SecurityScorecard

目录

SecurityScorecard Overview 产品概述

SecurityScorecard（以下统称为 SSC）产品是针对客户的网站进行网络安全评级，网络安全评估等工作的一个安全软件。

网络安全评级提供了一种客观监测组织网络安全架构健康状况、即时监测安全态势是否改善或恶化的手段。网络安全评级对于厂商风险管控、网络保险定价、信用担保和金融交易决策、并购尽职调查、管理层报告和组织自我监测具有重要的价值。网络安全评级和提供的丰富信息对于评估组织在遵守网络安全标准的合规性同样能起到重要作用。

其次，供应链攻击是目前网络安全防护中非常重要的一环，目前的网络黑客很容易通过产品相关的供应链处出现的漏洞问题进行攻击，从而进行对用户公司内部进行攻击窃取关键信息。在产品中同时也提供了关于供应链攻击的安全评级环节。这些都会在第二章结合相关的操作截图进行着重阐述。

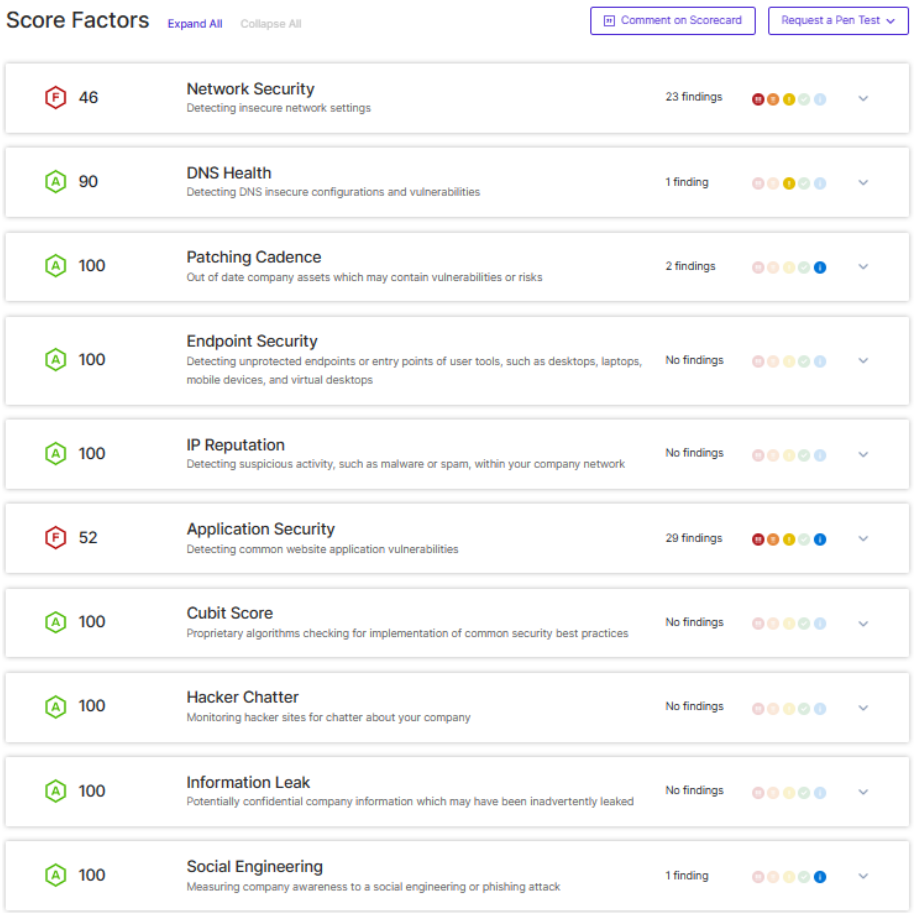
以上是产品的几个重要的工作内容，在第二章我将会更加仔细地为您阐述如何去使用我们的产品，以及在后面我们会针对您关心的一些问题进行答疑，所以这是我本篇文档所主要解决的一些问题。

请注意，第二章中我会针对您可能会非常关心的几个方面进行着重的阐述，篇幅可能会有点长，但请您认真阅读。

SecurityScorecard Functional Requirement 主要功能性需求

网络安全评级

针对网络安全评级环节，您所关心的就是如何去针对一个门户网站进行相关的网络安全评级操作。在这里我将用一个测试账号去为您演示如何进行网站的网络安全评级。在这里我会给您举一个网站评级的经典例子。



您可以看到，这是我在做完网络安全评级操作之后所看到的十个方面，在每一个方面都有从 A（绿色）到 F（红色）的不同分级，您可以理解为 A 是相比来讲很安全的，F 就是高危的，我们可以看到在一些方

面我们的网站表现得很好，但是有一些表现的并不好，总体来讲差强人意。接下来我会继续为您解读这十个方面都做了些什么。他们都在提示您站点的哪些安全问题。

Network Security 网络安全

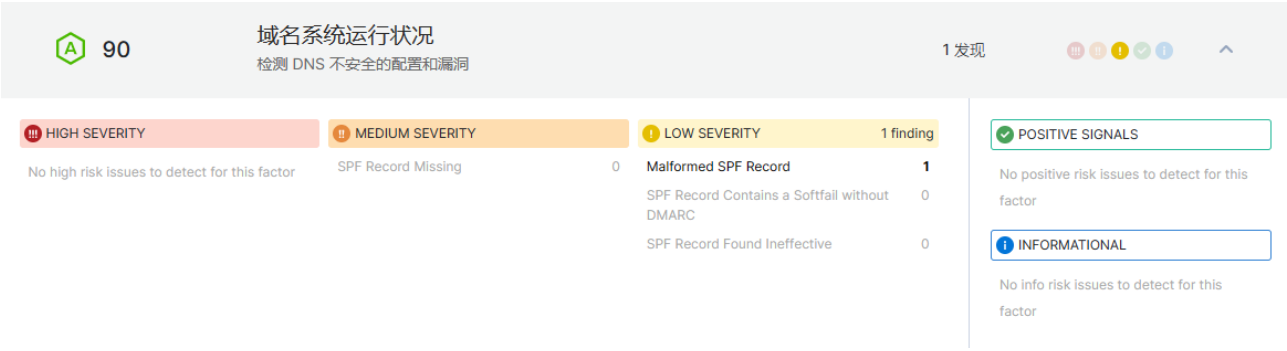
在这里我们可以看到关于网络安全的一些漏洞，在分级中主要分为五个等级，High Secerity 高危，Medium Secerity 中度威胁，Low Severity 低威胁，Positive Signals 潜在威胁，Informational 相关的一些安全信息。为了方便您的理解我会针对他爆出来的高位问题进行说明。

SSL/TLS Service Supports Weak Protocol

SSL/TLS 服务支持弱协议，其中这项主要说的就是没有禁用度量的证据列中列出的协议。因为目前的 HTTPS（Hypertext Transfer Protocol Secure）是在基础的 HTTP 中加入 SSL/TLS 协议进行加密传输，SSL/TLS 是用于保护网络通信的协议，它提供了加密和认证机制，确保数据在传输过程中的机密性和完整性。然而，早期版本的 SSL/TLS 协议存在一些安全漏洞和弱点，其中包括 SSL 2.0、SSL 3.0 和早期版本的 TLS（如 TLS 1.0 和 TLS 1.1），这些协议已经存在公开的漏洞，所以应当禁止使用。在网络上都有说明，例如 TLS1.0，TLS1.1 协议可能会受到 FREAK、POODLE、BEAST、CRIME 等漏洞的影响。其次，在传输的过程中，存在一个很有名的过程叫做**SSL 握手**，这个过程就是服务器端和客户端进行密钥交换，证书交换，确认日后使用的加密密钥，以及消息认证码算法等，这些在握手环节过程都会进行协商。这里说的就是过程中使用的密码算法过旧，或者已经过时了，这些密码算法应当被禁止使用。所以如果出现了以上的问题，我给您的修复建议就是去更新去取得一个最佳的 TLS/SSL 配置。

DNS（Domain Name System） Health 域名系统运行健康状况

在这里我们可以检测出针对 DNS 的不安全的配置以及关于 DNS 的漏洞。



在这里我们可以看到在 Low Severity 中爆出了一个问题。

SPF（Sender Policy Framework）发送方策略框架

SPF 是解决邮件防伪和垃圾邮件的一个新标准。只需要在域名的 DNS 中发布一条 SPF 记录，它就会标识经过了您授权的邮件发送服务器，而 ISP（Internet Service Provider）即互联网服务提供商的电子邮件接收系统会查询对应域名的 SPF 记录，检查邮件是否来自经过授权的邮件发送服务器。如果是垃圾邮件、钓鱼邮件伪造的“发件人”地址，则无法通过 SPF 校验。

但是您不用担心，这里不是说您的网站存在收到钓鱼邮件和垃圾邮件的风险，这一项说明的是您的 SPF 记录存在格式错误的问题。SPF 记录格式错误是指在域名的 DNS 记录中的 SPF 记录存在语法或格式上的问题，不符合 SPF 协议规定的要求。这可能导致 SPF 验证失败或无法正确解析 SPF 记录，从而影响电子邮件的认证和交付。

以下是一些可能导致 SPF 记录格式错误的常见问题：

1. **语法错误**：SPF 记录必须遵循特定的语法规则。如果在 SPF 记录中存在拼写错误、缺少或多余的空格、缺少必要的关键字或分隔符等语法错误，将导致 SPF 记录格式错误。

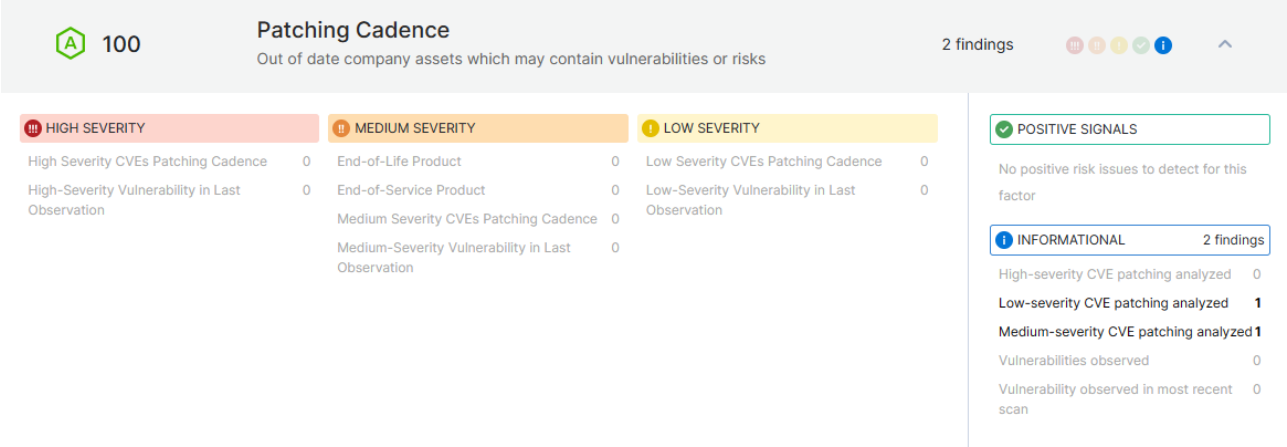
2. **限制长度超出**：SPF 记录的长度有限制，通常不能超过 255 个字符。如果 SPF 记录超过了这个限制，将被视为格式错误。

3. **缺少必要的关键字**：SPF 记录必须包含必要的关键字，如"v=spf1"作为 SPF 记录的起始，表示使用 SPF 版本 1。如果缺少这些必要的关键字，将导致 SPF 记录格式错误。

4. **无效的 IP 地址格式**：SPF 记录中涉及到的 IP 地址必须采用正确的格式，如 IPv4 地址（例如：192.0.2.1）或 IPv6 地址（例如：2001:0db8:85a3:0000:0000:8a2e:0370:7334）。如果 IP 地址格式不正确，将导致 SPF 记录格式错误。

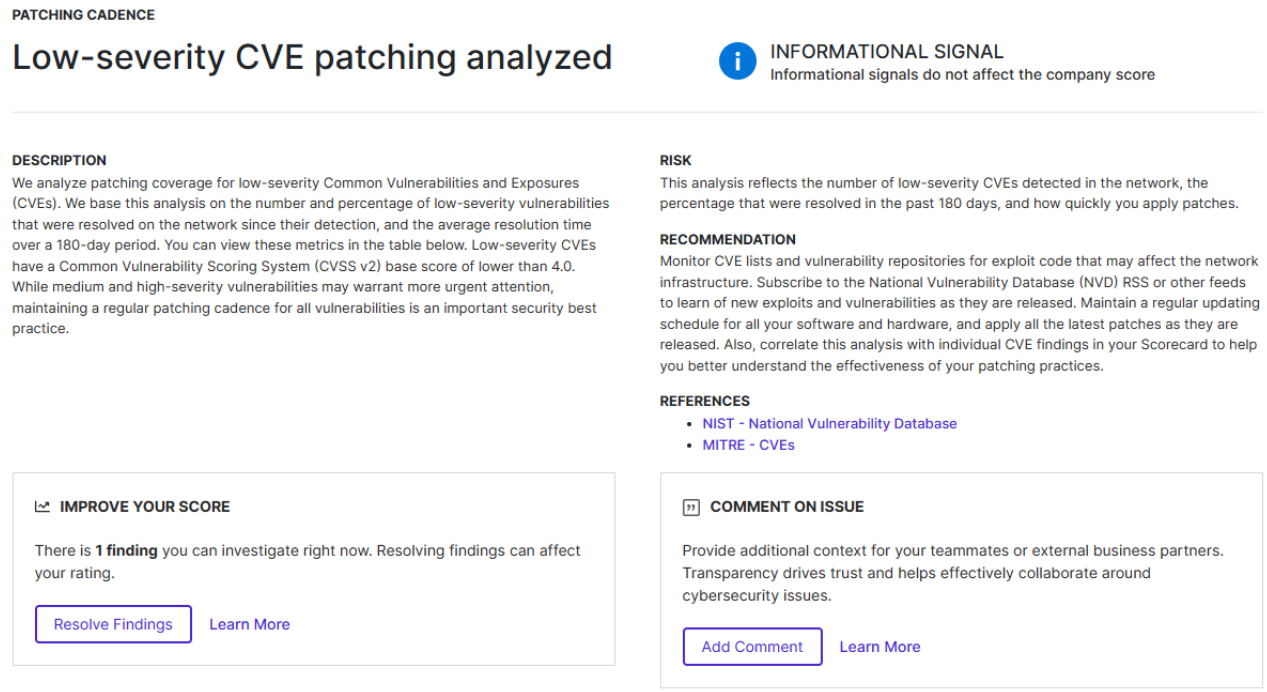
5. **重复的机制**：SPF 记录中不能包含重复的机制（如 include、ip4、ip6 等）。每个机制在 SPF 记录中只能出现一次。如果出现重复的机制，将导致 SPF 记录格式错误。

Patching Cadence 补丁节奏



我们都知道，在公司或者企业的日常维护中，“打补丁”是非常重要的，这一项就是检测可能包含的已知的 CVE（Common Vulnerabilities & Exposures）漏洞或者存在风险的过时的公司资产。在 Informational 这一项中我们可以看到：

Low-severity/Medium-severity CVE patching analyzed 即低/中威胁的 CVE 漏洞修复的分析，在这里如果您担心这项风险的成因或者描述的话，您可以点击进页面里，他会有更加详细的说明（上面的漏洞也都可以通过点击进行更加详细的说明分析）。需要注意的是，这只是 informational 的分级提示，所以这一项我们可以看到我们的评级是 A 级 100 分。



Endpoint Security 端点安全

Endpoint Security（端点安全）是指保护网络环境中终端设备的安全措施和技术。终端设备通常是指台式计算机、笔记本电脑、移动设备 (如智能手机和平板电脑)、服务器和其他连接到网络的设备。Endpoint Security 旨在确保这些设备的数据和系统免受威胁和攻击。

Endpoint Security 通常包括以下方面的功能和措施：

1. **防病毒和恶意软件保护**：使用防病毒和反恶意软件工具来检测、阻止和清除恶意软件、病毒、间谍软件等恶意代码。

2. **防火墙保护**：设置和管理终端设备上的防火墙，以监控和控制进出设备的网络流量，阻止未经授权的访问和攻击。

3. **设备控制和数据加密**：限制设备上的外部设备和可移动存储介质的使用，并使用数据加密技术来保护敏感数据的机密性。

4. **远程访问和 VPN 安全**：确保通过远程访问或虚拟专用网络（VPN）连接到企业网络的终端设备的

安全性，以防止未经授权的访问和数据泄露。

5. **弱点和漏洞管理**：识别和修复终端设备上存在的弱点和漏洞，包括操作系统、应用程序和组件的更新和补丁管理。

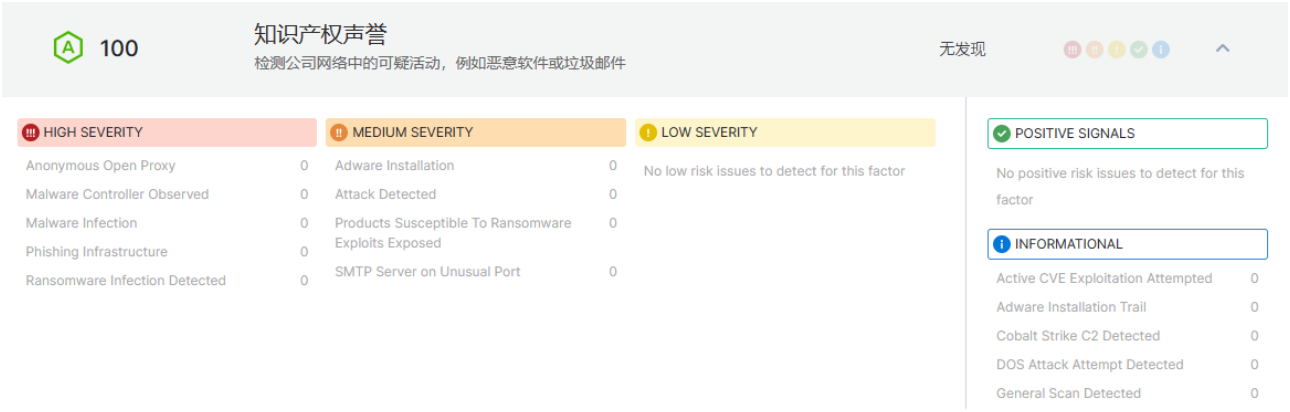
6. **行为分析和异常检测**：使用行为分析和异常检测技术来监测终端设备上的异常活动和威胁，并采取相应的响应措施。

7. **日志和审计**：记录终端设备上的活动日志，并进行审计和分析，以便检测和调查安全事件。

Endpoint Security 的目标是保护企业网络中的终端设备，防止数据泄露、恶意软件感染、未经授权的访问和其他安全威胁。它对于保护敏感信息、维护业务连续性和符合法规要求都至关重要。

IP Reputation 信誉评分技术

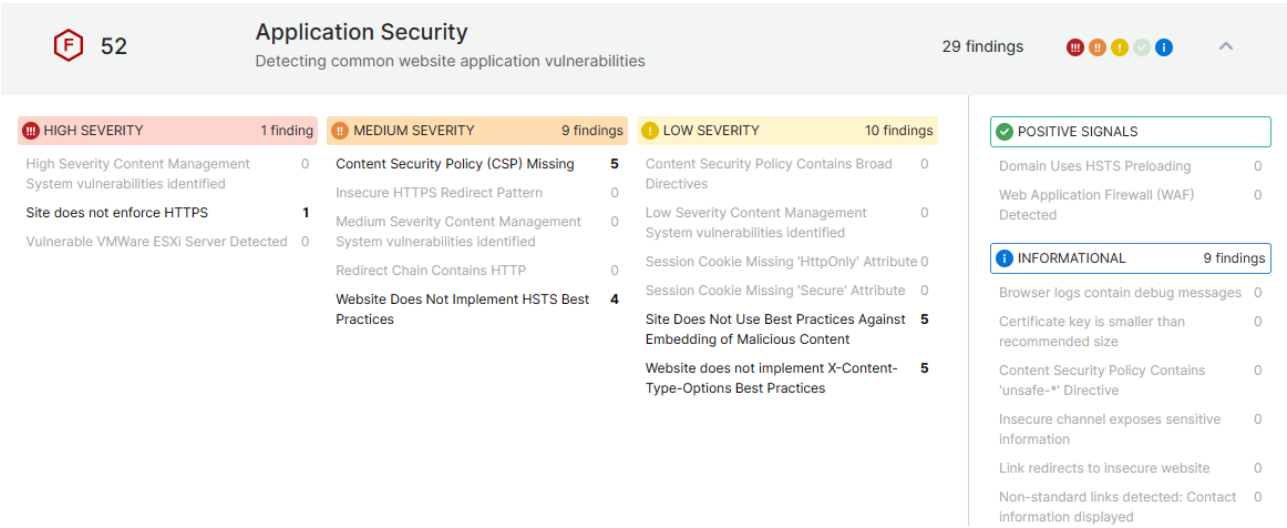
这一项会检查公司网络中的可以活动，例如恶意软件或者垃圾邮件。其中 IP Reputation 即 IP 信誉是信誉情报（Reputation Intelligence）也称为威胁情报的具体用例。它是识别发送非法请求 IP 地址的有用工具，使用 IP 信誉列表可以拒绝来自信誉不佳的 IP 的请求。例如，用户可以使用此功能去筛选出不想处理的请求来提升 WAF（Web Application Firewall）性能。其中 IP 信誉可能会包括以下几类信息：恶意的 IP 地址，匿名代理，TOR 网络，网络钓鱼网址，垃圾评论者，自动化僵尸网络等。



Application Security 应用安全

这一项是非常重要的一项，在这里我可能会花大篇幅来讲这一项的内容，这些内容结合了我自己和网络上已有的知识的理解，所以您不会觉得知识难以接受。

首先，针对 Application Security 即应用安全主要是针对 Web Application 即 Web 应用去进行的安全检测，他会检测网站是否存在应用安全漏洞以及风险。我们知道，每一年都会有当年的 OWASP（Open Web Application Security Project 开放式 Web 应用程序安全项目） TOP 10，在 2021 年的 TOP 10 中，它们分别是：**损坏的访问控制，加密错误，注入，不安全的设计，安全配置错误，易受攻击的和过时的组件，认证和授权错误或失败，软件和数据完整性受损，安全日志记录和监控失败，SSRF (Server-Side Request Forgery)。**在这里如果我要是和您具体的说他们的每一个漏洞的原理的话，可能会花费大量的时间和精力，所以如果您要是对这方面感兴趣的话，具体您可以上网进行查找。我想要告诉您的是，Application Security 这一项所使用的检测原理就是历年的 OWASP TOP 10 以及大部分应用服务。我们会针对这些漏洞从而对安全问题进行检测。



您可以看到，网站没有强制用户使用 HTTPS 进行信息传输。

CSP 即内容安全策略以及 X-Content-Type-Options 这些都是在请求头中可以看到的参数，这些可

以邮箱的防护 XSS 攻击，虽然近几年 XSS 的出现不再那么频繁了，但是 XSS 依旧是黑客们最喜欢用的钓鱼方式，这些我会在下文的社会工程学中继续阐述。可以看到，我们检测的网站主要针对于这些问题进行了检测，其次他还会检测网站的 Copyright，包括关于 Log4j，Spring4Shell 等这些有爆发过历史上非常惊人的漏洞的服务。其中 Log4j 离我们的时间非常近，在 2021 年的 12 月的晚上，Apache Log4j 爆出了一个非常严重的漏洞，即 Log4j 远程代码执行漏洞，黑客可以利用这一漏洞进行远程的恶意代码攻击，所有类型的在线应用程序，开源程序，云平台和电子邮件服务都可能面临网络安全风险。

Cubit Score Cubit 评分

专有算法检查常见安全最佳实践的实施情况。例如，我们检查公共威胁情报数据库的 IP 地址，这些地址已被标记。

Hacker Chatter 黑客通讯

"Hacker chatter"（黑客讨论）是指在网络上进行的黑客之间的交流、讨论和信息交换。这种讨论通常发生在黑客论坛、地下黑市、社交媒体、即时通讯平台和其他在线社区中。

黑客讨论的内容可以涉及多个方面，包括攻击技术、漏洞利用、网络安全工具、最新的安全威胁、目标系统或组织的弱点、新发现的漏洞等。黑客们可以分享攻击技术、开发新的恶意软件、交易或分享盗取的数据，或者互相提供技术支持和合作等。

黑客讨论的目的可以是多样化的，包括提升黑客技能、攻击目标系统、获取非法利益、参与集体行动（如分布式拒绝服务攻击）等。这种讨论可能涉及非法活动，例如计划或组织网络攻击、进行网络钓鱼、破解密码、非法获取机密信息等。

对于网络安全专业人员和执法机构来说，监测和分析黑客讨论是一种重要的情报收集手段，可以帮助了解黑客活动、安全威胁和攻击趋势，以便采取相应的安全措施和打击行动。

Information Leak 信息泄露

信息泄露模块会利用聊天记录监测和深层的网络监测功能来识别黑客传播的受损凭证。在这个模块中，我们会针对 IP 地址的暴露、用户名的暴露、密码的暴露、个人隐私信息（包括个人密码，物理地址，电话号码等）的暴露、凭证暴露等方面进行检测，最后得出我们对于这一模块的评分。

Social Engineering 社会工程学

社会工程学是黑客们在对网站进行攻击的过程中最喜欢用的一个手段，这里我举一个社会工程学攻击的例子，钓鱼攻击是一种通过欺骗和诱骗目标用户来获取敏感信息或进行恶意活动的攻击方式。以下是一个钓鱼攻击的示例过程：

攻击者伪装身份：攻击者伪装成可信任的实体，例如银行、电子邮件提供商、社交媒体平台或其他组织，以引起目标用户的信任。

发送欺骗性信息：攻击者通过电子邮件、短信、社交媒体消息或其他通信方式发送一条欺骗性信息给目标用户。该信息通常会声称存在紧急情况、账户安全问题或其他诱人的主题，以引起目标用户的关注和行动。

诱导用户点击恶意链接或下载文件：欺骗性信息中通常包含一个链接或附件，目的是引导目标用户点击该链接或下载附件。链接可能会指向一个恶意网站，而附件可能会包含恶意软件。

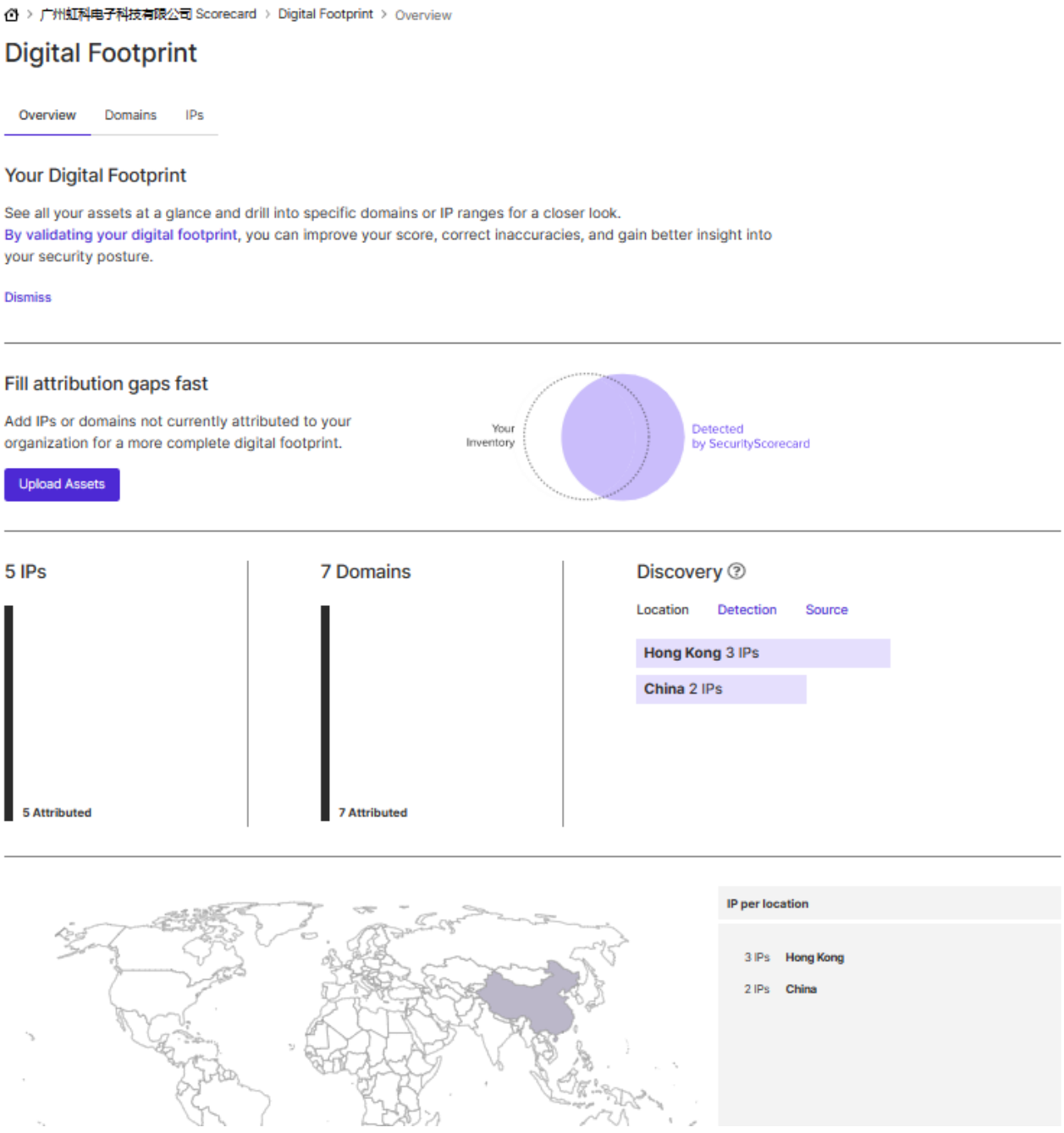
欺骗用户输入敏感信息：当目标用户点击链接或打开恶意附件时，可能会被引导到一个伪装的登录页面或信息收集表单，要求输入敏感信息，如用户名、密码、银行账户号码等。用户在被误导的情况下可能会提供这些敏感信息。

盗取或滥用敏感信息：一旦目标用户提供了敏感信息，攻击者就可以利用这些信息进行恶意活动，如盗取账户、身份盗窃、财务欺诈等。

钓鱼攻击利用了人们的信任和好奇心，通过欺骗性手段引导他们采取不安全的行动。为了防止钓鱼攻击，用户应保持警惕，验证接收到的信息的真实性，不轻易点击可疑链接或下载附件，并注意保护个人敏感信息的安全。组织应提供员工培训，加强安全意识，实施多层次的安全措施，如电子邮件过滤、网站黑名单等，以减少钓鱼攻击的风险。

Digital Footprint 数字足迹

在这一环节中我们可以看到公司所有的资产，并且针对特别的域或 IP 范围进行更仔细的检查。通过这种方式，我们可以查看子域名以及同级的域名，所有相关的域名产权我们都可以对其进行查看。



下图我们可以看到所有的子域名以及父域名，其中 Impact 项目中是该网站是否存在危险的漏洞问题。

非法子域名和父域名在网络安全中可能涉及以下问题：

1. **DNS 劫持**：攻击者可以通过劫持 DNS 解析的过程，将合法的子域名解析到恶意 IP 地址上。这可能导致用户被重定向到恶意网站或受到其他形式的攻击。

2. **子域名扫描和枚举**：攻击者可以使用自动化工具对目标域名进行子域名扫描和枚举，以发现存在的子域名。这可以提供攻击者有关目标组织的信息，包括子域名的架构、托管服务和相关系统的脆弱性。

3. **域名劫持**：攻击者可以通过入侵域名注册商账户或 DNS 管理界面，窃取域名的控制权，并修改子域名的解析记录。这可能导致用户被重定向到恶意网站、电子邮件被劫持，或者服务被中断。

4. **跨站点脚本（XSS）**：如果子域名存在 XSS 漏洞，攻击者可以注入恶意脚本，并通过子域名传递给用户。这可能导致用户在浏览器中执行恶意脚本，泄露敏感信息或进行其他恶意活动。

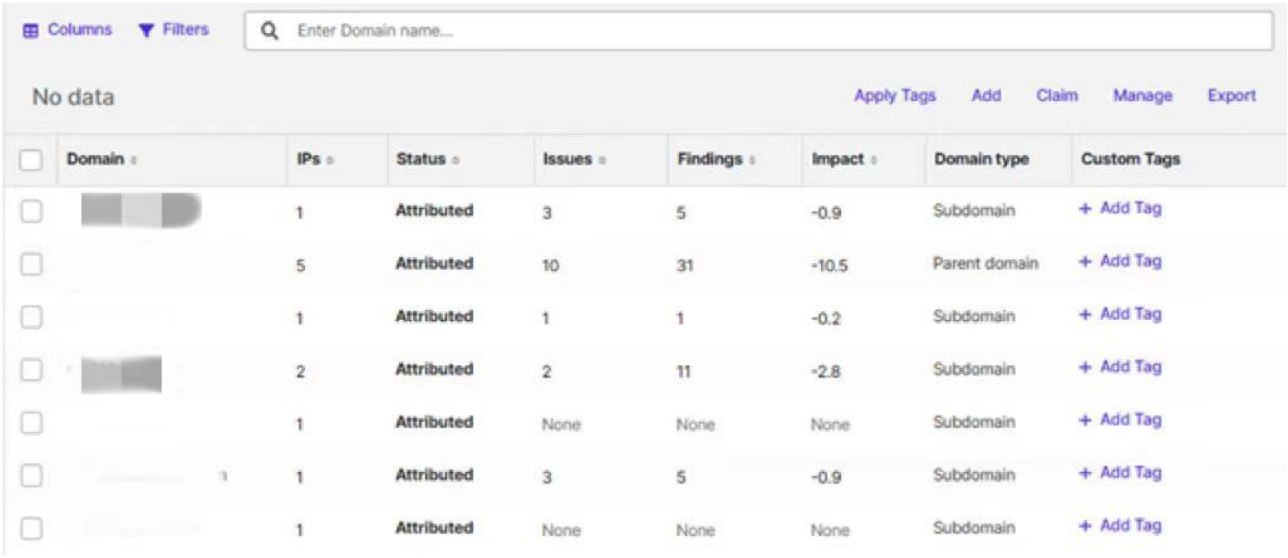
5. **跨站点请求伪造（CSRF）**：如果父域名允许跨域请求，并且子域名存在 CSRF 漏洞，攻击者可以伪造请求并利用用户的身份执行未经授权的操作。这可能导致用户执行恶意操作，例如更改账户设置或进行不当的操作。

6. **域名暴露和隐私泄露**：子域名的存在和结构可能泄露有关组织的敏感信息，例如内部系统、部门名称和架构。攻击者可以利用这些信息来进行有针对性的攻击、社会工程和其他网络攻击。

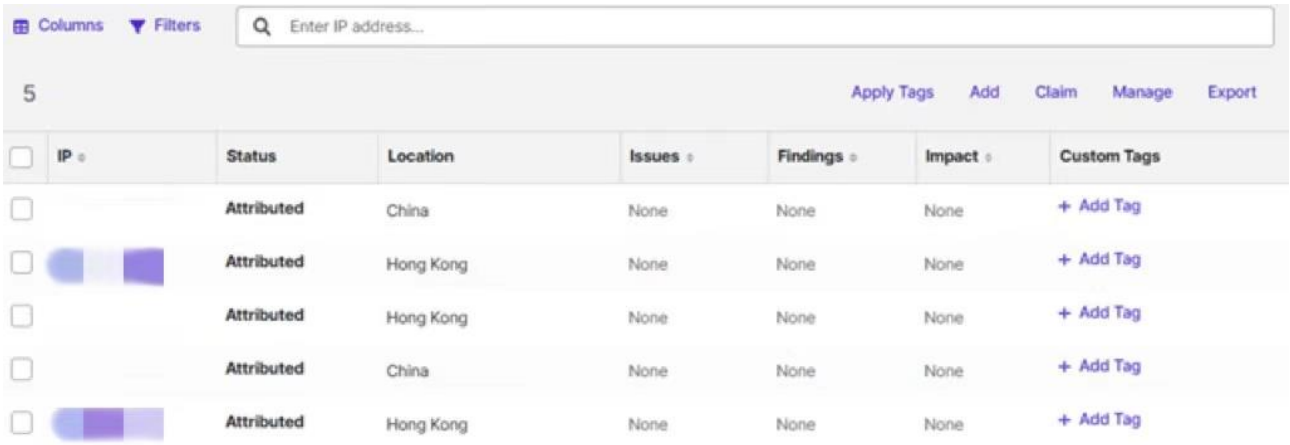
为了减轻这些风险，组织可以采取以下安全措施：

- 定期进行子域名枚举和扫描，识别存在的子域名并监控其安全状况。
- 实施强密码策略，特别是对于域名注册商和 DNS 管理界面的账户。
- 监控 DNS 解析记录的变化，并确保只有授权的人员可以对其进行修改。
- 实施安全开发和代码审查，以减少子域名上的漏洞，如 XSS 和 CSRF。
- 对域名注册商和 DNS 提供商进行安全评估，选择可信赖和安全的服务提供商。
- 定期更新和维护域名注册商、DNS 解析器和子域名相关的系统和软件，以减少已知的漏洞风险。

通过这些措施，可以增强子域名和父域名的安全性，并降低网络攻击的风险。所以您使用我们产品的此功能可以很好的对子域名和父域名进行定期维护，并且对其进行安全评估。



以下是相关的 IP 以及他们所在的国家。

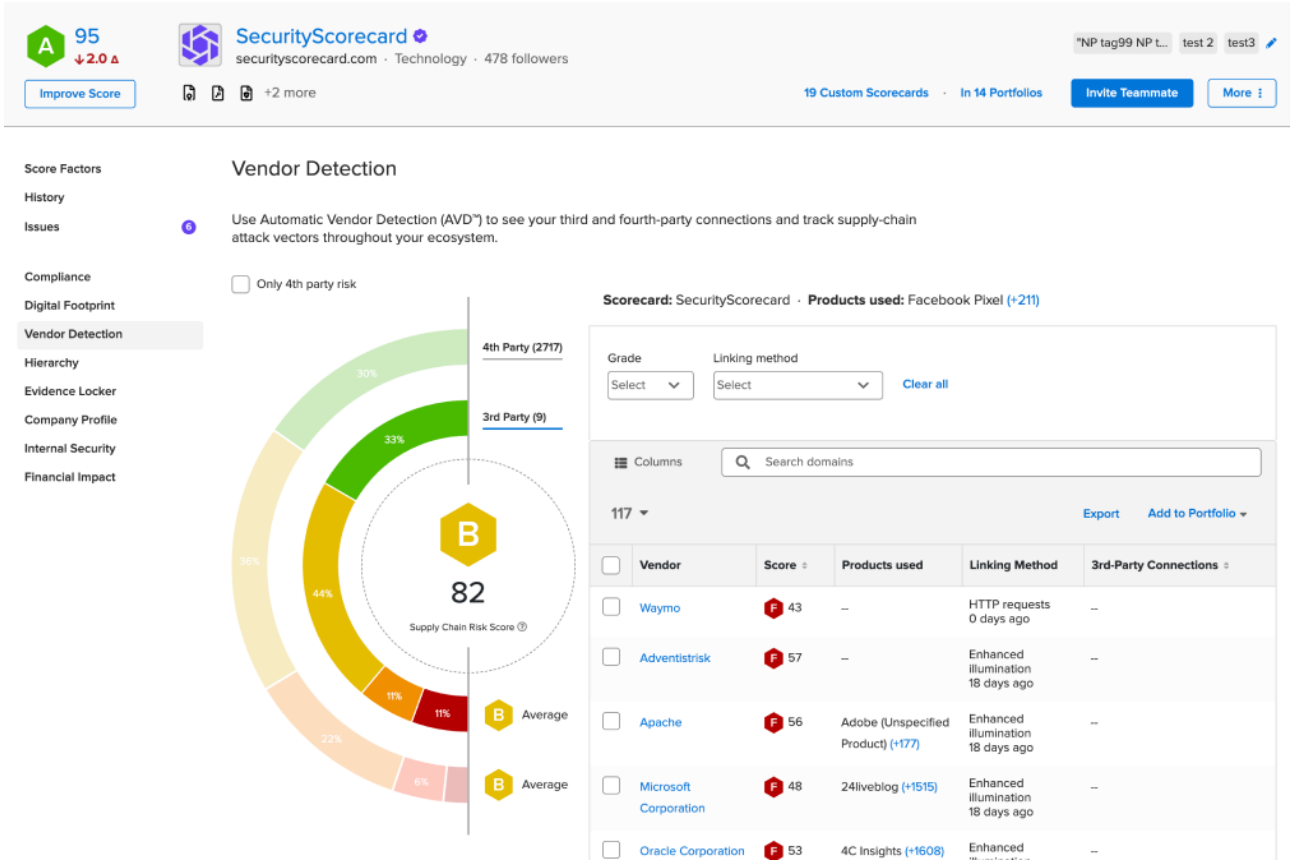


Vendor Detection 供应链检测

通过供应商检测，可以确定一个网站或应用程序使用的第三方组件，如广告服务、分析工具、内容交付网络（CDN）、社交媒体插件、支付处理服务等。这对于网站和应用程序的开发者、分析师和安全专家来说是非常有用的，因为它们可以了解应用程序的依赖关系、性能特征和潜在的安全风险。

供应商检测通常是通过分析网站或应用程序的代码、网络请求、脚本和其他技术特征来实现的。一些供应商检测工具和服务可以自动识别和报告使用的第三方供应商，从而提供更便捷的分析和洞察。

需要注意的是，供应商检测在合规性和隐私方面也可能引发一些问题。识别第三方供应商可能涉及到访问和分析网站或应用程序的数据和代码，因此在进行供应商检测时应遵循适用的法律法规和隐私政策，确保合规性和用户隐私的保护。但是您可以放心我们的供应链检测是符合隐私合规和用户隐私保护的。



Atlas

Atlas 是 SecurityScorecard 的自动问卷和证据交换平台，用于现代风险管理。Atlas 使发送方和接收方之间的网络安全问卷交换过程更快、更准确、更安全，关键见解在每个阶段都映射到 SecurityScorecard 评级。通过专有的机器学习算法利用安全记分卡评级和智能制图引擎，Atlas 自动提供对问卷回复有效性的洞察。Atlas 由内而外的方法与 SecurityScorecard 评级的由外而内视角相结合，为组织提供了任何供应商网络安全风险的 360° 视图。

无论您是发送问卷还是接收问卷，Atlas 都能将您的流程加速和简化多达 70%，使您的团队能够完成更多工作。Atlas 和 SecurityScorecard 拥有 1+ 百万家公司评级，使您能够自信地做出网络风险决策。

Atlas 如何帮助您发送和查看问卷

作为问卷发送者和审稿人，Atlas 和 SecurityScorecard 通过 4 个简单的步骤，让您 360°了解世界上任何公司的网络安全风险：

1. 上传或创建自定义调查表模板，或从 20 个行业标准模板调查表中进行选择。
2. 一次将调查问卷发送给一个或多个供应商。他们将收到登录邀请并直接在 Atlas 中完成。
3. 跟踪每个调查表的状态，查看截止日期，并查看所有调查表的周转时间。此外，通过自动提醒，您不必再发送提醒电子邮件。

4. 调查问卷完成后，您将收到电子邮件通知，并可以直接在 Atlas 中查看问卷和附件。Atlas 的智能地图引擎将安全记分卡评级映射到单个响应，允许您信任但验证问卷响应。

Atlas 如何帮助您接收和回答问卷

问卷和回复模块利用 Atlas 进行高效、准确和一致地回复。Atlas 独特的机器学习引擎标准化了各种输入，因此可以自动填写并更快地完成安全问题的答案。

1. 上传您之前填写的任何问卷，并将相关证据上传到您的答案和证据存储库。
2. 当您收到新的问卷时，请将其上传到 Atlas 以开始填写。
3. Atlas 的智能制图引擎将根据您之前填写的问卷自动识别并建议答案。
4. 在问题旁边使用 Atlas 的智能答案建议 - Atlas 会扫描您上传和收到的所有问卷，以建议您从类似问题中获得答案。
5. 与您的团队协作，直接在 Atlas 中提问，并将完成问卷的速度提高 70%。

Limitations

- SecurityScorecard 主张"从外到内"的方法对网络安全态势进行非侵入、非渗透的评估。针对目前黑客主流的攻击手段基本是从外部到内部的攻击方式，所以对于内部域的安全我们无法对其做出一个公平的、正确的评价，因此有时评分可能会变低。
- 互联网的动态特性对任何试图描述其当前状态的过程的准确性带来了根本性局限。这种努力的结果必然是概率性的，而不是确定性的。 对 SecurityScorecard 来说，这意味着虽然分数和归属基本正确，但总是会出现或存在一些误报错误。

Questions & Answers

Q: 我们使用你们的软件是否存在隐私信息泄露的可能性?

A: 我们产品所做出的所有的安全检测都是针对您网站已经公开的功能进行检查，所以在这发面您大可放心去使用我们的产品。唯一可能泄露的就是您的账号和密码了。

Q:你们的软件是否有中文对接的 API 接口? 毕竟让我们使用都是英文的软件不是那么容易。

A: 您好，针对这一方面，我们提供了 API 可供您的企业进行使用。

Q: 你们的安全评级系统会不会生成报告?

A: 您好，针对生成的评级报告，我们生成的报告里面详尽的解释了网站出现的问题以及对应的解决方案等。您的安全团队完全可以根据报告进行后续的安全修复。

Q: 你们会提供相关的安全服务支持吗?

A: 会的，如果您遇到了任何难以解决的问题，我们的技术团队会为您解决。

Q: 1-2 分的分数变化是否显著? 如果是 5-10 分呢?

A: 分数下降 5-10 分是显著的，用户需要立即采取补救措施，相比之下，分 数的微小变化 1-2 分不太可能反映安全态势方面有意义的改变。然而，当分数 降低 1-2 分导致安全评级发生变化时，例如从 B 变为 C，尽管分数变化不大， 但可能会产生心理影响。

About Us

网络安全评级的全球领导者 SecurityScorecard 由 Silver Lake Partners、Sequoia Capital、GV、Riverwood Capital 等世界级投资者投资支持，累计为超过一千两百万家企业持续提供网络安全评级服务。SecurityScorecard 由安全和风险专家 Dr. Aleksandr Yampolskiy 和 Sam Kassoumeh 于 2013 年成立，SecurityScorecard 的专利评级技术被超过 25,000 个组织使用，进行企业风险管理、第三方风险管理、董事会报告、尽职调查 和网络保险承保等。SecurityScorecard 通过改变董事会、员工和供应商对网络安全风险的了解、 改善和沟通方式，持续让世界变得更加安全。每个组织都拥有获得可信且透明的即时安全评级的普遍权利。

关于虹科网络安全

虹科是您的解决方案合作伙伴，通过创新帮助您成功。虹科网络安全事业部凭借深厚的行业经验和技术积累，近几年来与世界行业内顶级供应商 Morphisec，DataLocker，Lepide，SecurityScorecard，veracode，Mend，Onekey，Allegro，Profitap，Apposite 等建立了紧密的合作关系。提供包括网络全流量监控，数据安全，终端安全（动态防御），网络安全评级，网络仿真，软固件安全分析等行业领先解决方案。让网络安全更简单！

虹科电子科技有限公司

www.hocyber.com
hocyber@hkaco.com

广州市黄埔区神舟路 18 号润慧科技园 C 栋 6 层

T (+86)400-999-3848
M (+86)135 3349 1614

各分部：广州 | 成都 | 上海 | 苏州 | 西安 |

联系我们　获取更多资料　hocyber.com