ALEIYE

让 | 大 | 数 | 据 | 更 | 简 | 单

ALEIYE 运营商大数据解决方案

北京数介科技有限公司

目　录

行业背景

随着互联网业务和应用的迅猛发展以及移动互联网的爆炸式增长，电信运营商客户行为数据、网络运维数据等海量数据的存储与分析日益成为电信运营商的重要挑战，大数据技术的出现与发展为电信运营商深挖数据提供了新的技术手段，同时也为其更好地服务客户提供了新的机遇。

同时随着电信运营商全业务的开展，电信行业的竞争已经从传统的用户资源、资费方式的竞争，上升到以客户为核心的服务竞争。因此从运营角度出发，由于竞争加剧导致总体收益的下降，运营商当前迫切需要寻找新的业务增长点。从自身角度出发，在提供安全可靠的网络线路、各类增值服务的同时，必须解决由于网络攻击、病毒爆发等安全事件的影响，对用户服务质量的降低。

面临的挑战

在运营商内部，部署了大量的防火墙、入侵监测系统、虚拟专用网和防病毒软件等网络安全设备，从而保证网络的可用性和网络信息的机密性、完整性，防止来自外部或内部的攻击行为。这些工具和设备都已日志形式记录着大量的安全问题，这些信息成为网络安全工作中防御、监测和响应的重要基础依据。

- **如何面对多源异构的数据**

原始日志是安全管理过程中获取的重要内容，如：syslog 数据、snmp 数据、数据库等;由于不同数据种类存在在不同设备和不同系统中，做为数据预处理、关联分析和告警响应的重要信息来源，需要对上述的异构数据进行有效实时的采集，是运营商面临的第一个挑战。

- **如何对异构数据进行统一管理**

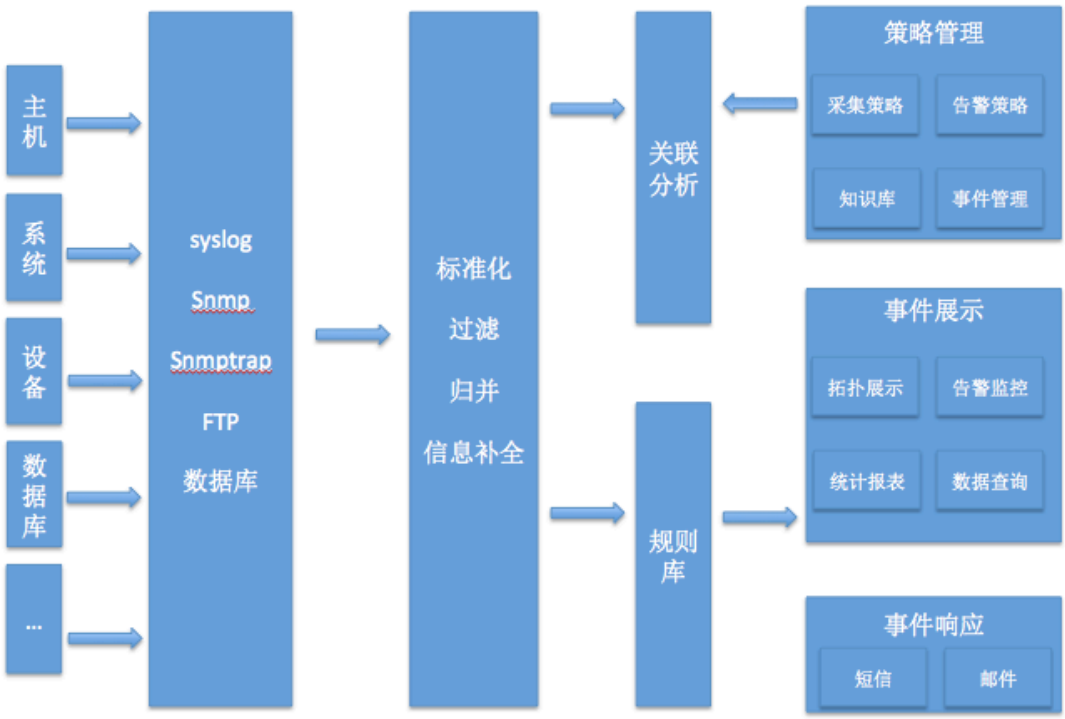
在对数据源统一管理的过程中，由于原始日志存在采集来源的不同，导致其

数据格式存在差异，例如通过 syslog 和 snmp 采集的同一类型的事件，但由于采集方式的不同，导致其数据格式不统一；数据源中，还会存在大量的重复信息、不可信信息和不重要信息，这些问题将会导致最终的数据统计分析结果的准确性降低，是运营商面临的第二个挑战。

- **如何对安全事件进行深入分析**

基于传统告警方式，对固定指标设定固定阀值的方式，无法更全面的重构安全事件攻击场景，如何利用不同设备、不同系统间的数据进行关联分析，实现真正的安全告警，从而降低误报率，帮助安全监控人员分析出网络中潜在的安全隐患，也是运营商面临的第三个挑战。

Aleiye 解决方案



数据采集

采集方式

数据采集层，主要是针对不同的业务系统和不同的安全设备中的日志进行采集，作为后续的数据处理和关联关系的信息来源，其采集方式重要包括 syslog、snmp、snmptrap、FTP、代理采集和数据库等几种方式。

- Syslog 方式：支持 syslog 内容解码。
- Snmp 方式：支持 snmpV1、V2、V3，内容解码。
- FTP 方式：支持 FTP 协议方式进行日志文件获取。
- 数据库方式：支持当前主流数据库并从中获取日志，其中包括：Oralce、Sybase、DB2、Informix、MySQL、Postgresql 等
- 代理采集：系统须具备在通过安装代理软件实现原始日志的采集功能。

采集管理

在分布式采集或单点采集的状况下，Aleiye 数据平台提供采集节点集中管理，实现对采集状态、采集规则和采集起始进行统一管理。

- 批量操作：在分布式采集的状况下，可以对各采集节点进行统一管理，如批量关闭、批量启动、批量暂停、批量下发操作。
- 策略复制：在分布式采集的状况下，可以将单采集节点中的采集策略复制到其他采集节点。
- 采集状态监控：可实时监控不同采集节点的采集状态，在数据传输过程中出现异常，系统会给与采集异常提示。

数据预处理

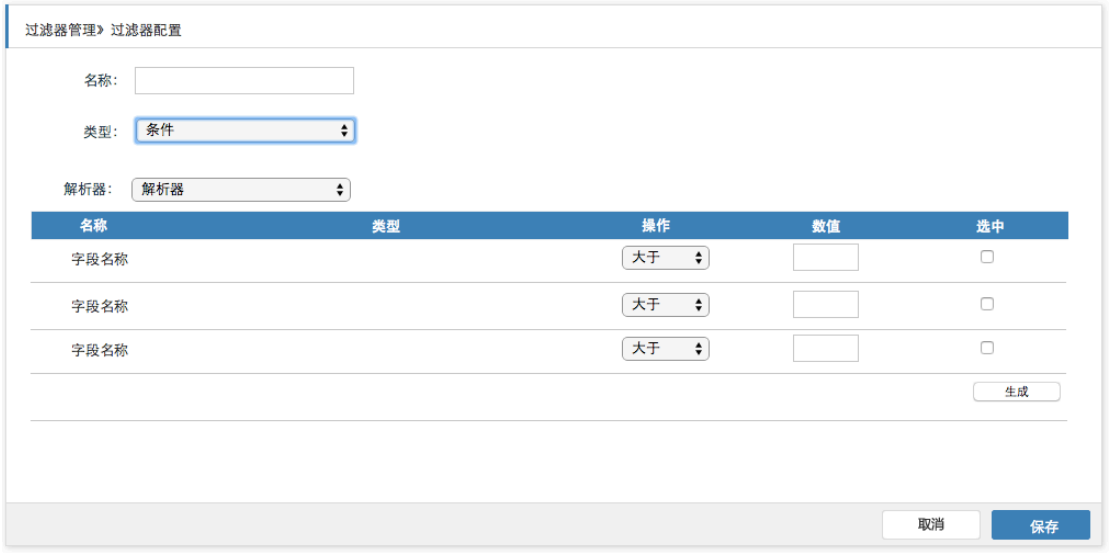
原始日志采集之后，需要进行数据预处理的过程，通过标准化配置，对数据源进行明确的数据类型划分，将日志格式进行统一转化和分类，根据划分好的数据类型进行过滤、归并、补全等规则操作，为后续的关联分析提供信息。最终输出明确的事件类型和各字段属性及补全后的安全对象信息等内容的标准事件

数据标准化

根据数据源的内容和格式，对应相应的事件类型进行字段提取、命名等操作，最终形成结构化数据。

事件过滤

事件过滤功能通过自定义设置，可对不影响后续分析的安全事件进行过滤，减少不可信、不重要的事件，过滤策略可根据字段间的条件进行有效过滤，字段件条件包括：大于、小于、等于、大于等于、小于等于、等于、不等于；还可以通过关键字和 IP 段进行过滤规则的配置。



事件归并

对于重复发生、大部分属性相同的疑似安全事件，在不影响后续事件分析的前提下，应对个体进行合并，减少事件个体数量，并可以对合并后的数据进行新事件的创建。

信息补全

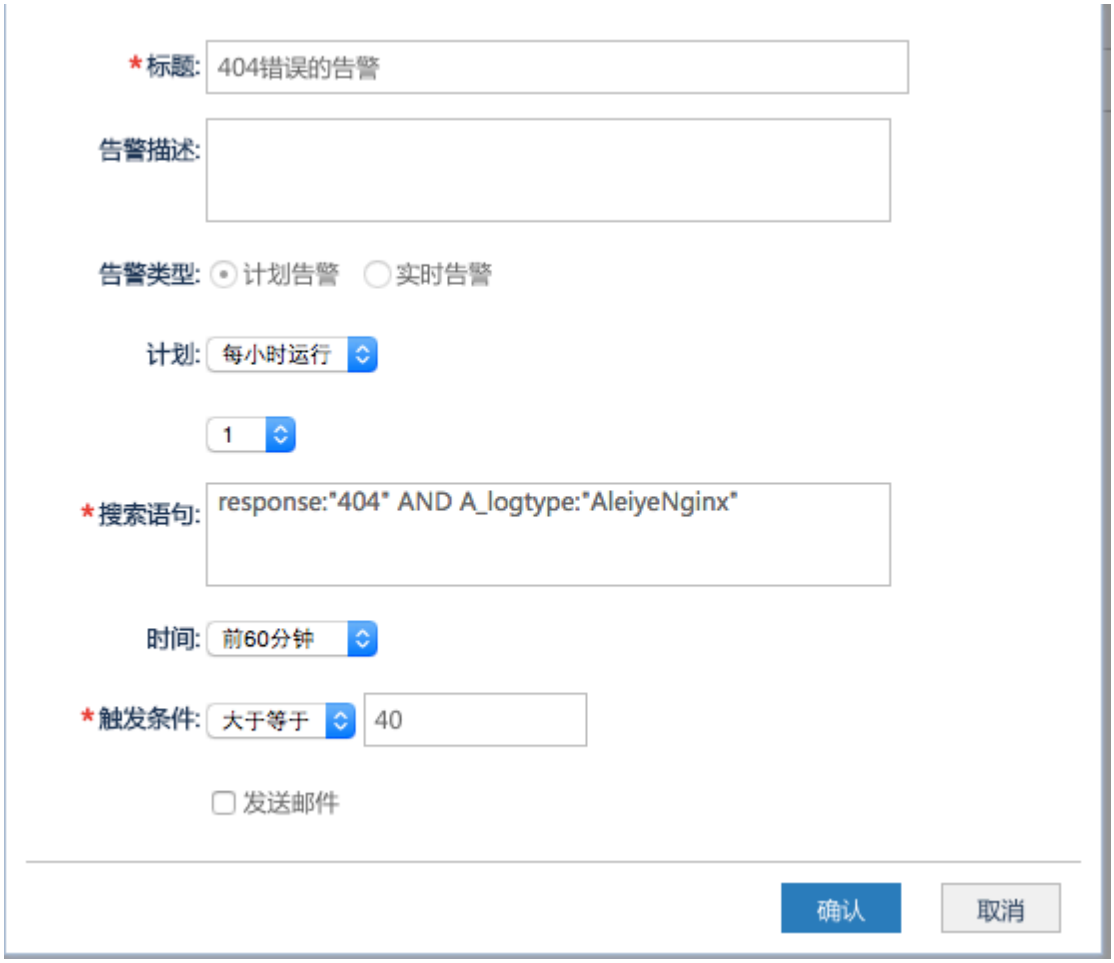
对于未直接体现在原始日志中的必要信息，事件管理模块应具备补全功能，主要为与事件相关的安全对象信息。

安全告警关联分析

安全告警关联分析是指安全告警的分析方法，以事件触发为基础，对实际业务情况进行深度挖掘，从而实现高可信度的安全告警信息。安全告警关联分析基于统计关联、模式关联两种方式进行组合，分析安全告警、挖掘安全隐患、判断安全事件的严重程度和实质影响。从而重构整个攻击场景，降低误报率，帮助安全监控人员分析出网络中潜在的安全隐患。

统计关联

使用计数器来统计某类事件发生的次数，并设定可以接受的数值范围，一旦在统计过程中发现事件超出了正常设定的阈值，就认为系统出现了异常，而生成告警。基于统计关联的方法适应于检查统计量发生次数有明确限制情况

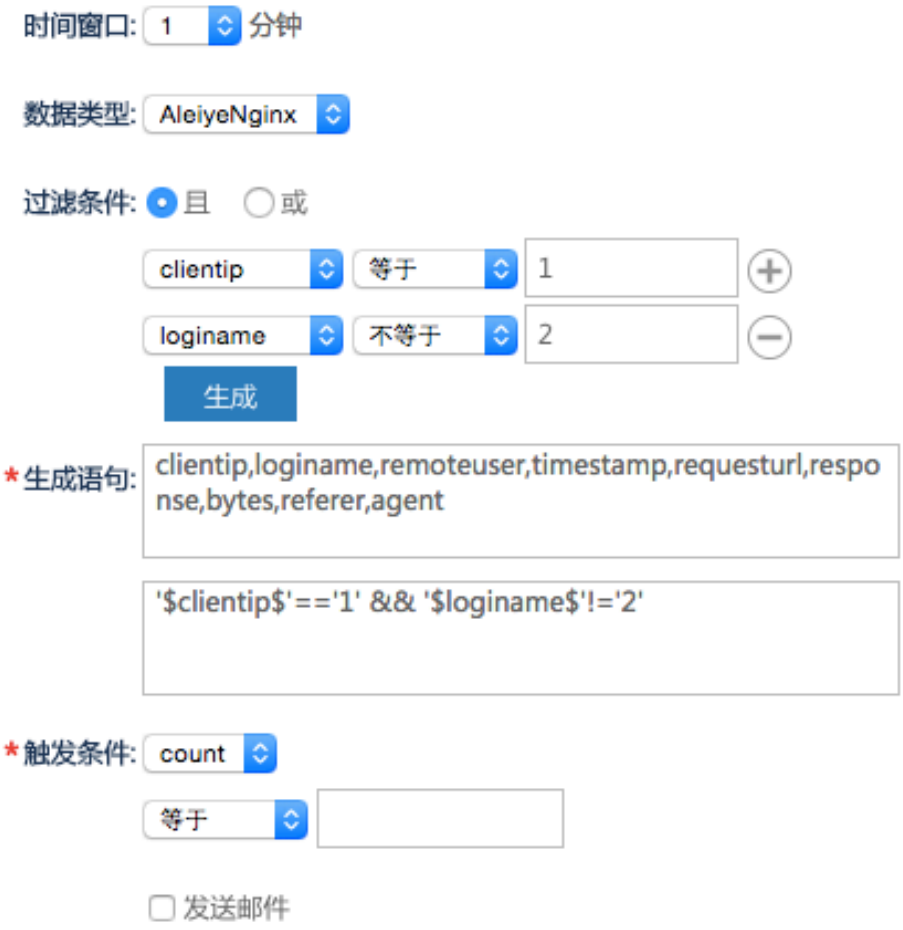


模式关联

基于模式的关联分析是指将可疑的安全活动场景（例如某潜在安全攻击行为的一系列安全事件序列）加以预先定义，对收集到的安全事件进行检查，确定该

事件是否和特定的模式匹配。

其中，条件为安全事件中某些属性的限制条件，具有检测事实存在与否、比较事实、根据标志检验事实等功能。条件可以由单个检测属性组成，也可以由多个检测属性组成，且各属性用逻辑符号 OR、AND、NOT 来表示多属性的逻辑关系。结果是新安全告警的输出，同时指定此安全告警的严重程度。



方案价值

Aleiye 数据平台可以整合各个安全设备数据，统一设备输出的事件，帮助安全管理人员从全局角度保证整体安全态势。