OpenText SIEM Open Data Platform

释放并持续提升您的网络安全解决方案的价值



关键功能

- 包含基于 Apache Kafka 构建的 SIEM Message Hub，可从任何来源采集数据并将其发送至任意位置
- 实时数据增强功能为原始数据添加安全上下文，使其可立即使用
- 超过 400 个开箱即用的连接器可从各种来源类型收集数据
- 包含 SIEM Management Center，可为您的安全环境提供端到端的整体视图

近期的一份报告显示，68% 的公司每年会遭遇 11 至 30 次外部攻击[1]。组织面临的网络攻击威胁逐年增加，某些攻击（如针对美高梅国际度假集团的攻击）单次造成的损失就超过 1 亿美元[2]。

安全数据是现代安全运营环境的支柱。不断增加的异构数据源和数据格式，使得构建单一数据架构来满足所有需求几乎成为不可能。我们每年创建和复制的数据量每两年就会翻倍，预计到 2028 年将从 2010 年的仅 2 ZB 增长至 394 ZB[3]。随着 IoT、物理、OT 和 IT 的数据量和速度呈指数级增长，安全运营中心 (SOC) 难以摄入和处理威胁检测所需的数据海啸。数据访问限制和关键系统连接限制会导致严重的延迟和高昂的成本。

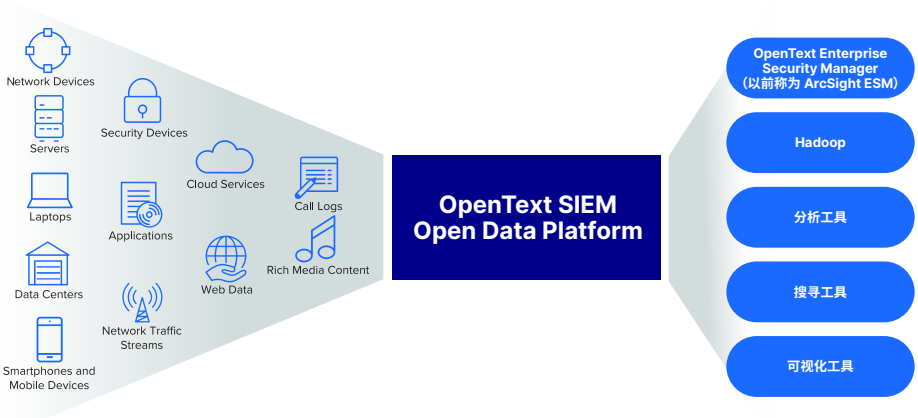


图 1. 数据无处不在，无所不至：开放式体系结构

优势

- 扩展数据可见性以降低受到攻击和声誉受损的风险
- 通过更快的威胁检测和响应来降低风险
- 高效利用您技术熟练的安全专业人员
- 通过将数据用于 Hadoop 和分析工具来提升投资回报
- 降低将数据提取并分发到多个目标位置的成本和复杂性

SOC 必须进行根本性重组，以适应不断增长的数据量、快速变化的威胁态势以及专业安全人员的短缺。

OpenText SIEM Open Data Platform 提供面向未来的数据解决方案，可实时增强数据并支持开放标准，从而提升威胁检测能力。使用 OpenText SmartConnectors，可实时收集并增强数据，为分析人员提供有序信息，以便即时采取行动。我们智能的 OpenText SIEM Message Hub 基于 Apache Kafka 构建，可帮助 SIEM Open Data Platform 从任何来源无缝采集、代理和分发数据至任意位置。

功能和优点

驾驭海量多样化数据，释放卓越扩展能力

借助 400 多个开箱即用的安全数据连接器和自定义连接器创建工具，SIEM Open Data Platform 允许您从各种类型的数据源收集数据。用于构建解析器的基于令牌的工具可提高一致性，并将构建新连接器的时间从数天缩短到数小时，从数小时缩短到数分钟。SIEM Message Hub 以每秒数十万个事件 (EPS) 的速率接收数据，并帮助将数据无缝路由到多个目标位置。

管理日益增多的异构数据源是一项单调乏味且耗时的工作。SIEM Open Data Platform 内置 OpenText Management Center，可通过直观的可视化界面和指标，展示您的安全数据管道的运行状况。所有设备、连接器和目标位置的端到端视图有助于即时识别数据问题并缩短修复所需时间。我们的管理控制台使 SOC 数据管道资源的管理变得前所未有的轻松。它引入了“即时连接器部署”功能，可帮助您轻松地对数百个连接器进行一次性操作，从而节省时间。

SIEM Open Data Platform 通过扩大安全数据覆盖范围，简化了安全数据操作，并有助于改进攻击检测。它能够优化对高速、海量、多样化数据的收集和管理。

利用实时安全上下文，交付深度洞察

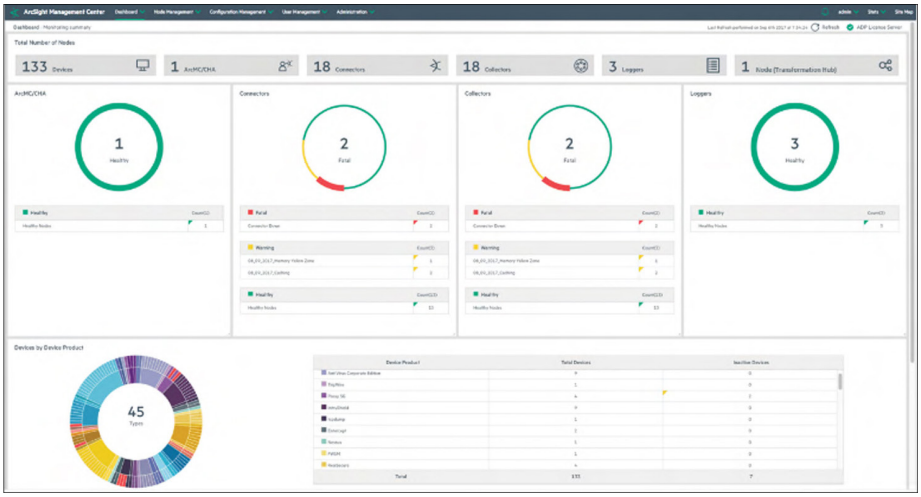


图 2. SIEM Open Data Platform 集中式管理控制台 - 仪表板

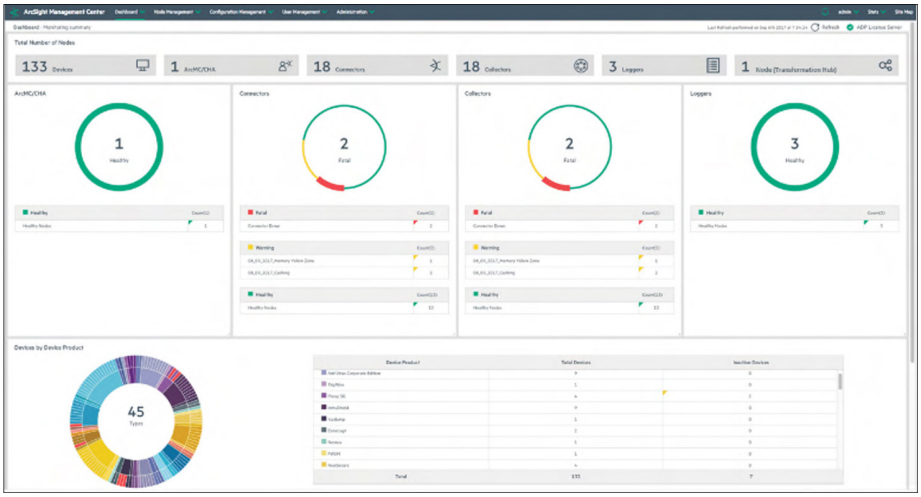


图 3. SIEM Open Data Platform 集中式管理控制台 - 端到端监控

SIEM Open Data Platform 利用 SmartConnectors 实时增强原始数据，为分析人员提供条理清晰、可立即采取行动的信息。SIEM Open Data Platform SmartConnectors 会在数据摄取过程中对数据进行规范化、分类和增强，体现 OpenText 数十年来积累的网络安全专业经验。因此，数据已经过结构化和整理，能够实现更快、更准确的调查和事件关联，以协助威胁检测。

为了满足合规性要求以及防止网络攻击导致数据篡改，确保数据的可靠性和完整性非常重要。SIEM Open Data Platform 会对安全日志数据进行加密处理，以降低数据被拦截的风险并保护数据完整性。所有传输中的数据均由传输层安全协议 (TLS) 提供保护。

善用开放式架构，创造核心价值

为满足实时分析和数据留存需求，安全运营部门需要接入更多安全数据源并处理日益增长的数据量，而 N:1 架构已成为制约其发展与需求满足的瓶颈。SIEM Open Data Platform 附带了 SIEM Message Hub，这是一种基于 Apache Kafka 的消息总线，提供了 N:M 体系结构，可从所有来源摄入数据并将其路由到多个目标位置。这使您可以开放您的安全环境，并利用通过现有数据湖、分析工具和其他安全设备收集的数据。这通过将收集的安全数据应用于多种使用场景，降低数据管道的复杂性，并为安全运营提供面向未来的保障，从而提升您的投资回报率。

开放式体系结构使您可以灵活地选择储存、搜索和分析数据的方式，并利用各类领先技术中的安全数据。

SIEM Open Data Platform 还通过 SIEM Message Hub Kafka 复制功能，提供先进的高可用性能力。

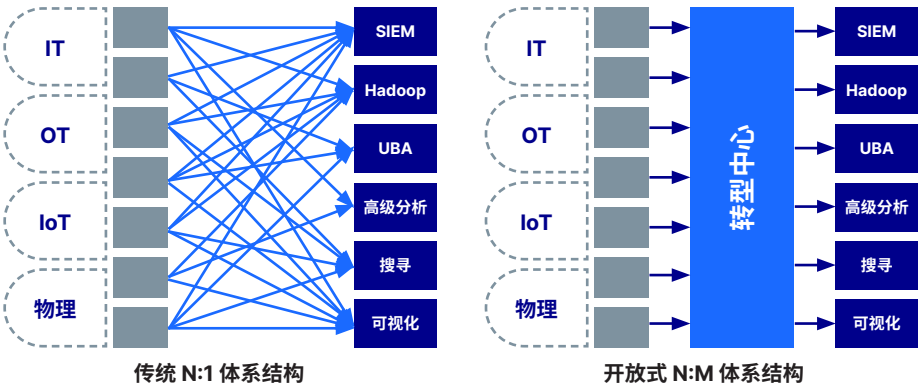
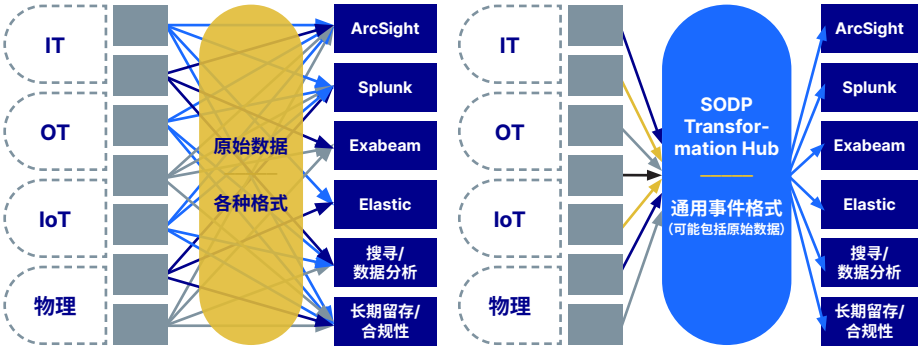


图 4. 智能消息总线体系结构

资源

如需了解更多信息，请访问
cybersecurity.opentext.com ›

总之，OpenText SIEM Open Data Platform 提供了面向未来的安全数据管道解决方案，可实时对安全数据进行标准化与增强，从而提升威胁检测能力。其开放式架构的消息总线使您能够从所有来源摄入数据，并将其路由至多个目标位置。SIEM Open Data Platform 可随企业发展而扩展，为安全分析师的数据赋予深层含义，并简化您的安全数据管道，确保其能满足未来需求。



未采用 OpenText SIEM Open Data Platform　　**已采用 OpenText SIEM Open Data Platform**

1 Ponemon Institute - Cost of Insider risk Global Report 2025
2 Verizon's 2024 Data Breach Investigations Report - 2024
3 IDC - Worldwide IDC Global DataSphere Forecast, 2024–2028: AI Everywhere, But Upsurge in Data Will Take Time

版权所有 © 2025 Open Text • 09.25 | 260-CN0407-001

opentext™