如何通过视觉分析改进IT网络安全思科认证 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/644/2021_2022__E5_A6_82_E4_BD_95_E9_80_9A_E8_c101_644511.htm 数据可视化已经流行了数十年，现代的桌面系统计算机已经有能力将原始数据转化为用于分析的互动式演示，让计算机安全分析师们可以应用视觉分析技术来解决日常的问题。 尽管现在有很多其他的工具在辅助企业保障计算机安全，从入侵检测和防御系统到防火墙和反病毒应用软件不一而足。但他们都不能像视觉分析软件那样有效的解决数据超载问题。这是因为数据分析问题的中心是有效的减少假性错误和多余数据，同时保留那些重要的信息(有时也被称为"提高信噪比")。 视觉分析能允许分析师交互式应用大范围工具来保留重要数据和让他们变得马上能让人理解。基本上说，视觉分析能够减少将大数量级信息转化为知识所需的时间。可能是因为以下的几个原因：原因一：视觉分析能允许计算机安全专业人员重新考虑如何采取风险和保护措施来应对网络威胁。然后还能帮助安全人员采取更为有效的攻击阻止措施，对可能发生的攻击进行更快的隔离和缓解。 原因二：视觉分析能让激活数字分析流程的主要方面，包括数据收集，发现，调查，检验，分析和汇报。视觉分析能让人们以以下三种独一无二的方法理解网络安全和计算机分析： 首先，计算机网络入侵检测系统日志文件数据可以被加载，通过视觉分析来检查计算机之间的恶意连接。这种数据可以和其他日志数据结合起来，让大家对安全泄露事故有更加全面的了解。 其次，可以检查电子邮件来建立通信模本，概括电子邮件的内容。第三，从目录架构显

示和过滤的文件修改次数来判断在什么时间发生了什么事情。多重文件系统能很快的进行对比来发现从一台计算机传输到另一台计算机的同类文件。 原因三：视觉分析能为安全人员提供信息发掘，处理和可视的能力，这种战术可以应用涉及计算机安全和分析的许多应用软件领域，包括： 1.在入侵事件发生后对计算机系统进行分析来判断攻击者如何进入系统，又做了些什么。 2分析目标硬件上的信息，特别是那些知识产权，军事和执法部门的硬件设备。 3.利用计算机分析技术来分析在法律案例中属于被告的计算机系统。 将视觉分析与企业的最佳实践相结合能帮助计算机安全专业人员快速甄别他们企业内部的网络风险。采取措施的时间越早，他们比竞争对手获得的先机就越多，这也会帮助企业在面对逐渐攀升的风险和日常攻击时，能取得明显的竞争优势。随着企业越来越依赖计算机和数字信息，通过视觉分析对对风险做出快速反应也愈发的受到关注。 这些原因也解释了美国政府为什么要在国家防御方面重金投资视觉分析项目，为什么对计算机安全会如此重视。国家视觉和分析中心就是一个例子。传统的资金支持都是通过国土安全部的批准，这次的项目却获得了学士和商界的大力支持。通过这个项目和其他联邦政府计划研发的许多产品目前已经开始应用到公共领域，这对企业从无数可视化分析类型和大容量数据中获取专业知识的能力也产生了巨大的影响。 显然，视觉分析有许多可供计算机安全专业人员和企业利用的优势。把视觉分析工具应用到计算机安全领域也是非常直接的，因为视觉分析与对话式图表结合起来能发挥很大的作用，学习视觉分析计算机安全数据的技巧和战术与其他专业人员已经研发和正在开发的其

他技术相比也是相对简单的。 随着视觉分析领域的逐渐成熟，我们会看到生产力的大幅提升，反应时间的减少，在面对日渐复杂的恶意威胁时，企业对这项新兴技术的接受和重视程度的不断加强。 编辑特别推荐: 解决网卡硬件损坏造成的局域网无法连通 在CiscoIOS上限制NAT的单用户连接数 CiscoIOS备份、升级、灾难恢复 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com