opentext™ | Cybersecurity

数据表

ArcSight Logger

统一机器数据的集合、存储和分析以获得安全智能。ArcSight Logger 是一款行业领导的数据集合解决方案，可随着企业的发展，同时满足网络安全性、合规性和 IT 运营日志管理需求。

产品亮点

随着网络安全威胁加剧，集中机器数据日志迅速成为重要的情报来源。如今，有效的日志管理在实现深入的安全分析方面发挥着重要作用。

OpenText™ ArcSight Logger 是一款全面的日志管理解决方案，通过统一和存储来自各个组织的机器数据日志，以及促进快速搜索和报告这些数据，减轻了合规性负担，并提高了安全专业人员的取证调查速度。ArcSight Logger 在 ArcSight 产品系列提供强大的分层分析和建立基础安全运营的使命中发挥着重要作用。

ArcSight Logger 使组织能够收集来自 480 多个来源的数据日志，并以整洁、标准化的格式存储日志数年，这要归功于其令人印象深刻的、经济高效的压缩比率。ArcSight Logger 每天不仅可以读取和存储数百万（甚至数十亿）个事件，还可以帮助安全专业人员使用这些数据，通过简化的搜索和可定制的仪表板高效发现异常并进行快速的取证调查。

ArcSight Logger 附带内置内容、仪表板和报告，有助于实现不间断的安全合规性。此外，Logger 还提供了内容包来提高 PCI、SOX、HIPAA 等的合规性。这将减轻审计负担，减少证明符合相关法规要求所需的时间。

总体而言，ArcSight Logger 为组织提供了一个解决方案，以简化数据收集、存储、合规性和搜索。

主要优势

综合数据集合

ArcSight Logger 每天收集来自任何来源（包括日志、点击流、传感器、流网络通讯、安全设备、Web 服务器、自定义应用程序、社交媒体和云服务）。使您能够搜索、监视、分析数据，从而获得整个组织中的宝贵安全情报。

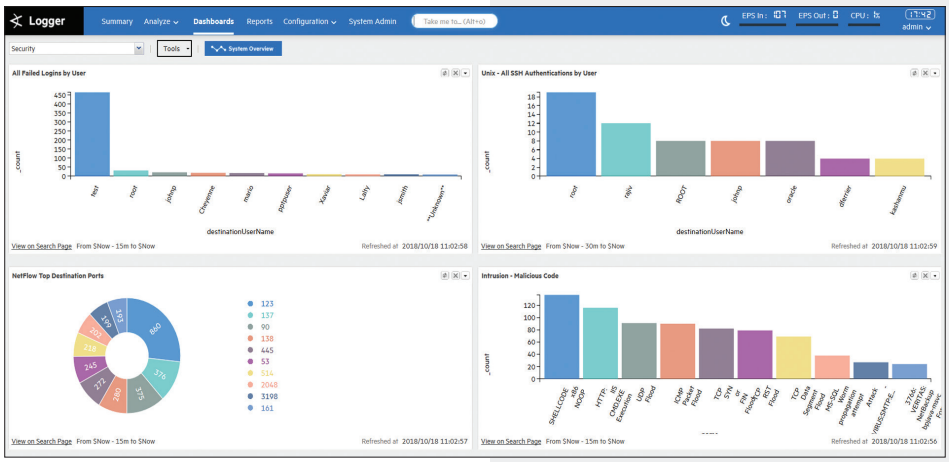

图 1. ArcSight Logger 仪表板

ArcSight Logger 概览

- 获取检测安全漏洞所必需的信息种类、数量和速度
- 只需点击几下鼠标即可设置、升级和维护
- 通过快速分布式对等搜索，经济高效地存储和搜索 TB 级数据

灵活的部署架构
ArcSight Logger 可以配置为提供装载平衡集合的群集，并在整个平台上分发搜索查询。它可以作为设备安装在 Linux 系统、VMware 虚拟机 (VM) 和云（AWS 和 Azure）中。ArcSight Logger 可以利用本地驱动器或现有 SAN 投资作为主数据存储。无论存储是机载存储还是非机载存储，数据都可以有效地压缩以降低存储和维护成本。

它采用一种称为通用事件格式 (CEF) 的可扩展、基于文本的高性能格式，因此企业管理系统（如 OpenText™ 支持的 ArcSight ESM、OpenText™ 支持的 ArcSight Investigate、OpenText™ 支持的 ArcSght Interest UEBA 或任何提供事件编排、自动化、关联、优先级划分、安全事件分析或以上所有内容的第三方应用程序）可以轻松收集和聚合数据以供分析。

安全可靠的数据收集
ArcSight Logger 软件可以为静态数据和动态数据提供加密、压缩的日志，从而确保数据不被截取、更改和删除。借助 OpenText™ 支持的 Voltage SecureData Enterprise，ArcSight Logger 支持：

- ArcSight Logger 设备上的安全加密功能可在静止时（存储时）对敏感数据进行加密。它还支持 TLS 和 SSL 加密协议以保护移动数据的安全。
- 安全管理和用户/组角色定义。管理员可以根据用户角色和组权限设置报告和报告类别的访问权限。他们还可以对特定数据列进行加密，并有选择地授予解密权限。
- OpenText™ 支持的 Voltage 格式保留加密技术 (FPE) 可防止未经授权泄露您的数据。保护闲置、传输和使用中的数据。
- 联邦信息处理标准 140-2 (FIPS 140-2)。

极速调查和取证
当几秒钟意味着一次成功或失败的攻击之间的差异时，在正确的时间获取正确的信息至关重要。ArcSight Logger 可通过简单的搜索界面对索引数据进行极速调查。趣味研究模式可以轻松转换为实时警报。

ArcSight Logger 还可通过机器学习数据科学内容加快调查速度。使用预构建内容或使用 python 脚本开发您自己的数据科学算法。

ArcSight Logger 可根据多年数据，在 10 秒内对数十亿事件进行临时搜索，从而帮助您识别违规行为并进行详细的违规分析。

不间断合规性
ArcSight Logger 附带内置内容，可用于网络安全性、合规性、应用程序安全和 IT 运营监控。针对 PCI、ITGOV、HIPAA、NERC 和 Sarbanes-Oxley (SOX) 的其他合规性内容包作为附加选项提供，并符合包括国家标准和技术研究所 (NIST) 800–53、ISO-17799 和 SANS 在内的驰名标准。

易于部署和管理
ArcSight Logger 可以通过 ArcSight 的管理中心进行配置、管理和监控，ArcSight 的管理中心是一个集中式管理控制台，您只需单击几下鼠标，即可轻松连接到数据。即使在大型部署中，它也可以轻松配置、管理和升级，让您可以专注于用例，而不是工具本身。

主要功能

- 综合数据集合
- 灵活的部署架构
- 安全可靠
- 极速搜索和调查
- 不间断合规性
- 易于部署和管理
- 机器学习数据科学内容

为何选择 ArcSight 产品系列?
OpenText™ 支持的 ArcSight SIEM 平台具有出色的可缩放性和强大的功能。这是由安全专家为安全专业人员开发的一款全面解决方案。它采用了一种全面的安全智能方法，通过先进的安全分析技术（包括搜寻、调查和 ArcSight Interset UEBA 解决方案），以独特的方式统一大数据收集、网络、用户和端点监控和取证。它提供实时威胁检测和响应、合规性自动化和保证以及 IT 运营智能，从而提供强大的分层分析方法，帮助企业实现自我保护。

“ArcSight Logger 让我们能够非常迅速地满足 PCI 要求，并帮助我们监控网络是否存在异常，以便我们能够应对新出现的威胁。”

安全官
财富 500 强金融服务公司

虽然许多供应商声称提供强大的 SIEM 解决方案，但 ArcSight SIEM 团队拥有丰富的安全专业知识、经验和领导力，很少有供应商能与之匹敌。

我们拥有下一代解决方案、成熟的方法和 18 年以上的经验，配合世界上规模最大、最复杂的 SOC，让 OpenText™ 具有独特的资质，可帮助您实现更高的安全状况和卓越的运营。

有关日志管理的详细信息，请访问 **www.microfocus.com/arcsightlogger**

与我们联系
www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity 为各种规模的公司和合作伙伴提供全面的安全解决方案。从预防、检测和响应，到恢复、调查和合规，我们统一的端到端平台可以通过全面的安全组合帮助客户构建网络恢复能力。基于我们的实时和环境相关威胁情报所提供的可操作见解，OpenText Cybersecurity 客户将从高效率产品、合规体验和简化的安全性中受益，能够帮助他们有效管理业务风险。

760-CN0047-002 | O | 12/23 |