360 态势感知与安全运营平台

产品白皮书

■文档编号	■密级
■版本编号	■日期

目录

1 产品概述

360 态势感知与安全运营平台（以下简称 NGSOC，Next Generation Security Operation Center）是 360 企业安全集团基于大数据架构自主构建的一套面向政企客户的新一代安全管理系统。该系统利用大数据等创新技术手段，结合 360 的安全能力和传统安全技术积累针对各种网络安全数据进行分析处理，可以为政企客户的安全管理者提供资产、威胁、脆弱性的相关管理，并能提供对威胁的事前预警、事中发现、事后回溯功能，贯穿威胁的整个生命周期管理。

NGSOC 产品继承了 360 企业安全集团下属网神子公司长期以来在 SOC 产品上的历史经验，同时将来自互联网公司的大数据技术注入到了产品的开发过程中，可以既满足海量日志下的快速计算分析需要，又能够兼顾大量基础管理功能，同时也汲取了国内 SOC 经常无人使用的失败经验，有针对性的在产品设计中考虑了更多有关提升使用效率、分析效率的相关实现，并对产品的后续服务提供了一整套相关方案以帮助用户更好的使用 NGSOC 产品。

NGSOC 产品在架构演进以外，也使用了大量新型安全技术，其中威胁情报能够快速的帮助单一企业补足在安全知识上的短板，既可以帮助企业发现威胁，也可以提供更广泛的威胁分析手段和能力。而其他诸如依赖于机器学习的 web 攻击发现功能等一系列威胁检测手段则能有效增强针对传统安全问题的检测率和准确度。

在架构革新和新技术的推动下，NGSOC 产品正在引领国内安全管理产品市场的变革，同时也获得着国内客户的认可。据权威资讯机构赛迪顾问的统计数据，360 企业安全的 NGSOC 产品在 2016 年中国安全管理平台产品市场中市场占有率第一。

2 平台介绍

2.1 产品组成

NGSOC 产品主要包括流量传感器、日志采集探针、关联规则引擎和分析平台 4 个硬件组件，同时能够对接 360 天眼新一代威胁感知系统中的文件威胁鉴定器和 360 天擎系统的 EDR 组件，如下图所示：

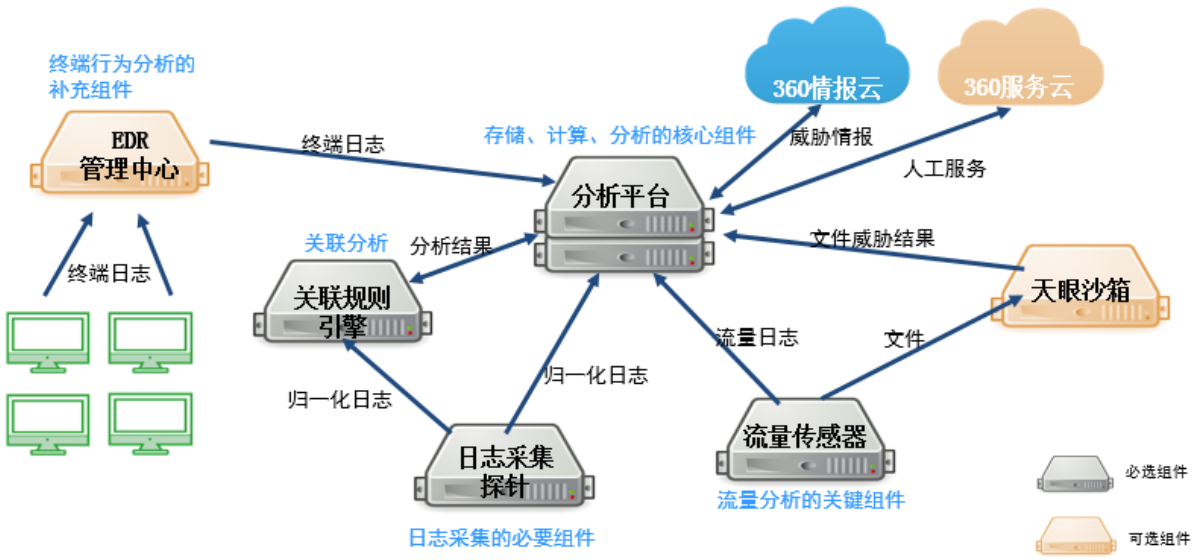


图 1 ： NGSOC 产品组成

1） 流量传感器

流量传感器的功能主要是采集网络中的流量数据，将原始的网络全流量转化为按 session 方式记录的格式化流量日志，全流量日志会加密传输给分析平台存储用于后期的审计和分析。同时对网络流量中传输的文件进行还原，还原后的文件会传输给文件威胁鉴定器用于判定文件是否有威胁。流量传感器内置了一级流量检测引擎，主要有三类检测规则：WEB 漏洞利用检测引擎、webshell 活动检测引擎、以及网络入侵检测引擎等，可实时的发现流量中存在攻击特征的行为。

流量传感器通常部署在网络出口交换机旁，或者其他需要监听流量的网络节点旁，接收镜像流量。

2） 日志采集探针

日志采集探针的主要功能是对网络内各业务应用系统、设备、服务器、终端等设备通过主动采集或被动接收等方式对日志进行采集并进行归一化预处理，方便数据流后面的关联规则和数据分析能够快速使用。同时日志采集探针还负责对内网资产进行扫描识别，收集资产数据。

3） 关联规则引擎

关联规则引擎主要负责对来自日志采集探针的大量日志信息进行实时流解析，并匹配关联规则，对异常行为产生关联告警。通常关联规则引擎与分析平台和日志采集探针部署在同一位置。

4） 分析平台

分析平台用于存储流量传感器和日志采集探针提交的流量日志、设备日志和系统日志，并同时提供应用交互界面。分析平台底层的数据检索模块采用了分布式计算和搜索引擎技术对所有数据进行处理，可通过多台设备建立集群以保证存储空间和计算能力的供应。

5） 文件威胁鉴定器（360 天眼新一代威胁感知系统相关组件）

文件威胁鉴定器接收流量中传输的文件，并通过静态和动态检测方法对文件特征和文件行为进行检测，及时发现有恶意行为的文件并产生告警。文件分析结果也会作为安全数据的一部分传给分析平台存储，以便威胁分析过程中进行调用。

6） 360 天擎终端安全管理系统

NGSOC 可以实现和 360 天擎终端安全管理系统的数据对接，由终端安全管理系统实时的将发生在终端上的各种主机行为日志发送至分析平台进行存储，为网络高级威胁发现及事件追踪溯源提供有力支撑。相关日志覆盖包含了终端进程网络行为日志、终端 DNS 请求行为、注册表更改、文件操作、文件传输（包含 IM、U 盘、邮箱等多种方式）等多个方面。

NGSOC 也可提供 EDR 自动响应功能，将相关告警推送到天擎终端管理系统执行在主机上的调查分析和阻断操作，完成威胁检测与响应闭环。

2.2 产品架构

NGSOC 将覆盖安全管理与运营的各个环节，下图为整个平台的缩略架构图。

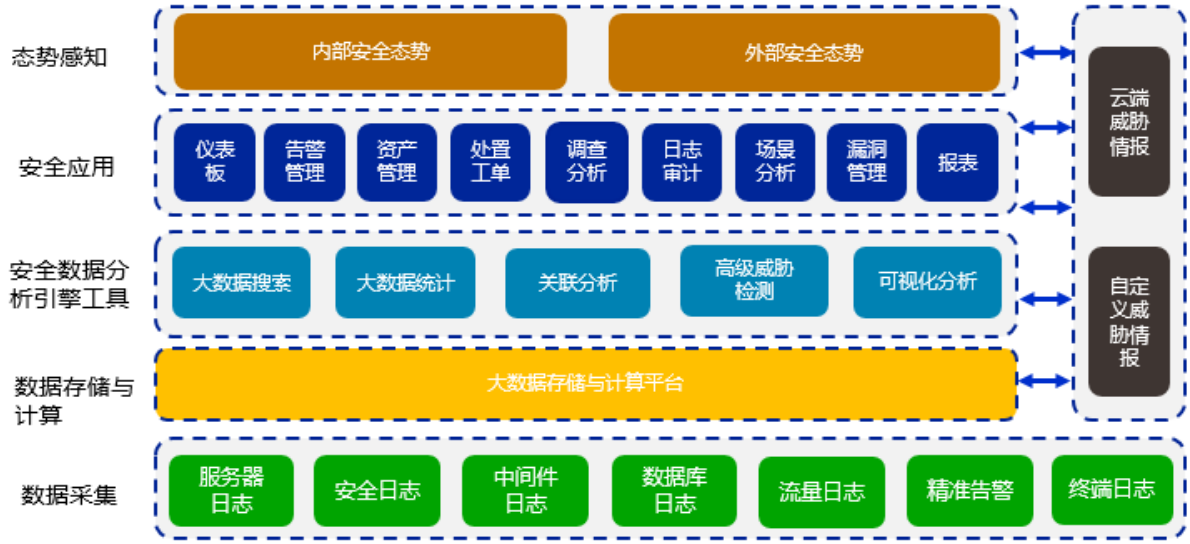


图 2 NGSOC 功能架构图

由图可见,NGSOC 将建设成一个以多种安全问题管理为目标、以数据为核心、威胁情报为特色、打通安全运营中的检测、响应、预警、防御多个领域环节的完整安全体系。

NGSOC 数据采集部分，除了传统的 Syslog、Flow、各种系统日志和安全设备日志以外还突破性的针对原始流量日志（依赖于流量传感器）和终端日志（依赖于天擎 EDR 组件）进行采集。依赖于更加原始的日志信息，NGSOC 产品可以发现隐藏更深的各种威胁，同时能够提供完整的事件回溯分析能力。

拥有更加全面的日志虽然提供了更强的分析能力,但也对产品架构提出了严苛的挑战。为此 NGSOC 产品在数据的存储和分析中大量使用大数据相关技术，在标准化产品组件中可以依赖于分布式全文检索技术提供接近 PB 级日志量的存储和快速计算，同时能够提供良好的可靠性保证，以解决意外断电、磁盘故障可能对系统带来的可靠性问题。

存储和分析能力之上，NGSOC 产品使用多种分析引擎针对不同的使用和管理目标提供相应支撑，关联分析、统计分析、快速搜索等功能相较于传统产品具有明显的性能优势。

产品最外层，针对安全分析与运营人员，NGSOC 产品可以提供友好、高效的交互管理页面，既满足了使用需求，又能够提升工作效率。再结合威胁情报、安全服务等来自于 360 特有的安全知识输入，NGSOC 可以极大的提升本地安全运营的相关效率。

3 技术特点

3.1 全面的数据采集与分析

NGSOC 产品为实现对企业内部安全管理的全面监控，在数据采集方面支持更加全面的采集范围。

针对传统事件(event)的采集,NGSOC 可以支持对各种安全设备、网络设备的 syslog 和 flow 日志进行采集，并能够提供适配 linux 与 windows 双平台的专业 Agent 针对数据库、系统日志、中间件日志、其他文本日志提供全方位的采集。

在传统的事件(event)采集外,还支持原始流量行为的还原与采集,区别于 netflow 等采样式流量采集方法,NGSOC 使用专有的流量采集设备-流量传感器对流量中的会话行为、事务、应用动作进行还原并形成相关日志进入存储和分析环节。由于并无采样，所以 NGSOC 能够还原的流量日志可以更加完整的还原流量行为，不存在类似 netflow 的丢具体会话信息的情况。

在传统事件信息、流量行为日志以外，NGSOC 还能对接来自 360 企业安全集团天擎终端安全管理系统的各种终端行为日志，目前能够采集包括终端进程流量行为、终端文件行为、U 盘文件传输、邮件文件传输、IM 文件传输等行为日志，由于终端日志相比网络日志更加具体、可以帮助分析人员发现启动恶意进程的相关文件，所以在整个威胁的发现、回溯过程中也会体现重大价值。

3.2 大数据基础架构

更全面的日志采集，即带来了分析的便利也带来了性能的烦恼。传统 SOC 产品在 10 亿条日志规模下会出现性能的剧烈下降，该问题主要受限于传统 SOC 产品普遍使用的关系型数据库自身设计上的局限性。如果由该架构实现来承接流量日志和终端日志，甚至是操作系统日志都可能导致灾难性的后果。为解决相关问题，NGSOC 产品在国内开创性的使用了大数据基础架构更替了传统的数据存储和计算方式。

为解决海量数据的快速存储和读取问题，NGSOC 产品使用了分布式全文检索技术，该技术可以在日志入库前针对日志建立全文索引，并进行分片存储于多台设备或多块磁盘。系统在进行日志查询时可以将对应查询指令分发到多台设备执行，并利用大内存再次提升检索性能。最终 NGSOC 产品可以面向千亿条日志提供存储查询功能，查询效率为秒级。

在海量日志场景下，数据的可靠性成为另一难题。NGSOC 产品可以将接收到的日志进行自动备份，并进行分片，再存储于不同的磁盘。通过该实现可以保证任意一块硬盘损坏后系统数据不丢失，可恢复。同时系统提供了良好的扩展机制，存储和计算能力都支持即插即用式的扩展，所有存储和计算的负载均衡均在后台自动处理，无需人工干预。

3.3 专业化日志搜索分析

用户的业务场景千差万别，针对用户不同的数据统计及呈现需求，传统 SOC/SIEM 产品往往需要通过定制化开发实现，将极大增加交付及维护成本。NGSOC 产品设计了专家搜索模式，将 SQL 的最佳功能与 Unix 管道语法封装为脚本命令，用户直接在搜索框里输入相关命令即可实现对海量日志的搜索、关联、分析和可视化。NGSOC 产品可提供 30 多种搜索命令，可灵活适应不同的应用场景。

例如使用功能强大的"stats"命令，以及 20 多种不同参数选项，能够计算统计数据并生成趋势。然后，在一定任何时间范围和粒度内图表化并可视化这些结果和统计数据。

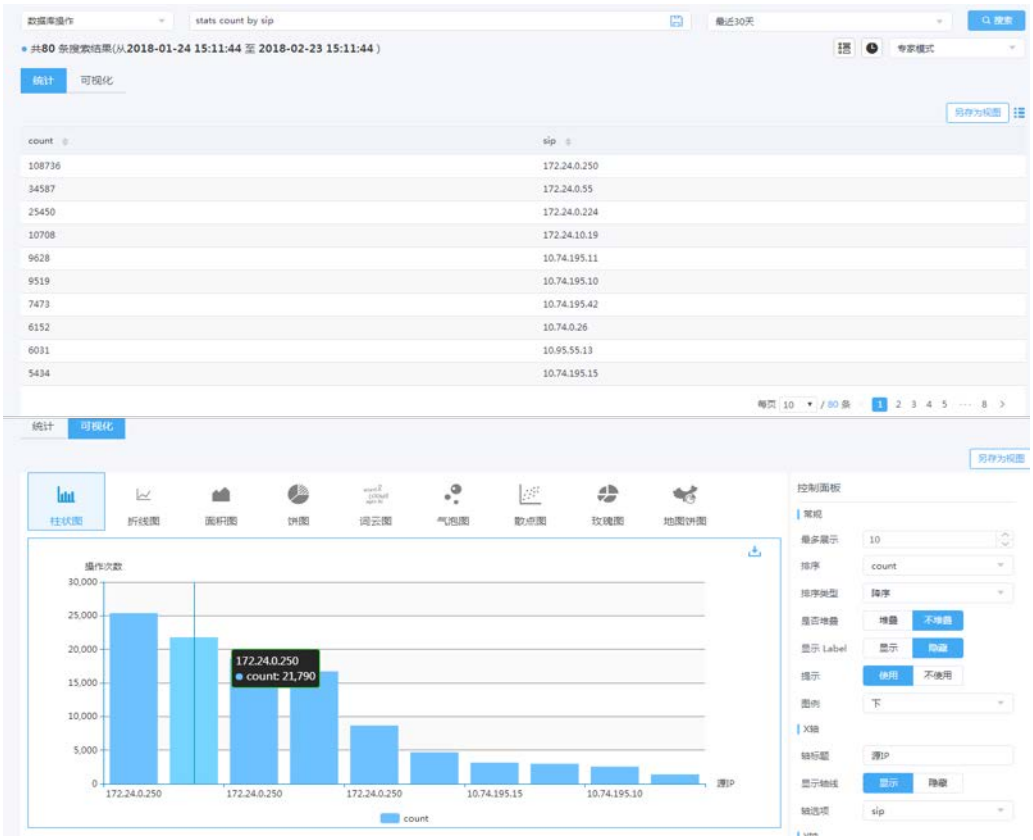


图 3 NGSOC 专家模式日志搜索结果呈现

3.4 高性能关联分析

关联分析作为传统 SIEM 产品的必备功能，往往承担了威胁发现的主要职责。但与定位相左的现实情况是，传统的关联分析往往仅能提供 3000EPS（Event per Second）到 5000EPS 的性能，这种性能完全无法应对当前动辄上百台安全设备、上千台服务器的客户 IT 环境。

为此，NGSOC 产品重新设计了关联分析的核心引擎，将 CEP（复杂事件处理）的技术实现结合安全业务场景进行了大量的实现加速、逻辑优化，最终可以提供 20000EPS（50 条规则）的关联性能。同时在关联规则引擎中独创性的加入了流量日志关联功能，用户可以将流量日志引入到关联分析过程中，通过回溯任务的方式对流量中的历史行为进行规则化分析。

3.5 丰富的威胁情报

传统 SOC 产品经过多年发展，可以面向用户提供全面的安全管理功能，但对于真正威胁的发现、分析、处理上并无法提供更多的知识输入，相关高级威胁的检测更多地还是依赖于 IPS 或 APT 检测类设备实现。为了解决相关问题，NGSOC 产品引入了 360 企业安全集团的核心威胁情报数据，可以通过失陷类威胁情报直接对高级威胁或 APT 攻击进行检测和跟踪、并使用云端威胁情报中心的海量数据情报对各种告警中的 IP、域名、文件 MD5 进行进一步分析和解释。

威胁情报的使用，直接可以扩展客户的安全视野，通过使用 360 企业安全集团的知识储备帮助客户理解自身的安全状况和突发情况的处置方式。而目前 360 企业安全集团开放的失陷类威胁情报中相关失陷指标数量多达数万条，同时保持着每天更新的快速更新频率以保证对高级威胁的及时跟踪。这些失陷类威胁情报中包含了 360 实时跟踪的几十个 APT 组织的活动信息，还有大量黑产使用的高级攻击方式。在云端威胁情报中心，360 更是提供了多达数亿的恶意样本的查询、全球域名 whois 信息查询、域名判定标签、IP 归属地及相关样本等高价值信息。

同时 NGSOC 产品也支持用户威胁情报的自定义和第三方威胁情报（OpenIOC、STIX 格式）的导入，通过这种方式可以为客户提供更加灵活和开放的失陷类情报管理。

3.6 精准的多维度威胁检测

企业用户经常会淹没在各种 IDS、WAF 设备的安全告警中，而这些告警的分析、处置往往成为另一头疼的问题。在这方面，传统安全管理产品往往会通过过滤、归并、关联等方式实现一定程度的告警量下降。但依靠这种方式无法对真正威胁做到有效追逐，因为告警的准确度会受限于 IDS 或 WAF 等检测设备的实现情况和告警的过滤、归并手段。任何一个环节有问题都将导致大量误报或漏报出现。而且传统检测技术更加侧重于所有攻击企图的发现，无法有效鉴别哪些攻击是真正造成恶劣影响的、是需要处理的。

为了解决相关问题，NGSOC 产品采集了大量的原始日志和流量信息，相关数据会经过多维度的检测手段进行分析，以帮助客户判断真正的威胁在哪里。除了关联分析、失

陷类情报关联以外，NGSOC 产品还使用了网站漏洞利用检测、WEBSHELL 检测、远控检测等一系列手段。

网站漏洞利用检测

NGSOC 产品可以依靠来自于机器学习算法的语料库规则对 WEB 攻击进行高精确度判断，再结合语义检测和动态响应特征检测技术，可以实时的发现利用成功的 WEB 漏洞攻击行为。通过该实现可以对 WEB 安全进行及时预警，也可解决海量 WAF 日志但无重点的问题。只要出现相关 WEB 漏洞利用告警，安全管理人员需要迅速做出相关响应动作。

WEBSHELL 检测

利用轻沙箱检测机制和控制指令监控功能，NGSOC 可以对 WEBSHELL 上传、控制等一系列攻击行为进行监测和跟踪，对 WEB 主要威胁进行针对性处理。

远控监测

通过对远控通道和指令进行监控，NGSOC 可以发现网络中存在的已经被恶意软件或黑客组织控制的主机，由于相关告警直接反映了网内主机失陷的情况，必须进行有针对性的处理，所以也是安全管理中的重要部分。

4 产品功能

4.1 威胁管理

NGSOC 产品提供面向威胁全生命周期的管理功能，可以通过多种威胁检测手段对威胁进行发现，并集中呈现全网的各种威胁情况。客户可结合各自需要对威胁进行筛选、标记、处置。同时 NGSOC 产品也支持针对威胁的处置工单下发，管理者可以指定对应威胁的处置责任人，通过邮件、短信、消息中心等方式进行通知，由其对威胁进行处理，并跟踪工单流转状态。NGSOC 产品也支持根据设定的动作进行自动化通知下发告警，提升日常运营工作的效率。如果方案中包含 360 天擎终端安全管理系统，还可以对其进行威胁情报告警的通报以推动相关 EDR 处置组件的运行。系统支持对威胁告警自定义各种维度的可视化统计分析，这些维度包括源 IP、目的 IP、危害等级、告警类型、告警状态、关注点、告警 IOC、单位等，可以进行两个维度的对比使用，统计出各种维度的告

警数量。用户可以生成各种所需维度的视图并进行展示，展示方式包括统计视图，视图种类包括柱状图、折线图、条形图、面积图、饼图、词云图、玫瑰图、表格等。同时可视化的告警视图可以被仪表板及报表系统调用。针对告警用户可以指定告警加白策略，指定哪些条件下的告警内容不进行告警展示。

4.2 资产管理

资产管理是 NGSOC 的重要功能模块，NGSOC 产品能够提供对网内资产的扫描发现、手工管理、资产变更比对、资产信息整合展示等基本功能。资产发现部分，NGSOC 可以通过 IP 扫描、SNMP 扫描、流量发现等手段对网内 IP 的存活情况进行跟踪，一旦发现超出当前管理范围的 IP，用户可以导出相关数据进行编辑再录入资产数据库。而对于已经录入资产数据库的资产，用户可以通过分组、标记等方式对资产作更加细致的管理，NGSOC 也会提供长期的服务、流量、威胁相关的监控，所有资产相关的监控数据在资产详情页均可查看。而且为了方便用户快速掌握资产信息，NGSOC 产品上任何一个威胁如果涉及到资产信息，用户均可直接在告警上查看到相关资产的基本信息并能够快速切换到资产页面查看对应详情。资产详情中将展现资产属性基本信息、资产相关告警信息、资产相关漏洞信息及资产相关账号信息，可视化呈现资产的多维度信息。系统支持对资产自定义各种维度的可视化统计分析，这些维度包括资产 IP 地址、资产组、责任人、责任部门、网关标识、操作系统类型、权重、厂家等，可以进行两个维度的对比使用，统计出各种维度的资产数量或待处置漏洞。用户可以生成各种所需维度的视图并进行展示，展示方式包括统计视图，视图种类包括柱状图、折线图、条形图、面积图、饼图、词云图、玫瑰图、表格等。同时可视化的资产视图可以被仪表板及报表系统调用，

4.3 拓扑管理（收费模块）

NGSOC 产品支持对企业网络拓扑进行扫描和发现，用户可以将管理好的资产直接添加到任何一个自定义网络拓扑中，并对拓扑进行相关编辑。在拓扑管理页面，用户可以连接任意资产、调整拓扑的展示布局、隐藏连接关系、隐藏资产名称、查看资产详情，完成拓扑绘制相关的所有工作。同时为了实现逻辑拓扑和实际拓扑的映射，NGSOC 产品提供了实际拓扑与逻辑拓扑图映射的功能，用户可以将实际拓扑上的关键设备映射到逻

辑拓扑图上的指定区域，以此帮助用户快速理解实际拓扑对应的管理责任。拓扑管理生成的拓扑图在态势感知模块中将作为重要展示元素结合风险值进行展示，以从宏观层面体现企业内网的安全情况。

4.4 漏洞管理（收费模块）

NGSOC 产品能够支持直接调度指定厂家的漏洞扫描器及人工漏扫报告，实现扫描任务的创建和下发。同时 NGSOC 产品支持导入多种厂家的漏洞报告，并且支持灵活自定义的漏洞报告解析规则，可以轻松适配不同客户的漏洞管理需求。对于导入的漏洞，NGSOC 产品将按照资产的情况进行漏洞的归并展示，帮助用户直观的掌握资产漏洞情况。漏洞详情描述支持关联查询漏洞知识库，漏洞详细信息为处置提供依据。NGSOC 产品支持针对漏洞进行处置状态管理、处置任务的工单下发，实现漏洞的闭环管理。系统支持对漏洞自定义各种维度的可视化统计分析，这些维度包括资产 IP 地址漏洞名称、发现时间、CNNVD 编号、CVE 编号等，可以进行两个维度的对比使用，统计出各种维度的漏洞数量。用户可以生成各种所需维度的视图并进行展示，展示方式包括统计视图，视图种类包括柱状图、折线图、条形图、面积图、饼图、词云图、玫瑰图、表格等。同时可视化的漏洞视图可以被仪表板及报表系统调用。

4.5 日志搜索

NGSOC 产品提供了三种针对事件/流量日志/终端日志的查询、检索模式，分别为快捷模式、高级模式及专家模式。用户可以使用快捷模式对日志中的各种字段进行查询。高级模式中支持与或非等逻辑语法，精确匹配、模糊匹配、通配符查询多种匹配方式，同时支持时间段、地址区间、数值范围等一系列区间查询，为用户提供了多样化的查询条件。NGSOC 产品创新提供了专家模式搜索，通过学习成本较低的类 SQL 数据分析语言，实现数据累加求和、排序、筛选、剔除重复数据、计算差值、替换空值、格式化、提取正则表达式、比较差异、计算相关性等统计计算功能，并支持查询结果的可视化展现，提供柱状图、折线图、面积图等 10 余种常见图表的配置展现。可下载或另存为视图供仪表板引用呈现。

为了方便用户的查询操作，NGSOC 提供搜索欢迎页面和搜索帮助中心，可快速了解快捷模式、高级模式、专家模式的使用说明和搜索结果字段说明。同时支持搜索规则的收藏和搜索历史记录。NGSOC 也提供了快速筛选和字段统计功能，每次查询完成后，NGSOC 产品都会形成搜索结果的时间轴分布图，用户可以直接在图表上通过拖拽进行时间段的筛选。用户也可以针对任意字段进行追加查询、撤销查询等操作对现有查询结果进行进一步过滤。由于系统架构的升级，所以以上查询功能都将在 1 分钟内返回查询结果。

4.6 场景化分析（收费模块）

场景是指在特定的主题下，通过一系列图、表等可视化手段，依据攻防等经验构造的数据展示形式。场景化分析旨在提供用户相关的视角来查看相关数据，为其发现、判断网络安全问题提供帮助。解决了规则判定时，无法确定具体阈值的问题，用户可根据自己网络特点和经验进行判断。NGSOC 可提供丰富的场景化分析结果呈现，包括内网安全、VPN 安全、账号安全及邮件安全等。

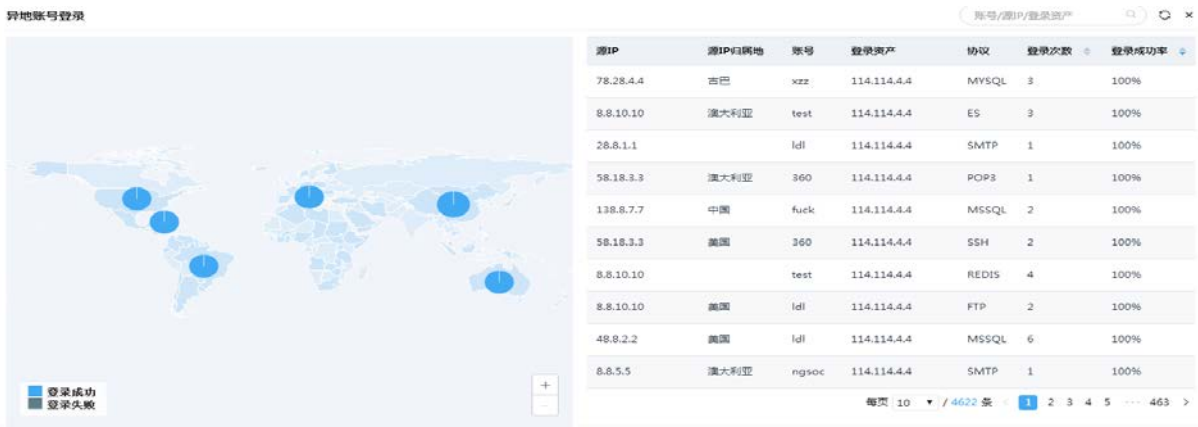


图 4 NGSOC 场景化分析功能呈现效果

4.7 工单

NGSOC 产品可提供流程化的工单管理功能，能够派发或接收针对威胁告警和漏洞的处置工单，并对与责任人相关的工单流转状态及处置进展进行跟踪。同时 NGSOC 产品支持根据待处置内容定义工单的级别及通知方式，可查看、编辑处置内容和工单任务，也支持对处置中的工单任务进行撤销及根据查询条件批量导出工单列表。

4.8 调查分析（收费模块）

在企业的日常安全管理中，安全工程师经常需要不断地对安全事件进行分析、定性、处置。这一系列工作中都需要广泛的调取各种数据信息以保证每次判断都是有事实依据的，而传统的 SOC 产品均忽略了相关功能，安全工程师只能以纸质报告和截图代替。为此 NGSOC 产品特别开发了调查分析模块。用户可使用该功能针对任何需要调查的安全问题创建实例（case），将所有与要调查的问题相关的告警、日志、甚至其他文本、图片信息都录入 case 中，然后通过时间趋势展示、标注等功能可以回溯并记录问题的发展过程和相关影响，再通过搜索等功能不断的扩展其他的日志线索，丰富该问题的相关证据。最后在有支撑的情况下形成调查结论。

4.9 知识库（收费模块）

NGSOC 产品提供知识库功能，预置漏洞知识库等，漏洞知识库可根据漏洞名称、漏洞类型、CVE 编号、CNNVD 编号进行快速查询搜索，同时支持对漏洞扫描报告结果详情进行关联查询，也允许用户在系统使用过程中不断丰富和完善知识库。

4.10 报表管理

NGSOC 产品可以提供灵活的报表管理功能，可以支持快速报表，实时的输出期望的报表内容，也可按照客户指定的周期自动生成报表以帮助用户周期回顾安全情况。同时系统提供了报表模板的灵活编辑，用户可以根据自身需要在数十个预置报表展示内容中选择自身需要内容，调整顺序以形成自身需要的报表。对于用户定制化的报表内容，360 企业安全团队可以根据情况进行报表定制以应对用户报表需要。

4.11 仪表展示

NGSOC 产品能够提供人性化的首页仪表板展示，用户可根据个人需要创建自己的仪表板，通过拖拽、拉伸等交互调整仪表板上每一个展示内容的布局和大小，以形成用户化的仪表板展示。同时用户可以选择是否将相关仪表板设置为首页、分享给其他用户。仪表板上目前预置了几十种具体展示内容，其中覆盖了威胁统计、资产统计、日志统计、

漏洞统计、工单分析等多个方面，可以帮助用户宏观的查看或监控整个企业的安全情况和 NGSOC 系统的工作情况，而且用户可以直接通过仪表板跳转到对应功能页面，实现由宏观到微观的工作流程。

4.12 态势感知（收费模块）

安全问题纷繁复杂，如何整体查看企业的安全情况并作出准确判断一直以来是安全管理的难题。NGSOC 产品可以在多种安全功能基础之上提供态势感知模块。该模块可以帮助用户快速的、宏观的了解整个企业的安全情况。目前 NGSOC 产品可以提供资产风险态势感知、外部威胁态势感知、网站安全态势感知三部分模块。

资产风险态势感知：按照不同的资产分组展示资产风险以及对应在逻辑拓扑上的安全问题分布、威胁变化趋势，帮助用户快速掌握风险的分布以及变化，有针对性的进行处置动作。

外部威胁态势感知：可以展示所有来自于企业外部安全威胁的攻击来源地分布，支持 3D 地球和 2D 地图切换展示，轻松掌握外部威胁趋势、威胁的主要分类、主要来源国，内网资产威胁，可以帮助用户快速感知外部威胁的攻击分布和攻击重点。

网站安全态势感知：用户购买使用网站云监测产品和网站安全态势感知系统后，可在 NGSOC 上直接调用网站安全态势感知系统大屏，大屏包括安全事件概况、网站安全态势感知、网站资产安全态势感知、事件详细信息态势感知等内容，可以第一时间感知网站篡改、挂马、黑词、暗链、漏洞、DDoS、可用性、网站钓鱼等网站安全威胁，并进行处置。

在常规态势感知以外，不同用户经常有自身的感知需求，360 企业安全可针对不同场景进行态势感知定制。

4.13 级联管理

级联管理提供了 NGSOC 分析平台的分级部署模式，可面向用户多分支单位进行多分析平台的级联部署及管理，级联部署可制定多分析平台的上下级关系。在级联部署中由上级平台集中维护各级平台的单位信息，并以单位为视角集中获取下级平台的告警数据，告警数据可在告警管理模块中按单位进行分组并向用户呈现。下级单位对告警的处置状

态也会自动同步到上级平台，使上级单位实时掌握下级组织中告警问题的解决情况。多级管理支持通过权限控制指定用户角色对下级告警的监视范围。

5 服务支持

5.1 安全规则运营服务

NGSOC 产品团队可以为客户提供事件解析文件编辑、关联规则编辑等安全运营服务，相关安全运营服务可有针对性的结合客户的业务或网络情况进行。通过服务的方式将 360 企业安全集团丰富的安全知识固化为企业客户的各种规则，输出高价值告警信息。接收 360 知识输入的同时，NGSOC 对客户的技术要求也会随着服务的引入而迅速降低，用户仅需要对运营服务人员提出有客户特色的管理要求或威胁判定标准，安全运营人员可自行转化为系统规则执行。

5.2 驻场运营服务

360 企业安全集团安全服务团队可在 NGSOC 产品上线后的持续运营阶段提供驻场运营服务，主要协助用户运维人员，从事 NGSOC 平台的日常告警处置、定期统计报告、流量分析、安全规则调优等工作，与后端产品专家和安全专家建立快速响应通道，能够做到事件的及时反馈与处理，提升安全运营工作效率。

5.3 威胁分析服务

360 企业安全集团安全服务团队可针对 NGSOC 产品提供威胁分析服务，该服务可以通过定期定次的服务方式帮助用户梳理已经采集到的流量日志信息，利用产品中提供的各种工具和接口对隐藏在流量中的攻击行为、失陷信息进行挖掘，发现企业面向互联网的攻击包路面，并结合 360 独有的数据信息为客户提供高级威胁告警的深入分析与判定。所有服务内容都将以报告形式详细的提供给客户。

6 应用价值

6.1 安全监控的范围更大

依赖于强大的大数据平台架构支撑，以及全面的日志采集能力，NGSOC 可以帮助企业客户对 IT 基础设施进行更广泛的安全监控。企业客户不用再纠结于现实中的数千台资产与传统 SOC 凌弱性能之间的矛盾，可以更细致、更全面的采集原始日志信息。即使出现存储空间或计算性能不足的情况，仍然可以通过水平扩展的方式快速的线性提升能力。

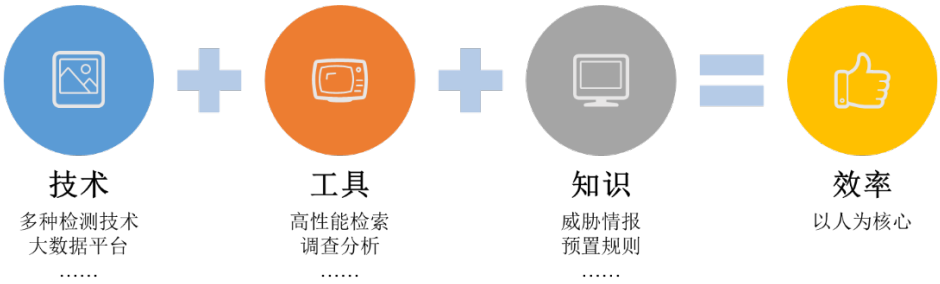
更广阔的监控范围将直接影响 NGSOC 产品的使用，它可以为威胁发现、态势感知提供基础数据支撑。NGSOC 产品之所以能够更及时、更准确的发现威胁，正是因为日志采集上并未遗漏那些可能记录威胁发生过程的日志。而相关日志的存储也可以帮助企业客户应对日志审计的合规检查。

6.2 威胁发现及时性提升

利用多种新型威胁监测手段，再结合威胁情报的使用，NGSOC 产品能够比传统 SOC 或 SIEM 产品更快的发现隐藏在各类日志中的安全问题。而借助于威胁情报中的 APT 类情报，NGSOC 还可对国际上 30 多个 APT 组织的入侵和活动行为进行跟踪，在被上级通报前主动发现问题。更早的发现威胁一方面可以帮助企业或单位在安全管理上更为从容，无需面临可能被通报追查的窘境，另一方面可以留下更多挽回损失的机会，为快速的弥补安全问题提供宝贵的时间窗口。

6.3 安全管理效率提升

NGSOC 产品注重技术、工具、知识三者的结合，希望以此推动安全管理效率的提升。



技术层面，NGSOC 不仅能够快速的发现威胁，还能够发现那些确认度更高的威胁。威胁确认度能够帮助安全工程师更容易的分辨不同威胁之间的重要度，对于那些确实已经造成恶劣影响的、已经绕过安全防御体系的威胁，可以采取更有针对性的处置动作，而对于那些失败了的攻击企图，完全无需耗费过多精力。通过告警确认度的提升，安全管理的效率相应的也会得到提升。

除了威胁管理的效率提升，NGSOC 还提供了高性能的日志检索查询工具和调查分析工具，可以极大的提升分析人员的分析效率。安全分析人员可以使用 NGSOC 灵活的、高效的进行数据分析，摆脱传统 SOC 一次查询需要等 10 分钟的噩梦，可以顺畅连续的进行数据下钻，搜索。同时可以对任何一条有意义的日志进行标记、记录、拓线，形成调查分析结论，一扫纸质分析报告的烦恼。

安全分析中，经常会面临知识缺乏而导致的分析无法进行或深入的情况。NGSOC 集成了 360 企业安全集团的威胁情报中心（https://ti.360.net/）接口，安全分析人员可以对 NGSOC 上出现的 IP、域名、文件 MD5 进行深入的情报判定，以此获得覆盖全球的安全知识数据。此外 NGSOC 产品内置了大量的关联分析规则，也可为用户提供广泛的规则配置指导。

6.4 降低宏观安全理解成本

安全管理并不如网络、业务等内容更容易被管理者理解，因为安全所涉及的技术内容纷繁复杂，存在天然的技术屏障。但同时，安全管理经常会涉及到多部门的重要业务或全公司的 IT 运行，此时安全又体现出其至关重要的一面。

传统 SOC 会借鉴风险管理的思路，依靠对资产的梳理、威胁预测、脆弱性评估等一系列手段实现风险级别的判定，但由于其更注重数值体现，而忽略了宏观图形展示，仍然难以让管理者快速理解并判断当前安全态势。

使用 NGSOC 后，用户可以直接通过态势感知模块直观的查看企业内部不同资产组的风险分布，相关风险值会在逻辑拓扑上直接映射，可以将风险以可视化的形式呈现的大屏幕上。外部威胁的攻击态势则能直接以地图展示的方式帮助管理者理解外部攻击的主要来源地，主要的外部攻击分类、本地最容易被攻击的资产等信息。所有态势感知的展示都可实时刷新，及时的将最新的安全态势呈现在管理者眼中。