreSQL取证分析
- 10.6.4. MongoDB取证分析

10.7. 云取证分析
- 10.7.1. 云的犯罪类型
  - 10.7.1.1.以云为主体
  - 10.7.1.2.云作为对象
  - 10.7.1.3.云作为工具
- 10.7.2. 云取证的挑战
- 10.7.3. 云储服务调查
- 10.7.4. 云取证工具

10.8. 电子邮件犯罪调查
- 10.8.1. 邮件系统
  - 10.8.1.1.邮件客户端
  - 10.8.1.2.邮件服务器
  - 10.8.1.3.SMTP 服务器
  - 10.8.1.4.POP3 服务器
  - 10.8.1.5.IMAP4 服务器
- 10.8.2. 邮件犯罪
- 10.8.3. 邮件信息
  - 10.8.3.1.标准标题
  - 10.8.3.2.扩展标题
- 10.8.4. 调查这些罪行的步骤
- 10.8.5. 电子邮件法医工具

10.9. 移动法医分析
- 10.9.1. 手机网络
  - 10.9.1.1.网络类型
  - 10.9.1.2.CDR内容
- 10.9.2. 用户识别模块 (SIM)
- 10.9.3. 逻辑获取
- 10.9.4. 物理获取
- 10.9.5 文件系统获取

10.10. 起草和提交法证报告
- 10.10.1. 取证报告的重要方面
- 10.10.2. 报告的分类和类型
- 10.10.3. 撰写报告指南
- 10.10.4. 提交报告
  - 10.10.4.1.作证前的准备
  - 10.10.4.2.证人陈述
  - 10.10.4.3.与媒体打交道

模块 11. 系统设计和开发的安全问题

11.1. 信息系统
- 11.1.1. 信息系统的领域
- 11.1.2. 信息系统的组成
- 11.1.3. 信息系统的活动
- 11.1.4. 信息系统的生命周期
- 11.1.5. 信息系统的资源

11.2. 信息系统。分类
- 11.2.1. 信息系统的类型
  - 11.2.1.1.商业
  - 11.2.1.2.战略
  - 11.2.1.3.视应用范围而定
  - 11.2.1.4.具体的
- 11.2.2. 信息系统。实际的例子
- 11.2.3. 信息系统的演变：阶段
- 11.2.4. 信息系统方法论

11.3. 信息系统的安全。法律影响
- 11.3.1. 数据访问
- 11.3.2. 安全威胁：漏洞
- 11.3.3. 法律影响：罪行
- 11.3.4. 信息系统维护程序

11.4. 信息系统的安全。安全协议
- 11.4.1. 信息系统的安全
  - 11.4.1.1.整合
  - 11.4.1.2.保密性
  - 11.4.1.3.可用性
  - 11.4.1.4.验证
- 11.4.2. 安全服务
- 11.4.3. 信息安全协议分类
- 11.4.4. 信息系统的敏感度

11.5. 信息系统中的安全性。访问控制措施和系统
- 11.5.1. 安防措施
- 11.5.2. 安全措施的类型
  - 11.5.2.1.预防
  - 11.5.2.2.探测
  - 11.5.2.3.纠正
- 11.5.3. 访问控制系统分类
- 11.5.4. 密码学

11.6. 网络和互联网安全
- 11.6.1. 防火墙
- 11.6.2. 数字识别
- 11.6.3. 病毒和蠕虫
- 11.6.4. 黑客攻击
- 11.6.5. 例子和真实案例

11.7. 网络犯罪
- 11.7.1. 网络犯罪
- 11.7.2. 网络犯罪。分类
- 11.7.3. 网络犯罪。攻击。类型
- 11.7.4. 虚拟现实案例
- 11.7.5. 犯罪者和受害者的简介。网络犯罪
- 11.7.6. 网络犯罪。例子和真实案例

11.8. 信息系统中的安全计划
- 11.8.1. 安全计划。目标
- 11.8.2. 安全计划。规划
- 11.8.3. 风险计划。分析
- 11.8.4. 安全政策。组织中的实施
- 11.8.5. 安全计划。组织中的实施
- 11.8.6. 安全程序。类型
- 11.8.7. 安全计划。实例

11.9. 应急计划
- 11.9.1. 应急计划。功能
- 11.9.2. 紧急计划。要点和目标
- 11.9.3. 组织的应急计划。实施
- 11.9.4 应急计划。实例

11.10. 信息系统安全治理
- 11.10.1. 标准
- 11.10.2. 认证
- 11.10.3. 技术

模块 12. 信息安全架构和模式

12.1. 信息安全架构
- 12.1.1. SGSI/PDS
- 12.1.2. 战略调整
- 12.1.3. 风险管理
- 12.1.4. 绩效衡量

12.2. 信息安全模型
- 12.2.1. 基于安全策略
- 12.2.2. 基于保护工具
- 12.2.3. 基于工作团队

12.3. 安全模型。关键零件
- 12.3.1. 风险识别
- 12.3.2. 控制的定义
- 12.3.3. 持续评估风险水平
- 12.3.4. 员工、供应商、合作伙伴等的意识计划

12.4. 风险管理流程
- 12.4.1. 资产识别
- 12.4.2. 威胁识别
- 12.4.3. 风险评估
- 12.4.4. 控制的优先级
- 12.4.5. 重新评估和剩余风险

12.5. 业务流程和信息安全
- 12.5.1. 业务流程
- 12.5.2. 基于业务参数的风险评估
- 12.5.3. 业务影响分析
- 12.5.4. 业务运营和信息安全

12.6. 持续改进过程
- 12.6.1. 戴明循环
  - 12.6.1.1.划规划
  - 12.6.1.2.做
  - 12.6.1.3.核实
  - 12.6.1.4.行动

12.7. 安全架构
- 12.7.1. 技术的选择和标准化
- 12.7.2. 身份管理。验证
- 12.7.3. 访问管理。授权
- 12.7.4. 网络基础设施安全
- 12.7.5. 加密技术和解决方案
- 12.7.6. 终端设备安全 (EDR)

12.8. 监管框架
- 12.8.1. 行业法规
- 12.8.2. 认证
- 12.8.3. 立法

12.9. ISO 27001 标准
- 12.9.1. 实施
- 12.9.2. 认证
- 12.9.3. 审计和渗透测试
- 12.9.4. 持续风险管理
- 12.9.5. 信息的分类

12.10. 隐私的立法。RGPD (GDPR)
- 12.10.1. 一般数据保护条例 (GDPR) 的适用范围
- 12.10.2. 个人资料
- 12.10.3. 个人数据处理的角色
- 12.10.4. ARCO 权利
- 12.10.5. DPO功能

模块 13. 信息安全管理系统 (SGSI)

13.1. 信息安全。关键问题
- 13.1.1. 信息安全
  - 13.1.1.1.保密性
  - 13.1.1.2.整合
  - 13.1.1.3.可用性
  - 13.1.1.4.信息安全措施

13.2. 信息安全管理体系
- 13.2.1. 信息安全管理模式
- 13.2.2. 实施SGSI的文件
- 13.2.3. SGSI的级别和控制

13.3. 国际规范和标准
- 13.3.1. 信息安全方面的国际标准
- 13.3.2. 标准的起源和演变
- 13.3.3. 国际信息安全管理标准
- 13.3.4. 其他参考标准

13.4. ISO/IEC 27.000标准
- 13.4.1. 目标和范围
- 13.4.2. 标准的结构
- 13.4.3. 认证
- 13.4.4. 认证的各个阶段
- 13.4.5. ISO/IEC 27.000标准的好处

13.5. 一般信息安全系统的设计和实施
- 13.5.1. 一般信息安全系统的实施阶段
- 13.5.2. 业务连续性计划

13.6. 第一阶段：诊断
- 13.6.1. 初步诊断
- 13.6.2. 确定分层的水平
- 13.6.3. 符合标准/规范的程度

13.7. 第二阶段:准备
- 13.7.1. 组织背景
- 13.7.2. 适用安全法规分析
- 13.7.3. 整个信息安全系统的范围
- 13.7.4. 一般信息安全系统政策
- 13.7.5. 总体信息安全系统的目标

13.8. 第三阶段:规划
- 13.8.1. 资产的分类
- 13.8.2. 风险评估
- 13.8.3. 识别威胁和风险

13.9. 第四阶段:实施和监测
- 13.9.1. 结果分析
- 13.9.2. 分配责任
- 13.9.3. 行动计划的时间安排
- 13.9.4 监测和审计

13.10. 事件管理中的安全政策
- 13.10.1. 阶段
- 13.10.2. 事件的分类
- 13.10.3. 事件流程和事件管理

模块 14. IT安全管理

14.1. 安全管理
- 14.1.1. 安全行动
- 14.1.2. 法律和监管方面
- 14.1.3. 业务赋能
- 14.1.4. 风险管理
- 14.1.5. 身份和访问管理

14.2. 安全区域的结构。CISO办公室
- 14.2.1. 组织结构。CISO 结构的位置
- 14.2.2. 防线
- 14.2.3. CISO办公室组织结构图
- 14.2.4 预算管理

14.3. 安全政府
- 14.3.1. 安全委员会
- 14.3.2. 风险监察委员会
- 14.3.3. 审计委员会
- 14.3.4. 危机委员会

14.4. 安全政府功能
- 14.4.1. 政策和标准
- 14.4.2. 安全总计划
- 14.4.3. 仪表板
- 14.4.4. 意识和培训
- 14.4.5. 供应链安全

14.5. 安全行动
- 14.5.1. 身份和访问管理
- 14.5.2. 网络安全规则的配置。防火墙
- 14.5.3. IDS/IPS 平台管理
- 14.5.4. 漏洞扫描

14.6. 网络安全框架。NIST CSF
- 14.6.1. 方法论 NIST
  - 14.6.1.1.识别
  - 14.6.1.2.保护
  - 14.6.1.3.探测
  - 14.6.1.4.回复
  - 14.6.1.5.恢复

14.7. 安全运营中心 (SOC)功能
- 14.7.1. 保护 Red Team, pentesting, threat intelligence
- 14.7.2. 检测。SIEM, user behavior analytics, fraud prevention
- 14.7.3. 答案

14.8. 安全审计
- 14.8.1. 渗透测试
- 14.8.2. red team练习
- 14.8.3. 源代码审计。安全发展
- 14.8.4 组件安全 (软件供应链)
- 14.8.5. 法医分析

14.9. 事件响应
- 14.9.1. 准备工作
- 14.9.2. 检测、分析和通知
- 14.9.3. 遏制、根除和恢复
- 14.9.4. 事后活动
  - 14.9.4.1.证据保留
  - 14.9.4.2.法医分析
  - 14.9.4.3.差距管理
- 14.9.5. 官方网络事件管理指南

14.10. 漏洞管理
- 14.10.1. 漏洞扫描
- 14.10.2. 漏洞评估
- 14.10.3. 系统硬化
- 14.10.4. 第 0 天漏洞零日

模块 15. 安全事件管理政策

15.1. 信息安全事件管理政策和改进措施
- 15.1.1. 事故管理
- 15.1.2. 责任和流程
- 15.1.3. 事件通知

15.2. 入侵检测和预防系统(IDS/IPS)
- 15.2.1. 系统运行数据
- 15.2.2. 入侵检测系统的类型
- 15.2.3. IDS/IPS安置的标准

15.3. 安全事件响应
- 15.3.1. 信息收集流程
- 15.3.2. 入侵验证流程
- 15.3.3. CERT机构

15.4. 入侵企图通知和管理过程
- 15.4.1. 通知过程中的责任
- 15.4.2. 事件的分类
- 15.4.3. 解决和恢复过程

15.5. 作为安全政策的取证分析
- 15.5.1. 挥发性和非挥发性证据
- 15.5.2. 分析和收集电子证据
  - 15.5.2.1.对电子证据的分析
  - 15.5.2.2.收集电子证据

15.6. 入侵检测和预防系统(IDS/IPS)工具
- 15.6.1. Snort
- 15.6.2. Suricata
- 15.6.3. Solar-Winds

15.7. 活动集中化工具
- 15.7.1. SIM
- 15.7.2. SEM.
- 15.7.3. SIEM

15.8. CCN-STIC安全指南 817
- 15.8.1. 网络事件管理
- 15.8.2. 度量和指标

15.9. NIST SP800-61
- 15.9.1. 计算机安全事件响应能力
- 15.9.2. 事件处理
- 15.9.3. 协调和信息共享

15.10. ISO 27035
- 15.10.1. ISO 27035事件管理的原则
- 15.10.2. 制定事故管理计划的准则
- 15.10.3. 事故应对行动指南

模块 16. 风险分析和IT安全环境

16.1. 环境分析
- 16.1.1. 现状分析
  - 16.1.1.1. VUCA 环境
    - 16.1.1.1.1. 变化大
    - 16.1.1.1.2. 不确定
    - 16.1.1.1.3. 复杂
    - 16.1.1.1.4. 模糊

16.1.1.2. BANI 环境
16.1.1.2.1. 易碎
16.1.1.2.2. 焦虑
16.1.1.2.3. 非线性
16.1.1.2.4. 无法理解
16.1.2. 大环境分析。PESTEL
16.1.2.1. 政治
16.1.2.2. 经济
16.1.2.3. 社会
16.1.2.4. 技术
16.1.2.5. 生态/环境
16.1.2.6. 法律
16.1.3. 内部情况分析。DAFO分析
16.1.3.1. 目标
16.1.3.2. 威胁
16.1.3.3. 机会
16.1.3.4. 优势
16.2. 风险和不确定性
16.2.1. 风险
16.2.2. 风险管理
16.2.3. 风险管理标准
16.3. ISO 31,000.2018 风险管理指南
16.3.1. 目标
16.3.2. 原则
16.3.3. 参考框架
16.3.4. 过程
16.4. 信息系统风险分析和管理方法 (MAGERIT)
16.4.1. MAGERIT 方
16.4.1.1. 目标
16.4.1.2. 方法
16.4.1.3. 元素
16.4.1.4. 技术
16.4.1.5. 可用工具 (PILAR)
16.5. 网络风险转移
16.5.1. 风险转移
16.5.2. 网络风险分类
16.5.3. 网络风险保险
16.6. 风险管理的敏捷方法
16.6.1. 敏捷方法
16.6.2. Scrum 风险管理
16.6.3. 敏捷风险管理
16.7. 风险管理技术
16.7.1. 人工智能应用于风险管理
16.7.2. 区块链和密码学。保值方法
16.7.3. 量子计算机会或威胁
16.8. 基于敏捷方法的 IT 风险图的准备
16.8.1. 敏捷环境中概率和影响的表示
16.8.2. 作为价值威胁的风险
16.8.3. 基于 KRI 的项目管理和敏捷流程的再进化
16.9. 风险管理中的风险驱动
16.9.1. 风险驱动
16.9.2. 风险管理中的风险驱动
16.9.3. 开发风险驱动的业务管理模式
16.10. IT风险管理的创新与数字化转型
16.10.1. 敏捷风险管理是业务创新的源泉
16.10.2. 将数据转化为对决策有用的信息
16.10.3. 通过风险的公司整体愿景

模块 17. IT系统中威胁分析的安全政策

17.1. 安全政策中的威胁管理
17.1.1. 风险管理
17.1.2. 安全风险
17.1.3. 威胁管理的方法论
17.1.4. 方法论的实施

17.2. 威胁管理的各个阶段
- 17.2.1. 识别
- 17.2.2. 分析
- 17.2.3. 地点
- 17.2.4. 保障措施

17.3. 威胁定位的审计系统
- 17.3.1. 分类和信息流
- 17.3.2. 分析脆弱的程序

17.4. 风险分类
- 17.4.1. 风险的类型
- 17.4.2. 威胁概率的计算
- 17.4.3. 剩余风险

17.5. 风险处理
- 17.5.1. 保障措施的实施
- 17.5.2. 转让或接管

17.6. 风险控制
- 17.6.1. 持续的风险管理过程
- 17.6.2. 实施安全衡量标准
- 17.6.3. 信息安全度量的战略模式

17.7. 威胁分析和监测的实用方法
- 17.7.1. 威胁目录
- 17.7.2. 控制措施目录
- 17.7.3. 保障措施目录

17.8. ISO 27005
- 17.8.1. 风险识别
- 17.8.2. 风险分析
- 17.8.3. 风险评估

17.9. 风险、影响和威胁矩阵
- 17.9.1. 数据、系统和人员
- 17.9.2. 威胁的概率
- 17.9.3. 损害的程度

17.10. 危害分析中阶段和过程的设计
- 17.10.1. 确定组织的关键因素
- 17.10.2. 确定威胁和影响
- 17.10.3. 影响和风险分析
- 17.10.4. 方法

模块 18. 面对攻击时安全政策的实际执行情况

18.1. 系统黑客攻击
- 18.1.1. 风险和弱点
- 18.1.2. 反措施

18.2. 服务中的DoS
- 18.2.1. 风险和弱点
- 18.2.2. 反措施

18.3. 会话Hijacking
- 18.3.1. 劫持行为过程
- 18.3.2. 劫持行为的反措施

18.4. Firewalls and Honeypots的规避IDS
- 18.4.1. 躲避技巧
- 18.4.2. 实施反措施

18.5. 黑客攻击网络服务器
- 18.5.1. 对网络服务器的攻击
- 18.5.2. 实施防御措施

18.6. 黑客攻击网络应用程序
- 18.6.1. 对网络应用程序的攻击
- 18.6.2. 实施防御措施

18.7. 黑客攻击无线网络
- 18.7.1. 无线网络的弱点
- 18.7.2. 实施防御措施

18.8. 黑客攻击移动平台
- 18.8.1. 移动平台的弱点
- 18.8.2. 实施反措施

18.9. 勒索软件
- 18.9.1. 导致勒索软件的漏洞
- 18.9.2. 实施反措施

18.10. 社会工程
- 18.10.1. 社会工程的类型
- 18.10.2. 社会工程的对策

模块 19. 信息技术的密码学

19.1. 密码学
- 19.1.1. 密码学
- 19.1.2. 数学基础

19.2. 密码学
- 19.2.1. 密码学
- 19.2.2. 密码分析
- 19.2.3. 隐写术和隐写分析

19.3. 密码协议
- 19.3.1. 基础块
- 19.3.2. 基础协议
- 19.3.3. 中间协议
- 19.3.4. 高级协议
- 19.3.5. 公开协议

19.4. 密码技术
- 19.4.1. 密钥长度
- 19.4.2. 密钥处理
- 19.4.3. 算法类型
- 19.4.4. 汇总函数Hash
- 19.4.5. 伪随机数发生器
- 19.4.6. 算法的使用

19.5. 对称密码学
- 19.5.1. 分组密码
- 19.5.2. DES（数据加密标准）
- 19.5.3. RC4算法
- 19.5.4. AES（高级加密标准）
- 19.5.5. 分组密码的组合
- 19.5.6. 密钥派生

19.6. 非对称密码学
- 19.6.1. Diffie-Hellman
- 19.6.2. DSA（数字签名算法）
- 19.6.3. RSA (Rivest、Shamir 和 Adleman)
- 19.6.4. 椭圆曲线
- 19.6.5. 非对称密码学分类

19.7. 数字证书
- 19.7.1. 电子签名
- 19.7.2. X509 证书
- 19.7.3. 公钥基础设施 (PKI)

19.8. 执行
- 19.8.1. Kerberos
- 19.8.2. IBM CCA
- 19.8.3. Pretty Good Privacy (PGP)
- 19.8.4. ISO 认证框架
- 19.8.5. SSL 和 TLS
- 19.8.6. 支付方式中的智能卡 (EMV)
- 19.8.7. 手机协议
- 19.8.8. 区块链

19.9. 隐写术
- 19.9.1. 隐写术
- 19.9.2. 隐写分析
- 19.9.3. 应用和用途

19.10. 量子密码学
- 19.10.1. 量子算法
- 19.10.2. 保护算法免受量子计算
- 19.10.3. 量子密钥分发

模块 20. IT安全中的身份和访问管理

20.1. 身份和访问管理 (IAM)
- 20.1.1. 数字身份
- 20.1.2. 身份管理
- 20.1.3. 身份联盟

20.2. 物理访问控制
- 20.2.1. 保护系统
- 20.2.2. 区域安全
- 20.2.3. 恢复设施

20.3. 逻辑访问控制
- 20.1.1. 验证：分类
- 20.1.2. 身份验证协议
- 20.1.3. 认证攻击

20.4. 逻辑访问控制。MFA认证
- 20.4.1. 逻辑访问控制。MFA认证
- 20.4.2. 密码。重要性
- 20.4.3. 认证攻击

20.5. 逻辑访问控制。生物特征认证
- 20.5.1. 逻辑访问控制。生物特征认证
  - 20.5.1.1. 生物特征认证要求
- 20.5.2. 运作原理
- 20.5.3. 模型和技术

20.6. 认证管理系统
- 20.6.1. 单点登录
- 20.6.2. Kerberos
- 20.6.3. AAA系统

20.7. 认证管理系统：AAA系统
- 20.7.1. TACACS
- 20.7.2. RADIUS
- 20.7.3. DIAMETER

20.8. 访问控制服务
- 20.8.1. FW - 防火墙
- 20.8.2. VPN - 虚拟专用网络
- 20.8.3. IDS - 入侵检测系统

20.9. 建立网页链接的控制
- 20.9.1. NAC
- 20.9.2. 结构和元素
- 20.9.3. 运营标准化

20.10. 无线网页链接
- 20.10.1. 网络类型
- 20.10.2. 无线网络安全
- 20.10.3. 对无线网络的攻击

模块 21. 通信和软件运行的安全性

21.1. 通信和软件操作中的计算安全
- 21.1.1. 信息安全
- 21.1.2. 网络安全
- 21.1.3. 云安全

21.2. 通信和软件操作中的计算安全。分类
- 21.2.1. 实体安全
- 21.2.2. 逻辑安全

21.3. 通讯安全
- 21.3.1. 主要元素
- 21.3.2. 网络安全
- 21.3.3. 最佳实践

21.4. 网络情报
- 21.4.1. 社会工程学
- 21.4.2. 深层网络
- 21.4.3. 网络钓鱼
- 21.4.4. 恶意软件

21.5. 通信和软件操作的安全开发
- 21.1.1. 安全发展。HTTP 协议
- 21.1.2. 安全发展。生命周期
- 21.1.3. 安全发展。PHP 安全
- 21.1.4. 安全发展。NET 安全
- 21.1.5. 安全发展。最佳实践

21.6. 通信和软件操作的信息安全管理系统
- 21.6.1. GDPR
- 21.6.2. ISO 27021
- 21.6.3. ISO 27017/18

21.7. SIEM 技术
- 21.7.1. SIEM 技术
- 21.7.2. SOC操作
- 21.7.3. SIEM 供应商

21.8. 安全在组织中的作用
- 21.8.1. 在组织中的角色
- 21.8.2. 物联网专家在公司中的作用
- 21.8.3. 市场认可的认证

21.9. 法医分析
- 21.9.1. 法医分析
- 21.9.2. 法医分析。方法
- 21.9.3. 法医分析。工具和实施

21.10. 当今的网络安全
- 21.10.1. 主计算机攻击
- 21.10.2. 就业能力预测
- 21.10.3. 挑战

模块 22. 云环境的安全性

22.1. 云计算 环境中的安全问题
- 22.1.1. 云计算 环境中的安全问题
- 22.1.2. 云计算 环境中的安全安全威胁和风险
- 22.1.3. 云计算 环境中的安全关键安全方面

22.2. 云基础设施的类型
- 22.2.1. 公众
- 22.2.2. 私人
- 22.2.3. 混合

22.3. 共享管理模式
- 22.3.1. 供应商管理的安全元素
- 22.3.2. 客户管理的项目
- 22.3.3. 安全策略的定义

22.4. 预防机制
- 22.4.1. 认证管理系统
- 22.4.2. 授权管理系统访问政策
- 22.4.3. 密钥管理系统

22.5. 系统安全
- 22.5.1. 存储系统的安全
- 22.5.2. 保护数据库系统
- 22.5.3. 传输中数据的安全性

22.6. 基础设施保护
- 22.6.1. 安全网络设计和实施
- 22.6.2. 计算资源安全
- 22.6.3. 基础设施保护的工具和资源

22.7. 检测威胁和攻击
- 22.7.1. 审计、日志 和监控系统
- 22.7.2. 事件和警报系统
- 22.7.3. SIEM系统

22.8. 事件响应
- 22.8.1. 事件响应计划
- 22.8.2. 业务连续性
- 22.8.3. 同性质事件的取证分析和补救

22.9. 公共 云 的安全性
- 22.9.1. AWS（亚马逊网络服务）
- 22.9.2. Microsoft Azure
- 22.9.3. Google GCP
- 22.9.4. Oracle Cloud

22.10. 法规和合规性
- 22.10.1. 遵守安全法规
- 22.10.2. 风险管理
- 22.10.3. 组织的人员和流程

模块 23. 信息系统安全政策中的监测工具

23.1. 信息系统监测政策
- 23.1.1. 系统监测
- 23.1.2. 衡量标准
- 23.1.3. 衡量标准的类型

23.2. 系统审计和日志记录
- 23.2.1. Windows审计和日志记录
- 23.2.2. Linux上的审计和日志记录

23.3. SNMP协议 Simple Network Management Protocol
- 23.3.1. SNMP 协议
- 23.3.2. SNMP的操作
- 23.3.3. SNMP工具

23.4. 网络监控
- 23.4.1. 控制系统中的网络监控
- 23.4.2. 控制系统的监测工具

23.5. Nagios网络监控系统
- 23.5.1. Nagios
- 23.5.2. Nagios的操作
- 23.5.3. 安装Nagios

23.6. Zabbix.网络监控系统
- 23.6.1. Zabbix.
- 23.6.2. Zabbix的运作
- 23.6.3. Zabbix的安装

23.7. Cacti.网络监控系统
- 23.7.1. Cacti.
- 23.7.2. Cacti 的运作
- 23.7.3. Cacti 的安装

23.8. Pandora.网络监控系统
- 23.8.1. Pandora
- 23.8.2. Pandora的运作
- 23.8.3. Pandora的安装

23.9. SolarWinds.网络监控系统
- 23.9.1. SolarWinds.
- 23.9.2. 操作SolarWinds
- 23.9.3. SolarWinds的安装

23.10. 监控条例
- 23.10.1. CIS对审计和记录的控制
- 23.10.2. NIST 800-123 (EEUU)

模块 24. 物联网设备通信的安全性

24.1. 从遥测到物联网
- 24.1.1. 遥测
- 24.1.2. M2M 连接
- 24.1.3. 遥测民主化

24.2. 物联网参考模型
- 24.2.1. 物联网参考模型
- 24.2.2. 简化的物联网架构

24.3. 物联网安全漏洞
- 24.3.1. 物联网设备
- 24.3.2. 物联网设备。使用案例
- 24.3.3. 物联网设备。漏洞

24.4. 物联网连接
- 24.4.1. PAN、LAN、WAN 网络
- 24.4.2. 非物联网无线技术
- 24.4.3. LPWAN 无线技术

24.5. LPWAN 技术
- 24.5.1. LPWAN 网络的铁三角
- 24.5.2. 免费频段比授权频段
- 24.5.3. LPWAN 技术选项

24.6. LoRaWAN 技术
- 24.6.1. LoRaWAN 技术
- 24.6.2. LoRaWAN 用例生态系统
- 24.6.3. LoRaWAN 中的安全性

24.7. 西格福克斯技术
- 24.7.1. 西格福克斯技术
- 24.7.2. 西格福克斯用例生态系统
- 24.7.3. 西格福克斯的安全性

24.8. 蜂窝物联网技术
- 24.8.1. 蜂窝物联网技术（NB-IoT 和 LTE-M）
- 24.8.2. 蜂窝物联网用例。生态系统
- 24.8.3. 蜂窝物联网安全

24.9. WiSUN技术
- 24.9.1. WiSUN技术
- 24.9.2. WiSUN 用例。生态系统
- 24.9.3. WiSUN的安全

24.10. 其他物联网技术
- 24.10.1. 其他物联网技术
- 24.10.2. 其他物联网技术的用例和生态系统
- 24.10.3. 其他物联网技术的安全性

模块 25. 与安全有关的业务连续性计划

25.1. 业务连续性计划
- 25.1.1. 业务连续性计划 (PCN)
- 25.1.2. 业务连续性计划 (PCN)。关键问题
- 25.1.3. 用于公司估值的业务连续性计划 (PCN)

25.2. 业务连续性计划 (PCN) 中的指标
- 25.2.1. Recovery time objective (RTO) y recovery point objective (RPO)
- 25.2.2. 最大容许时间 (MTD)
- 25.2.3. 最低恢复水平 (ROL)
- 25.2.4. 恢复点目标 (RPO)

25.3. 连续性项目分类
- 25.3.1. 业务连续性计划 (PCN)
- 25.3.2. ICT 连续性计划 (PCTIC)
- 25.3.3. 灾难恢复计划(PRD)

25.4. 与 PCN 相关的风险管理
- 25.4.1. 业务影响分析
- 25.4.2. 实施 PCN 的好处
- 25.4.3. 基于风险的心态

25.5. 业务连续性计划的生命周期
- 25.5.1. 第 1 阶段：组织的分析
- 25.5.2. 第 2 阶段：确定连续性策略
- 25.5.3. 第 3 阶段：应急反应
- 25.5.4. 第 4 阶段：测试、维护和审查

25.6. 国家联络点组织的分析阶段
- 25.6.1. 识别 PCN 范围内的流程
- 25.6.2. 确定关键业务领域
- 25.6.3. 识别区域和流程之间的依赖关系
- 25.6.4. 确定合适的最佳可行技术
- 25.6.5. 可交付的成果。创建项目

25.7. PCN 中连续性策略的确定阶段
- 25.7.1. 战略确定阶段的角色
- 25.7.2. 战略确定阶段的任务
- 25.7.3. 可交付的成果

25.8. PCN 中的应急响应阶段
- 25.8.1. 响应阶段的角色
- 25.8.2. 这个阶段的任务
- 25.8.3. 可交付的成果

25.9. PCN 的测试、维护和审查阶段
- 25.9.1. 测试、维护和审查阶段的角色
- 25.9.2. 测试、维护和审查阶段的任务
- 25.9.3. 可交付的成果

25.10. 与业务连续性计划 (PCN) 相关的 ISO 标准
- 25.10.1. ISO 22301.2019大学课程
- 25.10.2. ISO 22313.2020大学课程
- 25.10.3. 其他 ISO 和国际标准

模块 26. 实用的安全灾难恢复政策

26.1. DRP.灾难恢复计划
- 26.1.1. 灾难恢复计划的目标
- 26.1.2. 灾难恢复计划的好处
- 26.1.3. 没有DRP和不保持更新的后果

26.2. 定义DRP（灾难恢复计划）的指南
- 26.2.1. 范围和目标
- 26.2.2. 设计恢复战略
- 26.2.3. 角色和责任的分配
- 26.2.4. 执行硬件，软件和服务的清单
- 26.2.5. 对停工和数据丢失的容忍度
- 26.2.6. 确定所需的DRP的具体类型
- 26.2.7. 实施培训、认识和沟通计划

26.3. DRP（灾难恢复计划）的范围和目标
- 26.3.1. 确保响应
- 26.3.2. 技术组成部分
- 26.3.3. 连续性政策的范围

26.4. DRP（灾难恢复）战略的设计
- 26.4.1. 灾难恢复战略
- 26.4.2. 预算
- 26.4.3. 人力和人力资源
- 26.4.4. 有风险的管理职位
- 26.4.5. 技术
- 26.4.6. 数据

26.5. 信息流程的连续性
- 26.5.1. 连续性规划
- 26.5.2. 连续性的实施
- 26.5.3. 连续性的验证和评价

26.6. BCP（业务连续性计划）的范围
- 26.6.1. 确定最关键的流程
- 26.6.2. 基于资产的方法
- 26.6.3. 过程方法

26.7. 实施安全的商业流程
- 26.7.1. 优先活动（AP）。
- 26.7.2. 理想恢复时间（TRI）
- 26.7.3. 生存策略

26.8. 组织的分析
- 26.8.1. 信息收集
- 26.8.2. 业务影响分析（BIA）
- 26.8.3. 组织风险分析

26.9. 应急反应
- 26.9.1. 危机计划
- 26.9.2. 运行环境恢复计划
- 26.9.3. 技术工作或事故程序

26.10. 国际标准ISO 27031 BCP
- 26.10.1. 目标
- 26.10.2. 术语和定义
- 26.10.3. 运作

模块 27. 在企业中实施安全和环境安全政策

27.1. 安全领域
- 27.1.1. 实体安全周界
- 27.1.2. 在安全区域工作
- 27.1.3. 办事处、办公室和资源的安全

27.2. 实际进入控制
- 27.2.1. 实物进入控制政策
- 27.2.2. 实物进入控制系统

27.3. 实物访问的脆弱性
- 27.3.1. 主要的物理漏洞
- 27.3.2. 保障措施的实施

27.4. 生理生物识别系统
- 27.4.1. 指纹
- 27.4.2. 面部识别
- 27.4.3. 虹膜和视网膜识别
- 27.4.4. 其他生理学生物识别系统

27.5. 行为生物识别系统
- 27.5.1. 签名识别
- 27.5.2. 书写者识别
- 27.5.3. 语音识别
- 27.5.4. 其他生物识别行为系统

27.6. 生物统计风险管理
- 27.6.1. 实施生物识别系统
- 27.6.2. 生物识别系统的脆弱性

27.7. 在 hosts政策的实施
- 27.7.1. 布线配置和安全的安装
- 27.7.2. 设备管理
- 27.7.3. 设备在场所外的出口
- 27.7.4. 无人看管的IT设备和明确的岗位政策

27.8. 环境保护
- 27.8.1. 消防系统
- 27.8.2. 地震防护系统
- 27.8.3. 地震防护系统

27.9. 数据处理中心安全
- 27.9.1. 安全门
- 27.9.2. 视频监控系统 (CCTV)
- 27.9.3. 安全控制

27.10. 国际实体安全法规
- 27.10.1. IEC 62443-2-1 (欧洲)
- 27.10.2. NERC CIP-005-5 (美国)
- 27.10.3. NERC CIP-014-2 (美国)

模块 28. 企业中的安全通信政策

28.1. 网络安全管理
- 28.1.1. 网络控制和监测
- 28.1.2. 网络隔离
- 28.1.3. 网络安全系统

28.2. 安全通信协议
- 28.2.1. TCP/IP模式
- 28.2.2. IPSEC 协议
- 28.2.3. TLS 协议

28.3. TLS 1.3协议
- 28.3.1. TLS过程的各个阶段1.3
- 28.3.2. 握手协议
- 28.3.3. 注册协议
- 28.3.4. 与TLS 1.2的区别

28.4. 加密算法
- 28.4.1. 通讯中使用的加密算法
- 28.4.2. 密码套件
- 28.4.3. TLS 1.3允许的加密算法

28.5. 文摘功能
- 28.5.1. MD6
- 28.5.2. SHA

28.6. PKI.公钥基础设施
- 28.6.1. 公钥基础设施及其实体
- 28.6.2. 数字证书
- 28.6.3. 数字证书的类型

28.7. 隧道和运输通信
- 28.7.1. 隧道通信
- 28.7.2. 运输通信
- 28.7.3. 加密隧道的实施

28.8. SSH. Secure Shell
- 28.8.1. SSH. 安全胶囊
- 28.8.2. SSH的操作
- 28.8.3. SSH工具

28.9. 加密系统的审计
- 28.9.1. 完整性测试
- 28.9.2. 加密系统测试

28.10. 密码系统
- 28.10.1. 加密系统的漏洞
- 28.10.2. 密码保障措施

模块 29. 信息安全政策的组织方面

29.1. 内部组织
- 29.1.1. 分配责任
- 29.1.2. 职责分离
- 29.1.3. 与当局的联系
- 29.1.4. 项目管理中的信息安全

29.2. 资产管理
- 29.2.1. 资产负债
- 29.2.2. 信息的分类
- 29.2.3. 存储介质的处理

29.3. 业务流程中的安全政策
- 29.3.1. 对易受攻击的业务流程的分析
- 29.3.2. 业务影响分析
- 29.3.3. 在业务影响方面对流程进行排序

29.4. 与人力资源有关的安全政策
- 29.4.1. 签约前
- 29.4.2. 签约期间
- 29.4.3. 终止或改变职位

29.5. 管理层面的安全政策
- 29.5.1. 信息安全的管理准则
- 29.5.2. BIA - 分析影响
- 29.5.3. 恢复计划作为安全政策

29.6. 信息系统的获取和维护
- 29.6.1. 要求信息系统的安全
- 29.6.2. 开发和支持数据的安全
- 29.6.3. 测试数据

29.7. 与供应商的安全
- 29.7.1. 与供应商的IT安全
- 29.7.2. 与担保提供服务的管理
- 29.7.3. 供应链安全

29.8. 运营安全
- 29.8.1. 业务责任
- 29.8.2. 对恶意代码的保护
- 29.8.3. 备份副本
- 29.8.4. 活动和监测记录

29.9. 安全管理和法规
- 29.9.1. 遵守法律要求
- 29.9.2. 信息安全审查

29.10. 业务连续性管理中的安全
- 29.10.1. 信息安全的延续性
- 29.10.2. 冗余

> 完整的TECH课程将教你如何成为一个有远见的领导者，保证组织的长期保护”

04

教学目标

网络安全高级管理（CISO）高级硕士旨在培养能够管理任何类型组织的信息安全的战略领导者。在整个课程中，参与者将培养识别、评估和减轻网络风险的技能，实施有效的安全政策。此外，他们还将深入了解安全架构中的新兴技术和最佳实践，确保数据保护和业务连续性。该课程还促进了网络安全的综合商业愿景，使举措与企业目标保持一致并确保遵守国际法规。学生将准备成为变革的推动者并促进以数字保护为重点的组织文化。

在这个 100% 在线的专业中，你将找到有关大学领域最新的教学材料和研究”

总体目标

- 培养能够管理全球组织数字资产和技术基础设施保护的战略网络安全领导者
- 将网络安全融入业务战略，使数字保护举措与组织的整体目标保持一致
- 培训网络安全政策和监管框架的实施，确保遵守法规并保护数字环境中的信息
- 提升网络安全团队的领导力和管理能力，提高在危机情况下做出战略决策的能力以及在组织层面管理安全项目的能力

> 加入 TECH，培养成为预测威胁和加强机遇的领导者所需的技能”

具体目标

模块 1.网络情报与网络安全

- 培养实施网络情报和网络安全战略所需的技能
- 通过收集、分析和使用数字情报保护计算机系统免受网络威胁

模块 2.主机的安全

- 主机系统安全措施实施培训
- 确保服务器和设备免受漏洞，恶意软件和未经授权的访问

模块 3.网络安全（周边）

- 提供在外围层面保护计算机网络所需的知识
- 管理安全技术和工具，如防火墙、VPN 和入侵检测系统

模块 4.智能手机的安全

- 提供对移动安全的全面了解
- 深入研究如何防范恶意软件，数据丢失和通过移动应用程序进行的攻击等威胁

模块 5.IoT安全

- IoT设备安全策略实施培训
- 保护通过IoT网络和平台连接的设备产生的基础设施和数据

模块 6.道德黑客

- 培养使用道德黑客技术执行渗透测试和安全审计所需的技能
- 能够识别漏洞并防止攻击

模块 7.逆向工程
- 掌握逆向工程技术来分析和理解软件和硬件的功能
- 识别潜在的安全漏洞和解决方案

模块 8.安全发展
- 教授安全软件开发的最佳实践
- 在整个开发生命周期中应用安全原则，以最大限度地减少应用程序中的风险和漏洞

模块 9.软件和硬件中安全策略的实际实施
- 提供设计和实施软件和硬件中强大安全策略所需的知识
- 确保防范内部和外部威胁

模块 10.法医分析
- 培养数字法医技能
- 分析计算机安全事件中数字证据的收集、保存和分析

模块 11.系统设计和开发的安全问题
- 从计算机系统设计和开发阶段开始解决安全措施的整合
- 从项目开始就确保防范潜在的漏洞

模块 12.信息安全架构和模式
- 提供信息安全架构和模型的必要知识
- 设计和实施保护组织数据和资源的强大系统

模块 13.信息安全管理系统（SGSI）
- 实施信息安全管理系统
- 有效保护商业信息，确保遵守法规和良好实践

模块 14.IT安全管理
- 提供必要的知识以有效管理公司技术基础设施的安全
- 最大程度降低风险并确保运营连续性

模块 15.安全事件管理政策
- 培训制定和应用有效的安全事件管理政策
- 建立明确的协议来检测、分析和应对安全漏洞

模块 16.风险分析和IT安全环境
- 提供在 IT 环境中进行风险分析、识别威胁和漏洞所需的知识
- 应用缓解策略来保护技术基础设施

模块 17.IT系统中威胁分析的安全政策
- 培训制定安全政策以识别、分析和减轻对计算机系统的威胁
- 使用适当的工具和方法保护组织的数字资产

模块 18.面对攻击时安全政策的实际执行情况
- 实施有效的安全策略以抵御可能的攻击
- 确保组织中关键系统和信息的保护

模块 19.信息技术的密码学
- 教授信息技术领域的密码学基础知识及其应用
- 在数据传输中实现加密和安全算法

模块 20.IT安全中的身份和访问管理
- 培养管理 IT 系统中身份和访问所需的技能
- 建立身份验证和访问控制策略来保护组织的资源和数据

模块 21.通信和软件运行的安全性
- 提供数字通信保护和软件操作安全措施实施方面的培训
- 确保信息的机密性、完整性和可用性

模块 22.云环境的安全性
- 在云计算环境中实施安全策略
- 确保数据和应用程序免受未经授权的访问和攻击

模块 23.信息系统安全政策中的监测工具
- 培训使用监控工具来评估信息系统安全政策的有效性
- 深入研究漏洞和攻击的早期检测

模块 24.IoT设备通信的安全性
- 培养实施安全措施以保护IoT设备之间通信的技能
- 最大限度地降低联网设备之间数据交换相关的风险

模块 25.与安全有关的业务连续性计划
- 制定业务连续性计划，确保系统的保护和快速恢复
- 建立协议以在发生安全事件时保护重要数据

模块 26.实用的安全灾难恢复政策
- 创建灾难恢复策略
- 确保在发生严重安全事件时快速恢复系统并保护数据

模块 27.在企业中实施安全和环境安全政策
- 培训实施物理和环境安全政策，以保护组织的物理资源
- 确保技术系统安全运行的适当环境

模块 28.企业中的安全通信政策
- 提供在组织内制定安全通信政策的知识
- 保护网络和通信渠道免遭间谍活动和信息泄露

模块 29.信息安全政策的组织方面
- 提供实施信息安全管理组织政策所需的工具
- 建立适当的角色、职责和流程来保护信息资产

05

职业前景

完成网络安全高级管理高级硕士课程后，毕业生将接受全面培训，在各个组织中承担信息安全保护和管理方面的关键角色。此外，他们还将能够领导跨国公司的安全战略，管理和减轻网络风险。他们还将准备填补需要技能来领导网络安全计划并确保任何领域的数字资产保护的职位。

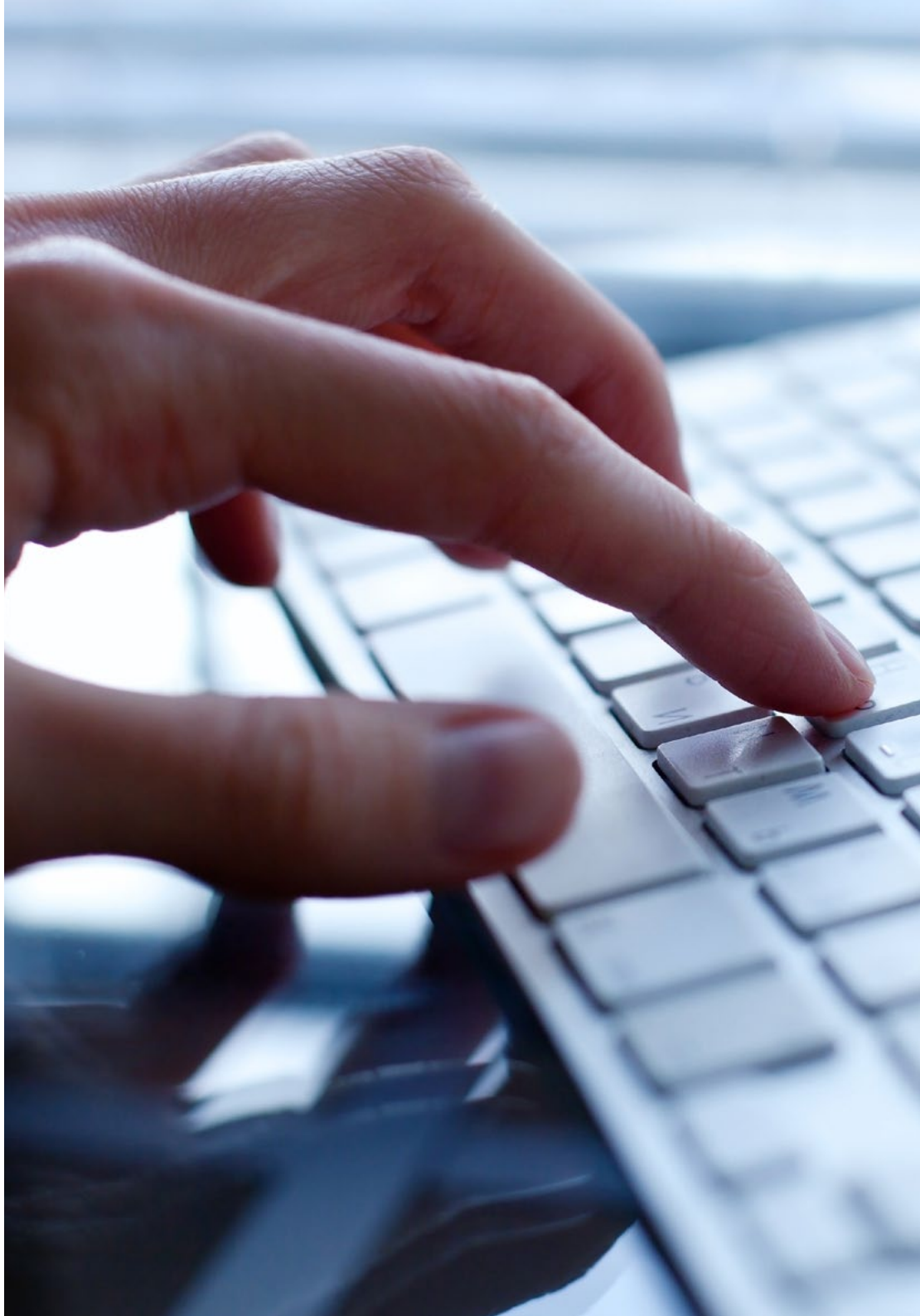
在这个高级硕士的指导下，你将成为一名能够预测风险并保护关键信息的主管”

毕业生简介

网络安全高级管理(CISO)高级硕士毕业生将成为全球组织背景下对信息安全有深刻理解的战略领导者。您将能够设计和实施先进的安全策略并领导多学科团队。您还将拥有强大的管理和治理技能,使您能够应对各个领域的网络安全挑战,确保数字资产的安全。这个机会将为您提供工具,使您能够紧跟最新的技术趋势并适应数字领域的快速变化。

> 准备成为最优秀的专业人士之一,最大限度地减少网络攻击的影响并迅速让一切恢复正常。

- **战略领导力和适应性:**能够领导多学科团队并管理安全政策,适应网络安全领域的快速技术和新兴变化
- **风险管理和明智决策:**能够识别、评估和减轻网络风险,并根据详细数据和分析做出决策
- **关键分析和事件管理:**能够识别漏洞,管理安全事件并协调危机响应,确保业务连续性
- **有效沟通和战略思维:**能够向不同的利益相关者清楚地传达风险和解决方案,采用全球性和战略性的方法来保护数字资产



完成高级硕士课程后，您将能够在以下职位上运用您的知识和技能：

1. **Chief Information Security Officer (CISO):** 负责整个组织的信息保护和网络安全的战略领导者，制定政策并监督数字安全基础设施
2. **网络安全总监：**负责管理和监督IT安全团队，制定和实施保护公司技术基础设施的策略
3. **信息安全经理:** 负责管理和协调数字安全政策，监督数据和计算机系统免受可能的威胁的保护
4. **网络安全顾问:** 专门为公司提供有关如何实施和管理网络安全政策的最佳建议，帮助降低风险并遵守国际法规
5. **IT风险管理经理：**负责识别、评估和减轻可能影响组织信息和技术系统安全的网络风险
6. **首席信息安全官：**负责监督和协调组织内与数据和计算机系统保护有关的所有举措的领导者

> 有了只有 TECH 才能提供的高级硕士服务，您距离提升自己的职业生涯只有一步之遥”

06

学习方法

TECH 是世界上第一所将案例研究方法与 Relearning一种基于指导性重复的100% 在线学习系统相结合的大学。

这种颠覆性的教学策略旨在为专业人员提供机会，以强化和严格的方式更新知识和发展技能。这种学习模式将学生置于学习过程的中心，让他们发挥主导作用，适应他们的需求，摒弃传统方法。

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获得事业上的成功"

学生:所有TECH课程的首要任务

在 TECH 的学习方法中,学生是绝对的主角。

每个课程的教学工具的选择都考虑到了时间,可用性和学术严谨性的要求,这些要求如今不仅是学生的要求也是市场上最具竞争力的职位的要求。

通过TECH的异步教育模式,学生可以选择分配学习的时间,决定如何建立自己的日常生活以及所有这一切,而这一切都可以在他们选择的电子设备上舒适地进行。学生不需要参加现场课程,而他们很多时候都不能参加。您将在适合您的时候进行学习活动。您始终可以决定何时何地学习。

> 在TECH,你不会有线下课程(那些你永远不能参加)”

国际上最全面的学习计划

TECH的特点是提供大学环境中最完整的学术大纲。这种全面性是通过创建教学大纲来实现的，教学大纲不仅包括基本知识，还包括每个领域的最新创新。

通过不断更新，这些课程使学生能够跟上市场变化并获得雇主最看重的技能。通过这种方式，那些在TECH完成学业的人可以获得全面的准备，为他们的职业发展提供显着的竞争优势。

更重要的是，他们可以通过任何设备，个人电脑，平板电脑或智能手机来完成的。

> TECH模型是异步的，因此将您随时随地使用PC，平板电脑或智能手机学习，学习时间不限”

案例研究或案例方法

案例法一直是世界上最好的院系最广泛使用的学习系统。该课程于1912年开发，目的是让法学专业学生不仅能在理论内容的基础上学习法律，还能向他们展示复杂的现实生活情境。因此，他们可以做出决策并就如何解决问题做出明智的价值判断。1924年被确立为哈佛大学的一种标准教学方法。

在这种教学模式下，学生自己可以通过耶鲁大学或斯坦福大学等其他知名机构使用的边做边学或设计思维等策略来建立自己的专业能力。

这种以行动为导向的方法将应用于学生在TECH进行的整个学术大纲。这样你将面临多种真实情况，必须整合知识，调查，论证和捍卫你的想法和决定。这一切的前提是回答他在日常工作中面对复杂的特定事件时如何定位自己的问题。

学习方法

在TECH，案例研究通过最好的100%在线教学方法得到加强：Relearning。

这种方法打破了传统的教学技术，将学生置于等式的中心，为他们提供不同格式的最佳内容。通过这种方式，您可以回顾和重申每个主题的关键概念并学习将它们应用到实际环境中。

沿着这些思路，根据多项科学研究，重复是最好的学习方式。因此，TECH在同一课程中以不同的方式重复每个关键概念8到16 次，目的是确保在学习过程中充分巩固知识。

Relearning 将使你的学习事半功倍，让你更多地参与到专业学习中，培养批判精神，捍卫论点，对比观点：这是通往成功的直接等式。

100%在线虚拟校园，拥有最好的教学材料

为了有效地应用其方法论，TECH 专注于为毕业生提供不同格式的教材：文本，互动视频，插图和知识图谱等。这些课程均由合格的教师设计，他们的工作重点是通过模拟将真实案例与复杂情况的解决结合起来，研究应用于每个职业生涯的背景并通过音频，演示，动画，图像等基于重复的学习。

神经科学领域的最新科学证据表明，在开始新的学习之前考虑访问内容的地点和背景非常重要。能够以个性化的方式调整这些变量可以帮助人们记住知识并将其存储在海马体中，以长期保留它。这是一种称为神经认知情境依赖电子学习的模型，有意识地应用于该大学学位。

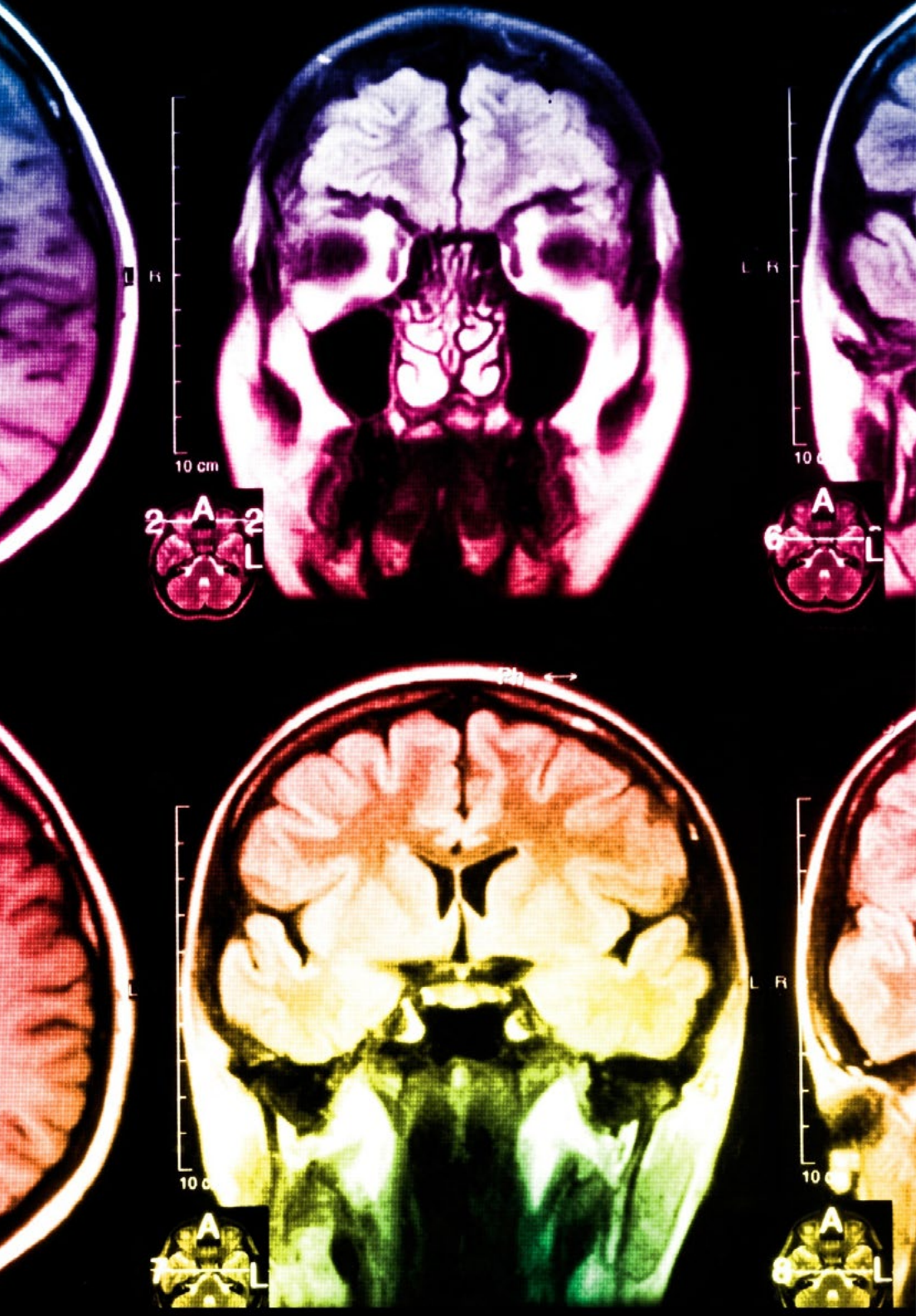
另一方面，也是为了尽可能促进指导者与被指导者之间的联系，提供了多种实时和延 迟交流的可能性（内部信息，论坛，电话服务，与技术秘书处的电子邮件联系，聊天和视频会议）。

同样，这个非常完整的虚拟校园将TECH学生根据个人时间或工作任务安排学习时间。通过这种方式，您将根据您加速的专业更新，对学术内容及其教学工具进行全局控制。

> 该课程的在线学习模式将您安排您的时间和学习进度，使其适应您的日程安排”

这个方法的有效性由四个关键成果来证明：

1. 遵循这种方法的学生不仅实现了对概念的吸收，而且还通过练习评估真实情况和应用知识来发展自己的心理能力。
2. 学习扎根于实践技能使学生能够更好地融入现实世界。
3. 由于使用了现实中出现的情况，思想和概念的学习变得更加容易和有效。
4. 感受到努力的成效对学生是一种重要的激励，这会转化为对学习更大的兴趣并增加学习时间。



最受学生重视的大学方法

这种创新学术模式的成果可以从TECH毕业生的整体满意度中看出。

学生对教学质量，教材质量，课程结构及其目标的评价非常好。毫不奇怪，在Trustpilot评议平台上，该校成为学生评分最高的大学，获得了4.9分的高分（满分5分）。

由于TECH掌握着最新的技术和教学前沿，因此可以从任何具有互联网连接的设备（计算机，平板电脑，智能手机）访问学习内容。

你可以利用模拟学习环境和观察学习法（即向专家学习）的优势进行学习。

因此，在这门课程中，将提供精心准备的最好的教育材料：

学习材料

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

这些内容之后被应用于视听格式，这将创造我们的在线工作方式，采用最新的技术，使我们能够保证给你提供的每一件作品都有高质量。

技能和能力的实践

你将开展活动以发展每个学科领域的具体能力和技能。在我们所处的全球化框架内我们提供实践和氛围帮你获得成为专家所需的技能和能力。

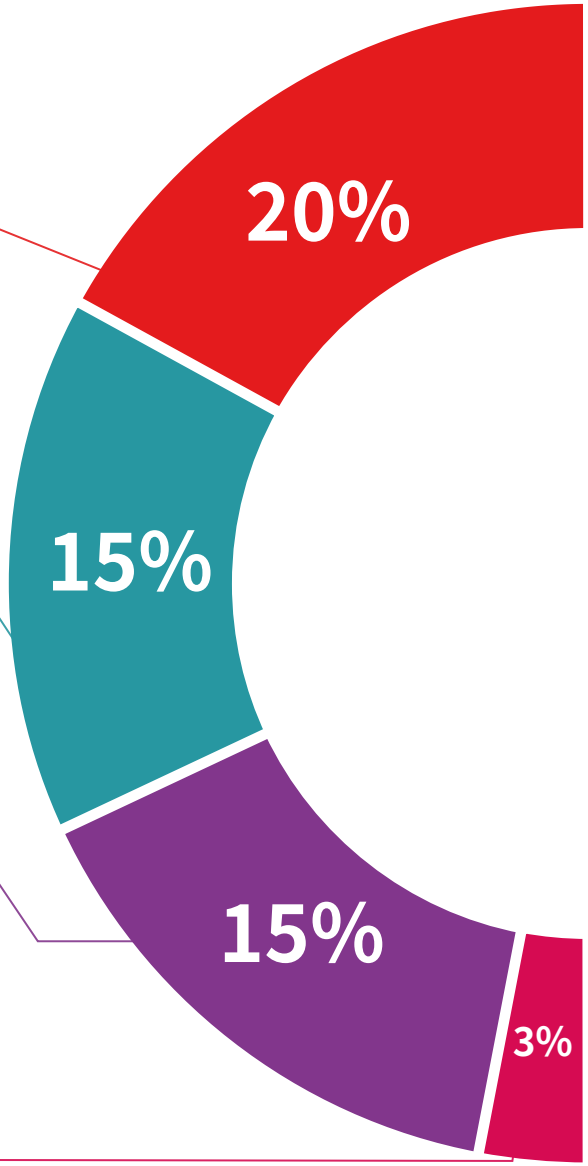
互动式总结

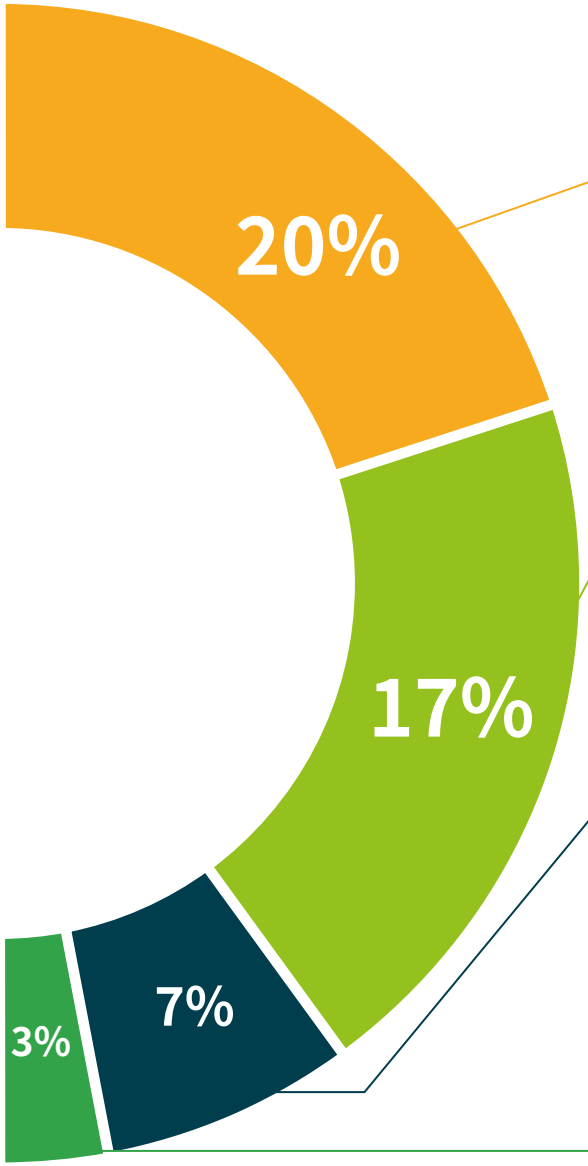
我们以有吸引力和动态的方式将内容呈现在多媒体中，包括音频，视频，图像，图表和概念图，以巩固知识。

这一用于展示多媒体内容的独特教育系统被微软公司评为 "欧洲成功案例"。

延伸阅读

最新文章，共识文件，国际指南...在我们的虚拟图书馆中，您将可以访问完成培训所需的一切。





案例研究

您将完成一系列有关该主题的最佳案例研究。由国际上最优秀的专家介绍，分析和指导案例。

Testing & Retesting

在整个课程中，我们会定期评估和重新评估你的知识。我们在米勒金字塔的4个层次中的3个层次上这样做。

大师班

科学证据表明第三方专家观察的效果显著。

向专家学习可以增强知识和记忆力、，并为我们今后做出艰难的决定建立信心。

快速行动指南

TECH以工作表或快速行动指南的形式提供课程中最相关的内容。一种帮助学生在学习中进步的综合,实用和有效的方法。

07

教学人员

这个网络安全高级管理（CISO，首席信息安全官）高级硕士课程的教师队伍由活跃的专业人士组成，他们对该领域的现状了如指掌，因此会将当前网络安全的所有关键传授给学生。通过这种方式，该课程的学生可以确保获得该领域的最新进展，并通过 TECH 选拔的著名教师获得这些进展。

TECH 为您提供最专业的主管和教师，以便您的方法和学习是最好的”

国际客座董事

Frederic Lemieux博士是国际公认的情报、国家安全、国土安全、网络安全和颠覆性技术领域的创新专家和灵感领袖。情报、国土安全、国土安全、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相关贡献，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、私人和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。就这样，他享有盛誉的学术生涯使他成为了 MPS 项目的实践教授和教员主任。**应用情报、网络安全风险管理、技术管理和信息技术管理**，在 **乔治城大学**。

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

> 通过TECH你将能够与世界上最优秀的专业人士一起学习”

管理

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硕士: Docker 和 KubernetesCas-培训
- 微软 Azure 安全技术E-Council

Olalla Bonal, Martín 先生

- 安永高级 区块链 业务经理
- IBM 区块链客户端技术专家
- Blocknitive的架构总监
- IBM子公司WedoIT非关系型分布式数据库团队协调员
- Bankia的基础设施架构师
- T-Systems的布局部门主管
- Bing Data Spain SL的部门协调人员

教师

Marcos Sbarbaro, Victoria Alicia 女士

- B60 。的原生 Android 移动应用程序开发人员英国
- 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
- 设备迁移及 PDA 移动设备管理、维护和培训的系统技术员
- 加泰罗尼亚开放大学的计算机系统技术工程专业
- 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

Entrenas, Alejandro 博士

- 网络安全项目经理。Entelgy Innotec Security
- 网络安全顾问。Entelgy
- 信息安全分析员西班牙 Innovery
- 信息安全分析员。Atos
- 科尔多瓦大学计算机系统技术工程学士
- 马德里理工大学信息安全方向与管理硕士
- ITIL v4 IT 服务管理基础证书。ITIL 认证
- IBM Security QRadar SIEM 7.1 Advanced.Avnet
- IBM Security QRadar SIEM 7.1 Foundations.Avnet

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
- 在位于巴伦西亚的福特工厂担任电子技术员

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

Gonzalo Alonso, Félix 先生

- Smart REM Solutions 首席执行官兼创始人
- Dynargy 风险与创新工程主管
- 技术咨询公司 Risknova 的常务董事和创始合伙人
- 保险公司合作研究所保险管理硕士学位
- 科米亚斯主教大学工业技术工程学位，工业电子专业。

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

Redondo, Jesús Serrano 先生
- 网络开发和网络安全技术员
- 帕伦西亚 Roams 网络开发人员
- 西班牙马德里 Telefónica 前端开发人员
- 马德里 Best Pro Consulting SL 前端开发 员
- 卡斯蒂利亚-莱昂齐纳集团电信设备和服务安装工
- 卡斯蒂利亚-莱昂 Lican Comunicaciones SL 电信设备和服务安装工
- 由马德里Getafe CFTIC颁发的信息安全证书
- 由巴伦西亚Trinidad Arroyo IES颁发的高级电信与信息系统技术员
- 帕伦西亚特立尼达阿罗约 IES 中压和低压电工安装高级技师
- Incibe黑客学院提供的逆向工程、速记和加密培训

Nogales Ávila, Javier 先生
- Quint 企业云和采购高级顾问
- Indra云技术顾问
- 埃森哲公司协理技术顾问
- 哈恩大学工业组织工程专业毕业。
- 博尔商学院工商管理 MBA 学位

Gómez Rodríguez, Antonio 先生
- 甲骨文首席云解决方案工程师
- 马拉加开发者聚会联合组织者
- Sopra集团和Everis的专家顾问
- System Dynamics的团队负责人
- SGO软件公司的软件开发人员
- 拉萨尔商学院电子商务硕士学位
- 加泰罗尼亚理工学院技术和信息系统研究所
- 毕业于加泰罗尼亚理工大学电信工程专业

Rodrigo Estébanez, Juan Manuel 先生
- Ismet Tech 联合创始人
- Ecix 集团信息安全经理
- Atos IT Solutions and Services A/S业务安全官
- 大学网络安全管理讲师
- 毕业于巴利亚多利德大学工程系。
- CEU San Pablo 大学综合管理系统硕士学位

Del Valle Arias, Jorge 先生
- 电信工程师，擅长业务开发
- 西班牙智能城市解决方案和软件业务开发经理。Itron, Inc
- 物联网顾问
- 临时物联网业务总监。TCOMET
- 物联网、工业 4.0 业务部负责人。西班牙二极管
- 物联网和电信地区销售经理。Aicox 解决方案
- 首席技术官（CTO）和业务开发经理。TELYC 咨询公司
- 传感器智能创始人兼CEO
- 业务和项目负责人。Codio

- Codium Networks 运营总监
- 首席硬件和固件设计工程师。AITEMIN
- 射频规划和优化区域主管 - LMDS 3.5 GHz 网络。Clearwire
- 马德里理工大学电信工程师
- 马德里拉萨尔国际研究生院行政工商管理硕士
- 可再生能源硕士。CEPYME

Gozalo Fernández, Juan Luis 先生

- Open Canarias的基于区块链的产品经理
- Alastria 的区块链 DevOps 总监
- 西班牙桑坦德银行的服务水平技术总监
- Tinkerlink 移动应用开发总监 Cronos Telecom
- 西班牙巴克莱银行 IT 服务管理技术总监
- 在UNED获得计算机工程学位 (UNED)
- DeepLearning.ai 的 Deep Learning专业

Jurado Jabonero, Lorena 博士

- Grupo Pascual 信息安全主管 (CISO)
- 毕马威会计师事务所网络安全经理。西班牙
- 银行信息技术流程和基础设施项目控制与管理顾问
- 达尔基亚操作工具工程师
- 大众银行集团开发人员

- 马德里理工大学应用程序开发人员。
- 毕业于 Alfonso X El Sabio 大学计算机工程专业
- 马德里理工大学计算机管理技术工程师
- ISACA 认证的数据隐私解决方案工程师 (CDPSE)

Ortega Esteban, Octavio 先生

- 营销和网络开发专家
- 应用程序开发员和自由职业网页开发者
- Smallsquid SL首席运营官
- Ortega y Serrano 电子商务管理员
- 信息与通信领域职业资格课程讲师
- 网络安全课程讲师
- 加泰罗尼亚开放大学心理学毕业生
- 软件分析、设计和解决方案高级大学技术员
- 高级编程高级大学技术员

Embid Ruiz, Mario 先生

- Martínez-Echevarría Abogados 律师事务所信息和通信技术与数据保护专家
- Branddocs SL 法律负责人
- BBVA 中小型企业部门风险分析师
- 大学法律研究生课程讲师
- 胡安-卡洛斯国王大学法律学位
- Rey Juan Carlos大学工商管理专业毕业
- Villanueva 大学研究中心新技术、互联网和视听法硕士学位

> 趁此了解这个领域的最新发展并将其应用到你的日常工作中的机会"

08

学位

网络安全高级管理（CIS O，Chief Information Security Officer）高级硕士课程除了保证最严格和最新的培训外，还可以获得由 TECH 科技大学颁发的高级硕士学位证书。

顺利完成该课程后你将获得大学学位证书
无需出门或办理其他手续"

这个**网络安全高级管理(CIS O, Chief Information Security Officer)高级硕士**包含了市场上最完整和最新的课程。

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**高级硕士**学位。

学位由**TECH科技大学**颁发,证明在高级硕士学位中所获得的资质,并满足工作交流,竞争性考试和职业评估委员会的要求。

学位:**网络安全高级管理(CIS O, Chief Information Security Officer)高级硕士**

模式:**在线**

时长: **2年**


tech 科学技术大学

授予

文凭

_____先生/女士, 身份证号码_____

顺利通过并获得认证的课程是

高级硕士

网络安全高级管理(CIS O, Chief Information Security Officer)

这是一个由本大学授予的学位,相当于3,000个小时,
开始日期是 dd/mm/aaaa,结束日期是dd/mm/aaaa。

截至2018年6月28日,TECH是一所被公共教育部认可的私立高等教育机构。

2020年六月17日

Tere Guevara Navarro女士
校长

Unique TECH Code: AFWORD23S techtitute.com/certificates


网络安全高级管理(CIS O, Chief Information Security Officer)高级硕士

教学大纲概况

学期	学科	小时	性质
1°	网络情报与网络安全	103	必修
1°	主机的安全	103	必修
1°	网络安全(周边)	103	必修
1°	智能手机的安全	103	必修
1°	IoT安全	103	必修
1°	道德黑客	103	必修
1°	逆向工程	103	必修
1°	安全发展	103	必修
1°	软件和硬件中安全策略的实际实施	103	必修
1°	法医分析	103	必修
1°	系统设计和开发的安全问题	103	必修
1°	信息安全架构和模式	103	必修
1°	信息安全管理系统(SGSI)	103	必修
1°	IT安全管理	103	必修
1°	安全事件管理政策	103	必修

学期	学科	小时	性质
2°	风险分析和IT安全环境	103	必修
2°	IT系统中威胁分析的安全政策	103	必修
2°	面对攻击时安全政策的实际执行情况	103	必修
2°	信息技术的密码学	103	必修
2°	IT安全中的身份和访问管理	103	必修
2°	通信和软件运行的安全性	103	必修
2°	云环境的安全性	103	必修
2°	信息系统安全政策中的监测工具	103	必修
2°	IoT设备通信的安全性	103	必修
2°	与安全有关的业务连续性计划	103	必修
2°	实用的安全灾难恢复政策	103	必修
2°	在企业中实施安全和环境安全政策	103	必修
2°	企业中的安全通信政策	103	必修
2°	信息安全政策的组织方面	116	必修

Dr. Pedro Navarro Illana
Rector

tech global university

*海牙加注。如果学生要求为他们的纸质资格证书提供海牙加注,TECH EDUCATION将采取必要的措施来获得,但需要额外的费用。

tech 科学技术大学

高级硕士
网络安全高级管理 (CISO, Chief Information Security Officer)

- 模式:**在线**
- 时长: **2年**
- 学位: **TECH 科技大学**
- 课程表:**自由安排时间**
- 考试模式:**在线**

高级硕士
网络安全高级管理 (CIS O, Chief Information Security Officer)

tech 科学技术大学