联想集团通过Splunk Enterprise实现灵活、高效的安全运营

执行摘要：

作为全球电脑市场的领导企业，联想从事开发、制造并销售可靠的、安全易用的技术产品及优质专业的服务，帮助全球客户和合作伙伴取得成功。联想在全球180个国家和地区开展业务，全球研发基地15个，全球员工超过57,000人。联想位列2019《财富》世界500强的第212位，2018至2019财年营业额达3,422亿人民币。联想的业务发展，产生了大量来自不同层面的数据，希望找寻合适的工具进行数据管理和分析，以实现更高质量的安全运营，保障集团整体的数据安全、网络安全和业务安全。在部署Splunk Enterprise后，联想体现了以下几方面的优点：

- 实现了对IDS（入侵检测系统）日志，防火墙日志，终端安全软件日志、基础设施日志等的统一、实时、高效的收集和分析；
- 实现了对安全态势的实时检测和安全问题的深度分析，事件处理便捷高效；
- 大大节省了时间和人力成本，提升了整体安全运营的质量。

为什么选择Splunk：

联想的数据主要来自基础架构日志，安全软件日志，应用日志等三个层面，数据量达到2TB/天。如何对这些海量数据进行高效、智能的监控和分析，及时发现并快速响应各种日常安全事件，实施全面深入的安全调查，是联想安全团队面临的一项重要挑战。使用Splunk之前，联想需要从不同系统中获取相关的日志，然后依赖安全工程师的手工关联分析把重要信息和可视化功能整合在一起，故障处理流程很长，例如处理安全染毒事件，先去终端管理软件获得终端数据信息，然后再去多个终端安全软件管理平台获取事件信息，再将多个数据进行关联，耗时较长。

在选择安全分析工具的调研过程中，联想试用了Splunk Enterprise，并通过衡量和对比，以及充分考虑到时间和费用成本，最后发现Splunk解决方案性能稳定，减少开发投入，更适合自身的需求。

全面、实时的可视化分析大幅度提高安全运营效率

联想组织内部的多个团队（应用团队，安全团队等）都在使用Splunk解决方案，用于日常的工作。具体应用例子包括：搜索，报告、警报和蜜罐监控等方面。通过Splunk平台将不同来源数据汇总，自动进行监控，包括日志分析和精确提取，并用以可视化的方式呈现出来，一目了然，实现了实时的可视化分析，大大提高了工作效率。

统一的数据互联分析极大节约人员成本

过去，联想使用开源的IT监测平台，需要多名技术人员进行大工作量的开发和集成，同时，还需要在各个部门间进行多次反复的沟通、协调，耗费的人工成本和时间成本巨大。而Splunk平台将日志统一在一个平台上，用统一的方式进行互联和分析，一次性完成日志导入、集成和分析工作，减少额外的人工参与，极大节省了人力、时间和成本，最大程度消除来自内外部的威胁和风险，提升了企业整体IT运维的质量。

Lenovo 联想

概观

行业：

- IT

Splunk使用案例：

- 日志监控
- 安全运营

挑战：

- 整个集团数据源众多，数据量巨大，需要全面的数据监控，以便尽早发现安全问题，提高日常事件响应和安全调查效率
- 解决IT数据分散，需要更多的资源投入，提取数据缓慢
- 改变日志的分析不灵活，需要大量的前期定制，可用性差
- 加强多系统数据关联，提高安全运营能力

业务影响：

- 大幅度提高安全运营效率
- 完善的安全隐患预测和安全事故的及时响应
- 减少开发时间和人力成本

数据源：

- 基础架构日志
- 安全设备日志
- 安全软件日志

Splunk产品：

- Splunk Enterprise

顺应IT发展趋势，为公有云战略部署保驾护航

此外，Splunk平台所提供的可靠而智能化的解决方案特别契合当今IT运维向公有云发展的趋势，解决了之前部署中遇到的困难，正是在实施Splunk解决方案的过程中切实体验到这一点，联想计划未来将Splunk方案应用于公有云日志收入和增加应用安全日志读入，并与AWS等基础设施合作伙伴基于Splunk平台共同推动企业战略决策智能化。Splunk平台将为加速联想公有云部署起到积极的推动作用。

“Splunk解决方案性能稳定且智能，帮助我们从海量庞杂的原数据中快速分析出高质量的决策信息，实现了高效的安全运维和监控。我们很高兴选择了Splunk，并期待未来有更加深入的合作。”

联想中国
IT安全总监
余盛立

2020-Splunk-IT-Lenovo-A4-101-CS-CH