17-08-C2-ZN

新一代 SOC 研究报告

技术指南

版权声明

免责声明

前言

近几年，威胁和风险环境已经发生了巨大的变化，主动攻击行为与高级攻击技术（APT）的复杂性不断升级。而随着云计算与大数据技术的发展，新一代的高级安全技术和防护策略也取得了快速发展，比如以风险或杀伤链为基础的方法，大量利用了威胁情报和大数据分析技术。这就要求传统的安全运营中心（SOC）来适应这些新的变化，企业需要认识到传统的以防护为核心的策略已经失效，企业资产可能已经被破坏。企业安全体系必须切换到以监控和响应为核心，通过持续监测，及时响应来减轻和限制攻击造成的损失。

新一代安全运营中心（SOC）必须以数据和情报驱动，采用自适应安全架构来进行环境和态势感知，通过自动化或半自动化工具、流程和策略来对抗新一代威胁。

本报告描述了新一代 SOC 的基本要素，介绍了 SOC 的技术实现原理，探讨了 SOC 运营体系的能力建设、重点和难点，以及在不同场景不同层面上，协助包括基础作业层、专业技术层和管理决策层用户等人员更好地完成安全工作，并此基础上结合整体防御体系探讨了 SOC 的未来发展趋势。

本报告由安全牛顾问团队，通过调查国内在新一代 SOC 相关技术产品上做的较为突出的公司，并结合当前最新的相关资料撰写。

关键发现

- 预计到 2020 年，以数据和情报驱动的新一代 SOC 为中心的市场占有率将从现在的 5% 提升到 50%；
- 新一代 SOC 将遵循大数据化、情报驱动、多维度化、智能化、交互化、可视化、协同化等理念进行建设；
- 新一代 SOC 将成为企业安全能力中心，具备安全防御、持续监测、快速响应、溯源取证、风险预警等能力；
- 新一代 SOC 必须采用大数据平台架构，来提升数据的分析和处理能力；
- 新一代 SOC 应采用来自多个来源的战略级和战术级威胁情报；
- 新一代 SOC 应具备大数据安全分析能力，通过机器学习提升分析能力；
- 新一代 SOC 尽可能实现安全运营的自动化；
- 新一代 SOC 采用了自适应安全体系架构；
- 新一代 SOC 采用主动威胁溯源和调查技术；
- 新一代 SOC 可应用在微观运营、中观管理和宏观决策各个层面；
- 新一代 SOC 尚面临诸多的建设难点，如情报共享、团队建设、定制化等

目录

1. SOC 的定义

传统安全运营中心（SOC）是指以信息资产为核心，通过针对网络、系统、应用、安全设备的日志和报警事件进行监控和分析，建立一套实时的资产风险模型，以安全事件管理为核心流程，协助安全管理员进行事件分析、风险分析、预警和应急响应处理的集中安全管理系统。

SOC 从名称来看：

S->Security（安全），即 SOC 处理的事件或流程应该是与企业网络安全相关的；

O->Operations（运营），代表着一种动态的动作，包括但不限于实时的检测和响应；

C->Center（中心），体系化的建设，多领域安全产品、服务“叠加”而成的综合防线。

传统的 SOC 主要采用安全信息和事件管理（SIEM）系统，为防火墙、入侵检测 / 保护系统、漏洞扫描等安全设备提供设备管理和监控服务。然而，让员工手动分析成堆的数据，从孤立的事件和指标中寻找联系，被证明是低效、不可持续且令人难以承受的，尤其是在数据量持续暴增，而合格的安全分析师严重不足的情况下。另外，主动攻击行为与高级攻击技术（APT）的复杂性不断升级，攻击也越来越不可检测，由于缺乏更高级的机制来连接不同的传感器和行为数据，就更加不可能检测出愈趋复杂的威胁。

因此，新一代 SOC 建设必须以数据和威胁情报驱动，采用自适应安全架构来进行情景感知、行为感知和态势感知，通过自动化或半自动化工具、流程和策略来对抗新兴威胁。SOC 建设不再仅仅是交付产品或系统，更应当交付安全能力，通过数据采集、威胁情报、分析平台、响应工具、体系建设、人员能力培养等，打造企业的新型网络安全运营中心。

1.1. 传统 SOC 的问题

众所周知，安全运营中心 (SOC) 在中国的落地一直不算成功。仅靠设备日志分析、告警事件、终端安全等工具的堆砌，缺乏足够的知识和人才来运营，难以与 IT、业务、管理层和监管等部门进行有机的联动，远没有达到成熟安全运营中心应具有的能力。

当前网络与信息安全领域，正面临着全新的挑战。一方面，伴随大数据和云计算时代的到来，安全问题正在变成一个大数据问题，企业和组织的网络及信息系统每天都在产生大量的安全数据，并且产生的速度越来越快。另一方面，国家、企业和组织所面对的网络空间安全形势严峻，需要应对的攻击和威胁变得日益复杂，这些威胁具有隐蔽性强、潜伏期长、持续性强的特点。

面对这些新挑战，传统 SOC 的局限性显露无遗，主要体现在以下几个方面：

缺乏安全攻防对抗的能力：传统 SOC 以安全日志和事件的采集为基础，被动进行事件分析和响应，没有从威胁来源和攻击者视角来分析问题。从黑客攻击杀伤链来看，检测点和响应措施严重不足；

缺乏大量数据处理的能力：传统 SOC 以关系型数据库为底层数据架构，处理能力相当有限，在当前海量数据、异构数据、多维数据的情况下，采集、分析、处理、存储遇到了很大的困难；

缺乏安全智能分析的能力：传统 SOC 以基于规则的关联分析为主，只能识别已知并且已描述的攻击，难以识别复杂的攻击和未知的攻击。并且传统 SOC 缺乏内外部威胁情报的导入，难以满足当前的攻防对抗环境；

缺乏有效响应协同的能力：传统 SOC 缺乏响应协同的工具和流程，无法做到与网关设备、终端 EDR 等联动响应，以及与企业内外部资源共享威胁情报、协同处置安全威胁；

缺乏专业人员运营的能力：传统 SOC 重在安全管理系统的建设，缺少对安全运营人员的培养，而 SOC 要想真正发挥作用，安全分析和安全运营人员的专业性必须具备。

1.2. 新一代 SOC 的理念

要想解决传统 SOC 的问题，安全牛提出新一代 SOC 建设必须遵循如下理念：

1、大数据化：数据驱动是新一代 SOC 的基本属性，必须采用大数据平台架构为支撑，支持超大数据量的采集、融合、存储、检索、分析、态势感知和可视化；

2、情报驱动：新一代 SOC 的安全分析将非常依赖安全情报。借助安全情报，可以大大提升分析的效率。安全情报分为战略层情报和战术层情报，从技术上可以分为基础数据情报、漏洞情报、威胁情报、重大事件情报等；

3、多维度化：新一代 SOC 支持多维数据源的采集，包括各类设备日志、原始流量、终端与用户行为等；覆盖预警、防护、监测、响应各个环节，能够集成资产配置库（CMDB）、漏洞管理、配置核查、身份管理等数据源，并引入外部威胁情报数据，进行积极的预警和防御；

4、智能化：新一代 SOC 需要建立起智能化的安全分析能力，通过对数据进行情境关联来丰富数据，建立业务、资产、漏洞、威胁、身份、行为等数据的关联关系，并借助高级统计技术、数据挖掘技术、行为分析技术、机器学习、人工智能等技术来实现智能分析；

5、交互化：新一代 SOC 需要支持人机交互的能力。系统应提供尽可能多的可视化的分析工具，安全分

析人员可以根据收到的线索进行人机交互查询和分析，尤其是高级安全分析和威胁追捕（Threat Hunting）；

6、可视化：新一代 SOC 应当支持资产的可视化、类攻击可视化、策略可视化、风险可视化、合规可视化、业务安全可视化以及可视化攻击分析等；

7、协同化：新一代 SOC 应当以开放 API 接口模式，支持跨组织之间的情报共享，响应协作，以及设备之间的协同响应处理。

2. SOC 能力建设

安全不是口号、不是漏洞、不是产品。安全牛认为，安全传递的是一种信任，而这种信任来自于企业自身的安全能力。**安全是一种能力，新一代企业安全观将实现“以人为本、以数据为核心、以技术为支撑”的安全能力，而 SOC 建设正是打造企业安全能力的中心。**

人是安全能力的载体，SOC 建设要重点考虑人的主观能动因素，企业的普通员工、专业技术人员以及企业管理层在安全体系中都是重要的环节，都需要培养其安全意识与安全能力。

数据是安全能力的核心，数据驱动的 SOC 将使得安全更好的融入企业的业务与管理，更好的体现安全的价值，基于数据的威胁情报共享机制也将极大的提高业界整体的安全防御水平。

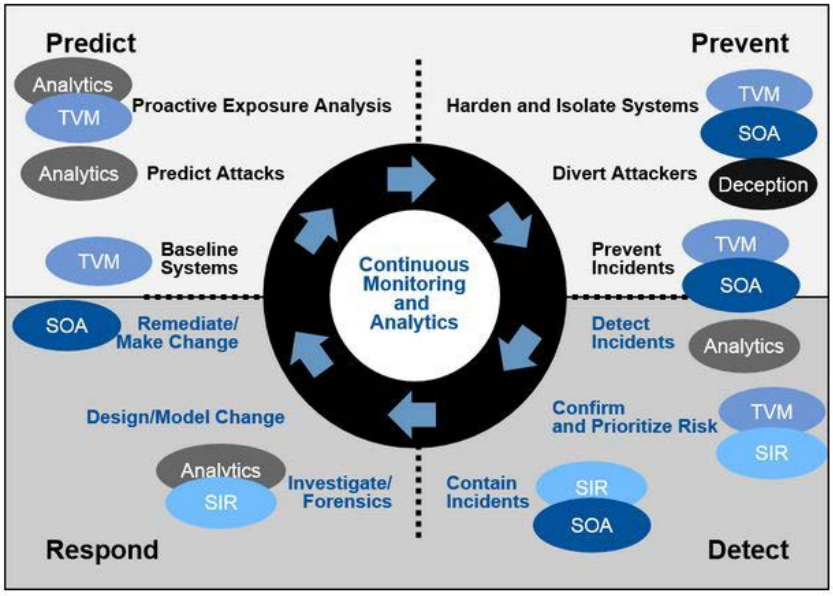
技术是安全能力支撑的工具，安全技术未来将更加深入细分到更多的业务领域，安全产品和服务将更加多样性。

安全牛建议新一代 SOC 建设的目标至少包含如下三点：

- **风险可见化：**Visibility 未知攻，焉知防，看见风险才能防范风险；
- **防御主动化：**Proactive 最好的防守是进攻，主动防御，纵深防御是设计的目标；
- **运营自动化：**Automotive 全天候自动化的安全运营才能保障安全体系的落实。

在安全牛之前发布的《企业安全能力框架设计》中，我们参考了 NIST Cybersecurity Framework 的核心内容，简称为 IPDRR 模型。IPDRR 能力框架模型包括风险识别（Identify）、安全防御（Protect）、安全检测（Detect）、安全响应（Response）和安全恢复（Recovery）五大能力，可以作为 SOC 建设的参考模型。

Gartner 于 2014 年提出的面向下一代的安全体系，自适应安全架构（Adaptive Security Architecture，以下简称 ASA），也是新一代 SOC 能力建设的重要参考模型。云时代的 SOC 应该以持续监控和分析为核心，覆盖防御、检测、响应、预测四个维度，可自适应于不同基础架构和业务变化，并能形成统一安全策略应对未来更加隐蔽、专业的高级攻击。



Source: Gartner (November 2015)

2.1 安全防御

安全防御能力仍然是 SOC 最基础的能力。各类安全设备如防火墙、入侵防御、终端保护、Web 应用防火墙等提供了基本的安全防护能力。在新一代 SOC 体系中，SOC 将为安全设备提供安全智能引擎和情报数据，采用深度防御策略，自动化协同安全能力，并逐步实现安全策略的可视化。

新一代 SOC 的安全防御能力建设包括：

（1）与企业资产管理系统集成，打造自动化的信息资产识别与管理能力；尤其针对数据资产，构建数据资产识别、分类分级、安全防护的能力；

（2）由于边界安全防护逐步失效，新一代 SOC 需要构建微边界的保护能力，与容器技术结合，针对每个服务、应用和数据进行安全防护；

（3）增加网络沙箱和云端沙箱，实现恶意代码的深度防御；

（4）与漏洞扫描与管理产品结合，实现资产漏洞和补丁的自动化管理；

（5）与基线安全产品结合，在服务器端实施基线安全策略；重要服务器增加白名单保护措施；

（6）终端保护策略纳入 SOC 运营体系；

（7）提供威胁情报交换平台与数据，为各类安全设备提供智能化防御能力；

（8）引入欺骗防御技术和产品，快速定位和隔离攻击者。

2.2 持续检测

持续检测和监控能力是新一代 SOC 最重要的能力升级。可见性（Visibility）一直是这几年安全行业共同追求的目标，由于云计算与大数据等技术的成熟，新一代 SOC 具备了处理大规模数据的能力基础，从而能够实现安全持续监测。

新一代 SOC 的持续检测和监控能力建设将包括：

（1）采用大数据平台架构，大大提升数据处理的能力；

（2）增加网络流量分析（NTA）技术和产品，大大提升对 APT 的检测能力；

（3）增加针对 DNS 访问数据（pDNS）采集和分析的技术，提升对恶意代码、僵尸网络、APT 等的检测能力；

（4）采用用户与实体行为分析（UEBA）技术和产品，检测内外部用户的恶意行为；

（5）增加终端检测和响应（EDR）技术和产品，提升对恶意代码的检测能力；

（6）采用威胁情报平台（TIP）技术和产品，与业界进行威胁情报数据的共享，大大提升威胁的检测能力和响应速度；

（7）与资产、业务和管理结合，提供多层次的实时风险监测能力；

（8）打造合格的安全分析师队伍，持续针对威胁线索进行人工交互分析，及时发现安全事件并进行处理。

2.3 快速响应

快速响应能力建设是 SOC 能力建设的重要一环。发现任何可疑行为或攻击行为时，SOC 应当自动调配安全响应团队进行事件响应，将技术、流程、人员有效结合起来，并提供自动化的设备联动能力，从而实现快速有效的应急响应能力。

因此，新一代 SOC 的快速响应能力建设包括：

（1）采用事件响应平台（IRP），收到安全报警后可实现自动化编排响应行动，提供有价值的情报和事件上下文，并能对复杂的网络威胁作出自适应响应；

（2）针对各类异常或攻击事件的复杂性，设计各类安全事件的动态响应预案，平台可根据事件触发的

条件，自动形成安全响应的步骤分发给企业的安全相关人员；

（3）应能与各类 SIEM、IT Help Desk 系统集成，自动或手动触发响应工单，实现安全策略变更和控制，如关闭漏洞、关闭网络端口、升级系统配置、修改用户权限或者提升信息防护的强度等；

（4）逐步做到与安全设备联动，自动化分发安全策略，实现自动响应。

2.4 溯源取证

溯源取证能力是新一代 SOC 能力建设中需要加强的。传统 SOC 由于缺乏相关的手段，无法做到对攻击者的溯源取证，而现在随着威胁情报、攻击欺骗、高级分析技术等发展，已经具备了对攻击者进行深入分析，形成攻击者画像，和溯源取证的能力。

新一代 SOC 将重点打造威胁追捕（Threat Hunting）的能力。

（1）威胁追捕是指采用人工分析和机器辅助的方法，针对网络和数据进行主动的和反复的搜索，从而检测出逃避现有的安全防御措施的高级持续性威胁攻击（APT）。

（2）使用威胁追捕平台提高了高级威胁的检测能力、增加了寻找威胁的新方式、发现了他们之前没有发现过的威胁、减少了调查时间等。威胁追捕平台的特点是使用机器学习方法来进行自动决策，调查取证和自动分析。

威胁追捕类型	描述
假设驱动	这种类型的威胁溯源是先基于一个假设，比如假设攻击者是一个已知黑客团体的 TTP，或者某个竞争对手
IOC 驱动	根据攻击的数据和相关 IOC，从已知攻击者 IOC 库中进行深入调查和分析
分析驱动	采用高级分析技术、机器学习、人工智能等技术来辅助识别

（3）所有攻击者都有签名，用以识别攻击者的身份和攻击方式，这些签名包括攻击者的 IP 地址、网络 / 主机指纹信息，攻击工具以及战术、技术和程序（TTPs）。总的来讲，这些方法统称为 IOC（Indicators of Compromise），通过识别和使用相关的 IOC，追捕者们可以使攻击者的攻击增加阻碍，使得攻击更加耗时、成本更高或者更加困难。追捕者通过行为分析和收集到的情报，挑选出 IOC，查明并阻止攻击者潜在的攻击行为。

2.5 风险预警

风险预警能力是新一代 SOC 实现闭环的重要能力。预测能力使安全系统可从外部监测黑客行动，主动预

测对现有系统和信息具有威胁的新型攻击，主动评估风险并优先解决暴露的问题。该情报将反馈到防御和检测功能，从而构成整个处理流程的闭环。

新一代 SOC 的风险预警能力建设将包括：

（1）主动对企业信息资产进行风险评估、预测威胁；
（2）持续更新，对终端、服务器、云服务、端口、进程等设定安全基线；
（3）对安全漏洞的发布进行跟踪分析，有能力预测重大漏洞可能引起的攻击；
（4）通过威胁情报共享，及时发现同行业的攻击行为，并提前做好攻击预警；
（5）通过检测黑客意图、关注黑客市场和新闻，培养对信息的敏感性，以帮助企业调整安全策略应对未知的攻击。

3. SOC 技术实现

新一代 SOC 中的技术平台是一个由多种技术和产品关联集成在一起的大型安全系统，该系统通过融合管控网络设备、主机系统、业务应用、安全设备、流量检测等各类产品，对各类安全相关数据进行汇聚、存储、关联分析、统计分析、数据挖掘、风险分析等，通过自动化分析与专业团队人工交互，发现真正的安全威胁，并提供自动化响应的工具平台。

SOC 系统应具备大数据处理分析、安全智能分析、实时风险计算、安全态势分析及数据可视化能力，协助用户掌握全局的网络安全态势，实时监测网络中的安全攻击事件，调整网络安全产品的安全策略，及时应对网络安全威胁，构建安全的网络空间。

根据 SOC 的能力建设要求，SOC 应具备的关键功能模块包含基础设施安全防御，大数据采集存储管理，大数据安全高级分析，威胁情报交互共享、安全威胁溯源与预警、安全事件响应调度、安全态势分析等。

3.1 SOC 平台架构

SOC 的有效运营依赖于人员（People）、流程（Process）、技术（Technology）的高度融合。SOC 的平台架构也需要融合多种 IT 和安全技术。

新一代 SOC 的平台架构包括：

1、数据采集平台

2、大数据存储与计算平台

3、大数据分析引擎

4、威胁情报平台

5、可视化展示与分析

6、威胁溯源 / 追捕平台

7、自动化响应平台

8、风险分析与预警平台

同时，SOC 还将与众多第三方 IT 和安全系统工具进行集成，包括资产管理（CMDB）、漏洞管理（TVM）、终端检测响应（EDR）、身份管理系统（IDM）、用户与实体行为分析系统（UEBA）、流量分析系统（NTA）、风险管理平台（GRC）、工单系统（Service Desk）等。

3.2 数据采集建议

SOC 平台的数据采集是进行安全分析、监测和响应的基础。新一代 SOC 的大数据处理能力使得我们可以采集更多的安全相关数据。当前 SOC 的数据采集并没有相关的标准，主要根据业务场景需求和安全分析的需求来决定采集哪些数据。

我们建议 SOC 的数据采集可以包括 IT 资产数据、IT 资产监控指标数据、IT 资产的日志和报警数据、网络流量数据、威胁情报数据，以及支持第三方产品相关数据的导入等。根据各厂商提供的资料，我们给出一些

基本的数据内容供大家参考。

IT 资产监控数据（可从网管系统导入）

设备对象	监控指标
网络设备	设备名称、IP 信息、描述、节点状态、运行时间、接口信息、路由信息、网络状态信息、网络性能信息
安全设备	设备名称、IP 信息、描述、节点状态、运行时间、接口信息、路由信息、网络状态信息、网络性能信息
虚拟化系统	ESX 的名称、IP、描述、节点状态、运行时间、CPU 利用率、内存利用率、网络状况、数据存储、磁盘 IO、虚拟机列表；ESX 中的每个 VM 的名称、IP、描述、节点状态、运行时间、CPU 利用率、内存利用率、网络状况、数据存储、磁盘 IO
服务器	名称、IP、描述、节点状态、运行时间、网络接口信息、CPU 利用率、内存利用率、磁盘利用率、磁盘 IO、文件系统、安装软件、安装服务、运行进程、 网络连接，支持自定义指标
数据库	名称、版本、端口、主机名、内存信息、运行状态、事务信息、缓存信息、连接信息、锁信息、SQL 统计、命中率信息、表空间信息、访问方法明细、数据库明细
中间件	名称、版本、端口、连通性、运行状态、CPU、内存、事务、JVM Runtime、队列、Servlet 会话、线程池、EJB、JDBC 连接
应用	邮件服务（SMTP/POP3）的连通性、响应延迟、工作状态、收发邮件速率；Lotus Domino 的连通性、命令缓存、NSF、请求、会话、邮件收发性能；WEB 应用的连通性、响应、传输、用户访问数、URL 监控；通用服务（TCP、DNS、DHCP）协议的连通性、响应时间
其它	要支持 SNMP、JMX、ODBC/JDBC 协议即可

IT 与安全设备日志数据

设备类型	常见厂商或产品
交换机	Cisco、Extreme、Juniper、博科、华为、中兴、H3C、神州数码、锐捷、博达、Force10、Foundry、F5
路由器	Cisco、Extreme、Juniper、华为、H3C、神州数码、锐捷、阿尔卡特

防火墙 /UTM/USG	天融信、启明星辰、360 网神、山石网科、网御星云、东软、方正、网神、亿阳信通、中科网威、中网、阿姆瑞特、卫士通、H3C、迪普、Cisco、Juniper Netscreen、飞塔、Checkpoint、Nokia、Bluecoat
VPN	天融信、启明星辰、360 网神、网御星云、Array、Juniper
网闸	网御星云、国保金泰、天行网安、南瑞
IDS/IPS/IDP	启明星辰、绿盟、网御星云、东软、H3C、迪普、天融信、360 网神、Cisco、McAfee、IBM、HP Tipping Point、Snort
漏洞扫描	绿盟、启明星辰、榕基、天融信、安恒
终端安全	360、瑞星、金山、北信源、冠群金辰、Symantec、TrendMicro、McAfee
Anti-DDoS	绿盟、金盾、启明星辰、天融信
WAF	安恒信息、Imperva、绿盟、启明星辰
负载均衡设备器	F5、信安世纪
安全审计系统	启明星辰、网御星云、复旦光华、汉邦、深信服
运维审计	启明星辰、齐治、谐润
身份认证	格尔、吉大正元、思科 ASA、安盟
服务器	IBM AIX 、HP-UX 、Microsoft Windows、SUN Solaris、Linux 及其变种
数据库	Oracle、SQL Server、DB2、MySQL、Informix、Sybase、国产数据库
中间件	WebLogic、WebShpere、JBoss、Apache、Tomcat、Domino
网管系统	HP OpenView NNM、IBM NetCool、CiscoWorks
存储系统	HP、IBM、EMC、VERITA
业务系统	各种用户自有的业务系统（需要定制）
其它	任意 Syslog 日志源、SNMP Trap 日志源

网络流量数据

- 网络出口和关键节点的原始流量数据（短期分析）
- 网络出口和关键节点的 netflow 数据（长期存储）
- 企业 DNS 解析记录数据等

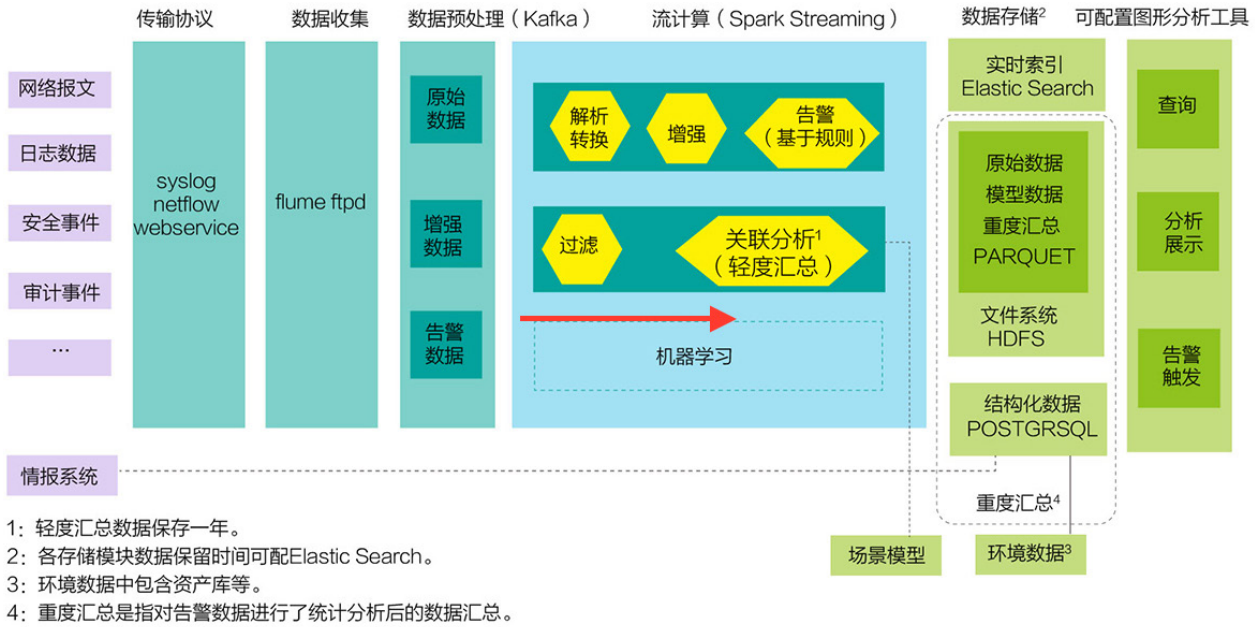
☑威胁情报数据（详见 4.5 节）

☑第三方产品数据

- 漏洞管理数据
- 配置管理数据
- 身份管理数据
- 文件完整性校验数据
- CMDB 数据等

3.3 大数据处理平台

根据安全牛的调研结果，目前国内绝大部分厂商在新一代 SOC 中采用了融合大数据的技术架构，并采用了主流的 Hadoop/Spark 等大数据分布式计算框架，我们综合业界主流的技术趋势，给出开源大数据处理平台的架构建议供大家参考。



常用大数据处理平台组件如下，SOC 应该根据具体的工作场景选择不同的组件。

• 数据采集 Flume

Cloudera 提供的一个高可用的、高可靠的、分布式的海量日志采集、聚合和传输的系统。Flume 支持在日志系统中定制各类数据发送方，用于收集数据。同时，Flume 支持对数据进行简单处理，并写入各种数据接受方（可定制）。

Flume 用作前置采集服务，采集各类日志或事件，根据情况可以是侵入式或非侵入式方式采集。

• 数据预处理队列 Kafka

一种高吞吐量的分布式发布订阅消息系统，它可以处理消费者规模网站中的所有动作流数据，目前已成为大数据系统在异步和分布式消息之间的最佳选择。

Kafka 充当实时的消息队列，通过此模块，可以完成与数据源的解耦，并且有效的平衡峰值时后台处理的能力。

• 解析转换工具 ETL

一般需要自行开发 ETL 工具从 Kafka 中接收数据，并且根据配置的解析规则和字段补全规则，完成数据的解析。最终将解析的数据存入 Elastic Search 中以便后续进行短周期的展示和统计分析。同时可以旁路一份数据留存到 HDFS 文件系统上，以便长周期的留存和离线分析。

• 流计算框架 Spark Streaming

实现微批处理，目标是很方便的建立可扩展、容错的流应用，支持 Java、Scala 和 Python，和 Spark 无缝集成。Spark Streaming 可以读取数据 HDFS，Flume，Kafka，Twitter 和 ZeroMQ，也可以读取自定义数据。

• 流计算 Spark

一个高速、通用大数据计算处理引擎。拥有 Hadoop MapReduce 所具有的优点，但不同的是 Job 的中间输出结果可以保存在内存中，从而不再需要读写 HDFS，因此 Spark 能更好地适用于数据挖掘与机器学习等需要迭代的 MapReduce 的算法。它可以与 Hadoop 和 Apache Mesos 一起使用，也可以独立使用。

通过 Spark 可以进行长周期的离线建模和 T+1 的事件分析。Spark 还会从 ES 上获取近一个月的数据进行基线告警分析。

• 分布式文件系统 HDFS

Hadoop Distributed File System，简称 HDFS，是一个分布式文件系统。HDFS 是一个高度容错性的系统，适合部署在廉价的机器上。HDFS 能提供高吞吐量的数据访问，非常适合大规模数据集上的应用。

可以将原始的事件 / 日志保存一份到 HDFS 上，以供未来进行长周期的查询。Spark 的长周期建模也依赖与 HDFS，通常需要至少一个月以上的数据进行。

• 实时搜索引擎 ElasticSearch

ES 是一个基于 Lucene 的搜索服务器。它提供了一个分布式、支持多用户的全文搜索引擎，基于 RESTful Web 接口。ElasticSearch 是用 Java 开发的，并作为 Apache 许可条款下的开放源码发布，是当

前流行的企业级搜索引擎。设计用于云计算中，能够达到实时搜索、稳定、可靠、快速、安装使用方便。

ES 保存解析及丰富化后的事件 / 日志信息，分析模型的分析结果，以供平台进行展现，溯源和关联。

• 数据库 HBase

HBase 是 Hadoop 的数据库，一个分布式、可扩展、大数据的存储，是为有数十亿行和数百万列的超大表设计的，是一种分布式数据库，可以对大数据进行随机性的实时读取 / 写入访问。提供类似谷歌 Bigtable 的存储能力，基于 Hadoop 和 Hadoop 分布式文件系统（HDFS）而建。

• 热点数据存储 Redis

Redis 是一个高性能的 key-value 存储系统，和 Memcached 类似，它支持存储的 value 类型相对更多，包括 string（字符串）、list（链表）、set（集合）和 zset（有序集合）。Redis 的出现，很大程度补偿了 memcached 这类 key/value 存储的不足，在部分场合可以对关系数据库起到很好的补充作用。

• 大数据处理能力

SOC 大数据平台的存储与计算处理能力取决于平台的架构以及硬件基础设施，应当达到：

日存储数据超过 1T，支持千亿条数据的秒级处理，PB 级数据管理与应用；

在安全日志采集方面，可实现 5-10 万 EPS（Event Per Second）的事件入库能力；

在流数据采集方面，可以实现 20 万 FPS（Flow per Second）的采集入库能力。

3.4 大数据安全分析

SOC 平台建设除了大数据处理平台的建设外，更重要的是构建大数据安全分析的模型和引擎。

基于规则的关联分析是传统 SOC 就具备的分析能力，一般是定义基于攻击场景的关联分析规则库。完全基于人工定义的关联规则只适用于较为简单的攻击场景，新一代 SOC 中需要构建新的基于机器学习的数据分析引擎，包括全文检索引擎、语义分析引擎、可视化分析引擎、交互分析引擎、数据回放引擎等，充分实现实时分析、离线数据的批量分析和迭代计算、实时和离线数据挖掘，人工交互式分析等方式。

大数据分析的五个基本方面

• Analytic Visualizations（可视化分析）

不管是对数据分析专家还是普通用户，数据可视化是数据分析工具最基本的要求。可视化可以直观的展示数据，让数据自己说话，让观众看到结果。

• Data Mining Algorithms（数据挖掘算法）

可视化是给人看的，数据挖掘就是给机器看的。集群、分割、孤立点分析还有其他的算法让我们深入数据

内部，挖掘价值。这些算法不仅要处理大数据的量，也要处理大数据的速度。

• **Predictive Analytic Capabilities（预测性分析能力）**

数据挖掘可以让分析员更好的理解数据，而预测性分析可以让分析员根据可视化分析和数据挖掘的结果做出一些预测性的判断。

• **Semantic Engines（语义引擎）**

我们知道由于非结构化数据的多样性带来了数据分析的新的挑战，我们需要一系列的工具去解析，提取，分析数据。语义引擎需要被设计成能够从“文档”中智能提取信息。

• **Data Quality and Master Data Management（数据质量和数据管理）**

数据质量和数据管理是一些管理方面的最佳实践。通过标准化的流程和工具对数据进行处理可以保证一个预先定义好的高质量的分析结果。

对于机器学习算法选择问题上，最近机器学习杂志 JMLR 上有一篇论文，作者比较了 179 种不同的分类学习方法（分类学习算法）在 121 个数据集上的性能，发现 Random Forest（随机森林）和 SVM（支持向量机）分类准确率最高，在大多数情况下超过其他方法。

大数据分析主要依靠机器学习和大规模计算。机器学习包括监督学习、非监督学习、强化学习等，而监督学习又包括分类学习、回归学习、排序学习、匹配学习等。分类是最常见的机器学习应用问题，比如垃圾邮件过滤、用户画像、文本情感分析、网页归类等，本质上都是分类问题。分类学习也是机器学习领域，研究最彻底、使用最广泛的一个分支。

大数据分析性能的好坏，也就是说机器学习预测的准确率，与使用的学习算法、问题的性质、数据集的特性包括数据规模、数据特征等都有关系。没有一种方法可以“包打天下”。Random Forest、SVM 等方法一般性能最好，但不是在什么条件下性能都最好。不同的方法，当数据规模小的时候，性能往往有较大差异，但当数据规模增大时，性能都会逐渐提升且差异逐渐减小。对于简单问题，Random Forest、SVM 等方法基本可行，但是对于复杂问题，比如图像识别，最近流行的深度学习方法往往效果更好。深度学习本质是复杂模型学习，是今后研究的重点。

在实际应用中，要提高分类的准确率，选择特征比选择算法更重要。好的特征会带来更好的分类结果，而好的特征的提取需要对问题的深入理解。建立大数据分析平台时，选择实现若干种有代表性的方法即可。当然，不仅要考虑预测的准确率，还要考虑学习效率、开发成本、模型可读性等其他因素。大数据分析平台固然重要，同时需要有一批能够深入理解安全攻防和安全管理问题，自如使用分析工具的工程师和分析人员。只有善工利

器，大数据分析才能真正发挥威力。

3.5 威胁情报共享

• 威胁情报数据分类

威胁情报共享已被证明是对抗今天复杂的网络攻击者的关键。目前，越来越多的组织积极共享威胁情报数据来得到更完整的对手活动情况，以此来帮助优化组织的网络防御。

企业应该收集的威胁情报包括：

基本数据

利用自动化和非自动化的手段，通过主动和被动的方法采集到的网络安全有关数据，例如：设备指纹、安全报警、流量日志、蜜网蜜罐记录、描述安全事件的消息等以数据形态存在的信息。

威胁指标

或可称为 IOC。常见的类型例如：与攻击有关的哈希、签名、IP 地址、DNS、IP 黑名单等等。黑名单数据库是第三方评价资源安全性的主要参考因素，或者通过 MD5 或 SHA-1 对恶意文件样本进行哈希运算，创建唯一的标示，进而形成威胁指标，验证文件、地址，定位病毒，蠕虫，木马，Rootkit，键盘记录器或其他类型的恶意代码。

威胁数据源

威胁数据源所提供的信息，可以辅助对威胁指标进行分析。它可以帮助安全分析员对攻击进行识别，同时通过对恶意软件特征分析，也可以帮助应急团队了解恶意软件的行为。

• 威胁情报平台建设

企业 SOC 建设中应当包括威胁情报平台的建设，以及威胁情报数据的获取。威胁情报包括了来自企业外部的威胁情报以及企业内部安全分析得到的内部威胁情报。

威胁情报平台应当包括如下的基本功能：

1. 情报获取：

可通过 API 数据接口获取不同来源的与企业自身资产相关的威胁情报，并进行分类、去重、汇总并实时下载到本地。

2. 情报下发

支持 SOC 通过 API 接口实时获取相关资产、漏洞、威胁的情报数据，并支持安全设备通过 API 标准化接口获取 STIX 标准格式的情报数据。

SOC 的高级安全分析模块，可通过协议还原、沙箱行为分析、用户行为分析、动态域名分析、恶意程序特征匹配、动 / 静态 IP 黑白名单等检测与分析技术，及时发现用户本地环境下正在发生的安全威胁，并与云端推送的情报数据进行多维匹配（如 IP 匹配、域名匹配、URL 匹配、邮箱匹配、样本 MD5 值匹配等），产生精准的本地安全威胁告警（如病毒木马、恶意程序、异常主机、信息泄露等），提高用户对未知威胁的发现和处置能力。

关于威胁情报详细分析，可参见安全牛发布的《威胁情报技术指南与市场指南报告》。

3.6 可视化展示与分析

SOC 的可视化展示与分析功能让企业相关的 SOC 安全运营人员、风险管理人员、业务人员、决策层领导更容易理解和分析面临的安全攻击、当前的网络安全态势、企业的风险状况、合规状况等。因此可视化功能模块应当包括：

- **资产可视化**

通过地理位置、拓扑结构、关联关系等，展现当前企业各类信息资产的状态；

- **攻击可视化**

展现攻击者的攻击类型、攻击手法、攻击来源、攻击次数、攻击路径等；

- **策略可视化**

展现当前防御体系的安全策略、访问控制关系、基线部署情况等；

- **风险可视化**

对资产、漏洞、威胁进行综合风险分析，展现各领域的安全风险；

- **合规可视化**

根据等级保护要求、ISO27001、行业监管要求等，生成各类要求的合规状态；

- **业务安全可视化**

根据业务分类，将安全的影响映射到企业的各类业务，展示业务安全状态；

• 可视化攻击分析

提供可视化交互分析工具，让安全分析师进行深入的安全攻击分析。

企业 SOC 建设的可视化开发组件有很多，有很多的开源工具和商业工具可以选用。业界比较常用的开源可视化组件工具有：

• 百度 Echarts

ECharts，一个纯 Javascript 的图表库，可以流畅的运行在 PC 和移动设备上，兼容当前绝大部分浏览器（IE8/9/10/11，Chrome，Firefox，Safari 等），底层依赖轻量级的 Canvas 类库 ZRender，提供直观，生动，可交互，可高度个性化定制的数据可视化图表。

ECharts 3 中更是加入了更多丰富的交互功能以及更多的可视化效果，并且对移动端做了深度的优化。

具体参考：http://echarts.baidu.com/

• D3.js

D3（Data Driven Documents）是支持 SVG 渲染的另一种 JavaScript 库。但是 D3 能够提供大量线性图和条形图之外的复杂图表样式，例如 Voronoi 图、树形图、圆形集群和单词云等。虽然 D3 能够提供非常花哨的互动图表，但你在选择数据可视化工具时，需要牢记的一点是：知道在何时保持简洁。

D3.js 是开源工具，使用数据驱动的方式创建漂亮的网页。 D3.js 可实现实时交互。

具体参考：https://d3js.org/

3.7 自动化响应平台

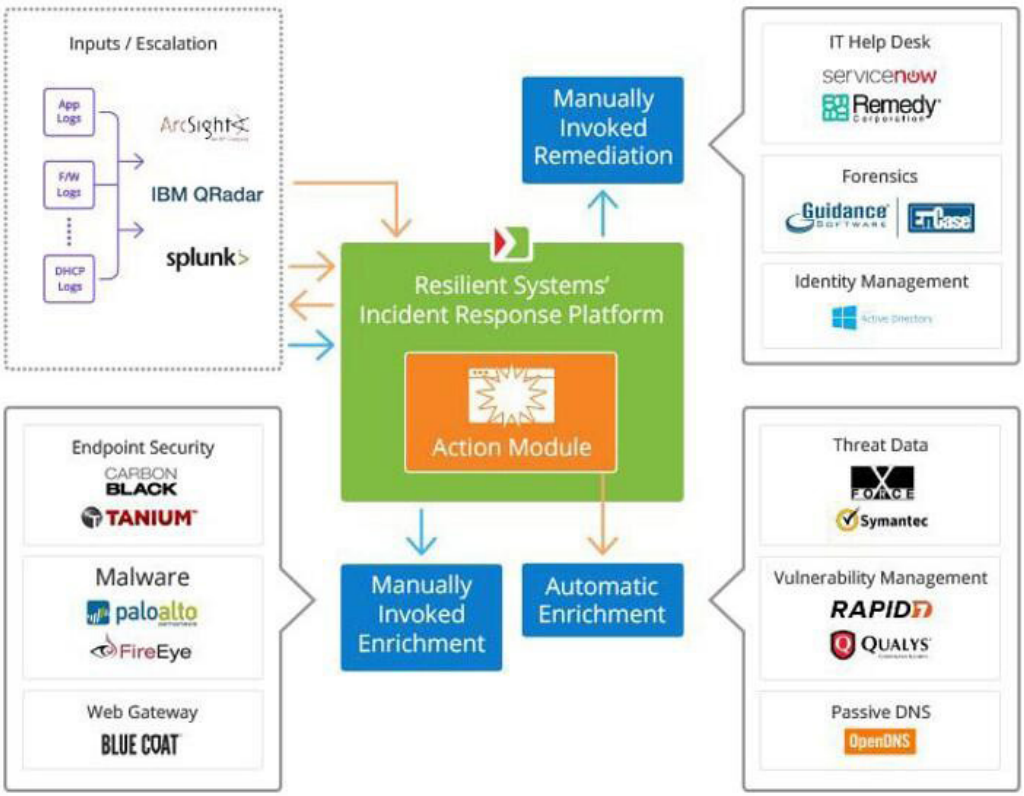
当前 SOC 的运营中，对于事件的响应和处理往往只是将报警的事件发送的工单系统，由安全工程师进行人工的分析和响应。由于误报较多，且工程师在处理事件时无法拿到有效的攻击数据和情境数据，事件响应效率比较低下。

而新一代 SOC 未来将加强自动化事件响应平台的建设。事件响应平台接受报警事件后，通过情境数据关联和威胁情报数据，自动化或半自动化来丰富威胁报警数据，使得安全工程师迅速定位威胁源和相关联的资产和业务，根据既定的事件类型和响应步骤，自动分发安全响应的任务到所有相关人员，及时进行事件的响应和取证。并且随着设备之间的联动策略逐步完善，事件响应平台可以自动化或半自动化及时下发安全策略，大大提升了安全响应的效率。

目前国内厂商尚没有完善的自动化事件响应平台产品，IBM 在 2016 年收购的 Resilience 公司提供了类

似这样的平台。

以此为例，简要说明一下事件响应平台的工作机制：



Resilient 系统架构图

除了事件响应平台的建设，事件响应流程的建设也非常重要。

我们推荐的事件响应的十大关键成功要素如下

1) 确保充足的员工参与；
2) 明确定义角色与职责；
3) 提升用户安全意识，培训相关知识；
4) 正式定义事件响应的流程和步骤；
5) 提升漏洞管理能力；
6) 从以前的事故和泄露事件中汲取教训；
7) 建立正式的事件跟踪机制；
8) 部署实时的、集中式的安全监控与报警机制；
9) 提升取证分析溯源的能力；
10) 开发并使用威胁情报。

3.8 SOC 运营体系

SOC 要想发挥真正的作用，离不开完善的运营体系建设。除了建设技术平台，人员和流程的建设也是必不可少的。

• SOC 运营组织建设

首先应当定义 SOC 运营组织人员的角色和责任，以及其他相关人员的角色和责任。新一代的 SOC 运营组织应面向攻击过程，针对攻击杀伤链的各个阶段，形成从发现到调查，再到响应的组织和职责体系。

• 安全运营中心经理

负责对整个安全运营中心的全面管理和协调工作，包括一线安全分析师的日常管理、二线安全专家的协调，以及与企业其他部门安全事件的协调与汇报工作等。

• 安全分析师团队

安全分析师是安全运营中心的日常工作团队，利用安全运营中心平台的各类系统组件，对全网的信息资产进行监视、对安全事件进行分析、生成必要的警告和报警，以维护企业日常安全。

• 安全专家团队

专家团队由经验丰富的安全工作人员组成，对由安全运营中心呈现的安全事件进行人机交互分析，制定安全运营中心的安全策略，指导安全分析师团队开展工作，是安全运营中心的大脑。

• SOC 运营人员能力培训

SOC 运营的效率取决于运营人员的能力，安全运营团队至少应掌握：

- 企业网络安全管理技能；
- 主流系统管理员技能；
- 主流数据库管理员技能；
- Web 应用安全技能；
- 渗透测试与攻击防御技能；
- 漏洞管理与威胁管理技能；
- 大数据安全分析技能；
- 调查取证与溯源技能；
- 高级安全管理技能等。

• **SOC 运营流程建设**

新一代 SOC 的运营流程应当更加符合自动化运维的特点，尽可能将流程集成到各类技术响应平台中去，主要包括：

- 安全事件监控操作流程；
- 安全事件通报流程；
- 安全事件应急处理流程；
- 安全预警发布流程；
- 配置变更管理流程。
- 灾难恢复计划；
- 风险评估计划；
- 内部审计计划与流程等；

4.SOC 应用场景

新一代 SOC 作为企业的安全运营中心或安全能力中心，将成为企业安全中枢，适用于很多的企业场景。我们可以从三个层面来了解 SOC 的具体应用场景。

4.1 微观运营

SOC 首先能够实现企业运营层面的安全支撑。在安全运维、安全开发、攻防对抗、安全监控、事件响应、取证调查等安全运营工作方面提供数据分析能力。

1）支撑基础设施的常态化安全运维

2）支撑研发过程与应用上线的安全

3）对 APT 攻击的深度检测与取证溯源

4）对重大安全事件的监控与响应

5）对核心数据的防护与泄密事件调查等

4.2 中观管理

SOC 能够对企业各个安全相关的管理领域提供支撑。

1）企业信息资产的风险管理

2）企业满足等级保护、ISO27001、行业监管的合规管理

3）企业安全策略的统一管理

4）企业内控与风险管理

5）企业业务安全支撑与管理

4.3 宏观决策

SOC 能够根据实时采集到的数据，展示实时的风险状况，这种展示包括当前攻击行为的展示，当前漏洞情况的展示，当前风险分布的展示等，并具备对未来可能发生风险的预测能力，对未来可能发生的攻击型态进行预测和预防，供高层进行快速的判断与决策。

1）对重大安全事件和风险的预警和通报；
2）对企业各部门、各业务的风险进行综合分析与展示；
3）对企业网络安全整体的态势感知等。

5. SOC 建设难点

在我们的调研过程中发现，SOC 在真正落地实施建设时，常常会遇到很多的困难，主要是由于甲方客户、产品厂商、服务商、行业主管部门、国家监管机构等各方的利益诉求不一致，涉及到 SOC 相关各方的投入产出、利益协调、协作机制等。我们这里也只能将难点问题提出来，在具体的 SOC 建设过程中，各方需要进行充分的沟通与讨论，对这些问题予以足够的重视，才能保证 SOC 的成功。

5.1 产品化还是定制化

从本报告之前的 SOC 能力要求、技术实现和应用场景章节可以看出，SOC 建设是一个非常复杂且耗时耗力的工作。对于安全厂商而言，尽可能将 SOC 平台模块化产品化，能够比较快的交付才能获得较好的收益。而对于甲方客户而言，由于行业和企业自身需求的不同，大量定制化的需求导致任何厂商的产品都无法直接满足，需要定制化开发才能发挥作用，这样就导致人力和资金的投入较大。不少 SOC 建设项目都面临这个难题，厂商与甲方客户在交付过程中都痛苦不堪。

安全牛建议：新一代的 SOC 建设不是一蹴而就、一劳永逸的项目，甲方客户应当充分预估 SOC 建设的困难，申请足够的资金与人力资源来支持 SOC 的建设，必要的情况下可以进行分期建设，便于项目的控制与实施效果的落地。而安全厂商应该在产品化与定制化之间取得平衡，新一代 SOC 绝不是一个产品平台可以交付的，需要满足客户在部分核心功能的定制化需求。另外，尽可能深入到某几个行业，掌握行业客户的共性需求，通过不同客户的实施逐步形成满足特定行业客户的 SOC 产品化。

5.2 大数据平台如何构建

大数据处理平台是新一代 SOC 的核心技术，是必不可少的系统平台组件。对于企业而言，大数据战略和数字化转型也是绝大多数大型企业正在开展的工作，大数据处理平台也纳入在企业的整体技术平台架构中。企业一般不会为了安全分析重新再部署一套大数据处理平台导致重复建设，这样就导致 SOC 大数据分析平台的建设就需要等待企业大数据平台的统一规划部署，在项目的进度、质量、资源调度方面可能会产生冲突。

安全牛建议：对于大型企业级客户而言，SOC 的大数据平台建设应当尽可能采用企业统一的大数据存储与计算平台，从而满足最佳的投入产出比。安全部门应参与企业的大数据平台建设，提出性能、容量、功能、安全等要求，安全数据也统一存储在大数据平台，也更加有利于与企业的业务和管理进行融合。而安全运营部门的核心能力应放在大数据的安全分析模型、安全攻防能力、分析能力、响应能力上。

5.3 运营团队如何建设

人的因素是 SOC 运营最大的挑战。尽管我们都梦想通过完全自动化整个检测和响应过程，来解决技术人才短缺问题。但是，在可预见的未来都无法实现完全自动化。运营团队一直是 SOC 建设之痛，很多客户甚至没有人员编制来运营 SOC，导致 SOC 无法有效利用。

安全牛建议：一方面尽可能使用机器学习、人工智能和自动化分析工具，来最小化 SOC 运营团队所需的知识，并在手动操作上降低 SOC 一线运营人员的能力要求；另一方面必须要有正式的运营团队来实施日常的安全运营工作。由于安全运营的专业性要求较高，甲方客户在人员受限的情况下，应考虑采用运营外包服务，Gartner 也定义了此类服务为管理威胁与响应服务（MDR）。安全厂商或服务商则应当提供正式的 SOC 运营支持服务，而不仅仅是 SOC 产品的升级或维保服务。通过云平台，可以逐步建设分级的 SOC 运营支持来提升运营效率。

5.4 情报共享机制如何建立

威胁情报是新一代 SOC 的核心驱动力，很多能力的实现需要通过威胁情报的共享来实现。而国内的现状是大部分安全厂商并不具备威胁情报的输入和输出能力，业内也尚未形成有效的情报共享机制，国家也没有未正式发布威胁情报共享的相关标准。与国际上威胁情报和信息共享已经成为行业标准和基本属性的现状不同，国内的发展比较滞后，目前还很难形成全行业有效的情报共享。

安全牛建议：国家主管机构应尽快着手编写和发布正式的威胁情报共享标准，统一信息的规范接口；行业主管部门应当推动行业内客户的威胁情报和信息尽可能共享，提高威胁响应的效率和效果；甲方客户应当考虑

采购相关的威胁情报服务来满足 SOC 建设的需求；而安全厂商应首先提升自身的情报输出输入能力，并尽可能形成威胁情报共享联盟，来协同应对新的威胁与攻击。

6. SOC 关联技术

SOC 除了自身的一些功能和技术平台，还要与企业众多的其他 IT 和安全平台进行对接，输入或输出相关的数据，协同工作。主要的 SOC 关联技术包括：

6.1 CMDB 配置管理

CMDB --Configuration Management Database 配置管理数据库

CMDB 存储与管理企业 IT 架构中设备的各种配置信息，它与所有服务支持和服务交付流程都紧密相联，支持这些流程的运转、发挥配置信息的价值，同时依靠相关流程保证数据的准确性。

6.2 VM 漏洞管理

VM-- Vulnerability Management 漏洞管理

漏洞管理是企业通过资产管理、漏洞扫描、补丁管理、统计分析等软件功能，定期扫描企业网络中所有设备，发现存在的漏洞，并及时进行修补。在大型网络中，漏洞管理是必不可少的一个环节。

6.3 EDR 端点检测和响应

EDR-- Endpoint Detect&Response 端点检测和响应

端点检测和响应（EDR）定义为具有以下四个主要功能的解决方案：

检测安全事件。主要通过监测终端的活动和对象，监控是否违反安全策略，或通过验证外部提供的 IOC；

调查安全事件。该功能主要包括确定历史时间线的所有终端发生的事件，包括技术方面的变化（如文件、注册表、网络、驱动和执行活动）和业务影响（即遍历，特权升级、传播、泄露，指挥和控制 [C & C]，和地理位置等）。

提供端点发生事件的内容，比如网络流量或远程控制的进程执行。

修复端点到感染前的状态。理想情况下，解决方案将删除恶意文件，回滚和修复其他更改。

6.4 IAM 身份与访问管理

IAM--Identity and Access Management 身份与访问管理

IAM 是一套全面的建立和维护数字身份，并提供有效地、安全地 IT 资源访问的业务流程和管理手段，从而实现组织信息资产统一的身份认证、授权和身份数据集中管理与审计。具有单点登录、强大的认证管理、基于策略的集中式授权和审计、动态授权、企业可管理性等功能。

6.5 UEBA 用户与实体行为分析

UEBA--User and Entity Behavior Analysis 用户与实体行为分析

UEBA 关联了用户活动和其它实体，例如受控或非受控的终端，应用（包括云、移动和其它内部应用）、网络和外部威胁。通过实施 UEBA，使得组织在内部威胁已经存在的情况下免受外部威胁的影响，从而达到保护数据不外泄的目的。

6.6 NTA 网络流量分析

NTA--Network Traffic Analysis 网络流量分析

NTA 提供网络链路全流量存储、全数据分析能力。借助全流量存储分析，安全分析人员可以对已经发生的攻击行为进行多角度、全方位、可反复回溯的深度检测，从而更容易检测出潜在的入侵行为，发现被其他工具漏掉的攻击。为用户识别和发现失陷主机、漏洞利用、高级木马通讯、APT 攻击、数据窃密等已知和未知的安全威胁，对网络攻击进行定位和取证。帮助安全分析人员从海量的数据中聚焦真正的入侵行为，从而缩短对 APT 攻击的响应时间，帮助用户提升安全分析能力和响应能力，最终降低安全损失。

网络流量分析除了原始全流量分析外，在大型网络中也常常使用 Netflow 流分析以及 DNS 流量数据分析技术。

6.7 Service Desk 服务台

当信息技术大规模应用于服务行业之后，帮助台概念也被引用进来。最初是应用于 IT 设备密集型行业如金融、电信业，当硬件设备如故障或有麻烦时，人们被告知可以找 " 帮助台 " 的人来解决问题，这个 " 帮助台 " 就是 IT 设备运维中心 , 而他们为方便工作而使用的软件就是最初的 "HelpDesk/ServiceDesk 软件 "。

而对 IT 服务提供商来说，有必要采取一定的信息技术服务管理（Information Technology Service Management，ITSM）措施，以便更好地为用户提供服务。最著名的 IT 服务理论就是 ITIL，而根据 ITIL 理

论设定的各种服务功能汇总到一起，形成一个面向客户的统一的服务平台，这就是 Service Desk 服务台。

6.8 GRC 风险与合规软件

GRC-- Govenance，Risk and Compliance 治理、风险与合规

GRC 软件使组织能用有系统、有组织的方法来管理与 GRC 有关的战略。管理员可以使用单一的框架来监测和执行规则和程序。GRC 软件使各组织能管理风险，减少设施费用，并且能尽量减少管理的复杂性。

GRC 软件实施通常比较复杂，其中涉及多个部门数据的协调，包括商业、信息技术、安全、法规遵从和审计。管理员可以用仪表板和数据分析工具来确定一个组织的风险承担能力，衡量季度目标进展情况或迅速进行信息审计。

7. SOC 未来趋势

随着云计算、大数据、机器学习、人工智能等技术的不断完善，安全平台化趋势的日益增强，安全建设已经逐步进入到了一个全新的阶段。新一代 SOC 承载了企业整体安全能力的建设，承担着最为关键的作用。

而国内随着政府政策层面不断提出在态势感知方面的要求，未来几年新一代 SOC 及其态势感知肯定是市场的热门之一，市场前景十分看好。由于新一代 SOC 涉及的技术层面比较复杂，同时不同的客户对 SOC 有着不同的需求，SOC 市场会不断分化，面向具体行业客户需求的、与客户自身业务紧密结合的 SOC 是发展大势，在不同的细分市场上会出现不同的 SOC 产品。同时，SOC 也不一定都以固化的产品形态出现，SaaS、MSS、混合式 SOC 都会出现并且在不同的细分市场找到自己的定位，泛 SOC 市场将会蓬勃发展。

SOC 未来的技术也将不断智能化和专业化，贴近用户需求。安全厂商可能会在某一个或几个 SOC 涉及的技术层面深入探索，发展出独立的 SOC 相关产品和服务。

7.1 从 SOC 到态势感知

由于国家政策的引导，态势感知目前在国内市场比较热门，很多客户都提出了类似的需求。而态势感知技术与 SOC 有天然的联系，是 SOC 未来发展的方向之一。我们所理解的态势感知不仅仅是对资产和漏洞的感知，应当由 SOC 的情景感知，逐步过渡到行为感知最后到态势感知。当前国内尚处于情景感知与行为感知阶段，很多问题还未解决，还需要数年的发展，最后才能实现真正的态势感知。

情境感知

SOC 首先要实现的是情境感知。通过对企业现在 IT 资产和环境的全面把控，包括对企业现有的硬件、软件、应用、业务的资产和安全状况进行全面评估和详尽记录，可以将威胁信息关联企业 IT、业务场景上下文，同时通过情报共享机制，实现情境感知，从而能够实现各类威胁的快速定位和快速响应等。

行为感知

行为感知阶段重要的特点是通过大数据的安全分析，掌握内部用户和外部黑客的行为特征，逐步形成用户画像、黑客画像，通过行为建模实现对所有人的行为感知。

态势感知

态势感知阶段是未来 SOC 发展的方向。机器学习目前已经在大数据安全分析中有所应用，但很多场景下还需要人工对攻击特征的分析和交互。未来随着深度学习和人工智能技术的不断成熟，机器将替代人工进行深入分析，并通过自适应安全体系，逐步实现安全的自动化和真正的态势感知。

7.2 机器学习与人工智能

机器学习当前已有一些厂商在应用，更多是采用监督学习技术在某些特定场景下使用，离人工智能应用还差距较大。未来随着深度学习技术的发展，新一代 SOC 将全面应用机器学习和人工智能技术，在资产的自动化识别与分类分级、漏洞的挖掘、恶意代码的分析、威胁的定位与追捕、运营的自动化响应、风险的量化与展示等各个层面都将充分应用，最终将实现主动化和自动化的安全能力。

7.3 安全与业务融合

新一代 SOC 的未来将与企业业务的不断融合。现在已经有一些互联网公司在用 SOC 相关技术做一些反欺诈方面的工作，未来通过 SOC 的大数据分析，将建立符合更多业务场景的安全，比如反欺诈、财务内控、供应链安全、品牌保护等，SOC 将与业务和管理更深度的融合，提供更多的支撑。

垂询及订阅请联系

电话 /Tel：+86-10-51626974

邮箱 /E-mail：zuojing@aqniu.com

安全牛网址：http://www.aqniu.com

17-08-C2-ZN

新一代 SOC 研究报告

市场指南

安全牛 AQNIU.COM

版权声明

免责声明

前言

近几年，威胁和风险环境已经发生了巨大的变化，主动攻击行为与高级攻击技术（APT）的复杂性不断升级。而随着云计算与大数据技术的发展，新一代的高级安全技术和防护策略也取得了快速发展，比如以风险或杀伤链为基础的方法，大量利用了威胁情报和大数据分析技术。这就要求传统的安全运营中心（SOC）来适应这些新的变化，企业需要认识到传统的以防护为核心的策略已经失效，企业资产可能已经被破坏。企业安全体系必须切换到以监控和响应为核心，通过持续监测，及时响应来减轻和限制攻击造成的损失。

新一代安全运营中心（SOC）必须以数据和情报驱动，采用自适应安全架构来进行环境和态势感知，通过自动化或半自动化工具、流程和策略来对抗新一代威胁。

本报告描述了新一代 SOC 的市场需求，分析了 SOC 建设的必要性、模式和相关服务，从市场成熟度、目标客户、发展预测等方面进行市场和客户群分析，对 SOC 的交付模式和发展趋势给出建议。并从客户维度给出了 SOC 建设的选购指南，使得客户了解如何选择合格的厂商和服务商来提供服务。另外，报告选择了当前市场主流的新一代 SOC 厂商进行分析和评价。

本报告由安全牛顾问团队，通过调查国内在新一代 SOC 市场上较为突出的公司，并结合当前最新的相关资料撰写。

关键发现

- 预计到 2020 年，以数据和情报驱动的新一代 SOC 中心的市场占有率将从现在的 5% 提升到 50%。

- 当前 SOC 市场规模约 10 亿元左右，预计到 2020 年，市场规模将提升到 50-100 亿元。

- SOC 建设对企业业务的影响是非常重要和关键的，投入也较为巨大。企业一旦决定投入 SOC 建设就希望尽快见效，并将持续运营。

- 企业希望通过 SOC 建设来打造内部安全运营能力，因为他们想要对安全监控与响应流程进行控制，同时满足监管部门各种信息的交互与合规要求。

- 每个打算建设 SOC 的企业都是独特的，都有他们自己的行业特点和自身的商业价值。因此，任何一个通用方法论都无法满足所有客户的需求。

安全牛建议

厂商在销售过程中要根据客户的情况交付给客户更多的商业价值。让客户自由选择 SOC 的产品和服务，自行建设 SOC 几乎是不可能的。

厂商应根据客户的成熟度，规划客户 SOC 建设的蓝图和路径规划，使得客户可以根据预算情况，选择合适的服务目录，逐步开展 SOC 的建设，并逐步应用到客户的场景，提供更多的商业价值。

厂商应专注特定行业的应用案例，积累与客户行业相关的实施经验，帮助客户建设独特的适合客户自身的 SOC，才能取得竞争优势。

SOC 建设不仅仅是交付产品平台，更重要的是交付给客户安全运营的能力，厂商应结合安全服务商，提供更多的服务价值。

目录

1. 市场概述

近几年，威胁和风险环境已经发生了巨大的变化，主动攻击行为与高级攻击技术（APT）的复杂性不断升级。而随着云计算与大数据技术的发展，新一代的高级安全技术和防护策略也取得了快速发展。新一代安全运营中心（SOC）以情报和安全智能驱动，采用自适应安全架构来进行环境和态势感知，通过自动化或半自动化工具、流程和策略来对抗新一代威胁。预计未来很多企业都将开启各种模式的新一代 SOC 建设，打造自身的内部安全运营能力，这也为安全厂商和服务商开启了一个巨大的市场。加上国家和行业监管层面都提出了态势感知方面的需求，也驱动了企业进行 SOC 的建设。

在新的市场环境下，安全厂商和服务商可以通过新一代 SOC 建设，提供相关的安全服务，为每个客户建设定制化的独特的安全运营能力。

1.1 SOC 建设的必要性

SOC 的建设实际是企业打造自身内部安全运营能力的过程，这是一个非常耗时耗力的过程，需要根据企业情况不断优化不断运营，逐步提升运营效率。实际上之前大部分组织可能不会选择自建 SOC，而选择安全服务商来外包部分安全的职能。而随着技术的发展，新一代 SOC 使得企业希望建设自己的 SOC，**因为：**

缺少合适的安全服务商：当前市场上的安全服务商往往都是提供阶段式项目式的服务，不能提供实时的安全威胁检测和响应服务，缺少对日常管理和业务的日常安全支撑，往往在重大安全事件发生时显得能力不足；

数据保护的需求：随着数字经济和“互联网 +”等战略的实施，组织在通过数字技术提升绩效的同时也面临更大的安全风险，组织对数据保护的要求越来越高，也需要对企业拥有的数据资产进行有效的保护，并对安全事件进行及时的调查和响应；

监管合规的要求：虽然没有规定要求组织必须建设 SOC，然而，网信办、公安部、行业监管等部门往往在一些重大时间节点和重大安全事件发生时，要求企业在一定的时间内提交该事件的根本原因分析和调查。组织建设 SOC 就可以与监管机构进行更有建设性和有效的对话。

1.2 SOC 建设的模式

安全运营中心（SOC）不仅仅是一个系统平台，还应有一个合适的 7*24 小时安全运营队伍以及适合企业的安全运营流程，面向新时代的网络安全威胁和安全事件，来阻止、检测、响应、预防安全事件的发生，同时满足监管合规的要求和企业风险管理的要求等。

• 客户需求差异化决定了厂商 SOC 服务的差异化

一般而言，每个企业由于行业不同、业务不同、组织不同、职能不同，没有两个企业的 SOC 是完全一样的。有的企业合规职能并不属于 SOC，有的企业主要面向基础设施，有的企业 SOC 主要进行业务支撑等。有的组织有专门的庞大的安全运营队伍，有的采用了外包服务，有的只有几个甚至没有专业人员。这就决定了 SOC 建设的方法完全不一样。

厂商在向客户提供 SOC 建设服务时，应当考虑客户的特点，采取不同的 SOC 建设模式。只有大型企业客户才有能力建设专有的完全自主运营的安全运营中心。很多中大型组织只能采取外包部分安全检测、监控和响应能力。这就决定了 SOC 的市场将呈现多样化模式，有些客户是自建 SOC 模式，有的采取混合 SOC 模式，有的采取完全外包服务模式等。厂商应提供多样化的服务类型跟进客户的情况选择合适的 SOC 模式。

SOC 对组织而言是一个战略级的，非常耗费资源的项目，对企业的业务绩效和品牌都有重要的影响。因此，一旦一个企业决定投资建设 SOC，他们都希望很快能够成功运营并见效。这对厂商就提出了很高的要求。安全厂商和服务商将随着 SOC 的建设和运营，逐步取得客户的深度信任，成为客户重要的合作伙伴，并在一个客户那里能取得越来越多的营收。

很多不同类型的厂商都宣称能够提供 SOC 服务，但我们通过深入调查后发现会有很多的不同。大部分厂商其实也面临和客户一样的问题，缺少专业的安全运营和安全分析队伍，缺少实际的安全运营经验，客户在选择厂商时尤其要注意这一点。客户需要知道 SOC 建设和运营的具体特点，而厂商可以根据自己的资源状况，提供差异化的服务和产品，提供不同的价值，从而获取各自的市场份额。

• SOC 建设模式分析

根据不同的客户的需求，SOC 建设模式可以分为以下几类

SOC 模式	特点	面向客户群
专有 SOC	• 独有的机房和基础设施 • 专职的运营队伍 • 完全内部运营控制 •7x24 小时运营	关键基础设施企业，大型集团企业总部，政府部委，高风险组织等
虚拟 SOC	• 没有独有的机房 • 兼职运营队伍 • 响应式运营，重大报警或事件发生时响应 • 日常主要依赖安全服务商	中型组织，集团企业二级单位

分布式 SOC	• 一般为二级 SOC • 专职或兼职运营人员 • 5x8 小时运营 • 与安全服务商共同运营	中小型组织，集团企业二三级单位
SOC 指挥中心	• 与其他 SOC 协作工作 • 提供威胁情报、态势感知和其他经验 • 很少参与日常运营	巨大型企业总部，政府主管部门，军队指挥中心，情报中心等
多功能 SOC/NOC	• 独有机房，专业运营队伍 但不仅仅负责安全，往往还负责企业 IT 基础设施的日常运营，与 NOC 整合运营	中小型企业，网络与安全职能由同一队伍承担
融合 SOC	除了传统 SOC 职能外，还加上威胁情报中心，应急响应中心、生产安全中心等	大型组织，业务有更广泛的安全需求，SOC 提供更多的业务安全支撑

除了上述的模式之外，也有部分客户采取完全外包的模式。由服务商来建设和运营 SOC。这种模式一般是客户的整个 IT 也完全外包。这种情况下客户需要关注对事件响应的控制和对业务安全的控制。

1.3 SOC 建设的相关安全服务

SOC 建设和运营是一个非常复杂的工作，只依赖厂商提供的平台无法实现有效的 SOC 运营。

厂商还应与服务商一起提供如下服务：

安全咨询	安全实施	安全外包
• SOC 架构与流程设计 • SOC 成熟度评估 • 威胁溯源与追捕 • 漏洞管理体系 • 渗透测试 • 安全培训与安全意识教育	• 技术平台选择 • 集成与实施服务 • SOC 相关产品支持	• 安全运营人员外包 • 管理安全服务 • 管理监测和响应

在不同 SOC 建设模式下客户有不同的服务需求

SOC 模式	主要的服务需求
专有 SOC	咨询、实施、外包
虚拟 SOC	实施、外包
分布式 SOC	咨询、实施、外包
SOC 指挥中心	咨询、实施、外包
多功能 SOC/NOC	外包
融合 SOC	咨询、实施

2. 市场分析

安全牛调研了国内领先的十多家 SOC 厂商，并走访了一些正在实施新一代 SOC 的客户，从客户当前对新一代 SOC 的认知，市场的规模，目标客户的类型、驱动力、客户需求、厂商投入情况等进行了综合分析。

2.1 市场成熟度

从调研结果看，厂商普遍认为，当前客户对新一代 SOC 的认知水平基本限定在一些特定行业，主要包括公安、政府、金融、运营商、教育、医疗等对安全要求比较高的行业，并且各厂家基本都在行业典型客户得到了一些验证。当前 SOC 整体的市场规模大约 10 个亿左右，大概只有 5-10% 是完全按照新一代 SOC 架构来实施，新一代 SOC 在国内市场还需要 1 年左右时间沉淀，才能逐步被用户接受，但发展的速度将会非常快。

在1-2年时间内，市场将呈现百花齐放的状态，传统SOC厂家、创业公司、所有老牌安全厂家都会进入市场，提供各个层面的解决方案。在国家政策、监管要求、行业技术趋势各方面的影响下，国内客户对新一代 SOC 和态势感知将表现出较强的兴趣，今年将有大量态势感知和新一代 SOC 项目出现，客户也将更加理性的选择产品和服务。

2.2 目标客户分析

我们从目前各厂家取得的典型案例状况，对新一代 SOC 的目标客户群做一个简要分析。

• 金融行业

金融行业是对网络安全要求最高的行业之一。随着大数据技术的发展，金融行业建设新一代的 SOC 需求凸显。目前在四大行、股份制银行、部分商业银行都已经正在或考虑通过大数据技术建设新一代的安全运营中心。

由于银行业的整体大数据平台建设正在进行中，以大数据处理为基础的新一代 SOC 将稍滞后一段时间。随着大数据平台的建设逐步完成，各个业务应用都将基于平台来改造，明后年将迎来新一代 SOC 建设需求的爆发。

另外，金融行业有更多的业务场景，需要 SOC 提供更深入的安全运营能力，比如业务反欺诈将成为金融行业安全中心的核心业务应用。风险管理部门、审计部门也将与 SOC 进行数据对接，提供基于数据的实时风险管理和审计。

• 政府行业

几乎所有的 SOC 厂商都已经在政府行业进行了布局，并取得了典型客户案例。政府行业主要受到国家政策层面态势感知的要求，部分中央部委、地方政府机构已经开展了态势感知项目的试点。试点成功后将有机会在部委范围内进行全国性推广。政府行业需求的特点重点在对外部攻击的防范，APT 的检测，安全状态的感知等。

• 公安系统

公安系统主要承担着国家关键基础设施保护，国家等级保护制度落实，和社会公共安全相关的职能。因此，公安部门和企业需求完全不同，他们更多是建设态势感知平台，对管辖范围内的关键基础设施，企事业单位的安全态势感知，掌握等保落实情况，及时发现安全隐患，并推动整改等。

当然，在公安系统内部，态势感知和大数据安全平台也要与公安的业务相结合，协助案件办理，追踪违法犯罪分子等。

• 运营商行业

运营商是国内第一代 SOC 的主要客户群，移动和电信总部和各省都投入巨资相继开展了 SOC 的建设，并配备了较为专业的 SOC 专职运营人员，有非常好的基础。但由于技术的限制，SOC 的运营并未取得预期的效果。随着新一代 SOC 技术的不断成熟，运营商已经开始逐步尝试升级原有的 SOC 平台。不少省级运营商已经在开展试点工作，部分在运营商行业有较好基础的厂商也取得了成功案例。运营商有着其他行业不可比拟的资源优势，有丰富的数据资源，其 SOC 不仅为自身的安全服务，也可以联合厂商建设面向政企客户群的 SOC 运营服务，并提供一系列的增值服务，是各厂家都尽力争取的案例。

• 电力行业

电力行业有非常庞大的信息资产，也有较好的安全基础。我们在调查中发现国网、南网都已经有了成功案例，未来随着试点的成功会在全集团不断推广实施，有广阔的市场空间。而几大发电集团由于网络安全基础相对薄弱，还没有形成成熟的运营体系，刚刚开始整体的安全体系和 SOC 的规划建设，离新一代 SOC 建设尚有一段距离，在未来几年会逐步考虑部署新一代 SOC。

2.3 市场发展预测

• 市场规模

在未来一到三年，SOC 市场会将有一波爆发式的增长，一方面由于国家政策和监管层面都提出了态势感知的需求，另一方面技术的不断成熟，新一代 SOC 作为企业安全能力的中心，会越来越重要。同时，各大安全厂商都在积极推进客户的相关项目，会使得市场快速增长。在我们的调查中，70% 的厂商认为 SOC 市场未来会增长到 50-100 亿，部分甚至认为会超过 100 亿。我们预测到 2020 年，SOC 市场整体会增长到 50-100 亿，其中 50% 以上会采用新一代 SOC 架构。

• 市场发展方向

下一代 SOC 可能会向两个方向发展：其一是针对中小客户的基础版，强调简单部署和入门级的成本，能够尽可能少地要求用户参与，并由供应商提供一站式的检测、响应和事件处置服务；其二是针对大型企业的集成化和模块化版本，将 SOC 的分析能力与企业自身已有的大数据分析平台整合起来，并提供用户自己开发和调试的接口，安全公司提供的更多的是一个开放的框架而非封闭的产品。目前很多新技术在安全领域的应用还处在概念阶段，未来 1-3 年，随着新技术的应用日渐成熟，会产生出一批新型的安全能力。而这些安全能力也会影响 SOC 产品的发展，帮助 SOC 在安全运营管理方向上产生新的安全价值。

• 厂商发展方向

根据调研的情况，大型安全厂商将在新一代 SOC 建设中发挥主导作用，不同 SOC 厂商根据各自的优势，将逐渐体现出自己的特色。不同厂商将侧重不同行业的 SOC，解决不同业务场景下的安全问题。同时，大量新兴的小型安全厂商，将承担 SOC 体系中部分安全能力的建设，比如威胁情报、流量分析等，他们将与大厂一起协同合作，共同打造企业更全面的安全能力。另外，预计也将出现一批 SOC 方向的安全咨询、安全集成和安全运营的服务商，与厂商一起合作，真正实现 SOC 从产品交付到服务能力交付的转变。

3. 选购指南

SOC 作为企业的安全运营中心，是一套十分复杂的系统，SOC 产品仅仅是 SOC 的技术平台组成部分，不代表整体 SOC。完整的 SOC 除了有 SOC 技术平台外，还必须包括人、组织和流程，三者缺一不可。用

户在建设 SOC 的时候必须对 SOC 这个概念有正确和清晰的认知。最重要地，客户要对自己的需求有较为清晰的认识，要设定合理的目标，要技术和管理并进，不能盲目地和被动地接受 SOC 厂商的灌输。我们建议客户在选购 SOC 产品和服务厂商时要考虑如下因素。

3.1 安全服务能力

SOC 建设不是一次性产品采购和产品建设，而是一个长期运营的过程。除了产品自身的能力特性以外，还要考虑供应商的安全架构能力、安全分析能力、持续运营能力、本地支持能力、应急响应能力等是否满足客户自身运营的需要。

3.2 行业典型案例

产品是否有同行业的典型案例，分析场景和分析能力是否能覆盖实际需求。一般而言，各厂家最终都会在某个或某几个行业沉淀出相对成功的案例，形成各自的行业优势。每个客户的业务场景都是不一样的，厂商提供的 SOC 产品或方案需要与客户业务管理需求契合，能够形成针对客户业务的场景化应用。

3.3 技术平台成熟度

基本上所有厂家都会宣称自己的 SOC 平台具备技术的领先性和创新性，但从实际来看并不是这样。随着技术的不断成熟，各厂家的 SOC 平台采用的技术架构都采用了通用的开源架构，更多的技术能力将体现在对业务场景的建模，数据分析算法和引擎，以及多源数据和威胁情报数据的获取能力与解析能力上。另外在产品的可视化交互分析，可视化策略，自动化程度，用户易用性方面将有较大的差距。客户应仔细评估各厂商在这些方面的能力水平，考察技术平台具体的应用情况和成熟度。

3.4 自身安全成熟度

说到所谓新一代的 SOC 建设，往往都跟大数据架构挂钩。那么，客户在选择的时候，更加不能盲目。有的客户自身安全数据无论从量上、种类上都不具备大数据的特征，盲目跟风上大数据 SOC 可能适得其反。

还有，有的大型企业的确需要大数据 SOC，但如何选择大数据技术路线需要仔细斟酌。安全大数据架构是否要与企业的业务大数据架构保持一致？是把大数据 SOC 作为一个工具来建设还是作为一个平台来建设？如果是希望做成一个安全分析的统一大平台，那么开放性、扩展性和可伸缩性就尤为重要，如何去进行这方面的评估？

新一代 SOC 的建设成本高昂，在自己的企业中是否能产生足够的商业价值?

总之，面对新一代 SOC，用户需要更加理性，需要更加了解自身，而不是更加了解 SOC 供应商。根据自身的安全发展水平和业务需求，选择合适的安全厂商和服务商，共同打造企业的安全能力。

4. 相关厂商

我们根据厂商调研的结果、客户的反馈、业界的口碑、公开技术宣讲、产品的白皮书、研发人员数量、服务人员数量、专利获取情况、去年销售额及当年预期销售额情况等内容，对主流的 SOC 厂商进行了分析，并提供安全牛新一代 SOC 厂商矩阵图供大家参考。

4.1 启明星辰

启明星辰是国内老牌的安全厂商之一，是 SOC 理念和业务的领先者。近十年来 SOC 一直作为公司的重要业务之一，并专门成立了泰合中心负责泰合信息安全运营中心系统及其相关管理类系统的研发、咨询、项目实施与运维。泰合中心分别在北京、上海设有研发中心，总人数超过 200 人。

在技术方面，启明星辰也一直位于国内 SOC 技术的前沿，很早就率先引入流（Flow）分析技术和情境感知技术，在 SOC 中实现了基于资产、拓扑、性能、业务的情境关联技术等。从 2009 年开始就尝试使用高级分析模型进行宏观态势感知，包括熵模型、聚类模型和指标体系模型，并在 2010 年就发布了态势感知模块。

2015 年启明星辰正式对外发布了 SOC3.0 战略，并发布了融合大数据的新一代 SOC 和新一代日志分析产品。同年，还发布了面向云计算环境的 CloudSOC，以及面向工控网络环境的工控 SOC。2016 年正式启动了“泰合安全威胁分析合作计划”，以泰合 SOC 安管平台为依托，连接业界优秀的安全威胁分析能力，共同为政企客户交付安全价值。

启明星辰在 SOC 领域长时间的技术投入和积累，以及对政企客户需求的深度理解，使得其在新一代 SOC 建设中也独具优势，其产品化程度高，客户全周期协作能力强，工程化实施和运营支撑也具备一定的优势，在规模和影响力方面是其他厂商暂时无法超越的。技术创新方面，由于威胁情报、大数据分析、机器学习、人工智能等新技术发展较快，会受到新兴厂商和技术的冲击，需要继续加大新技术应用的探索。在行业案例方面，启明星辰侧重于政府、能源、军队等，在金融和运营商等领域也期待进一步的突破。

4.2 绿盟科技

绿盟科技是国内领先的安全产品和安全服务领导厂商之一，因公司的产品化和标准化战略，其在早期的 SOC 领域并未深度参与。近年来，随着大数据技术的逐步成熟，绿盟也推出了新一代智能安全运营解决方案，目前在研发上投入超过 100 人。

绿盟新一代智能 SOC 以大数据框架为基础，结合威胁情报系统，通过攻防场景模型的大数据分析及可视化展示等手段，协助企业建立和完善安全态势全面监控、安全威胁实时预警、安全事故紧急响应的能力。通过结合情境上下文分析，协助安全专家快速发现和分析安全问题，并能通过运维手段实现安全闭环处理。

绿盟科技在安全攻防和安全服务能力上有十多年的积累和优势，其 SOC 采用了基于攻击链的安全分析模型，更加准确的识别高危入侵事件，提供事件追溯能力。同时，近两年绿盟推出了云安全服务，具备了一定的威胁数据资源，SOC 与威胁情报相结合能产生更强安全能力。绿盟科技目前在其优势的运营商行业、能源行业、政府行业均取得了典型案例，期待其在更多领域更多场景下取得突破。

4.3 360 企业安全

360 企业安全是国内最早提出“数据驱动安全”理念的厂商，符合新一代 SOC 建设的理念，其在国内最早推出支持安全自适应方式安全运营的新一代 SOC 产品，提供检测、分析、响应、调查分析、情报共享一体化的安全威胁管理能力，提供本地事件分析、云端溯源调查结合的整体性方案。360 企业安全目前在新一代 SOC 和态势感知解决方案上投入研发超过 100 人，并常年有近百人的分析师队伍，能够提供安全运营服务的支撑。

360 企业安全之前收购的网神在 SOC 领域有一定的技术和行业积累，结合 360 的互联网大数据技术，以及 360 强大的恶意样本和基础数据获取能力，其威胁情报能力在国内处于领导地位，并且相关能力在 SOC 上已经充分集成，有比较明显的技术优势。近年来 360 集团和企业安全吸引了众多的安全攻防、安全研究人员加入，成立了十多个安全研究院，在国内厂商中首屈一指，增强了 SOC 解决方案的底蕴。

目前 360 企业安全也已经在一些大型政企客户取得了规模较大的典型案例，SOC 和态势感知平台的业务发展速度也非常快，有望拉开与其他厂商的差距。360 企业安全侧重于攻防能力，其在行业应用场景方面还需要进一步的探索，尤其是规模较大的金融行业客户，对新一代 SOC 有更多的业务场景需要去满足。

4.4 亚信安全

亚信安全是亚信软件的安全事业部与趋势科技中国合并而成，原来的亚信安全事业部在运营商的 SOC 建设领域有着丰富的经验和积累，而趋势科技在恶意代码分析和威胁分析方面具备全球性的优势。双方整合后目前在 SOC 方向投入研发超过 100 人，期待在新一代 SOC 建设方面有所突破。

亚信安全主推的安全态势感知平台，采用业内先进的大数据架构，通过采集企业内所有 IT 基础设施数据，利用机器学习、规则引擎、场景建模、行为识别、关联分析等方法对企业内所有机器数据进行统一分析，实现对网络攻击行为、安全异常事件、未知威胁的发现和告警。平台提供了对企业信息数据的集中存储、全文检索、态势场景、可视化展现功等能、同时搭载亚信威胁情报中心和可灵活扩展的配套安全探针。

亚信安全在运营商、政府行业和金融行业领域均有良好的客户基础和技术积累，且这几个行业将是新一代 SOC 建设需求最多的行业，亚信安全预期在 SOC 领域会有非常好的发展预期和收益。

4.5 瀚思

瀚思成立于 2014 年，提出以“数据驱动安全”为愿景，是大数据安全领域领先的创业公司。瀚思作为国内第一个以大数据安全为核心技术和产品的专业公司，拥有核心安全分析、 算法、 sandbox 领域以及异常检测 （ Anomaly Detection ） 和用户行为分析（ User Behavior Analysis ）的世界级专家，以及该领域 18 项全球核心专利，并积极倡导将机器学习应用于信息安全。

瀚思成立之初就采用了大数据平台架构来构建新一代安全运营中心，推出了国内唯一商用的用户行为分析 UBA 产品，开发了关联分析、用户行为分析、机器学习、威胁情报、流量分析 5 大安全分析引擎，在机器学习与深度学习应用在网络安全分析领域有比较领先的探索。同时在金融业务安全反欺诈领域也取得了客户应用案例。

瀚思在大数据安全分析领域的内在价值已被很多企业用户和投资者认可，在金融、政府、运营商的标杆客户中取得了典型应用案例，技术创新力和影响力都处于业界领先地位，也开发出了新一代SOC很多的应用场景。其新一轮1个亿的融资将推动瀚思建设行业营销队伍，在更多行业取得更大的规模营收。

4.6 东软

东软安全事业部近10年来一直是SOC建设领域的参与者，其在早期SOC市场中曾取得过明显的技术和市场优势。结合东软公司自身在部分特定行业的客户优势和软件定制化优势，东软SOC有良好的发展基础。目前东软安全事业部大约有50-100人从事SOC相关研发和技术工作，在金融行业、能源行业等取得了新一代SOC的典型案例。

东软新一代SOC解决方案在传统SOC的基础上，不仅有效集成了漏洞扫描、配置异动、策略基线、ITSM服务流程、等级合规，更是增添了极具创新性的业务应用建模监控，让用户随时随地掌控真正核心业务系统的运行状况。同时采用了大数据协同处理能力，与业务系统紧密结合，与友商共建安全生态体系，积极吸收威胁情报、舆论情报等情报，主动防御等。东软在提升自身技术能力，取得更多客户案例的同时，还应当注重打造业界的影响力。同时，在新一代SOC体系构建中，还应当加强SOC攻防能力和人机交互能力的建设，加强对威胁情报的利用，以及自动化响应机制的建设等。

4.7 华为

华为安全虽然只是华为公司很小的一块业务，但其有着深厚的网络设备厂商背景和强大的技术实力，是国内网络安全领域最重要的厂商之一。华为公司承建了很多行业客户的大数据平台，而新一代SOC作为大数据在安全行业的典型应用，自然为华为安全赢得了很多的项目机会和客户案例。目前华为安全已经形成了业界较为完备的新一代SOC和态势感知解决方案，拥有100多人的研发团队，其技术实力不容小觑。

华为的新一代SOC支持基于攻击链进行事件调查，通过不同的攻击阶段关联流量元数据，在流量元数据检索结果列表可以下载元数据相关的PCAP文件，在同一个界面方便安全运维分析人员进一步取证分析，调查效率高效快速。同时配备有专门的大数据威胁分析团队，研究机器学习算法，实现精准快速的威胁判定和异常行为检测。并通过威胁地图直观展示企业在全球范围内面的威胁和最近发现的威胁事件，方便安全运维分析人员能及时发现威胁、预判全网安全走势。

华为的新一代SOC解决方案在技术架构、研发能力、创新能力和协同能力上有着明显的优势，目前在金融、政府、公安等领域也取得了不错的业绩。结合其在网络基础设施领域的绝对领先优势，其高投入高产出的业务运营模式对其他厂商而言是一个压力。华为SOC解决方案技术领先、功能完备、性能卓越，其价格也较为昂贵，

偏向高端行业客户群。作为网络设备厂商，缺乏足够的安全专业服务队伍来辅助 SOC 的实施，需要与更多的合作伙伴一起，给客户真正交付安全运营的能力。

4.8 安恒

安恒是国内安全领域的新兴力量，经过十年的发展，已经由专注于 Web 和数据库安全的厂商，发展成为涵盖云计算安全，大数据安全以及应用安全、数据库安全、移动互联网安全、智慧城市安全等，包括安全态势感知、威胁情报分析、攻防实战培训、顶层设计、标准制定、课题和安全技术研究、产品研发、产品及服务综合解决方案提供商。

安恒新推出的关键信息基础设施安全防护管理平台，是一款针对等级保护、实时监测、态势感知、通报预警、快速处置的综合管理平台，是新一代 SOC 平台的典型模式。安恒的新一代 SOC 更侧重于态势感知能力的打造，融合了公司数据大脑的高级威胁情报关联分析能力，具备自学习能力，能自适应所处的分析环境，生成分析模型。如在公网自动生成潜伏型数据窃取分析模型；基于内部办公网络，自学习生成行为分析模型。具备工控、物联网安全分析能力，融合了公司安全研究院、海特实验室、卫兵实验室的安全研究成果等。

因此，安恒的新一代 SOC 更适用于政府和公安行业的态势感知需求，也取得了不多的客户案例和市场规模。目前投入上百人的研发队伍，不断完善解决方案，期待在更多的行业取得突破。

4.9 深信服

深信服成立于 2000 年，由最初的 VPN 和上网行为管理产品商，逐步发展成为在内容安全、边界安全、移动安全、云安全、应用交付、虚拟化、超融合等领域均取得重要地位的综合性网络和安全供应商。其推出的 SOC 和态势感知方案由于其独特的背景也具备独特的优势。

深信服作为国内最大的企业级上网行为管理和下一代防火墙设备供应商，提供了大量企业级信息安全威胁情报和安全事件处置经验，有丰富的威胁情报积累和分析能力。另外，深信服具备很强的应用识别能力和网络原始流量分析能力，而这正是新一代 SOC 的重要基础能力之一。目前深信服也投入了几十人的 SOC 研发人员，并拥有数百人的专业安全实验室团队，跟踪分析最前沿的攻击技术、专职的大数据建模博士团队，确保分析平台总是能够得到最新行为分析技术支持。

深信服在企业级市场有良好口碑和客户基础，也为其 SOC 解决方案在政府和企业级客户取得了不错的案例。随着新一代 SOC 和态势感知市场的不断成熟，深信服也将整合更多的资源投入这一领域，并取得更大的规模和影响力。

4.10 新华三

新华三是国内著名的网络设备公司，有庞大的企业级网络客户市场。在安全领域也推出了一系列的网络安全设备和产品，规模增长迅速，取得了重要的行业位置。H3C 的 SOC 和态势感知解决方案也是今年推广的重点。

在安全管控上，H3C 具备天然的优势。当发现安全事件时，通过新一代 SOC 产品，可以直接对接入交换机进行操控，比如将攻击源下线，从而达到构建立体防御体系的目的。目前 H3C 以新一代 SOC 平台为核心，打通“云”、“网”、“端”各个区域。云端集合威胁情报数据，网端进行业务访问管控，终端审计用户行为。当用户上线后，可以针对用户身份自动向防火墙设备下发访问策略，有效提升管理效率。

另外 H3C 除了拥有自己的攻防团队，能够独立对发掘各种病毒、木马特征外，还积极和国内外伙伴合作，包括 CVE、MAPP、Commtouch 等，同时是 CNVD、CNNVD 的一级成员单位，能够及时获取最新、最及时的威胁特征等。

新华三的 SOC 解决方案依托其在企业级网络基础设施的优势，在政府、教育、医疗等领域有明显的行业优势，也取得了不少的案例，随着市场的不断成熟，新华三有望不断扩大市场规模，并在中大型客户群取得一定的优势。

4.11 上海观安

上海观安成立于 2013 年，是国内新兴的以大数据为核心技术的专业安全公司，发展非常迅速，推出了大数据安全分析平台产品和安全风险感知产品等。

观安的安全与研发团队在安全领域具备十多年的经验，具备较强的安全分析和产品工程化能力。利用安全态势平台的威胁情报中心，收集企业外部的安全风险信息，结合内外部面临的安全威胁进行全面的安全态势感知。利用大数据平台强大的数据存储和处理能力，存储内外部海量的数据，并利用大数据算法分析模型对海量数据进行挖掘，对潜在的安全风险进行分析等。

上海观安目前已经投入了数十人的研发力量专注在大数据安全分析平台和态势感知产品，在移动运营商、能源和企业级客户也取得了典型案例，具备了一定的规模和影响力，是新兴安全公司在这一领域的代表力量。

4.12 兰云科技

兰云科技成立于 2016 年初，主要定位于未知威胁防御、大数据安全、网络安全态势感知、云安全解决方案等领域，对外提供的产品包括兰眼下一代威胁感知系统和兰天网络安全态势感知平台，提供的服务包括高级威胁应急响应服务和 DDoS 流量清洗服务等。

兰云科技的核心人员来自于华为、阿里巴巴等领先企业，其推出的安全态势感知平台，在融合各种网络安全要素的基础上从宏观的角度实时评估网络的安全态势，并在一定条件下对网络安全态势的发展趋势进行预测。通过数据采集、机器学习、语义网络、关联分析、情报分析、数据挖掘等大数据分析技术手段，实时评估网络的安全态势，提高网络的监控能力、应急响应能力和预测网络安全的发展趋势等。

兰云科技属于新一代的安全创业公司，大数据、机器学习是其发展基因，具备良好的技术能力。随着市场的成熟和公司的成长，其规模和影响力也将逐步增强。

4.13 安博通

安博通成立于 2007 年，以“看透安全，体验价值”理念为核心，致力于新一代网络应用安全和数据分析的产品研发及技术服务，是网络安全可视化理念的率先实践者。安博通安全威胁态势可视化平台，基于已有信息化和数据建设成果，首先通过广泛的数据采集手段收集网络中的流量和安全事件信息，然后运用先进数据建模、机器学习、关联匹配技术进行数据分析；最后利用大数据分析技术结合用户自身业务情况对网络进行实时监测和全局安全威胁态势感知。

安博通的态势感知解决方案在提供传统 SOC 和态势感知安全威胁列表及图形呈现方式的同时，还提供了一种以全网安全策略态势和访问路径为视角的信息安全管理与态势感知呈现方式，为安全威胁的分析和发现提供一种全新视角；尤其在策略可视化方面有比较明显的优势，协助客户看深、看透企业内部网络安全，实现对企业内部架构和威胁的可视化。

垂询及订阅请联系

电话 /Tel：+86-10-51626974

邮箱 /E-mail：zuojing@aqniu.com

安全牛网址：http://www.aqniu.com