高级硕士

Secure Information Management

tech global university

tech global university

高级硕士
Secure Information Management

- 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-degree/advanced-master-degree-secure-information-management**

目录

01

课程介绍

在当今数字时代，各个领域的活动通过互联网进行综合管理。娱乐、工作以及与朋友和家人的沟通越来越依赖在线工具和资源。每天都有大量的信息被传输，从社交媒体和消息应用中的简单数据到存储在银行或企业平台上的个人和职业敏感信息。这一局面要求具备处理和保护信息能力的专业人士，能够在不同的环境中确保信息安全。因此，TECH设计了这门软件工程课程，旨在培养具备有效管理和保护信息所需技能的专业人员，应对当前的数字挑战，并为创建更安全，更可靠的技术环境做出贡献。

面对持续的威胁，保护数据是关键。你可以成为这些宝贵信息的守护者”

每秒钟，数字环境中都会生成、共享和存储数千个数据。从在线支付，获取教育服务到协调商业活动或保护数字身份，技术已经成为不断改变我们生活和工作方式的重要支柱。这些互动时刻都会产生和传输大量数据，从个人信息到与公司和机构相关的敏感文件。这种持续的数据流凸显了适当的管理的必要性，以确保其安全性和隐私性。

管理和保护这些数据并非易事，因为它需要结合网络安全和信息管理等领域的高度专业知识。这些学科虽然不同，但必须结合起来才能应对当今数字环境的复杂挑战。在这种背景下，Secure Information Management高级硕士为有兴趣获得全面视野的工程师和 IT 专业人士提供了一个独特的机会，使他们能够掌握两个领域并将自己定位为不断发展的领域的领导者。

许多公司和机构面临保护关键和高度敏感数据的需要，但缺乏能够确保有效管理、保存和监控其数字信息的专家。为了满足这种需求，TECH 设计了一个将最好的内容与具有认可的职业生涯的教学团队相结合的课程。这种方法可确保学生获得在就业市场中脱颖而出并在寻求加强信息安全性的组织中获得战略职位所需的工具和知识。

这个**Secure Information Management 高级硕士高级硕士**包含市场上最完整和最新的课程。主要特点是：

- Secure Information Management 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
- 它特别强调Secure Information Management方向的创新方法
- 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

> 获得在竞争激烈的数字环境中确保安全和有效管理数据所需的技能”

探索 TECH 设计的最具创新性的教育方法，以保证沉浸式和情境化的学习。

访问 100% 在线课程，您可以随时随地按照自己的节奏学习。

> 利用Secure Information Management高级课程中包含的众多实践资源巩固你的理论知识”

其教学人员包括来自金融领域的专业人士，他们将自己的工作经验带入这个课程，以及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。其中包括波士顿凯尔特人队的表现教练 Isaiah Covington、哈佛大学MetaLAB的首席研究员Magda Romanska、MD Anderson癌症中心转化分子病理学部主席Ignacio Wistumba以及时代杂志的创意总监D.W Pine等，都是著名的教授、研究人员和跨国公司的高级管理人员。

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。

Forbes
Mejor universidad online del mundo

Plan
de estudios
más completo

Profesorado
TOP
Internacional

La metodología
más eficaz

nº1
Mundial
Mayor universidad online del mundo

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。还提供创新的教育资源，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

该Secure Information Management高级硕士课程的教材是由网络安全和数据管理专家团队开发的。通过这种方式，课程深入探讨了主要的数字威胁以及最先进的信息保护和管理方法。这将使毕业生能够识别特定的风险并制定有效的解决方案，以确保各种专业环境中的数据安全。该大纲还涉及该领域最具创新性的工具，推广旨在保护组织数字资产的战略。

> 您将为保护敏感数据和创建安全系统做出贡献，以保证公司和机构的运营连续性”

模块 1. 商业组织的数据分析

1.1. 商业分析
- 1.1.1. 商业分析
- 1.1.2. 数据结构
- 1.1.3. 阶段和元素

1.2. 公司的数据分析
- 1.2.1. 按部门划分的仪表板和 Kpi
- 1.2.2. 运营，战术和策略报告
- 1.2.3. 应用于每个部门的数据分析
  - 1.2.3.1. 营销与传播
  - 1.2.3.2. 商业
  - 1.2.3.3. 客户服务
  - 1.2.3.4. 采购
  - 1.2.3.5. 行政管理
  - 1.2.3.6. 人力资源
  - 1.2.3.7. 生产
  - 1.2.3.8. IT

1.3. 营销与传播
- 1.3.1. 用于衡量、应用和收益的KPI'
- 1.3.2. 营销系统和**数据库**
- 1.3.3. 在营销中实施数据分析结构
- 1.3.4. 营销和传播计划
- 1.3.5. 策略，预测和活动管理

1.4. 贸易和销售
- 1.4.1. 数据分析在商业领域的贡献
- 1.4.2. 销售部门的需求
- 1.4.3. 市场研究

1.5. 客户服务
- 1.5.1. 忠诚度
- 1.5.2. 个人素质和情商
- 1.5.3. 顾客满意度

1.6. 采购
- 1.6.1. 用于市场研究的数据分析
- 1.6.2. 竞争研究的数据分析
- 1.6.3. 其他应用

1.7. 行政管理
- 1.7.1. 行政部门的需求
- 1.7.2. **数据仓库**和财务风险分析
- 1.7.3. **数据仓库**和信用风险分析

1.8. 人力资源
- 1.8.1. 人力资源和数据分析的好处
- 1.8.2. 人力资源部门的数据分析工具
- 1.8.3. 数据分析在人力资源中的应用

1.9. 生产
- 1.9.1. 生产部门的数据分析
- 1.9.2. 应用
- 1.9.3. 益处

1.10. IT
- 1.10.1. IT部门
- 1.10.2. 数据分析和数字化转型
- 1.10.3. 创新和生产力

模块 2. 数据科学的数据和信息管理和操作

2.1. 统计数据变量，指数和比率
- 2.1.1. 统计数据
- 2.1.2. 统计维度
- 2.1.3. 变量，指数和比率

2.2. 数据类型
- 2.2.1. 定性的
- 2.2.2. 定量的
- 2.2.3. 表征和类别

2.3. 了解测量数据
- 2.3.1. 集中化措施
- 2.3.2. 分散的措施
- 2.3.3. 相关性

2.4. 从图表中理解数据
- 2.4.1. 根据数据类型进行可视化
- 2.4.2. 图文信息解读
- 2.4.3. 使用R自定义图形

2.5. 概率
- 2.5.1. 概率
- 2.5.2. 概率函数
- 2.5.3. 分布

2.6. 数据收集
- 2.6.1. 收集方法
- 2.6.2. 收集工具
- 2.6.3. 收集渠道

2.7. 数据清理
- 2.7.1. 数据清理阶段
- 2.7.2. 数据质量
- 2.7.3. 数据操作(使用 R)

2.8. 数据分析,解释和结果评估
- 2.8.1. 统计措施
- 2.8.2. 关系指数
- 2.8.3. 数据挖掘

2.9. 数据仓库 (Datawarehouse)
- 2.9.1. 元素
- 2.9.2. 设计

2.10. 可用性数据
- 2.10.1. 访问
- 2.10.2. 实用性
- 2.10.3. 安全

模块 3.物联网设备和平台作为数据科学的基础

3.1. 物联网
- 3.1.1. 未来的互联网,物联网
- 3.1.2. 工业互联网联盟

3.2. 参考架构
- 3.2.1. 参考架构
- 3.2.2. 图层
- 3.2.3. 组件

3.3. 传感器和物联网设备
- 3.3.1. 主要部分
- 3.3.2. 传感器和执行器

3.4. 通信和协议
- 3.4.1. 协议OSI模型
- 3.4.2. 通讯技术

3.5. 物联网和工业物联网的 云平台
- 3.5.1. 通用平台
- 3.5.2. 工业平台
- 3.5.3. 开源平台

3.6. 物联网平台的数据管理
- 3.6.1. 数据管理机制开放数据
- 3.6.2. 数据交换和可视化

3.7. 物联网安全
- 3.7.1. 要求和安全领域
- 3.7.2. 工业物联网安全策略

3.8. 物联网应用程式
- 3.8.1. 智慧城市
- 3.8.2. 健康和身体情况
- 3.8.3. 智能家居
- 3.8.4. 其他应用

3.9. 工业物联网应用
- 3.9.1. 制造业
- 3.9.2. 运输
- 3.9.3. 能源
- 3.9.4. 农业和畜牧业
- 3.9.5. 其他行业

3.10. 工业4.0
- 3.10.1. 物联网(机器人物联网)
- 3.10.2. 3D增材制造
- 3.10.3. 大数据分析

模块 4. 用于数据分析的图形

4.1. 探索性分析
- 4.1.1. 信息分析的展示
- 4.1.2. 图形展示的价值
- 4.1.3. 图形展示的新范式

4.2. 数据科学优化
- 4.2.1. 颜色范围和设计
- 4.2.2. 图形中的格式塔
- 4.2.3. 要避免的错误和提示

4.3. 基础数据来源
- 4.3.1. 质量代表
- 4.3.2. 用于数量表示
- 4.3.3. 用于时间表示

4.4. 复杂的数据源
- 4.4.1. 文件，列表和 BBDD
- 4.4.2. 开放数据
- 4.4.3. 不断产生的数据

4.5. 图表类型
- 4.5.1. 基本表述
- 4.5.2. 区块
- 4.5.3. 分散分析的代表
- 4.5.4. 圆形代表
- 4.5.5. 气泡代表
- 4.5.6. 地理代表

4.6. 显示类型
- 4.6.1. 比较和有关联的
- 4.6.2. 分布
- 4.6.3. 分层

4.7. 具有图形的报告设计
- 4.7.1. 图表在营销报告中的应用
- 4.7.2. 图表在仪表板和 Kpi 中的应用
- 4.7.3. 图表在策略计划中的应用
- 4.7.4. 其他用途：科学，健康，商业

4.8. 图解叙述
- 4.8.1. 图解叙述
- 4.8.2. 进化
- 4.8.3. 实用性

4.9. 面向可视化的工具
- 4.9.1. 高级工具
- 4.9.2. 在线软件
- 4.9.3. 开源

4.10. 数据可视化新技术
- 4.10.1. 现实虚拟化系统
- 4.10.2. 用于增强和增强现实的系统
- 4.10.3. 智能系统

模块 5. 数据科学工具

5.1. 数据科学
- 5.1.1. 数据科学
- 5.1.2. 数据科学的高级工具

5.2. 数据，信息和知识
- 5.2.1. 数据，信息和知识
- 5.2.2. 数据类型
- 5.2.3. 数据源

5.3. 从数据到信息
- 5.3.1. 数据分析
- 5.3.2. 分析类型
- 5.3.3. 从数据集中提取信息

5.4. 通过可视化提取信息
- 5.4.1. 可视化作为分析工具
- 5.4.2. 可视化方法
- 5.4.3. 查看数据集

5.5. 数据质量
- 5.5.1. 质量数据
- 5.5.2. 数据清理
- 5.5.3. 基本数据预处理

5.6. 数据集
- 5.6.1. 丰富数据集
- 5.6.2. 维度的祸害
- 5.6.3. 修改我们的数据集

5.7. 不平衡
- 5.7.1. 阶级不平衡
- 5.7.2. 不平衡缓解技术
- 5.7.3. 平衡数据集

5.8. 无监督模型
- 5.8.1. 无监督模型
- 5.8.2. 方法
- 5.8.3. 使用无监督模型进行分类

5.9. 监督模型
- 5.9.1. 监督模型
- 5.9.2. 方法
- 5.9.3. 使用监督模型进行分类

5.10. 工具和好的做法
- 5.10.1. 数据科学的正确实践
- 5.10.2. 最佳模型
- 5.10.3. 有用的工具

模块 6. 数据挖掘。选择、预处理和转换

6.1. 统计推断
- 6.1.1. 描述性统计对统计推断
- 6.1.2. 参数化程序
- 6.1.3. 非参数过程

6.2. 探索性分析
- 6.2.1. 描述性分析
- 6.2.2. 视觉化
- 6.2.3. 数据准备

6.3. 数据准备
- 6.3.1. 数据整合和清理
- 6.3.2. 数据标准化
- 6.3.3. 转换属性

6.4. 缺失值
- 6.4.1. 缺失值的处理
- 6.4.2. 最大似然插补方法
- 6.4.3. 使用机械学习估算缺失值

6.5. 数据中的噪音
- 6.5.1. 噪声类别和属性
- 6.5.2. 噪声过滤
- 6.5.3. 噪音的影响

6.6. 维度的祸害
- 6.6.1. Oversampling
- 6.6.2. Undersampling
- 6.6.3. 多维数据缩减

6.7. 从连续属性到离散属性
- 6.7.1. 连续数据与离散数据
- 6.7.2. 离散化过程

6.8. 数据
- 6.8.1. 数据选择
- 6.8.2. 前景与选择标准
- 6.8.3. 挑选方法

6.9. 选择阶段
- 6.9.1. 选择阶段的方法
- 6.9.2. 原型的选择
- 6.9.3. 选择阶段的高级方法

6.10. Big Data环境的数据预处理
- 6.10.1. 大数据
- 6.10.2. “经典”对批量预处理
- 6.10.3. 智能数据

模块 7. 随机现象的可预测性和分析

7.1. 时间序列
- 7.1.1. 时间序列
- 7.1.2. 实用性和适用性
- 7.1.3. 相关案例

7.2. 时序
- 7.2.1. ST 季节性趋势
- 7.2.2. 典型变化
- 7.2.3. 废料分析

7.3. 类型
- 7.3.1. 周期性
- 7.3.2. 非周期性
- 7.3.3. 转型与调整

7.4. 时间序列方案
- 7.4.1. 添加方案(模型)
- 7.4.2. 乘法方案(模型)
- 7.4.3. 确定模型类型的流程

7.5. 基本预测方法
- 7.5.1. 平均值
- 7.5.2. Naïve
- 7.5.3. 季节性Naïve
- 7.5.4. 方法比较

7.6. 废料分析
- 7.6.1. 自相关
- 7.6.2. 废料的ACF
- 7.6.3. 相关性检验

7.7. 时间序列的回归
- 7.7.1. ANOVA
- 7.7.2. 基础知识
- 7.7.3. 实际应用

7.8. 时间序列预测模型
- 7.8.1. ARIMA
- 7.8.2. 指数平滑

7.9. 用 R 操作和分析时间序列
- 7.9.1. 数据准备
- 7.9.2. 识别模式
- 7.9.3. 模型分析
- 7.9.4. 预测

7.10. 与R相结合的图形分析
- 7.10.1. 常见情况
- 7.10.2. 解决简单问题的实际应用
- 7.10.3. 高级问题解决的实际应用

模块 8. 智能系统的设计与开发

8.1. 数据预处理
- 8.1.1. 数据预处理
- 8.1.2. 数据转换
- 8.1.3. 数据挖掘

8.2. 机器学习
- 8.2.1. 有监督和无监督的学习
- 8.2.2. 强化学习
- 8.2.3. 其他学习范式

8.3. 分类算法
- 8.3.1. 归纳机械式学习
- 8.3.2. SVM和KNN
- 8.3.3. 分类的指标和分数

8.4. 回归运算
- 8.4.1. 线性回归，逻辑回归和非线性模型
- 8.4.2. 时序
- 8.4.3. 回归的指标和分数

8.5. 聚类算法
- 8.5.1. 层次聚类技术
- 8.5.2. 部分聚类技术
- 8.5.3. 聚类的指标和分数

8.6. 关联规则技术
- 8.6.1. 提取规则的方法
- 8.6.2. 关联规则算法的指标和分数

8.7. 先进的分类技术多分类
- 8.7.1. Bagging算法
- 8.7.2. 随机森林分类器
- 8.7.3. 提升决策树

8.8. 概率图模型
- 8.8.1. 概率模型
- 8.8.2. 贝叶斯网络属性，表示和参数化
- 8.8.3. 其他概率图模型

8.9. 神经网络
- 8.9.1. 使用人工神经网络进行机械式学习
- 8.9.2. 前馈网络

8.10. 深度学习
- 8.10.1. 深度前馈网络
- 8.10.2. 卷积神经网络和序列模型
- 8.10.3. 实现深度神经网络的工具

模块 9. 用于密集使用数据的架构和系统

9.1. 非功能性需求大数据应用的支柱
- 9.1.1. 可靠性
- 9.1.2. 适应性
- 9.1.3. 可维护性

9.2. 数据模型
- 9.2.1. 关系模型
- 9.2.2. 纪录模型
- 9.2.3. 图数据模型

9.3. 数据库数据存储和检索管理
- 9.3.1. 指数
- 9.3.2. 结构化日志存储
- 9.3.3. B树

9.4. 数据编码格式
- 9.4.1. 特定语言格式
- 9.4.2. 标准化格式
- 9.4.3. 二进制编码格式
- 9.4.4. 进程之间的数据流

9.5. 复制
- 9.5.1. 复制目标
- 9.5.2. 复制模型
- 9.5.3. 复制问题

9.6. 分布式事务
- 9.6.1. 事务
- 9.6.2. 分布式事务的协议
- 9.6.3. 可序列化事务

9.7. 分区
- 9.7.1. 分区表格
- 9.7.2. 二级索引和分区的交互
- 9.7.3. 重新平衡分区

9.8. 离线数据处理
- 9.8.1. 批量处理
- 9.8.2. 分布式文件系统
- 9.8.3. MapReduce

9.9. 实时数据处理
- 9.9.1. 消息的 代理 类型
- 9.9.2. 将数据库表示为数据流
- 9.9.3. 数据流处理

9.10. 在公司的实际应用
- 9.10.1. 读数的一致性
- 9.10.2. 数据的整体方法
- 9.10.3. 扩展分布式服务

模块 10. 数据科学在商业活动领域的实际应用

10.1. 医疗保健领域
- 10.1.1. 人工智能和数据分析在医疗保健领域的影响
- 10.1.2. 机遇与挑战

10.2. 医疗保健的风险和趋势
- 10.2.1. 用于医疗保健领域
- 10.2.2. 使用人工智的相关潜在风险

10.3. 金融服务
- 10.3.1. 人工智能和数据分析对金融服务行业的影响
- 10.3.2. 用于金融服务业
- 10.3.3. 使用人工智的相关潜在风险

10.4. 零售
- 10.4.1. 人工智能和数据分析对零售业的影响
- 10.4.2. 用于零售
- 10.4.3. 使用人工智的相关潜在风险

10.5. 工业4.0
- 10.5.1. 人工智能和数据分析在工业 4.0 中的影响
- 10.5.2. 用于工业 4.0

10.6. 工业4.0的风险和趋势
- 10.6.1. 使用人工智的相关潜在风险

10.7. 公共行政
- 10.7.1. 人工智能和数据分析在公共管理中的意义
- 10.7.2. 用于公共管理
- 10.7.3. 使用人工智的相关潜在风险

10.8. 教育
- 10.8.1. 人工智能和数据分析在教育中的意义
- 10.8.2. 使用人工智的相关潜在风险

10.9. 林业和农业
- 10.9.1. 人工智能和数据分析对林业和农业的影响
- 10.9.2. 用于林业和农业
- 10.9.3. 使用人工智的相关潜在风险

10.10. 人力资源
- 10.10.1. 人工智能和数据分析在人力资源管理中的意义
- 10.10.2. 商业世界中的实际应用
- 10.10.3. 使用人工智的相关潜在风险

模块 11. 网络情报与网络安全

11.1. 网络情报
- 11.1.1. 网络情报
  - 11.1.1.1. 智能
    - 11.1.1.1.1. 情报周期
  - 11.1.1.2. 网络情报
  - 11.1.1.3. 网络情报与网络安全
- 11.1.2. 情报分析师
  - 11.1.2.1. 情报分析师的角色
  - 11.1.2.2. 情报分析员在评估活动中的偏见

11.2. 网络安全
- 11.2.1. 安全层
- 11.2.2. 识别网络威胁
  - 11.2.2.1. 外部威胁
  - 11.2.2.2. 内部威胁
- 11.2.3. 不利的行动
  - 11.2.3.1. 社会工程学
  - 11.2.3.2. 常用方法

11.3. 智能技术和工具
- 11.3.1. OSINT
- 11.3.2. SOCMINT
- 11.3.3. HUMIT
- 11.3.4. Linux 发行和工具
- 11.3.5. OWISAM
- 11.3.6. OWISAP
- 11.3.7. PTES
- 11.3.8. OSSTM

11.4. 评估方法
- 11.4.1. 情报分析
- 11.4.2. 组织获取信息的技术
- 11.4.3. 信息来源的可靠性和可信度
- 11.4.4. 分析方法
- 11.4.5. 情报结果展示

11.5. 审计和文件
- 11.5.1. IT安全审计
- 11.5.2. 审计文件和许可证
- 11.5.3. 审计的类型
- 11.5.4. 可交付的成果
  - 11.5.4.1. 技术报告
  - 11.5.4.2. 执行报告

11.6. 网络匿名
- 11.6.1. 使用匿名
- 11.6.2. 匿名技术（Proxy,, VPN）。
- 11.6.3. TOR、Freenet 和 IP2 网络

11.7. 威胁和安全类型
- 11.7.1. 威胁类型
- 11.7.2. 实体安全
- 11.7.3. 网络安全
- 11.7.4. 逻辑安全
- 11.7.5. Web 应用程序的安全性
- 11.7.6. 移动设备的安全

11.8. 法规和合规性
- 11.8.1. RGPD
- 11.8.2. 2019 年国家网络安全战略
- 11.8.3. ISO 27000 系列
- 11.8.4. NIST 网络安全框架
- 11.8.5. PIC
- 11.8.6. ISO 27032
- 11.8.7. 云法规
- 11.8.8. SOX
- 11.8.9. PCI

11.9. 风险分析和指标
- 11.9.1. 风险范围
- 11.9.2. 资产
- 11.9.3. 威胁
- 11.9.4. 漏洞
- 11.9.5. 风险评估
- 11.9.6. 风险处理

11.10. 网络安全领域的重要组织
- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. UNASUR - PROSUR

模块 12. 主机的安全

12.1. 备份副本
- 12.1.1. 备份策略
- 12.1.2. 适用于 Windows 的工具
- 12.1.3. Linux 的工具
- 12.1.4. macOS 的工具

12.2. 用户的防毒软件
- 12.2.1. 防毒软件的类型
- 12.2.2. 适用于 Windows 的防毒软件
- 12.2.3. linux 的防毒软件
- 12.2.4. MacOS的防毒软件
- 12.2.5. 智能手机的防毒软件

12.3. 入侵探测器 - HIDS
- 12.3.1. 入侵探测方法
- 12.3.2. Sagan
- 12.3.3. Aide
- 12.3.4. Rkhunter

12.4. 本地防火墙
- 12.4.1. 防火墙为Windows
- 12.4.2. 防火墙为Linux
- 12.4.3. 防火墙为MacOS

12.5. 密码管理器
- 12.5.1. Password
- 12.5.2. LastPass
- 12.5.3. KeePass
- 12.5.4. 粘性密码
- 12.5.5. RoboForm

12.6. 网络钓鱼检测器
- 12.6.1. 动手钓鱼 检测器
- 12.6.2. 网络 钓鱼工具

12.7. 间谍软件
- 12.7.1. 回避机制
- 12.7.2. 反间谍软件工具

12.8. 追踪器
- 12.8.1. 系统保护措施
- 12.8.2. 反跟踪工具

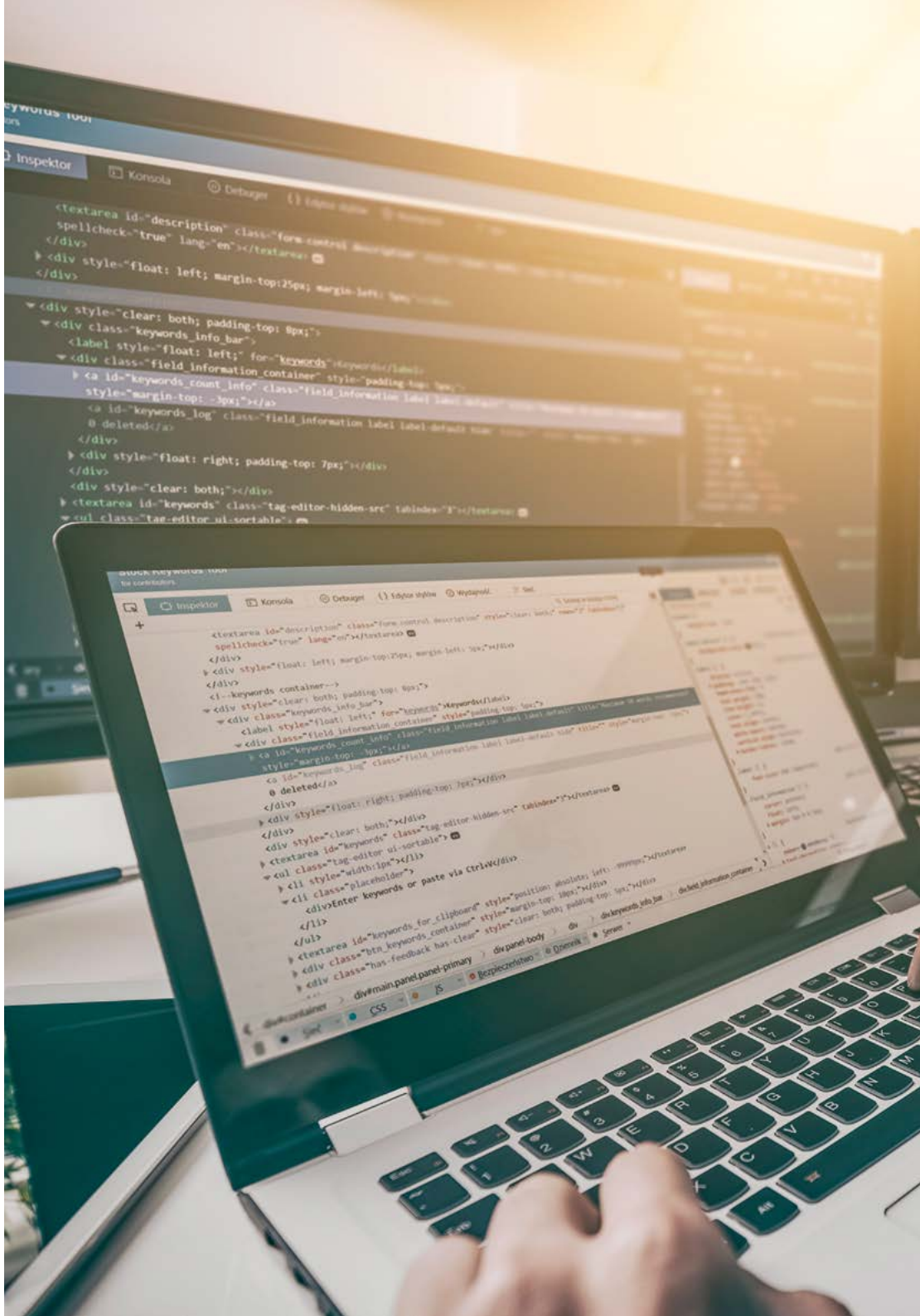
12.9. EDR-端点检测和响应
- 12.9.1. EDR 系统行为
- 12.9.2. EDR 和防病毒软件的区别
- 12.9.3. EDR系统的未来

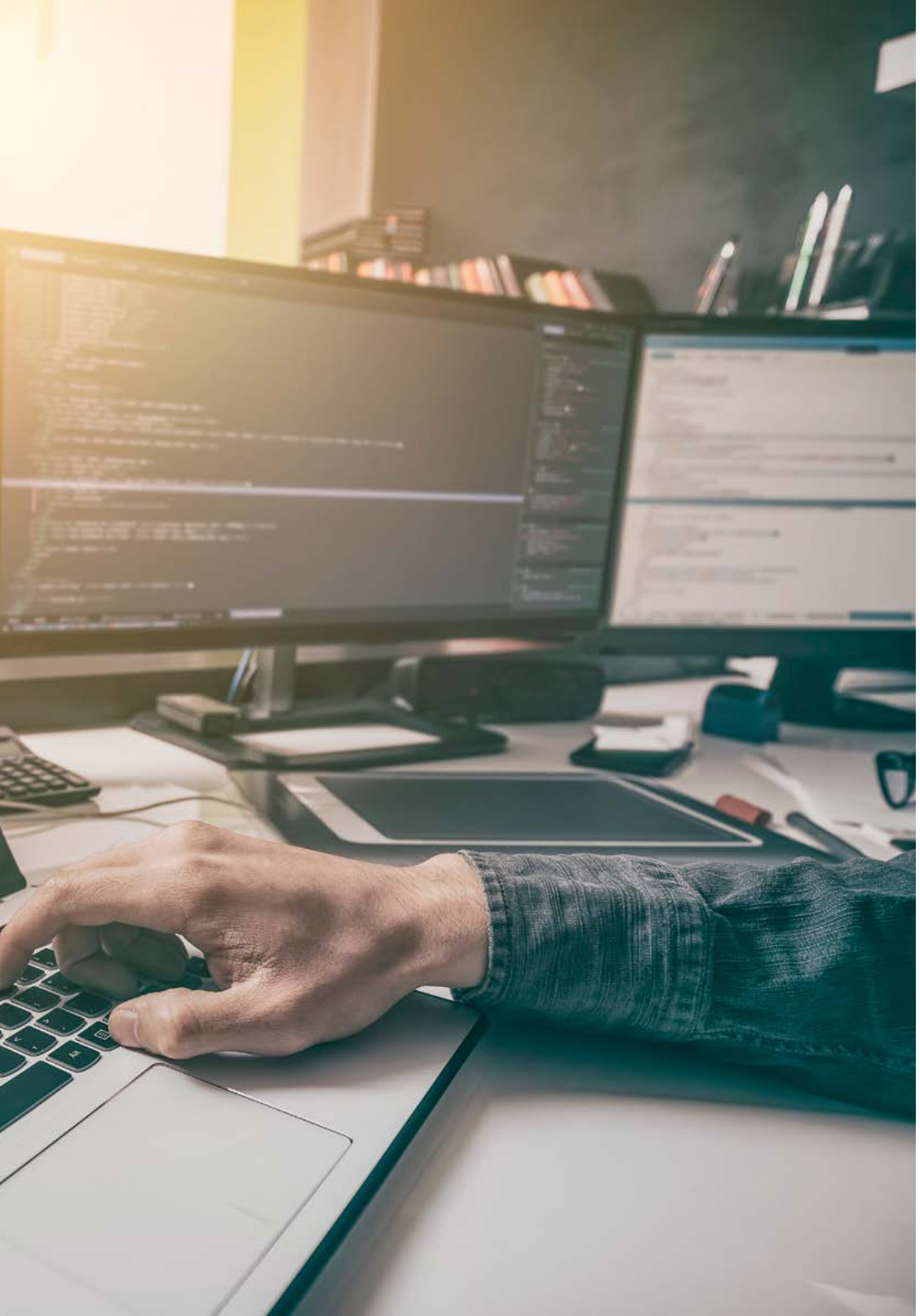
12.10. 控制安装软件
- 12.10.1. 存储库和软件商店
- 12.10.2. 允许或禁止的软件列表
- 12.10.3. 更新标准
- 12.10.4. 安装软件的权限

模块 13. 网络安全（周边）

13.1. 威胁检测和预防系统
- 13.1.1. 安全事件的总体框架
- 13.1.2. 目前的防御系统: Defense in Depth和 SOC
- 13.1.3. 当前的网络架构
- 13.1.4. 用于检测和预防事故的工具类型
  - 13.1.4.1. 基于网络的系统
  - 13.1.4.2. 基于主机的系统
  - 13.1.4.3. 集中式系统
- 13.1.5. 阶段/主机、容器和无服务器的通信和检测

13.2. 防火墙
- 13.2.1. 防火墙的类型
- 13.2.2. 攻击和缓解
- 13.2.3. Kernel Linux的常用防火墙
  - 13.2.3.1. UFW
  - 13.2.3.2. Nftables 和 iptables
  - 13.2.3.3. 火墙网（Firewalld）





13.2.4. 基于系统日志的检测系统
13.2.4.1. TCP 包装器
13.2.4.2. BlockHosts 和 DenyHosts
13.2.4.3. Fai2ban
13.3. 入侵检测和预防系统(IDS/IPS)
13.3.1. 对 IDS/IPS 的攻击
13.3.2. IDS/IPS 系统
13.3.2.1. Snort
13.3.2.2. Suricata
13.4. 下一代防火墙(NGFW)
13.4.1. NGFW与传统防火墙的区别
13.4.2. 核心能力
13.4.3. 商务解决方案
13.4.4. 云防火墙
13.4.4.1. cloud VPC 架构
13.4.4.2. cloud ACLs
13.4.4.3. Security Group
13.5. Proxy
13.5.1. Proxy类型
13.5.2. Proxy使用优点与缺点
13.6. 防毒引擎
13.6.1. 恶意软件和 IOC 的背景
13.6.2. 防毒引擎的问题
13.7. 邮件保护系统
13.7.1. 反垃圾邮件
13.7.1.1. 黑白名单
13.7.1.2. 贝叶斯过滤器
13.7.2. 邮件网关 (MGW)
13.8. SIEM
13.8.1. 组件和架构
13.8.2. 关联规则和用例
13.8.3. SIEM 系统的当前挑战

13.9. SOAR
- 13.9.1. SOAR 和 SIEM：敌人或盟友
- 13.9.2. SOAR系统的未来

13.10. 其他基于网络的系统
- 13.10.1. WAF
- 13.10.2. NAC
- 13.10.3. 蜜罐和蜜网
- 13.10.4. CASB

模块 14. 智能手机的安全

14.1. 移动设备的世界
- 14.1.1. 移动平台类型
- 14.1.2. iOS 设备
- 14.1.3. 安卓设备

14.2. 移动安全管理
- 14.2.1. OWASP 移动安全项目
  - 14.2.1.1. 十大漏洞
- 14.2.2. 通信、网络和连接模式

14.3. 商业环境的移动设备
- 14.3.1. 风险
- 14.3.2. 安全策略
- 14.3.3. 设备监控
- 14.3.4. 移动设备管理 (MDM)

14.4. 用户隐私和数据安全
- 14.4.1. 信息状态
- 14.4.2. 数据保护和保密
  - 14.4.2.1. 许可权
  - 14.4.2.2. 加密
- 14.4.3. 安全数据存储
  - 14.4.3.1. iOS 的安全存储
  - 14.4.3.2. 安卓的安全存储
- 14.4.4. 应用程序开发中的正确做法

14.5. 漏洞和攻击媒介
- 14.5.1. 漏洞
- 14.5.2. 攻击向量
  - 14.5.2.1. 恶意软件
  - 14.5.2.2. 泄露数据
  - 14.5.2.3. 操作数据

14.6. 主要威胁
- 14.6.1. 用户未强制
- 14.6.2. 恶意软件
  - 14.6.2.1. 恶意软件的类型
- 14.6.3. 社会工程学
- 14.6.4. 数据泄露
- 14.6.5. 信息盗窃
- 14.6.6. 不安全的 Wi-Fi 网络
- 14.6.7. 过时的软件
- 14.6.8. 恶意应用程序
- 14.6.9. 弱密码
- 14.6.10. 安全设置薄弱或不存在
- 14.6.11. 物理访问
- 14.6.12. 丢失或被盗的设备
- 14.6.13. 身份冒充（诚信）
- 14.6.14. 弱或损坏的密码学
- 14.6.15. 拒绝服务 (DoS)

14.7. 主要攻击
- 14.7.1. 网络钓鱼攻击
- 14.7.2. 与通信模式相关的攻击
- 14.7.3. 网络钓鱼攻击
- 14.7.4. Criptojacking持攻击
- 14.7.5. 中间人攻击

14.8. 黑客攻击
- 14.8.1. Rooting 和Jailbreaking
- 14.8.2. 移动攻击剖析
  - 14.8.2.1. 威胁传播
  - 14.8.2.2. 在设备上安装恶意软件
  - 14.8.2.3. 持久性
  - 14.8.2.4. 有效载荷执行和信息提取
- 14.8.3. 入侵 iOS 设备:机制和工具
- 14.8.4 入侵 Android 设备:机制和工具

14.9. 渗透测试
- 14.9.1. iOS 渗透测试
- 14.9.2. 安卓渗透测试
- 14.9.3. 工具

14.10. 保护和安全
- 14.10.1. 安全设定
  - 14.10.1.1. iOS 设备
  - 14.10.1.2. 安卓设备
- 14.10.2. 安防措施
- 14.10.3. 保护工具

模块 15. 物联网安全

15.1. 设备
- 15.1.1. 设备类型
- 15.1.2. 标准化架构
  - 15.1.2.1. ONEM2M
  - 15.1.2.2. IoTWF
- 15.1.3. 应用协议
- 15.1.4. 连接技术

15.2. 物联网设备。应用领域
- 15.2.1. 智能家居
- 15.2.2. 智慧城市
- 15.2.3. 运输
- 15.2.4. 可穿戴设备
- 15.2.5. 健康领域
- 15.2.6. IioT

15.3. 通讯协议
- 15.3.1. MQTT
- 15.3.2. LWM2M
- 15.3.3. OMA-DM
- 15.3.4. TR-069

15.4. 智能家居
- 15.4.1. 家庭自动化
- 15.4.2. 网络
- 15.4.3. 家用电器
- 15.4.4. 警惕和安全

15.5. 智慧城市
- 15.5.1. 照明
- 15.5.2. 气象
- 15.5.3. 安全

15.6. 运输
- 15.6.1. 地点
- 15.6.2. 付款和获得服务
- 15.6.3. 连接性

15.7. 可穿戴设备
- 15.7.1. 智能衣服
- 15.7.2. 智能首饰
- 15.7.3. 智能手表

15.8. 健康领域
- 15.8.1. 运动/心率监测
- 15.8.2. 监测患者和老年人
- 15.8.3. 可植入的
- 15.8.4. 手术机器人

15.9. 连接性
- 15.9.1. WiFi/网关
- 15.9.2. 蓝牙
- 15.9.3. 内置连接

15.10. 证券化
- 15.10.1. 专用网络
- 15.10.2. 密码管理器
- 15.10.3. 使用加密协议
- 15.10.4. 使用提示

模块 16. 道德黑客

16.1. 工作环境
- 16.1.1. Linux 发行版
  - 16.1.1.1. Kali Linux - 进攻性安全
  - 16.1.1.2. 鹦鹉系统
  - 16.1.1.3. Ubuntu
- 16.1.2. 虚拟化系统
- 16.1.3. Sandbox
- 16.1.4. 实验室部署

16.2. 方法
- 16.2.1. OSSTM
- 16.2.2. OWASP
- 16.2.3. 美国国家标准与技术研究院
- 16.2.4. PTES
- 16.2.5. ISSAF

16.3. Footprinting
- 16.3.1. 开源情报 (OSINT)
- 16.3.2. 搜索数据泄露和漏洞
- 16.3.3. 使用被动工具

16.4. 网络扫描
- 16.4.1. 扫描工具
  - 16.4.1.1. Nmap
  - 16.4.1.2. Hping3
  - 16.4.1.3. 其他扫描工具
- 16.4.2. 扫描技术
- 16.4.3. 防火墙 和 IDS 规避技术
- 16.4.4. Banner Grabbing
- 16.4.5. 网络图

16.5. 枚举
- 16.5.1. SMTP 枚举
- 16.5.2. DNS 枚举
- 16.5.3. NetBIOS 和 Samba 枚举
- 16.5.4. LDAP 枚举
- 16.5.5. SNMP 枚举
- 16.5.6. 其他枚举技术

16.6. 漏洞扫描
- 16.6.1. 漏洞分析解决方案
  - 16.6.1.1. Qualys
  - 16.6.1.2. Nessus
  - 16.6.1.3. CFI LanGuard
- 16.6.2. 漏洞评分系统
  - 16.6.2.1. CVSS
  - 16.6.2.2. CVE
  - 16.6.2.3. NVD

16.7. 无线网络攻击
- 16.7.1. 无线网络中的黑客方法
  - 16.7.1.1. Wi-Fi发现服
  - 16.7.1.2. 流量分析
  - 16.7.1.3. aircrack攻击
    - 16.7.1.3.1. WEP攻击
    - 16.7.1.3.2. WPA/WPA2攻击
  - 16.7.1.4. 孪生恶魔攻击
  - 16.7.1.5. WPS攻击
  - 16.7.1.6. 干扰
- 16.7.2. 无线安全工具

16.8. 入侵网络服务器
- 16.8.1. Cross site Scripting
- 16.8.2. CSRF
- 16.8.3. 会话Hijacking
- 16.8.4. SQL注入攻击

16.9. 利用漏洞
- 16.9.1. 使用已知漏洞
- 16.9.2. 使用metasploit
- 16.9.3. 使用恶意软件
  - 16.9.3.1. 定义和范围
  - 16.9.3.2. 生成恶意软件
  - 16.9.3.3. 绕过防病毒解决方案

16.10. 持久性
- 16.10.1. Rootkit 的安装
- 16.10.2. ncat 的使用
- 16.10.3. 为后门使用计划任务
- 16.10.4. 用户创建
- 16.10.5. HIDS 检测

模块 17. 逆向工程

17.1. 编译器
- 17.1.1. 代码类型
- 17.1.2. 编译器的阶段
- 17.1.3. 符号表
- 17.1.4. 错误的处理程序
- 17.1.5. GCC 编译器

17.2. 编译器中的解析类型
- 17.2.1. 词法分析
  - 17.2.1.1. 术语
  - 17.2.1.2. 词汇成分
  - 17.2.1.3. LEX 词法分析器
- 17.2.2. 句法分析
  - 17.2.2.1. 文法无上下文
  - 17.2.2.2. 解析类型
    - 17.2.2.2.1. 自上向下分析
    - 17.2.2.2.2. 自下而上分析
  - 17.2.2.3. 语法树和派生
  - 17.2.2.4. 解析器的类型
    - 17.2.2.4.1. LR(从左到右)解析器
    - 17.2.2.4.2. LALR 解析器
- 17.2.3. 语义分析
  - 17.2.3.1. 文法的属性
  - 17.2.3.2. S-属性
  - 17.2.3.3. L-属性

17.3. 汇编器数据结构
- 17.3.1. 变数
- 17.3.2. 数组
- 17.3.3. 指引
- 17.3.4. 结构
- 17.3.5. 物品

17.4. 汇编代码结构
- 17.4.1. 选择结构
  - 17.4.1.1. 如果，否则 如果，否则
  - 17.4.1.2. 转变
- 17.4.2. 迭代结构
  - 17.4.2.1. For
  - 17.4.2.2. While
  - 17.4.2.3. 休息时间的使用
- 17.4.3. 功能

17.5. x86硬件架构
- 17.5.1. x86 处理器架构
- 17.5.2. x86 数据结构
- 17.5.3. x86 代码结构

17.6. ARM硬件架构
- 17.6.1. ARM 处理器架构
- 17.6.2. ARM 数据结构
- 17.6.3. ARM 代码结构

17.7. 静态代码分析
- 17.7.1. 反汇编程序
- 17.7.2. IDA
- 17.7.3. 代码重建器

17.8. 动态代码分析
- 17.8.1. 行为分析
  - 17.8.1.1. 工业电子通讯
  - 17.8.1.2. 监测
- 17.8.2. Linux 代码调试器
- 17.8.3. Windows 的代码调试器

17.9. 沙盒
- 17.9.1. 沙盒架构
- 17.9.2. 沙盒规避
- 17.9.3. 检测技术
- 17.9.4. 躲避技巧
- 17.9.5. 反措施
- 17.9.6. Linux 的Sandbox
- 17.9.7. Windows的Sandbox
- 17.9.8. MacOS的Sandbox
- 17.9.9. 安卓的Sandbox

17.10. 恶意软件分析
- 17.10.1. 恶意软件分析方法
- 17.10.2. 恶意软件混淆技术
  - 17.10.2.1. 可执行的混淆
  - 17.10.2.2. 执行环境的限制
- 17.10.3. malware分析工具

模块 18. 安全发展

18.1. 安全发展
- 18.1.1. 质量、功能和安全
- 18.1.2. 保密性、完整性和可用性
- 18.1.3. 软件开发生命周期

18.2. 需求阶段
- 18.2.1. 认证控制
- 18.2.2. 控制角色和权限
- 18.2.3. 风险导向的要求
- 18.2.4. 特权批准

18.3. 分析和设计阶段
- 18.3.1. 访问组件和系统管理
- 18.3.2. 审计追踪
- 18.3.3. 会话管理
- 18.3.4. 历史数据
- 18.3.5. 正确的错误处理
- 18.3.6. 职责分开

18.4. 实施和编码阶段
- 18.4.1. 保护开发环境
- 18.4.2. 准备技术文件
- 18.4.3. 安全加密
- 18.4.4. 通讯安全

18.5. 安全编码最佳实践
- 18.5.1. 输入数据验证
- 18.5.2. 输出数据编码
- 18.5.3. 编程风格
- 18.5.4. 变更日志管理
- 18.5.5. 密码实践
- 18.5.6. 错误和日志管理
- 18.5.7. 文件管理
- 18.5.8. 内存管理
- 18.5.9. 安全功能的标准化和重用

18.6. 服务器准备和加固
- 18.6.1. 管理服务器上的用户、组别和角色
- 18.6.2. 软件安装
- 18.6.3. 服务器加固
- 18.6.4. 应用环境的配置

18.7. 数据库准备和加固
- 18.7.1. 优化数据库引擎优化
- 18.7.2. 为应用程序创建自己的用户
- 18.7.3. 为用户分配精确的权限
- 18.7.4. 数据库加固加固

18.8. 测试阶段
- 18.8.1. 质安全控制的质量控制
- 18.8.2. 阶段性代码检查
- 18.8.3. 配置管理验证
- 18.8.4. 黑盒测试

18.9. 准备生产步骤
- 18.9.1. 执行变更控制
- 18.9.2. 执行分步生产程序
- 18.9.3. 执行回滚过程
- 18.9.4. 预生产阶段的测试

18.10. 维护阶段
- 18.10.1. 基于风险的保险
- 18.10.2. 白盒安全维护测试
- 18.10.3. 黑盒安全维护测试

模块 19. 取证分析

19.1. 数据采集和复制
- 19.1.1. 易失性数据采集
  - 19.1.1.1. 系统信息
  - 19.1.1.2. 网络信息
  - 19.1.1.3. 波动率定律
- 19.1.2. 静态数据采集
  - 19.1.2.1. 创建重复图像
  - 19.1.2.2. 为监管链准备文件
- 19.1.3. 获取数据的验证方法
  - 19.1.3.1. 适用于Linux 的方法
  - 19.1.3.2. 适用于 Windows 的方法

19.2. 反取证技术的评估和失败
- 19.2.1. 反取证技术的目标
- 19.2.2. 删除数据
  - 19.2.2.1. 删除数据和文件
  - 19.2.2.2. 恢复文件
  - 19.2.2.3. 恢复已删除的分区
- 19.2.3. 密码保护
- 19.2.4. 隐写术
- 19.2.5. 安全删除设备
- 19.2.6. 加密

19.3. 操作系统的取证分析
- 19.3.1. Windows 取证
- 19.3.2. Linux 取证
- 19.3.3. Mac 取证

19.4. 网络取证
- 19.4.1. 日志分析
- 19.4.2. 数据相关
- 19.4.3. 网络研究
- 19.4.4. 网络取证要遵循的步骤

19.5. 网络取证
- 19.5.1. 网络攻击调查
- 19.5.2. 攻击检测
- 19.5.3. IP 地址的位置

19.6. 数据库取证
- 19.6.1. MSSQL取证分析
- 19.6.2. MySQL取证分析
- 19.6.3. PostgreSQL取证分析
- 19.6.4. MongoDB取证分析

19.7. 云法医分析
- 19.7.1. 云的犯罪类型
  - 19.7.1.1. 以Cloud为主体
  - 19.7.1.2. Cloud作为对象
  - 19.7.1.3. Cloud作为工具
- 19.7.2. 云法医分析的挑战
- 19.7.3. 云存储服务研究
- 19.7.4. 云法医分析工具

19.8. 电子邮件犯罪调查
- 19.8.1. 邮件系统
  - 19.8.1.1. 邮件客户端
  - 19.8.1.2. 邮件服务器
  - 19.8.1.3. SMTP 服务器
  - 19.8.1.4. POP3 服务器
  - 19.8.1.5. IMAP4 服务器
- 19.8.2. 邮件犯罪
- 19.8.3. 邮件信息
  - 19.8.3.1. 标准标题
  - 19.8.3.2. 扩展标题
- 19.8.4. 调查这些罪行的步骤
- 19.8.5. 电子邮件法医工具

19.9. 移动法医分析
- 19.9.1. 手机网络
  - 19.9.1.1. 网络类型
  - 19.9.1.2. CDR内容
- 19.9.2. 用户识别模块 (SIM)
- 19.9.3. 逻辑获取
- 19.9.4. 物理获取
- 19.9.5. 文件系统获取

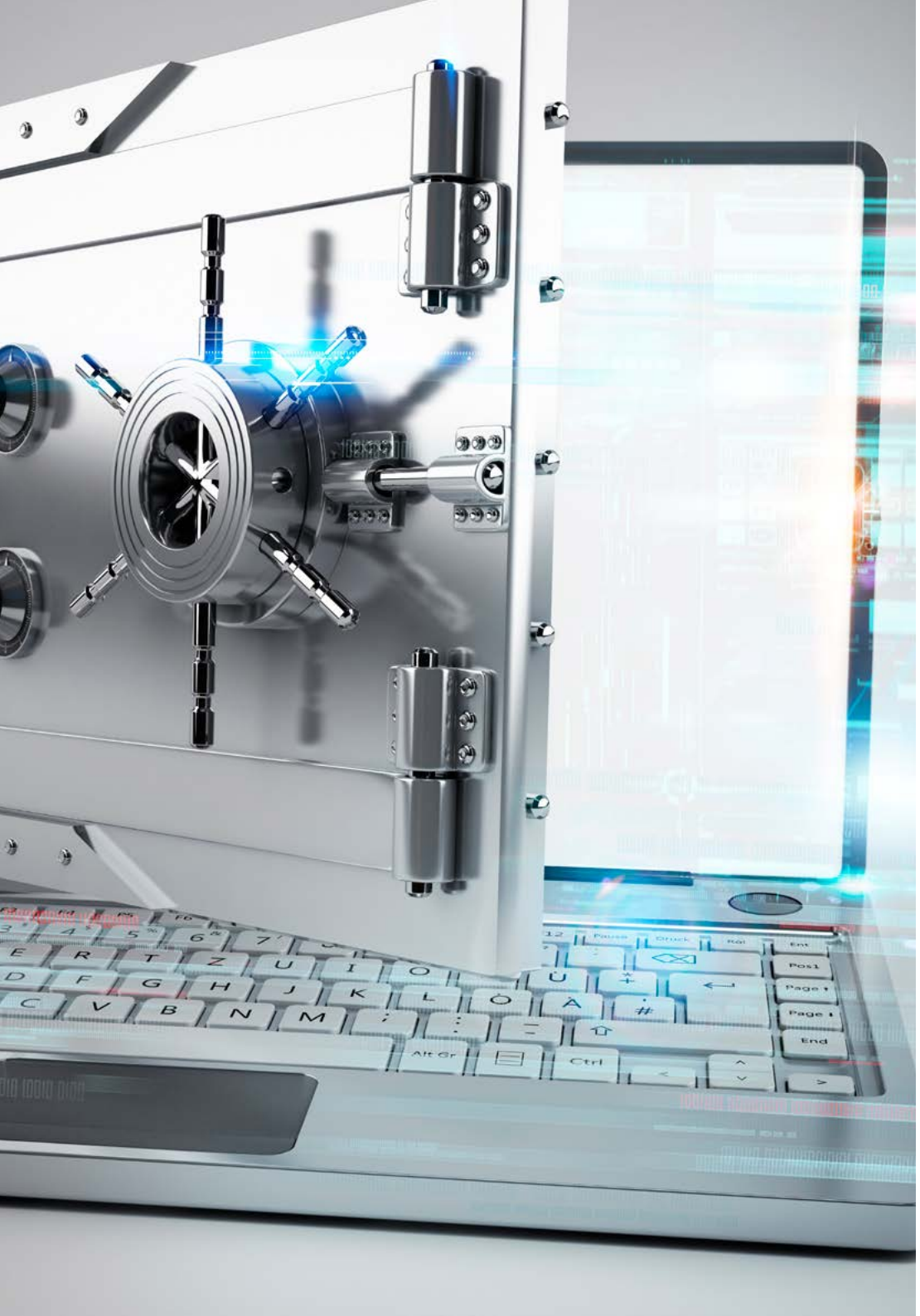
19.10. 起草和提交法证报告
- 19.10.1. 取证报告的重要方面
- 19.10.2. 报告的分类和类型
- 19.10.3. 撰写报告指南
- 19.10.4. 提交报告
  - 19.10.4.1. 作证前的准备
  - 19.10.4.2. 证人陈述
  - 19.10.4.3. 与媒体打交道

模块 20. 计算机安全现在和未来的挑战

20.1. 区块链技术
- 20.1.1. 应用的领域
- 20.1.2. 保密保证
- 20.1.3. 不可抵赖的保证

20.2. 数字货币
- 20.2.1. Bitcoins
- 20.2.2. 加密货币
- 20.2.3. 加密货币挖矿
- 20.2.4. 金字塔计划
- 20.2.5. 其他潜在的犯罪和问题

20.3. Deepfake
- 20.3.1. 媒体的影响
- 20.3.2. 对社会的危害
- 20.3.3. 检测机制



20.4. 人工智能的未来
- 20.4.1. 人工智能和认知计算
- 20.4.2. 用于简化客户服务

20.5. 数字隐私
- 20.5.1. 网络数据的价值
- 20.5.2. 网络数据的使用
- 20.5.3. 隐私和数字身份管理

20.6. 网络冲突、网络罪犯和网络攻击
- 20.6.1. 网络安全对国际冲突的影响
- 20.6.2. 网络攻击对普通人群的影响
- 20.6.3. 网络犯罪分子的类型保护措施

20.7. 远程办公
- 20.7.1. Covid19 期间和之后的远程办公革命
- 20.7.2. 访问瓶颈
- 20.7.3. 攻击面的变化
- 20.7.4. 工人的需要

20.8. 新兴无线 技术
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. 毫米波
- 20.8.4. Get Smart 而不是Get more

20.9. 网络的未来寻址
- 20.9.1. IP寻址的当前问题
- 20.9.2. IPv6
- 20.9.3. IPv4+
- 20.9.4. IPv4+ 相对于 IPv4 的优势
- 20.9.5. IPv6 相对于 IPv4 的优势

20.10. 提高民众早期和持续培训意识的挑战
- 20.10.1. 当前的政府策
- 20.10.2. 民众对学习的抵制
- 20.10.3. 公司将采用的培训计划

04

教学目标

Secure Information Management高级硕士课程的主要目标是为学生提供计算机科学和工程两个基本且互补的领域的优秀知识：数字环境中的数据管理和网络安全。该课程结合两个学科，培训专业人员实施先进的解决方案，使他们能够使用必要的工具来管理和保护组织中的敏感信息，以应对工作挑战。

通过这项创新的大师级课程改变您的职业生涯，旨在标记您在数据管理和网络安全专业化方面的前后情况”

总体目标

- 开发数据分析和网络安全方面的高级知识，以使用创新工具和技术优化业务流程
- 实施有效的安全策略，防止系统，网络和移动设备上的数字威胁
- 通过审计，逆向工程和基于证据的取证解决网络安全挑战
- 通过应用保护数字资产和先进系统的颠覆性解决方案来预测技术趋势

> 利用这一专业化课程引领数字环境中的数据管理和网络安全”

具体目标

模块 1. 商业组织的数据分析
- 培养使用数据分析技术的技能
- 生成有价值的信息，推动商业组织的战略决策，提高效率和竞争力

模块 2. 数据科学的数据和信息管理和操作
- 高效管理和处理大量数据的培训
- 应用方法和工具来构建、清理数据并将其转换为数据科学项目有用的信息

模块 3. 物联网设备和平台作为数据科学的基础
- 提供有关物联网平台和设备及其与数据科学集成的必要知识
- 深入研究实时数据的捕获、处理和分析

模块 4. 用于数据分析的图形
- 使用高级可视化工具和技术以图形方式表示数据
- 促进对大型数据集内的模式、趋势和关系的理解

模块 5. 数据科学工具
- 培训使用特定的数据科学工具和软件，例如 Python
- 深入研究各种专业背景下的数据收集、分析和呈现

模块 6. 数据挖掘。选择，预处理和转换
- 提供应用数据挖掘技术所需的知识和技能
- 分析数据选择、预处理和转换以提取有意义的模式和趋势

模块 7. 随机现象的可预测性和分析
- 培养随机现象建模和分析的技能
- 使用先进的统计方法预测不确定和动态环境中的行为和趋势

模块 8. 智能系统的设计与开发
- 培训智能系统的设计和开发，整合机器学习和人工智能技术
- 创建自动化解决方案以有效解决复杂问题

模块 9. 用于密集使用数据的架构和系统
- 提供关于创建能够有效处理大量数据的系统架构的知识
- 使用分布式数据库和并行处理等先进技术

模块 10. 数据科学在商业活动领域的实际应用
- 培养在各个业务领域应用数据科学实践的能力
- 整合获得的知识以改善公司的决策、流程优化和创新

模块 11. 网络情报与网络安全
- 提供应用网络情报和网络安全技术所需的知识和技能
- 保护业务系统和网络免受网络威胁并确保数据完整性

模块 12. 主机的安全
- 主机系统安全措施实施培训
- 通过使用 IT 安全工具和良好实践确保关键服务器和应用程序的保护

模块 13. 网络安全（周边）
- 提供有关外围网络和计算机系统保护的知识
- 管理防火墙、VPN 和其他工具，以确保公司网络基础设施的安全

模块 14. 智能手机的安全
- 培养确保移动设备安全的技能
- 了解常见漏洞并采取预防措施保护智能手机上的信息和应用程序

模块 15. IoT安全

- 提供在IoT设备上实施安全解决方案所需的知识
- 保护设备互连的网络和系统，并保证所生成数据的机密性和完整性

模块 16. 道德黑客

- 提供道德黑客实践培训，教授如何进行受控渗透测试
- 识别计算机系统中的漏洞，以提高安全性，防止其被攻击者利用

模块 17. 逆向工程

- 提供逆向工程技术知识，以便分析和理解软件和硬件的功能
- 检测安全漏洞或改进现有系统的功能

模块 18. 安全发展

- 提供安全软件开发方面的培训，在整个软件生命周期内教授良好的编码和安全实践
- 能够预防漏洞并保护计算机系统免受攻击

模块 19. 法医分析

- 掌握数字取证调查的必要技能
- 使用先进的工具和技术恢复、分析和保存计算机安全事件中的电子证据

模块 20. 计算机安全现在和未来的挑战

- 探索计算机安全领域的当前和未来挑战，分析新出现的威胁和新的保护技术
- 深入研究在不断变化的技术环境中降低风险的策略

05

职业前景

完成Secure Information Management高级硕士学位后，专业人士将对网络安全和数字数据管理方面最先进的策略有扎实的了解。毕业生将准备设计和实施解决方案，以确保敏感信息的保护并优化商业环境中的分析和决策过程。这样，他们将改善自己的就业前景，并担任网络安全分析师、情报顾问或关键数据经理等专业职位。

我们保证数字资产的安全，您将成为组织数字化转型的关键”

毕业生简介

Secure Information Management高级硕士毕业生将成为训练有素的专业人员，能够管理和保护数字环境中的信息。您将拥有网络安全、数字情报和数据分析等领域的高级知识，以及威胁防御策略设计和实施的实用技能。他的履历将深厚的技术理解与战略技能相结合，使他能够领导关键业务领域的项目。

> 您将成为数据保护和网络安全领域的领导者，与公司合作应对数字环境的挑战。

- **安全管理：** 培养识别风险，实施多层防御策略和确保数据机密性，完整性和可用性的能力
- **批判性分析和解决问题：**您将应用先进的技术来评估系统、检测漏洞并设计适合不同技术环境的解决方案
- **技术和数字能力：**您将掌握先进的数据分析工具、网络安全和情报系统，从而领导技术创新项目
- **战略思维：** 您将设计安全政策和业务战略，以响应数字环境的当前和未来需求
- **跨学科合作：**您将与多学科团队合作，应对复杂挑战并确保网络、物联网平台和移动设备的安全

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. **网络安全总监：**负责协调团队并设计策略以保护大型组织中的数字资产的领导者
2. **数据分析师：**预测分析和可视化系统设计师，以优化决策
3. **数字智能顾问：**专门提供基于情报和风险分析的先进解决方案的顾问
4. **IoT和安全专家：**连接设备和工业环境保护措施设计师
5. **道德黑客：**漏洞评估员，负责修复业务系统中的漏洞以防止网络攻击
6. **安全审计员：**执行审计和法医分析以确保遵守法规的检查员
7. **企业数据管理器：**管理员负责设计和管理存储和分析系统以提高运营效率

> 完成本课程，成为数字环境中最热门领域的专家”

05

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。

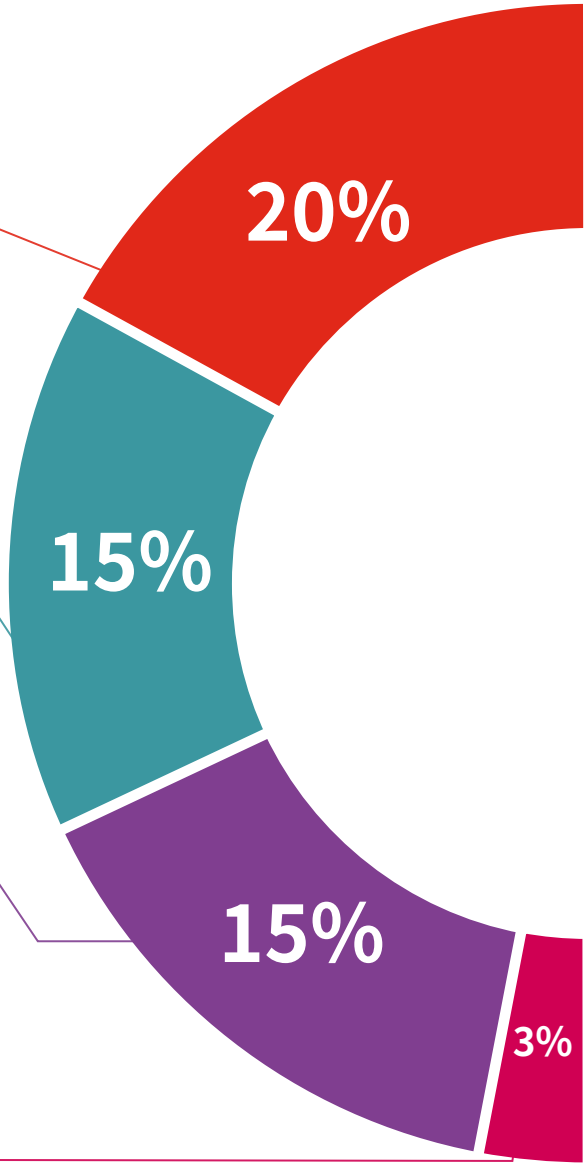
互动式总结

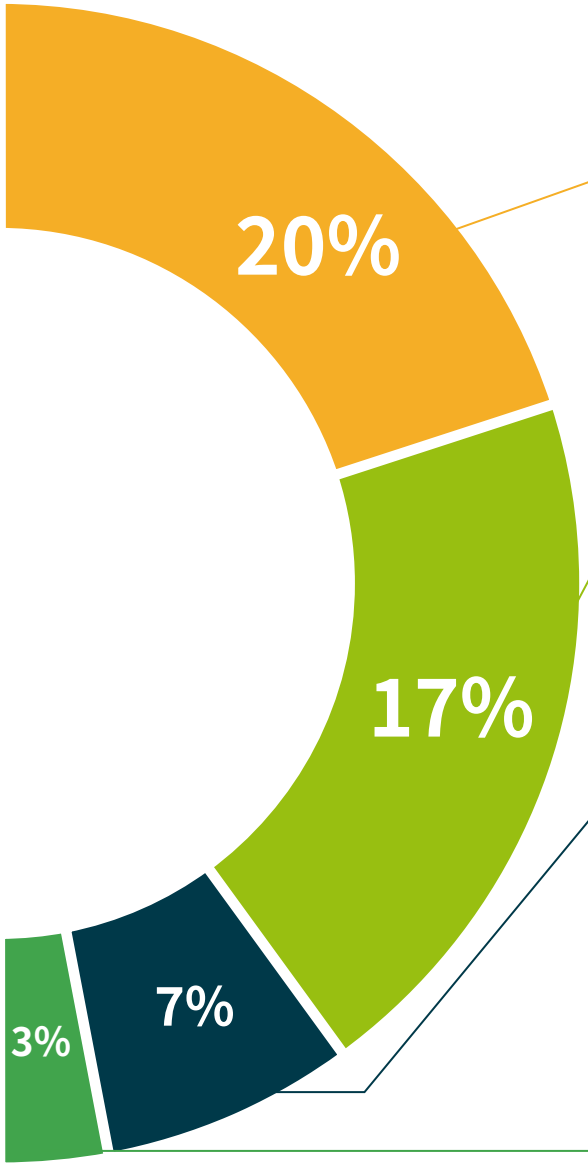
我们以有吸引力和动态的方式将内容呈现在多媒体中，包括音频，视频，图像，图表和概念图，以巩固知识。

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

该学位由网络安全和数字数据管理领域的顶尖专业人士授课他们的经验确保学生获得可直接应用于其职业生涯的全面、最新的内容。通过这种方式，Secure Information Management高级硕士的老师们分享他们的知识，培养出国际大公司所需的高素质专家。

与最优秀的人一起取得成功，并获得在数字环境中引领数据管理和网络安全的关键知识和技能”

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

Peralta Martín-Palomino, Arturo 博士

- Prometeus Global Solutions的首席执行官和首席技术官
- Korporate Technologies的首席技术官
- IA Shepherds GmbH 首席技术官
- 联盟医疗顾问兼业务策略顾问
- DocPath设计与开发总监
- -卡斯蒂利亚拉曼恰大学计算机工程博士
- 卡米洛-何塞-塞拉大学的经济学，商业和金融学博士
- -卡斯蒂利亚拉曼恰大学心理学博士
- 伊莎贝尔一世大学行政工商管理硕士
- 伊莎贝尔一世大学商业管理与营销硕士
- Hadoop培训大数据专家硕士
- -卡斯蒂利亚拉曼恰大学高级信息技术硕士
- SMILE研究组成员

Fernández Sapena, Sonia 女士

- 马德里赫塔菲国家计算机和电信参考中心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）、电信网络报警管理（IFCM0410）、语音和数据网络操作员（IFCM0110）以及互联网服务管理（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

教师

Montoro Montarroso, Andrés 先生

- Castilla-La Macha大学 SMILe小组研究员
- 格拉纳达大学研究员
- Prometeus Global Solutions的数据科学家
- CireBits 副总裁兼软件开发人员
- Haaga-Helia大学高级信息技术博士
- Haaga-Helia大学计算机工程学士
- 格拉纳达大学数据科学与计算机工程硕士
- 雷阿尔城计算机科学学院的知识系统主题客座教授，发表演讲：先进的人工智能技术：搜索和分析社交媒体中的潜在激进分子
- Escuela Superior de Informática de Ciudad Real 数据挖掘主题的客座教授在会议上发表演讲：自然语言处理的应用：社交网络中消息分析的模糊逻辑
- 在托莱多法律和社会科学学院举办的 公共管理部门预防腐败与人工智能研讨会上发表演讲：人工智能技术
- 第一届行政法与人工智能国际研讨会（DAIA）的演讲者。由路易斯-奥尔特加-阿尔瓦雷斯欧洲研究中心和TransJus研究所主办。题为通过情感分析防止社交媒体上的仇恨信息的会议

Peris Morillo, Luis Javier 先生

- HCL Technologies 高级技术主管和交付支持主管
- 贝尔东的技术编辑
- Mirai Advisory 的敏捷教练和运营总监
- DocPath 开发人员，团队领导，Scrum Master敏捷教练和产品经理
- ARCO 的技术专家
- Castilla-La Mancha大学计算机工程专业毕业
- CEOE 项目管理研究生课程（CEOE）

Fernández Meléndez, Galina 女士

- 大数据专家
- Aresi 数据分析师农场管理
- ADN 移动解决方案的数据分析师
- 毕业于阿拉瓜比森特纳利亚大学获得工商管理学位委内瑞拉加拉加斯
- 委内瑞拉规划学院规划和公共财政文凭
- 奥维耶多大学数据分析和商业智能硕士
- 巴塞罗那欧洲商学院工商管理 MBA
- 巴塞罗那欧洲商学院大数据和商业智能硕士

Pedrajas Perabá, María Elena 女士

- 管理解决方案公司新技术和数字化转型顾问
- 科尔多瓦大学计算机科学与数值分析系研究员
- 圣地亚哥德孔波斯特拉智能技术研究中心研究员
- 科尔多瓦大学计算机工程学位
- 格拉纳达大学数据科学与计算机工程硕士
- 科米亚斯主教大学商业咨询硕士学位

Martínez Cerrato, Yésica 女士

- 塞科利塔斯西班牙保安公司技术培训经理
- 教育，商业和营销专家
- 塞科利塔斯西班牙安保公司电子安保产品经理
- Ricopia Technologies的商业智能分析师
- 阿尔卡拉德埃纳雷斯大学IT技术员兼OTEC计算机教室主任
- ASALUMA 协会合作者
- 阿尔卡拉德埃纳雷斯大学高级政治学院电子通信工程学位

Fondón Alcalde, Rubén 先生

- 亚马逊网络服务（AWS）EMEA分析师
- 沃达丰西班牙客户价值管理业务分析师
- Entelgy 服务集成负责人，负责 Telefónica Global Solutions
- EDM Electronics 的克隆服务器在线客户经理
- 国际服务实施经理，沃达丰全球企业
- 西班牙和葡萄牙解决方案顾问，Telvent Global Services
- Vodafone Global Enterprise 南欧业务分析师
- 来自马德里欧洲大学的电信工程师
- 瓦伦西亚国际大学大数据与分析硕士

Díaz Díaz-Chirón, Tobias 先生

- 卡斯蒂利亚-拉曼查大学ArCO实验室研究员
- Blue Telecom的顾问
- 主要是电信部门的自由职业者，专门从事4G/5G
- OpenStack：部署和管理
- 卡斯蒂利亚-拉曼恰大学计算机科学工程师
- 专攻计算机架构和网络
- 卡斯蒂利亚-拉曼查大学兼职教授
- 在Sepecam的网络管理课程上发言

Tato Sánchez, Rafael 先生

- Indra Sistemas SA 技术总监
- ENA TRÁFICO SAU 系统工程师
- 在线大学授予工业 4.0 硕士学位
- 欧洲大学工业工程硕士学位
- 欧洲大学工业电子与自动化工程学位
- 马德里理工大学工业技术工程师

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

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

Armero Fernández, Rafael 先生

- SDG Group 商业智能顾问
- MI-GSO 数字工程师
- Torrecid SA 的物流工程师
- INDRA质量实习生
- 毕业于瓦伦西亚理工大学航空航天工程专业
- 阿尔卡拉德埃纳雷斯大学专业发展 4.0 硕士

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

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

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

> 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

Secure Information Management高级硕士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**Secure Information Management 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：**Secure Information Management 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

Secure Information Management

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


Secure Information Management高级硕士

教学大纲概况

学期	学科	小时	性质	学期	学科	小时	性质
1°	商业组织的数据分析	150	必修	2°	网络情报与网络安全	150	必修
1°	数据科学的数据和信息管理和操作	150	必修	2°	主机的安全	150	必修
1°	物联网设备和平台作为数据科学的基础	150	必修	2°	网络安全（周边）	150	必修
1°	用于数据分析的图形	150	必修	2°	食品卫生和安全	150	必修
1°	数据科学工具	150	必修	2°	智能手机的安全	150	必修
1°	数据挖掘。选择，预处理和转换	150	必修	2°	IoT安全	150	必修
1°	随机现象的可预测性和分析	150	必修	2°	道德黑客	150	必修
1°	智能系统的设计与开发	150	必修	2°	逆向工程	150	必修
1°	用于密集使用数据的架构和系统	150	必修	2°	安全发展	150	必修
1°	数据科学在商业活动领域的实际应用	150	必修	2°	法医分析	150	必修

Tere Guevara Navarro女士
校长

tech 科学技术大学

*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 global university

高级硕士
Secure Information Management

- 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

Secure Information Management

tech global university