姓名: _____ 日期: _____ 得分: _____

防病毒软件与终端防护指南

特征检测、启发式分析、行为监控、沙盒、更新

杀毒软件学习概览

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杀毒软件和端点保护。你将探索特征库、启发式扫描器、行为监控、沙盒虚拟文件和误报缓解。

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/antivirus/

你的杀毒软件策略学习路线图

- 区分基于特征码的恶意软件检测与启发式恶意软件检测。
- 了解行为监控和沙盒隔离协议。
- 评估实时扫描对系统性能和终端的影响。
- 使用数字证书验证来减少误报分类。
- 管理企业终端上每日病毒库更新的分发。

杀毒软件指南说明

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。将所学知识应用于终端防病毒安全。 最后完成附加活动: 快速思考。

杀毒保护与特征码扫描（简介）

防病毒软件通过识别、隔离和清除恶意软件来保护终端。现代系统将特征库（匹配已知威胁哈希值）与启发式分析（分析文件结构）和行为监控相结合，以检测零日漏洞利用。

仔细阅读每个检查点，选择或写出正确的

检查点 1: 单项选择挑战

1. 基于特征码的检测有什么局限?
   - A. 它无法识别未知或被修改的恶意软件
   - B. 它会产生很高的误报率
   - C. 它需要很高的 CPU 处理能力
   - D. 它仅在连接互联网时有效

2. 启发式扫描器如何检测新的恶意软件变种?
   - A. 通过识别可疑模式和代码结构
   - B. 将文件哈希值与威胁数据库进行匹配
   - C. 通过自动删除所有未签名的可执行文件
   - D. 通过将每个文件上传到公共云文件夹

3. 杀毒软件沙盒执行的目的是什么?
   - A. 在安全的虚拟保险库中隔离并分析文件
   - B. 加快本地文件系统备份的传输
   - C. 更新本地操作系统的安全补丁
   - D. 压缩大型文档文件以节省存储空间

4. 哪种检测方法可实时标记威胁行为?
   - A. 监控软件行为的行为分析
   - B. 夜间进行的历史日志检查
   - C. 由用户手动报告运行缓慢的应用
   - D. 每周手动检查已安装的程序

5. 为什么定期更新病毒库对扫描程序至关重要?
   - A. 为特征码引擎提供威胁标识符数据库
   - B. 在运行期间提高 CPU 时钟频率
   - C. 修改全球 DNS 名称服务器的缓存时间
   - D. 授权网络浏览器 Cookie 设置

检查点 2: 判断正误挑战

6 **问题 (判断) 6**

6. 特征检测将文件的加密哈希值与数据库列表进行匹配。

○ 正确 ○ 错误

7 **问题 (判断) 7**

7. 启发式扫描器可能会对安全文件触发误报警报。

○ 正确 ○ 错误

8 **问题 (判断) 8**

8. 沙盒允许恶意软件不受限制地访问网络文件。

○ 正确 ○ 错误

9 **问题 (判断) 9**

9. 行为扫描会在文件表现出恶意行为时将其拦截。

○ 正确 ○ 错误

10 **问题 (判断) 10**

10. 标准杀毒软件能完全阻止所有零日攻击。

○ 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. 杀毒软件通过 _____ 来检查文件，识别已知恶意软件。
2. 在隔离空间中运行可疑文件并观察其表现的方法称为 _____ 。
3. 杀毒软件会把可疑文件隔离在 _____ 中。
4. 实时监控会观察程序的 _____ ，以发现可疑活动。
5. 扫描器每天下载 _____ ，以识别新的威胁。
6. 被误判为恶意软件的安全程序会触发 _____ 警报。

词汇词库

病毒库更新　病毒扫描　恶意软件　哈希签名　沙箱环境　沙箱扫描　误报　行为

在此写下你的答案:

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

检查点 4: 安全概念配对

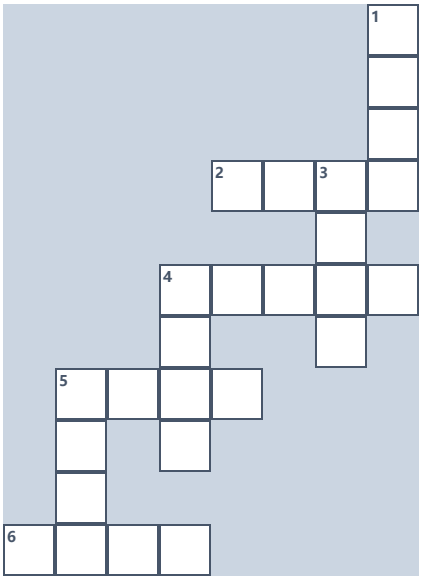
定义配对

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. 哈希签名	**A**	隔离可疑文件，以防止本地系统暴露。
	2. 代码启发式	**B**	扫描并保护终端免受漏洞利用的软件套件。
	3. 文件沙箱	**C**	监控正在运行的软件行为，以发现恶意操作模式。
	4. 行为扫描	**D**	用于识别已知威胁的唯一加密数据库特征。
	5. 每日更新	**E**	安全运行不受信任代码的虚拟测试环境。
	6. 误报	**F**	定期下载的病毒库定义，用于更新威胁数据库。
	7. 威胁隔离	**G**	基于规则的分析，标记代码布局可疑的文件。
	8. 杀毒工具	**H**	将安全软件错误归类为恶意软件的安全警报。

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. 旨在破坏或窃取信息的有害程序 (4)

4. 定期下载的特征定义，用于补充威胁数据库 (5)

5. 在隔离的虚拟空间中运行可疑文件并观察其表现 (4)

6. 把可疑文件限制在独立空间，防止其接触本地系统 (4)

纵向

1. 扫描并保护终端免受恶意代码侵害的软件套件 (4)

3. 为程序下载安装的新版本或补丁 (4)

4. 在文件中查找有害程序的检测过程 (4)

5. 可安全运行不受信任代码的受保护虚拟测试环境 (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。横向提示 纵向提示

横向

2 横向: 旨在破坏或窃取信息的有害程序 (4 字):

4 横向: 定期下载的特征定义，用于补充威胁数据库 (5 字):

5 横向: 在隔离的虚拟空间中运行可疑文件并观察其表现 (4 字):

6 横向: 把可疑文件限制在独立空间，防止其接触本地系统 (4 字):

纵向

1 纵向: 扫描并保护终端免受恶意代码侵害的软件套件 (4 字):

3 纵向: 为程序下载安装的新版本或补丁 (4 字):

4 纵向: 在文件中查找有害程序的检测过程 (4 字):

5 纵向: 可安全运行不受信任代码的受保护虚拟测试环境 (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 名 记 安 保 恶 户 接 意 览 箱 道 器 身 设
软 火 私 备 证 全 览 务 沙 安 共 防 件 接 离
务 描 用 全 攻 接 地 道 险 箱 息 系 信 管 议
器 扫 据 人 隔 安 私 名 病 址 环 地 隔 系 人
新 毒 安 传 议 病 用 议 扫 份 环 境 备 描 护
备 病 证 码 公 毒 地 杀 护 攻 输 份 备 扫 管
统 密 记 隧 道 库 户 墙 毒 名 据 网 数 加 件
描 墙 议 沙 火 更 扫 览 防 软 器 传 份 协 务
描 地 攻 险 火 新 理 设 私 风 件 风 理 公 人
扫 记 览 私 加 隧 管 系 问 共 据 新 务 道 境
箱 软 件 更 新 毒 密 隔 新 护 防 接 离 务 环
沙 险 器 传 恶 杀 设 加 录 数 网 离 击 境 务
火 络 器 统 意 器 息 连 址 务 公 理 隔 份 户
地 共 隔 隧 软 息 传 库 信 络 安 离 传 软 攻
设 记 描 管 件 议 公 记 人 服 险 箱 数 护 共

词汇列表

病毒库更新 **软件更新** **恶意软件** **杀毒软件** **病毒扫描** **沙箱扫描** **沙箱环境** **环境隔离**

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. 病毒库更新
B. 软件更新
C. 恶意软件
D. 杀毒软件
E. 病毒扫描
F. 沙箱扫描
G. 沙箱环境
H. 环境隔离

定义与配对字段
1. 扫描并保护终端免受恶意代码侵害的软件套件。
2. 把可疑文件限制在独立空间，防止其接触本地系统。
3. 在文件中查找有害程序的检测过程。
4. 为程序下载安装的新版本或补丁。
5. 可安全运行不受信任代码的受保护虚拟测试环境。
6. 定期下载的特征定义，用于补充威胁数据库。
7. 旨在破坏或窃取信息的有害程序。
8. 在隔离的虚拟空间中运行可疑文件并观察其表现。

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. 更 库 病 新 毒
2. 恶 软 件 意
3. 描 病 扫 毒
4. 境 环 沙 箱
5. 新 软 更 件
6. 软 件 杀 毒
7. 扫 沙 描 箱
8. 环 离 隔 境

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	更新软件的原因			
2	可以向其寻求 IT 帮助的人			
3	杀毒软件发现问题时要做的事			
4	计算机病毒的迹象			
5	被隔离的内容			
6	病毒藏身的地方			
7	你绝不应分享的信息			
8	恶意软件的类型			
9	你知道的安全工具			
10	杀毒软件扫描的内容			
11	你要备份的内容			
12	可能被黑客入侵的设备			
13	你知道的杀毒软件			
14	误报的原因			
15	你今天就可以开始的安全习惯			

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: 特征码扫描与启发式扫描



情景: 一名员工下载了另一个团队内部开发的自定义工具。特征码扫描器放行了它，但启发式扫描器将其标记为可疑。

讨论问题: 解释为什么会出现这种情况，以及如何核实该文件是否安全。

案例研究 2: 处理误报



情景: 一名软件开发人员编译了自己的应用程序。系统杀毒软件将新生成的可执行文件标记为恶意软件并将其隔离。

讨论问题: 概述加入白名单的风险，并说明正确的处理步骤。

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

发=1 新=2 环=3 恶=4 分=5 境=6 沙=7 杀=8 现=9 安=10

络=11 库=12 更=13 全=14 箱=15 据=16 数=17 扫=18 件=19 离=20

描=21 式=22 网=23 意=24 病=25 毒=26 隔=27 析=28 软=29 启=30

30	1	22	5	28		1	9		2	4	24	29	19

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: 杀毒软件如何识别恶意软件?

它通过数据库特征码匹配、启发式代码结构分析和实时行为监控来识别恶意软件。

Q2: 什么是基于特征码的检测?

这是一种扫描方法，将文件的加密哈希值与已知恶意软件威胁的数据库列表进行匹配。

Q3: 什么是启发式扫描器?

启发式检测会分析文件的结构和代码指令，标记恶意软件变种中常见的可疑模式。

Q4: 文件被隔离意味着什么?

杀毒软件会将文件移入安全的隔离文件夹，阻止其运行，以保护操作系统。

Q5: 什么是杀毒软件误报?

这是一种错误，即合法、安全的软件被扫描算法错误地标记为恶意软件。

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: 行为监控如何保护系统?

它会实时监控正在运行的软件，阻止试图进行可疑更改（如注入代码）的进程。

Q7: 沙箱测试为什么重要?

沙盒化在隔离的虚拟机中运行不受信任的文件，可安全地观察其行为而不会暴露系统。

Q8: 杀毒软件的病毒库应该多久更新一次?

扫描程序应每天或每小时更新病毒库，以识别新发现的恶意软件变种。

Q9: 杀毒软件与 EDR 有何区别?

防病毒软件侧重于文件扫描，而终端检测与响应（EDR）提供全网络范围的威胁跟踪和遏制。

Q10: 我可以同时运行两个杀毒程序吗?

不可以。同时运行两个活动的扫描程序会导致系统冲突、拖慢性能，并可能互相阻碍对方的操作。

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: 启发式规则如何最大限度减少威胁绕过?

启发式检测分析的是一般性威胁模式，而不是特定特征码，因此能捕获已知恶意软件家族的变种。

Q2: 什么是多态病毒?

这是一种每次执行时都会改变其文件结构和解密程序的恶意软件，使特征码扫描失效。

Q3: 沙箱如何检测虚拟机规避?

现代沙盒会模拟鼠标点击和系统运行时间，欺骗那些设计为在虚拟机中运行时隐藏自身的恶意软件。

Q4: 特征库更新的下载格式有哪些?

更新通常是轻量级的增量二进制差异文件，可最大限度减少客户端的网络带宽消耗。

Q5: 终端代理如何管理本地扫描?

代理执行轻量级后台检查，将深度加密哈希查找交给云端威胁数据库。

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: 什么是 Rootkit 检测扫描?

它扫描内核级内存表，绕过 rootkit 为隐藏其活动线程而挂钩的操作系统 API。

Q7: 行为扫描如何拦截勒索软件?

它能检测自动化的批量文件加密循环，在系统数据库被锁定之前终止宿主进程。

Q8: 什么是代码签名证书验证?

扫描程序会对照受信任的根证书颁发机构检查代码的数字签名，以验证软件开发者的身份。

Q9: 加壳程序如何影响扫描引擎?

加壳程序会压缩或加密恶意软件载荷。扫描器必须先在内存中解包文件，然后才能进行特征匹配。

Q10: EDR 工具如何自动隔离?

EDR 代理会在网络层面隔离受感染的终端，阻止横向移动，同时允许分析人员访问。

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

特征库存储已知恶意软件的哈希值，因此全新或被修改的文件在定义更新之前会被漏检。

2. 安全洞察

启发式引擎可以在特征码出现之前标记一些新的恶意软件变种，但代价是误报会增多。

3. 安全洞察

误报警报会让 IT 团队花费时间去核查和恢复被错误隔离的文件。

4. 安全洞察

多态恶意软件每个副本都会改变自身代码，因此防御者会将特征码与启发式和行为检查结合使用。

6. 安全洞察

恶意软件作者编写自定义代码来检测沙盒环境，并延迟执行以绕过计时器。

5. 安全洞察

基于云的杀毒引擎会近乎实时地将可疑文件的哈希值与大型在线威胁数据库进行比对。

7. 安全洞察

厂商会定期向终端推送病毒库更新，使扫描器能够识别新近确认的威胁。

8. 安全洞察

勒索软件行为监控器针对与文件加密和卷影副本删除相关的特定 Win32 API 调用。

9. 安全洞察

有效的代码签名可以降低误报风险，但已签名的文件仍会被扫描，因为恶意软件也可以被签名。

10. 安全洞察

Rootkit 会修改系统内核结构，需要专门的启动时扫描程序来检测和清除。

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

学术与行业参考资料

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.
https://csrc.nist.gov/pubs/sp/800/83/r1/final

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

[3] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[5] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

答案: 检查点 1 – 单项选择

1 **问题 1** 特征码 正确答案: A

教学提示

特征码扫描依赖已知的数据库哈希值，无法检测未知或经过修改的恶意软件。引用: OWASP 安全配置。

2 **问题 2** 启发式检测 正确答案: A

教学提示

启发式扫描会分析代码布局和命令，以识别新威胁变种的可疑特征。引用: 互联网安全中心（CIS）。

3 **问题 3** 沙盒化 正确答案: A

教学提示

沙盒会在隔离的虚拟机中运行可疑文件，以安全地观察其执行行为。引用: NIST 数字身份。

4 **问题 4** 行为的 正确答案: A

教学提示

行为扫描会实时监控正在运行的程序，以阻止未经授权的系统更改。引用: 互联网安全中心（CIS）。

5 **问题 5** 更新 正确答案: A

教学提示

扫描程序会下载每日增量病毒库更新，以与威胁形势保持同步。引用: OWASP 安全配置。

答案: 检查点 2 – 判断题（正确或错误）

6 **问题 6** 特征码 正确答案: 正确

教学提示

特征码工具会计算加密哈希值，并将其与已知威胁哈希值的数据库进行匹配。引用: OWASP 安全配置。

7 **问题 7** 启发式检测 正确答案: 正确

教学提示

启发式引擎运行基于规则的布局，可能会将合法、安全的文件标记为可疑。引用: 互联网安全中心（CIS）。

8 **问题 8** 沙盒化 正确答案: 错误

教学提示

沙盒在虚拟容器中运行代码，严格阻止对网络共享的访问。引用: NIST 数字身份。

9 **问题 9** 行为的 正确答案: 正确

教学提示

实时监控会标记试图进行非法写入或文件锁定的运行进程。引用: 互联网安全中心（CIS）。

10 **问题 10** 正确答案: 错误

教学提示

没有任何杀毒软件能阻止所有零日攻击；未知威胁可以躲过特征码和启发式检测。

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

D 1. 哈希签名	G 2. 代码启发式	E 3. 文件沙箱	C 4. 行为扫描
F 5. 每日更新	H 6. 误报	A 7. 威胁隔离	B 8. 杀毒工具

检查点 3: 答案 – 关键术语

1 病毒扫描	2 沙箱扫描	3 沙箱环境	4 行为
5 病毒库更新	6 误报		

检查点 6 替代活动: 答案 – 词语配对

1 D – 杀毒软件	2 H – 环境隔离	3 E – 病毒扫描	4 B – 软件更新
5 G – 沙箱环境	6 A – 病毒库更新	7 C – 恶意软件	8 F – 沙箱扫描

教师讨论提示

关键术语:
检查学生能否用自己的话解释哈希签名、代码启发式和文件沙箱，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。

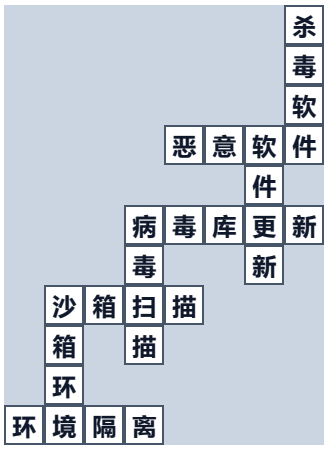
来源评估:
请学生根据练习单的参考资料至少核实一项说法，并讨论数字、价格和规则为什么可能随时间变化。

谜题答案与教师说明

找词答案

全	名	记	安	保	恶	户	接	意	览	箱	道	器	身	设
软	火	私	备	证	全	览	务	沙	安	共	防	件	接	离
务	描	用	全	攻	接	地	道	险	箱	息	系	信	管	议
器	扫	据	人	隔	安	私	名	病	址	环	地	隔	系	人
新	毒	安	传	议	病	用	议	扫	份	环	境	备	描	护
备	病	证	码	公	毒	地	杀	护	攻	输	份	备	扫	管
统	密	记	隧	道	库	户	墙	毒	名	据	网	数	加	件
描	墙	议	沙	火	更	扫	览	防	软	器	传	份	协	务
描	地	攻	险	火	新	理	设	私	风	件	风	理	公	人
扫	记	览	私	加	隧	管	系	问	共	据	新	务	道	境
箱	软	件	更	新	毒	密	隔	新	护	防	接	离	务	环
沙	险	器	传	恶	杀	设	加	录	数	网	离	击	境	务
火	络	器	统	意	器	息	连	址	务	公	理	隔	份	户
地	共	隔	隧	软	息	传	库	信	络	安	离	传	软	攻
设	记	描	管	件	议	公	记	人	服	险	箱	数	护	共

填字游戏答案



横向

2 横向: 恶意软件 旨在破坏或窃取信息的有害程序 (4 字)

4 横向: 病毒库更新 定期下载的特征定义，用于补充威胁数据库 (5 字)

5 横向: 沙箱扫描 在隔离的虚拟空间中运行可疑文件并观察其表现 (4 字)

6 横向: 环境隔离 把可疑文件限制在独立空间，防止其接触本地系统 (4 字)

纵向

1 纵向: 杀毒软件 扫描并保护终端免受恶意代码侵害的软件套件 (4 字)

3 纵向: 软件更新 为程序下载安装的新版本或补丁 (4 字)

4 纵向: 病毒扫描 在文件中查找有害程序的检测过程 (4 字)

5 纵向: 沙箱环境 可安全运行不受信任代码的受保护虚拟测试环境 (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. 更库病新毒 — **病毒库更新**
2. 恶软件意 — **恶意软件**
3. 描病扫毒 — **病毒扫描**
4. 境环沙箱 — **沙箱环境**
5. 新软更件 — **软件更新**
6. 软件杀毒 — **杀毒软件**
7. 扫沙描箱 — **沙箱扫描**
8. 环离隔境 — **环境隔离**

秘密密码挑战答案

“启发式分析发现新恶意软件”

案例研究答案

A 案例研究 1: 特征码扫描与启发式扫描

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一名员工下载了另一个团队内部开发的自定义工具。特征码扫描程序放行了它，但启发式扫描程序将其标记为可疑。
- 推荐策略与解决方案: 发生原因: 特征码扫描检查文件哈希；由于这是自定义文件，它不在威胁数据库中。启发式分析检查结构并标记了可疑行为（例如注册表写入）。验证方法: 在沙盒中运行该文件以观察其行为，检查数字签名，并将哈希提交到威胁情报门户。

B 案例研究 2: 处理误报

教师解答

评分指南

学生的回答应涵盖以下要点:

- 情景分析: 一位软件开发人员编译了自己的应用程序。系统杀毒软件将新的可执行文件标记为恶意软件并将其隔离。
- 推荐策略与解决方案: 加入白名单的风险: 绕过扫描程序可能会让真正被感染的代码运行。解决途径: 将文件提交给杀毒软件厂商分析，使用证书颁发机构对代码进行数字签名，并临时配置特定文件夹例外，而不是关闭杀毒软件。