姓名: _____ 日期: _____ 得分: _____

暗网与深网: 安全性与区别

搜索引擎索引、深网数据库、Tor 洋葱路由、网络匿名性与风险

暗网与深网学习概览

受保护
数据加密
256 位 AES 标准

合规的
全球标准
GDPR 与 CCPA 框架

零信任
访问策略
多重身份验证

欢迎！ 本活动手册将带你了解深网与暗网的区别。你将探索未索引的数据库、Tor 浏览器洋葱路由、.onion 加密域名和匿名性安全风险。

练习单检查点

- [ ] **第 1-4 部分: 掌握网络安全和威胁防范。**
- [ ] **第 5-7 部分: 解答填字游戏和单词搜索谜题。**
- [ ] **第 8-9 部分: 解答案例研究和密码挑战。**
- [ ] **第 10 部分: 查看基础和进阶 FAQ 页面。**
- [ ] **第 11 部分: 探索 10 个有趣的现实事实。**
- [ ] **附加: 快速思考挑战。**

打开 VPN.com 网络安全指南

URL: https://www.vpn.com/cybersecurity/dark-web-vs-deep-web/

你的深网与暗网策略学习路线图

- 对比深网（未被索引的数据库）与暗网（洋葱服务）。
- 了解洋葱路由如何加密并中继网络流量。
- 评估访问未经验证的 Tor 网络站点的安全风险。
- 为威胁情报爬取部署安全网关和沙箱策略。
- 分析洋葱服务域名的加密地址格式。

深网与暗网指南说明

回答单项选择题和判断题，使用词库完成填空句，配对定义，并解答填字游戏和找词游戏。将所学知识应用于深网和暗网隐私。 最后完成附加活动: 快速思考。

深网数据库与暗网洋葱路由（简介）

深网由密码和登录保护、未被索引的页面组成，例如私人电子邮件或企业银行门户。暗网是深网中刻意隐藏的一部分，需要使用专用浏览器（如 Tor）和洋葱网络才能匿名访问。

仔细阅读每个检查点，选择或写出正确的答案。

检查点 1: 单项选择挑战

1. 深网与表层网络有何区别?
   - A. 深网页面不会被公共搜索引擎索引
   - B. 深网流量是非法的，并受到执法部门的监控
   - C. 深网网站需要 Tor 等专用浏览器才能访问
   - D. 深网页面的加载速度总是比表层网络页面快

2. 如何访问暗网?
   - A. 通过使用洋葱路由网络的专用浏览器
   - B. 在标准路由器上配置自定义 DNS 设置
   - C. 通过仅限受邀的私有表层网络搜索控制台
   - D. 通过安装标准的广告拦截浏览器扩展

3. 哪种结构构成深网的最大部分?
   - A. 受密码保护的用户数据库和私人账户
   - B. 交易非法商品的非法黑市论坛
   - C. 未加密的点对点文件共享协议
   - D. 公共搜索引擎缓存数据库

4. 洋葱路由对网络流量有什么作用?
   - A. 它加密数据包并通过多个中继节点路由
   - B. 它通过绕过 ISP 节点来提高下载速度
   - C. 它将设备硬件序列号映射到 IP 记录
   - D. 它在每次点击后删除网络浏览器 Cookie

5. 哪个域名后缀专用于 Tor 网络?
   - A. 加密的 .onion 顶级扩展名
   - B. 标准的传统 .com 商业后缀
   - C. Web3 去中心化 .eth 区块链扩展名
   - D. 国家代码 .ai 技术扩展名

检查点 2: 判断正误挑战

6 问题 (判断) 6

6. 深网和暗网指的是同一个网络区域。

○ 正确 ○ 错误

7 问题 (判断) 7

7. 企业内部网门户属于深网的一部分。

○ 正确 ○ 错误

8 问题 (判断) 8

8. 洋葱路由会在每个中转节点完全解密数据包。

○ 正确 ○ 错误

9 问题 (判断) 9

9. 访问暗网会使设备面临很高的恶意软件风险。

○ 正确 ○ 错误

10 问题 (判断) 10

10. 标准网络搜索引擎会抓取并索引洋葱网站。

○ 正确 ○ 错误

检查点 3: 关键术语填空

阅读下面的每个句子，并从词库中选出正确的术语填空。

1. 私人银行门户位于未被索引的 _____ 部分。
2. 专门的 Tor 节点托管隐藏的 _____ 服务。
3. Tor 网站使用加密的 _____ 顶级后缀。
4. 经过加密的多层流量路径称为 _____ 。
5. 表层搜索引擎会抓取公开 _____ 的页面。
6. 洋葱网络会加密客户端 IP，以保持用户 _____ 。

词汇词库

暗网 | 被索引 | 后端记录 | 匿名性 | 深网 | 私有数据库 | 洋葱 | 洋葱路由

在此写下你的答案:

1.
2.
3.
4.
5.
6.

检查点 4: 安全概念配对

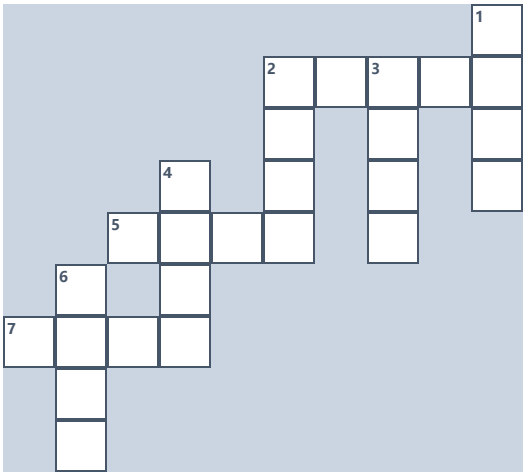
定义配对

将左侧的每个词汇与右侧正确的定义配对，在可填写的输入框中写出对应的字母（A-H）。

	1. 深网部分	**A**	只能通过特殊浏览器访问的加密网段。
	2. 暗网门户	**B**	分层加密数据并通过三个节点中继。
	3. Onion 扩展名	**C**	托管未索引系统记录的安全后端存储。
	4. Tor 路由	**D**	Tor 网络上使用的加密顶级域名后缀。
	5. 已索引页面	**E**	用于接入 Tor 网络的入口节点。
	6. 用户匿名性	**F**	已被 Google 收录并可搜索的表层网络内容。
	7. 私有数据库	**G**	对服务器隐藏客户端的公共 IP 地址。
	8. 入口网关	**H**	未被索引的网络内容，例如私人登录、电子邮件和数据库记录。

检查点 5: 填字游戏

在活动的白色方框中输入汉字，完成填字游戏。数字对应下面的提示。



横向

2. Tor 网络上使用的加密顶级域名后缀 (5)

5. 只能通过特殊浏览器访问的加密网络部分 (4)

7. 谷歌上编入索引并可搜索的表层网络内容 (4)

纵向

1. 向服务器隐藏客户端公网 IP 地址 (4)

2. 用于访问 Tor 网络的入口节点 (4)

3. 存放未索引系统记录的安全后端存储 (4)

4. 私人登录、电子邮件和数据库记录等未被索引的网络内容 (4)

6. 分层加密数据并经三个节点中继 (4)

检查点 5 替代活动: 无障碍填字线索

使用屏幕阅读器和键盘的用户可以直接在下面的文本框中输入填字游戏的答案。

横向

2 横向: Tor 网络上使用的加密顶级域名后缀 (5 字):

5 横向: 只能通过特殊浏览器访问的加密网络部分 (4 字):

7 横向: 谷歌上编入索引并可搜索的表层网络内容 (4 字):

纵向

1 纵向: 向服务器隐藏客户端公网 IP 地址 (4 字):

2 纵向: 用于访问 Tor 网络的入口节点 (4 字):

3 纵向: 存放未索引系统记录的安全后端存储 (4 字):

4 纵向: 私人登录、电子邮件和数据库记录等未被索引的网络内容 (4 字):

6 纵向: 分层加密数据并经三个节点中继 (4 字):

检查点 6: 隐藏单词搜索

在下方网格中找出隐藏的 8 个关键词汇。单词可以是水平、垂直或对角线方向。

全 协 洋 安 保 上 户 访 上 记 表 浏 用 份 备
件 墙 私 理 身 全 录 务 表 安 人 火 设 接 由
器 口 用 全 击 接 址 览 攻 层 息 统 息 理 防
器 入 据 隧 路 安 连 协 后 域 内 地 路 统 隧
口 网 安 输 议 洋 用 防 暗 风 层 容 管 内 护
管 暗 身 码 人 葱 址 后 隐 击 公 风 管 深 理
软 密 洋 道 览 后 户 认 端 协 据 网 数 密 设
内 认 防 容 墙 缀 深 录 火 记 器 输 风 议 器
容 址 击 攻 墙 名 传 备 连 险 录 险 传 共 道
内 录 记 私 加 道 理 软 问 隧 据 匿 务 浏 多
网 洋 葱 入 口 缀 密 路 匿 护 火 接 由 务 多
深 攻 器 输 匿 暗 备 加 葱 数 网 由 系 层 务
墙 络 器 软 名 器 息 接 址 务 共 传 路 风 户
址 人 路 浏 上 保 输 入 息 络 安 由 输 件 击
备 录 内 传 网 防 人 洋 隧 服 攻 表 数 护 隧

词汇列表

洋葱后缀名　洋葱入口　匿名上网　后端记录　暗网入口　深网内容　表层内容　多层路由

检查点 6 替代活动: 无障碍词汇配对

将词语搜索中的 8 个词汇与其正确的定义配对，在空白处写出字母（A-H）。

词汇术语
A. 洋葱后缀名
B. 洋葱入口
C. 匿名上网
D. 后端记录
E. 暗网入口
F. 深网内容
G. 表层内容
H. 多层路由

定义与配对字段
1. 私人登录、电子邮件和数据库记录等未被索引的网络内容。
2. 谷歌上编入索引并可搜索的表层网络内容。
3. 存放未索引系统记录的安全后端存储。
4. Tor 网络上使用的加密顶级域名后缀。
5. 用于访问 Tor 网络的入口节点。
6. 向服务器隐藏客户端公网 IP 地址。
7. 分层加密数据并经三个节点中继。
8. 只能通过特殊浏览器访问的加密网络部分。

检查点 7: 乱序单词挑战

把下面的汉字重新排列，找出关键的网络安全概念和术语。把答案写在提供的输入框中。

1. 缀后洋名葱 _____

2. 匿上网名 _____

3. 口暗入网 _____

4. 容内表层 _____

5. 口洋入葱 _____

6. 记录后端 _____

7. 内深容网 _____

8. 多由路层 _____

附加活动: 快速思考

每个类别写出 3 个答案。最先填完列表的人获胜。

1	远离暗网的原因			
2	搜索引擎找不到的内容			
3	可能被黑客入侵的设备			
4	使用 Tor 的合法原因			
5	更新软件的原因			
6	电子邮件中的警示信号			
7	在暗网上非法出售的东西			
8	可以向其寻求 IT 帮助的人			
9	你今天就可以开始的安全习惯			
10	数据泄露后要做的事			
11	属于深网的内容			
12	需要登录才能使用的网站			
13	与匿名相关的词语			
14	你绝不应分享的信息			
15	位于“水面之下”的事物			

检查点 8: 网络安全案例研究

运用你所学的概念来解决下面的真实情景。

案例研究 1: 数据泄漏识别



情景: 一次企业安全审计发现，敏感的客户数据库记录正在洋葱网站市场上交易。这些数据没有被 Google 索引。

讨论问题: 解释涉及哪些网络层面，以及这次泄露是如何发生的。

案例研究 2: 匿名性与恶意软件风险



情景: 一名分析师想在 Tor 网站上查看威胁情报信息源。他们下载了 Tor 浏览器并访问了该网站。

讨论问题: 评估匿名性带来的好处，并概述缓解恶意软件风险的步骤。

检查点 9: 破解密码

网络安全专业人员保护网络资产免受网络威胁行为者的攻击。使用下面的汉字与数字对照表，在空白处写出对应的汉字，解密这条信息。

汉字转数字加密密钥

匿=1 表=2 全=3 录=4 记=5 名=6 葱=7 端=8 入=9 口=10

由=11 层=12 多=13 络=14 洋=15 容=16 网=17 路=18 户=19 用=20

持=21 内=22 暗=23 数=24 深=25 保=26 缀=27 后=28 上=29 安=30

30	3	15	7	18	11		26	21		20	19	1	6

解码后的信息:

提示: 每个数字对应下方密钥中的一个汉字。

检查点 10: 基础网络安全常见问题 (A 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q1: 什么是深网?

深网包括搜索引擎无法索引的所有网页，例如网上银行、电子邮件数据库和付费期刊。

Q2: 什么是暗网?

暗网是深网中刻意隐藏的一小部分，只能通过使用洋葱网络的专用浏览器访问。

Q3: 搜索引擎如何为网页建立索引?

搜索引擎运行自动化程序（爬虫）来跟踪公开链接，为未通过 robots 指令禁止抓取的页面建立索引。

Q4: 为什么网上银行被视为深网的一部分?

银行门户网站设有登录墙和密码保护，因此公共搜索引擎无法索引账户对账单页面。

Q5: Tor 浏览器的洋葱路由是什么?

洋葱路由是一种传输方法，它将流量分层加密并经由多个中继传递，以隐藏用户的 IP 地址。

检查点 10: 基础网络安全常见问题 (B 部分)

回顾有关缓解网络威胁的常见问题和解答。

Q6: 访问暗网是违法的吗?

不会。在大多数国家，访问暗网是合法的，但参与非法市场或网络犯罪活动是被禁止的。

Q7: 暗网网站为什么加载缓慢?

流量至少经过三个全球中继（入口、中间、出口）进行路由和解密，这会增加传输延迟。

Q8: .onion 域名后缀是什么意思?

它是 Tor 网络上使用的一种专用顶级域名后缀，指向加密生成的地址，而不是标准 DNS 服务器。

Q9: 暗网链接有哪些风险?

这些网站没有安全筛查，使用户面临很高的恶意软件感染率、钓鱼脚本和交易诈骗风险。

Q10: 谁创建了 Tor 网络路由协议?

该技术最初由美国海军研究实验室于 1990 年代开发，用于保护政府通信。

检查点 10: 高级安全常见问题 (C 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q1: 中间节点如何保护 Tor 匿名性?

每个节点只解密一层路由数据，只知道上一跳和下一跳，而不会同时知道源和目的地。

Q2: 出口节点的作用是什么?

出口节点解密最后一层加密，并将流量发送到公共目标服务器或洋葱服务器。

Q3: 什么是 Tor 网桥网关?

网桥是未公开列出的 Tor 入口中继，用于在限制访问 Tor 浏览器的地区绕过 ISP 封锁和审查。

Q4: 暗网不法分子如何利用加密货币?

行为者使用匿名加密货币在暗网市场上进行金融交易，规避标准的银行交易检查。

Q5: 为什么标准搜索引擎无法抓取深层数据库?

爬虫无法输入登录凭据、解决安全验证码或运行访问深网数据库所需的后端 SQL 查询脚本。

检查点 10: 高级安全常见问题 (D 部分)

探索安全框架、恶意软件分析和数据合规的高级技术层面。

Q6: Tor 网络中的目录服务器是什么?

它是一台受信任的服务器，维护着客户端用来构建路由路径的活动入口、中继和出口中继列表。

Q7: 恶意行为者如何进行出口节点嗅探?

流氓出口节点运营者可以在未加密的 HTTP 流量离开 Tor 网络时将其拦截，窃取用户名和 Cookie。

Q8: Tor 与 I2P 有何区别?

Tor 使用集中式的中继目录和出口节点来访问公共网络，而 I2P 则使用去中心化的点对点结构来托管内部服务。

Q9: 执法机构如何追踪暗网市场?

执法机构使用区块链分析、定位物理服务器托管设施并开展诱捕行动来识别运营者。

Q10: DNS 泄露如何损害客户端匿名性?

DNS 泄漏是指浏览器的 DNS 查询直接通过本地 ISP 发送，而不是通过加密的 Tor 网络路由。

第 11 部分: 10 个现实中的网络安全事实与洞察

回顾有关安全漏洞、防御机制和合规标准的真实事实。

1. 安全洞察

深网远比可搜索的表层网络庞大，因为大部分内容位于登录和数据库之后。

2. 安全洞察

暗网是深网中刻意隐藏的一小部分，可借助 Tor 等工具访问。

3. 安全洞察

Tor 路由对数据包进行三次加密，在每个中继节点像剥洋葱一样剥去一层加密。

4. 安全洞察

Tor 源于美国海军研究实验室运行的洋葱路由项目，其代码已作为自由软件发布。 [1]

5. 安全洞察

洋葱地址是由公钥对通过密码学方式生成的 56 个字符的字母数字字符串。

6. 安全洞察

出口节点可以读取明文流量，这意味着在 Tor 上仍需要 TLS/HTTPS 来保护会话数据的安全。

7. 安全洞察

内网站点、云盘和私有数据库是深网中最大的数据存储部分。

8. 安全洞察

DuckDuckGo 等专业搜索引擎运营洋葱门户，以便在 Tor 网络上进行匿名搜索。

9. 安全洞察

每天有超过 2 百万用户连接 Tor 网络，以绕过审查并保护通信隐私。

10. 安全洞察

全球执法行动（如 Operation Bayonet）通过查封托管硬件，关闭了主要的暗网市场。

技术参考资料与来源

本学习指南和互动谜题根据全球 NIST、OWASP 以及数据隐私合规标准编写。

学术与行业参考资料

[1] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

答案: 检查点 1 – 单项选择

1 **搜索索引** 深网 正确答案: A

教学提示

深网页面位于登录墙和数据库之后，使搜索爬虫无法抓取。引用: IETF RFC 3986。

2 **Tor 访问** 暗网 正确答案: A

教学提示

暗网由只能通过 Tor 等浏览器访问的隐藏洋葱服务组成。引用: IETF RFC 3986。

3 **深层数据库** 数据库 正确答案: A

教学提示

受密码保护的账户和企业记录构成了深网中最大的部分。 引用: NIST Digital Identity。

4 **洋葱路由** TOR 网络 正确答案: A

教学提示

洋葱路由将数据包分层加密，并通过多个节点中继，以实现匿名。 引用: IETF RFC 3986。

5 **洋葱域名** 后缀 正确答案: A

教学提示

加密的.onion 域名后缀在 Tor 内部路由流量，无需公共 DNS。引用: IETF RFC 3986。

答案: 检查点 2 – 判断题（正确或错误）

6 **网络分段** 结构 正确答案: 错误

教学提示

深网涵盖所有未被索引的页面，而暗网只是其中规模很小的加密洋葱子集。引用: IETF RFC 3986。

7 **企业内部网** 深网 正确答案: 正确

教学提示

内网站点位于密码门户之后且未被索引，这意味着它们属于深网。引用来源: NIST Digital Identity。

8 **分层加密** 中继 正确答案: 错误

教学提示

洋葱中继只解密一层路由，以保护用户匿名性，绝不会解密整个数据包。 引用: IETF RFC 3986。

9 **恶意软件暴露风险** 威胁 正确答案: 正确

教学提示

暗网市场没有任何安全过滤，恶意软件感染风险极高。引用: Center for Internet Security (CIS)。

10 **问题 10** 正确答案: 错误

教学提示

普通搜索引擎爬虫不使用 Tor，因此无法访问或索引 .onion 网站。

词汇答案与评分标准

教师评分标准: 每个正确配对得 1 分（共 8 分），每个语境术语得 1 分（共 6 分）。

检查点 4: 答案 – 概念配对

H 1. 深网部分	A 2. 暗网门户	D 3. Onion 扩展名	B 4. Tor 路由
F 5. 已索引页面	G 6. 用户匿名性	C 7. 私有数据库	E 8. 入口网关

检查点 3: 答案 – 关键术语

1 深网	2 暗网	3 洋葱	4 洋葱路由
5 被索引	6 匿名性		

检查点 6 替代活动: 答案 – 词语配对

1 F – 深网内容	2 G – 表层内容	3 D – 后端记录	4 A – 洋葱后缀名
5 B – 洋葱入口	6 C – 匿名上网	7 H – 多层路由	8 E – 暗网入口

教师讨论提示

关键术语:
检查学生能否用自己的话解释深网部分、暗网门户和Onion 扩展名，并为每个术语举例。

案例研究:
请学生用练习单中的事实而不是个人观点来支持自己的建议。

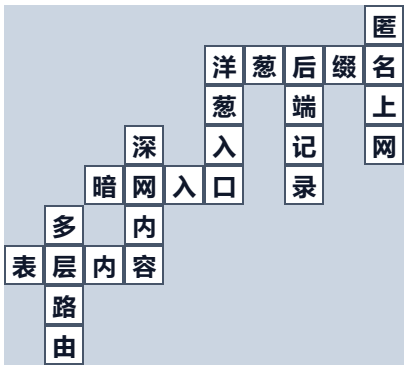
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全 协 洋 安 保 上 户 访 上 记 表 浏 用 份 备
件 墙 私 理 身 全 录 务 表 安 人 火 设 接 由
器 口 用 全 击 接 址 览 攻 层 息 统 息 理 防
器 入 据 隧 路 安 连 协 后 域 内 地 路 统 隧
口 网 安 输 议 洋 用 防 暗 风 层 容 管 内 护
管 暗 身 码 人 葱 址 后 隐 击 公 风 管 深 理
软 密 洋 道 览 后 户 认 端 协 据 网 数 密 设
内 认 防 容 墙 缀 深 录 火 记 器 输 风 议 器
容 址 击 攻 墙 名 传 备 连 险 录 险 传 共 道
内 录 记 私 加 道 理 软 问 隧 据 匿 务 浏 多
网 洋 葱 入 口 缀 密 路 匿 护 火 接 由 务 多
深 攻 器 输 匿 暗 备 加 葱 数 网 由 系 层 务
墙 络 器 软 名 器 息 接 址 务 共 传 路 风 户
址 人 路 浏 上 保 输 入 息 络 安 由 输 件 击
备 录 内 传 网 防 人 洋 隧 服 攻 表 数 护 隧

填字游戏答案



填字游戏答案教师指南

横向

2 横向: 洋葱后缀名 Tor 网络上使用的加密顶级域名后缀 (5 字)

5 横向: 暗网入口 只能通过特殊浏览器访问的加密网络部分 (4 字)

7 横向: 表层内容 谷歌上编入索引并可搜索的表层网络内容 (4 字)

纵向

1 纵向: 匿名上网 向服务器隐藏客户端公网 IP 地址 (4 字)

2 纵向: 洋葱入口 用于访问 Tor 网络的入口节点 (4 字)

3 纵向: 后端记录 存放未索引系统记录的安全后端存储 (4 字)

4 纵向: 深网内容 私人登录、电子邮件和数据库记录等未被索引的网络内容 (4 字)

6 纵向: 多层路由 分层加密数据并经三个节点中继 (4 字)

乱序单词与密码答案

词汇还原练习和秘密密码挑战的评分答案。

汉字重组答案

1. 缀后洋名葱 — **洋葱后缀名**
2. 匿上网名 — **匿名上网**
3. 口暗入网 — **暗网入口**
4. 容内表层 — **表层内容**
5. 口洋入葱 — **洋葱入口**
6. 记录后端 — **后端记录**
7. 内深容网 — **深网内容**
8. 多由路层 — **多层路由**

秘密密码挑战答案

“安全洋葱路由保持用户匿名”

案例研究答案

A 案例研究 1: 数据泄漏识别

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一次企业安全审计发现，敏感的客户数据库记录正在洋葱市场上交易。这些数据未被 Google 索引。
- 推荐策略与解决方案: 涉及的层面: 私有数据库属于深网（未被索引但安全）。交易被盗数据的市场位于暗网（洋葱网络）。事件经过: 黑客绕过服务器防御，从深网中窃取了数据库，并将其匿名挂到暗网上，以躲避执法部门的追踪。

B 案例研究 2: 匿名性与恶意软件风险

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一位分析师想在 Tor 网站上查看威胁情报源。他们下载了 Tor 浏览器并访问该网站。
- 建议策略与方案: 好处: Tor 通过三个节点路由流量，隐藏了分析师的企业 IP。风险与缓解: 暗网链接没有声誉筛查。分析师必须在隔离的虚拟机 (VM) 中运行 Tor，在 Tor 设置中禁用 JavaScript，并避免下载任何文件，以保护企业网络。