G00290113

魔力象限之安全信息和事件管理

发布于 2016 年 8 月 10 日

分析师： Kelly M. Kavanagh、Oliver Rochford、Toby Bussa

摘要

对定向攻击的早期检测和响应的需求，成为扩展已部署和新建设 SIEM 的主要驱动力，高层阶用户主动寻求具备高级侧写、分析和响应能力的 SIEM 平台。

战略规划预期

到 2017 年末，至少 60% 的主要 SIEM 提供商将提供一体化的高级分析和 UEBA （ USER + ENTITY BEHAVIOR ANALYTICS ）功能的产品。

市场定义/描述

安全信息及事件管理 (SIEM) 市场的存在是因为客户需要实时分析事件数据，尽早检测针对性攻击和数据漏洞，并收集、存储、调查和报告日志数据，以便进行事件响应、取证并实现监管合规性。我们的魔力象限分析中包括的供应商的产品也旨在实现这一目的，而且他们可主动将这些技术推销和出售给安全购买中心。

SIEM 技术集合了由安全设备、网络基础架构、系统和应用生成的事件数据。主要数据源为日志数据，但 SIEM 技术也可处理其它形式的数据，如 NetFlow 和网络数据包。可将事件数据与用户、资产、威胁和漏洞方面的情境信息结合起来。数据是标准化的，因此可关联并分析各种来源的事件、数据和情境信息，以便实现网络安全事件监控、用户活动监控和合规性报告等特定目的。借助该技术，可实时关联相关事件，进而对历史分析和其它的事件调查支持和合规性报告进行安全监控、查询和分析。

魔力象限

图 1. 安全信息和事件管理魔力象限

来源：Gartner（2016 年 8 月）

供应商优势和注意事项

AlienVault

AlienVault Unified Security Management (USM) 解决方案可提供 SIEM、漏洞评估 (VA)、资产发现、网络和主机入侵检测 (NIDS/HIDS)、流量和数据包获取和文件完整性监控 (FIM)。AlienVault USM 可针对所有 AlienVault 组件进行集中配置和管理。AlienVault USM for Amazon Web Services (AWS) 是一种 AWS 原生版本，可提供资产发现、漏洞评估、监控并提醒 CloudTrail、Simple Storage Service (S3) 和 Elastic Load Balancing (ELB) 访问、日志管理和事件关联。AlienVault USM 由开放式漏洞评估系统（OpenVAS；VA）、Snort、Suricata（入侵检测系统 [IDS]）和 OSSEC (HIDS/FIM) 等开源组件组成，而且可将这些组件与 SIEM 结合起来，以便提供统一的安全解决方案。USM 买家可访问基于订阅的威胁情报服务，该服务由关联指令、IDS 签名、漏洞检查、报告和响应模板组成。此外，免费的开放式威胁交互 (OTX) 及其社区有助于讨论并共享威胁信息。AlienVault 可提供开源 SIM (OSSIM) - 其解决方案的一种免费的开源版本，所具备的功能相对较少。AlienVault USM 可借助扩展增强功能、日志管理、统一管理和报告以及各种托管安全服务提供商 (MSSP)，对 OSSIM 进行扩展。

AlienVault USM 既可用于虚拟设备，也可用于硬件设备。USM 的传感器、记录器和服务器组件可部署在一个系统中，或作为横向和纵向层中的不同服务器进行部署，进而扩展至不同的客户环境。在过去的一年里，AlienVault 的功能更新包括改善资产曝光度和代理管理、加快报告更新速度并加强与 OTX 的集成。需要各种成本较低的集成安全功能的企业应考虑借助 AlienVault USM 平台实现内部部署环境和 AWS 环境。

优势

- AlienVault USM 可提供各种集成安全功能，包括 SIEM、文件完整性监控、漏洞评估、资产发现以及基于主机和基于网络的入侵检测系统。
- USM 具有精心设计的界面，能够导航事件、资产和威胁情报，进而根据杀伤链框架对事件进行调查。
- 客户表示，与 SIEM 领域的大部分竞争对手所提供的产品相比，USM 所提供的安全监控技术的成本更低、功能更多。
- AlienVault 能够根据所利用的设备而非事件数量或事件来源数量简化许可模型。

注意事项

- USM 可提供 NetFlow 捕获信息、资产的基本统计信息和情境，但无法从 NetFlow 生成相关提示。
- 与竞争产品相比，集成不支持的数据源是比较繁琐的。或者，用户可请求 AlienVault 开发一个插件，以便进行集成。

- 尽管身份活动可以与资产有关，但 USM 只可提供基本事件数据增强和用户情境；而且身份和访问管理 (IAM) 集成，仅限于 Active Directory 和 LDAP。
- AlienVault 的工作流功能不包括集成外部凭单系统或基于角色的工作流分配。

BlackStratus

BlackStratus 有三种产品：LOGStorm、SIEMStorm 和 CYBERShark。LOGStorm 可提供针对 MSSP 和中小型企业的日志管理功能，而且可作为虚拟设备和硬件设备。SIEMStorm 可提供多租户和安全事件管理 (SEM) 等功能，具体包括分析、历史关联性和威胁情报集成，而且可部署为软件或虚拟镜像。SIEMStorm 能够与 LOGStorm 一同部署，并将 LOGStorm 作为存储层和收集层。BlackStratus 最近引入了 CYBERShark，这是一种针对采用 LOGStorm 和 SIEMStorm 的中小型企业 (SMB) 的基于云的 SIEM 即服务产品。

LOGStorm 和 SIEMStorm 可提供基于 SANS 七步事件补救流程的集成事件管理凭单系统，而且 SIEMStorm 还有助于跟踪 SLA 指标，以便适应 MSSP 和以服务为中心的环境。

在过去的一年里，BlackStratus 已添加了一种新的合规性报告模板集，该模板集有助于为提供商打造门户品牌，而且 BlackStratus 还发布了重新设计且经过更新的 HTML5 Web 用户界面。

BlackStratus 非常适合于需要可定制 SIEM 平台的服务提供商，以及希望得到结构良好多租户支持的以服务为中心的终端企业用户。

优势

- SIEMStorm 和 LOGStorm 可部署为虚拟机，而且包含能够集成数据源的安装向导和无源自动发现功能。
- LOGStorm 和 SIEMStorm 可提供双向集成 API，因此能够启用自定义服务架构。
- LOGStorm 和 SIEMStorm 包含基于 SANS 事件处理流程的充分集成的事件和凭单管理系统。
- BlackStratus 因其响应速度和专业知识而得到了客户的一致好评。

注意事项

- 对于第三方数据源的开箱即用的支持是有限的，而且通常需要自定义脚本。
- 目前不支持网络取证、深度数据包检测 (DPI) 以及 IAM 集成等高级安全功能。尽管支持 Proofpoint，但其它商业威胁源需要供应商的支持才能产生影响。
- 客户反馈表明，日志事件数据的特别查询可以更精细一些，而且缺乏布尔逻辑。
- BlackStratus 专注于针对安全服务提供商的销售，而在终端用户部署的竞争性评估方面的优质不太明显。

EMC (RSA)

2016 年 7 月，EMC 安全部门 RSA 把 SIEM 产品命名为 RSA NetWitness Suite，包括 RSA NetWitness Logs、RSA NetWitness Packets、RSA NetWitness Endpoint、RSA NetWitness SecOps Manager（原来分别为 RSA Security Analytics、RSA Enterprise Compromise Assessment Tool (ECAT) 和 RSA SecOps）。RSA NetWitness Suite 可利用来自于安全事件和其它日志源、网络全数据包捕获、NetFlow 和终端（通过 NetWitness Endpoint）的数据提供对于威胁的可见性。RSA NetWitness 系统专注于实时监控、分析和报警，此外还支持主动威胁搜索、事件响应和取证调查。该平台可利用一个或多个物理或虚拟设备进行日志和数据包捕获（解码器）、查询和原始数据检索（集中器）、实时分析（事件流分析）、长期日志存储和报告（归档器）。混合设备（将解码器和集中器整合至一个系统）可用于较小的环境。解码器和集中器设备以及代理可支持大型区域性分布架构。NetWitness 服务器可提供统一的管理和分析界面。它还可提供一种报告恶意软件分析引擎的界面。RSA Live Connect 为基于云的服务，可自动更新检测规则、数据包和日志解析器、报告和威胁情报源等内容。RSA NetWitness Suite 用户也可利用 RSA NetWitness SecOps Management（RSA Archer 治理、风险和合规性 [GRC] 解决方案中的一个模块），进而增加高级事件管理工作流、运营战术、管理仪表盘和报告。

在过去的一年里，利用行为分析、选择性日志保留、事件源集成和分组等功能提升，RSA 已经增加了命令与控制通信检测，而且能够通过集成 CloudTrail 日志来支持 AWS 监控。

企业的专用安全运营中心 (SOC) 和事件响应团队或需要对日志和网络流量进行安全监控以检测、验证威胁并进行取证调查的那些企业应考虑采用 RSA NetWitness Suite。

优势

- RSA NetWitness 平台结合了各种网络流量、终端和其它安全事件和日志数据源的威胁检测分析和事件监控、调查和威胁情报。
- 借助模块化部署选项，客户可根据需要选择网络流量监控、事件和日志监控以及分析功能。
- RSA Live 可提供一种简单的自动化方法确保无缝交付并实施威胁情报、内容和其它更新。
- 通过与 RSA NetWitness SecOps Manager 集成提供统一的 SOC 功能。现有 Archer 用户将从能够在整个企业内进行集中式风险管理、度量和报告的集成中受益。

注意事项

- 据客户反映，RSA NetWitness Suite 是一种复杂的 SIEM 技术，需要为了达到预期的使用场景进行实施和调整。
- 与竞争产品相比，RSA NetWitness 的用户界面较为普通。与其它 SIEM 解决方案相比，原本开箱即用的仪表盘，需要更多的定制开发。
- RSA NetWitness 只可提供轻量级事件管理功能。RSA SecOps Manager 可提供 Richer 工作流功能。

EventTracker

EventTracker 的 SIEM 软件和服务产品主要针对的是具有安全事件管理和合规报告要求的中型企业和政府机构。EventTracker Security Center 可作为软件使用，其许可以数据源的数量为基础。标准组件包括关联、警报、行为分析、报告、仪表盘和大量事件源知识包。选项包括配置评估、变更审计 FIM、ntopng、威胁情报源（开源或商务订阅）和分析数据集市。服务产品包括与基于每日、每周的时间表进行的运行、观察、调整和遵守活动一致的年度订阅。AWS 和 Azure 中的收集和部署均具有本地支持。

在过去一年里添加的功能包括未知的流程检测和黑名单/白名单、IP 信誉集成和警报、第三方威胁分析仪表盘以及其它威胁情报源选项。添加了 JSON 支持和提取、转换和加载 (ETL) 格式日志，而且重写了用户界面，可支持触屏移动设备。

需要在内部部署 SIEM 或云端托管 SIEM 中通过可选、灵活的监控服务获取日志和事件管理软件解决方案、合规报告和操作监控的中型企业，应当考虑采用 EventTracker。

优势

- EventTracker 易于部署和维护，而且其合规性和特定使用实例知识包可提供预置的警报、关联规则和报告。
- 样板客户和 Gartner 客户对 EventTracker 的支持、打包报告和新的报告创建功能给予了较高的评价。
- EventTracker 包括一种具备基本分析和异常检测功能的行为分析模块。
- EventTracker 的与运行、观察、调整和遵守活动一致的系列服务产品是一种区别因素，能够满足其目标市场的需求。

注意事项

- 供应商的目标是中端市场，但在客户名单上其可见性并不如同样针对这一市场的 SIEM 供应商。
- EventTracker 的高级威胁检测功能是基本的，以 Windows 为中心的。在捕捉流量和数据包时，这些功能不会完全集成至核心产品，而且无法与第三方高级威胁检测/响应技术集成。
- 与针对企业部署的 SIEM 产品相比，EventTracker 的应用监控功能更为有限，因为它不能集成主要的应用包。
- 凭单等完整的事件管理需要外部解决方案。部分集成支持通过电子邮件和 XML 进行。

Fortinet (AccelOps)

2016 年 6 月，Fortinet 宣布已经收购 AccelOps，计划将其 SIEM 产品更名为 FortiSIEM 并集成至 Fortinet Security Fabric；举例来说，与 Fortinet 的专注于网络和云环境监控的 APM 解决方案集成。AccelOps SIEM 可提供 SIM 和 SEM、文件完整性监控、配置管理数据库 (CMDB)、可用性和性能监控 (APM) 功能。AccelOps 主要专注于为安全运营、托管服务提供商 (MSP) 和 MSSP 提供解决方案。

AccelOps 具有数量不大的 MSP 和 MSSP 客户，这些客户可利用其 SIEM、CMDB 和 FIM 功能进行安全和网络监控，而且 AccelOps 是具有 IT 和网络运营使用实例功能的少数供应商之一。Fortinet 现在有机会将 AccelOps SIEM 销售范围扩大至其服务提供商和终端用户客户群。

在过去的一年里，AccelOps 扩展了其 SIEM 产品范围，并将基于云的 SIEM 即服务产品纳入至针对 MSP、MSSP 以及使用 AWS 和 Azuretiers (Basic, Plus and Pro) 的企业的三种层次的产品（基本版、加强版和专业版）。其它增强功能包括对于虚拟化和公有云服务（Hyper-V、Xen、OpenStack 和 Azure）的额外支持, 改善威胁源集成以及对于网络和终端高级威胁检测解决方案的额外支持。AccelOps 还通过引入 Apache Kafka 更新了其架构，进而更好地集成大数据平台。

AccelOps SIEM 非常适合于中端市场企业以及需要集合安全监控、APM 以及集成式 CMDB 功能的 MSP 和 MSSP。此外，AccelOps SIEM 也非常适合于具有综合性 IT、网络和安全运营功能的 IT 运营团队，以及需要多租户功能以分离角色和职责的企业。

优势

- IT、网络和安全运营团队可利用 AccelOps SIEM 的安全和运营功能来提供整个企业的统一环境视图，包括物理和虚拟环境以及公有云、私有云和混合云。
- 对整个 IT 环境具有集中监控和响应责任的中端市场企业将从能够启用统一平台的 AccelOps 集成中受益。
- AccelOps 主要专注于集成运营和安全功能，以便支持修复和事件管理。
- 据客户反映，该技术相对较易部署，而且客户给出了对于定制的深度和灵活性的积极反馈。

注意事项

- 现有 AccelOps 客户应要求 Fortinet 保证 SIEM 和相关平台产品的开发路线图将继续支持第三方技术或扩大对于第三方技术的支持范围。
- AccelOps SIEM 在高级分析功能、直接与 Hadoop 等大数据平台集成、集成用户和实体行为分析 (UEBA) 等补充性解决方案方面的竞争中较为落后。
- AccelOps 在 Gartner 客户的 SIEM 竞争性评估中的受关注程度非常低。Fortinet 在 SIEM 市场中的销售和部署支持功能尚未得到证明。

HPE

Hewlett Packard Enterprise (HPE) 销售 ArcSight SIEM 平台给中型企业、大型企业和服务提供商。该平台具有三种变体：ArcSight Data Platform (ADP)，提供日志收集、管理和报告；ArcSight Enterprise Security Management (ESM) 软件，进行大规模安全监控部署；ArcSight Express，针对中端市场的一种基于设备的一体化产品，提供预配置监控和报告以及简化的数据管理。

ArcSight Data Platform（由 ArcSight Connectors、ArcSight Management Center [ArcMC：一种管理控制台] 和 Logger 组成）可独立部署为一种日志管理解决方案，但也可用作 ArcSight ESM 部署环境的数据收集层。增加用户和实体行为分析 (ArcSight User Behavior Analytics [UBA])、DNS 恶意软件检测 (ArcSight DNS Malware Analytics) 和威胁情报 (ArcSight Reputation Security Monitor [RepSM]) 等功能的高级模块可扩展 SIEM 的功能。

HPE ArcSight 可部署为一种设备、软件或虚拟实例，而且可借助能够管理大型部署和复杂部署的 HPE ArcSight Management Center 来支持可扩展的 n 层架构。HPE ArcSight Express 只可作为一种设备。

2015 年，HPE 重新设计并简化了 ArcSight SIEM 架构和许可模型。其它增强功能包括分析师使用管理界面中新功能，这些新功能有助于更为严格地控制传入事件和突发事件。新版本的模块包括 HPE ArcSight UBA（来自 Securonix 的许可）、提供基于 DNS 流量分析的恶意软件检测的 HPE ArcSight DNS Malware Analytics、能够与其它供应商解决方案集成的一种社区 HPE ArcSight Marketplace 以及仪表盘和报告模板等 SIEM 情境。

ArcSight Express 应用于需要大量第三方连接器支持的中型 SIEM 部署环境。HPE ArcSight ESM 非常适合于大规模部署和希望来构建专用 SOC 的企业。

优势

- ArcSight ESM 可提供一整套能够支持大规模 SOC 的 SIEM 功能，包括全面的事件调查、管理工作流以及专用的部署管理控制台。
- HPE ArcSight User Behavior Analytics 可提供与 SIEM 有关的完整的 UBA 功能。
- HPE ArcSight 具有各种开箱即用的第三方技术连接器和集成。

注意事项

- 与同类产品相比，HPE ArcSight 产品通常需要包含更专业的服务支持。
- 客户反馈表明，与其它领先的解决方案相比，HPE ArcSight ESM 更为复杂而且部署、配置和运营成本更高。

- 尽管 ArcSight 在对于 Gartner 客户的竞争曝光度方面为四大顶级供应商之一，但是趋势表明对于新安装的客户和越来越多的竞争性替代产品而言这种优势在日益淡化。
- HPE 正致力于开发并重建核心 ArcSight 技术平台。客户和潜在买方应对开发计划进行跟踪，以便确保支持现有或规划部署环境所需功能的可用性。

IBM

IBM 的 QRadar Security Intelligence Platform 由 QRadar Log Manager、Data Node、SIEM、Risk Manager、Vulnerability Manager、QFlow、VFlow Collectors 和 Incident Forensics 组成。可利用物理和虚拟设备以及基础架构即服务（IaaS，如公有云或私有云服务）部署 QRadar。QRadar 还提供作为服务的解决方案(IBM QRadar on Cloud)，该解决方案完全由 IBM 管理并拥有的安全事件监控团队 IBM Managed Security Services 提供 。部署选项涵盖一体化全交付或拼图式集成各种设备的各项功能的扩展。在 QRadar 平台中对全部支持的数据源，进行汇集并分析安全事件和日志数据、使用深度数据包检测对 NetFlow，网络流量监控，甚至数据全包捕获和行为分析。

IBM 介绍过去 12 个月里的一些新功能和能力，包括共享威胁情报的 IBM X-Force Exchange 以及由 QRadar Application Framework 支持的 IBM Security App Exchange 应用商店。 2016 年 4 月 IBM 还收购了 Resilient Systems，为延伸扩展 QRadar 平台的安全应急事件响应能力。功能增强来自多租户支持、系统管理（运行状态监控和补丁管理）和搜索性能均得以提升。

拥有通用 SIEM 需求的中型及大型企业，包括为建设自身 SOC 安全运营中心的安全事件监控和响应平台的企业应考虑采用 QRadar。甚至希望找到一个能够灵活部署实施、运营托管和监控的解决方案的中型企业也应考虑采用 QRadar。

优势

- QRadar 提供集成视角的日志和事件数据、网络监控流量和数据包、漏洞和资产数据以及威胁情报的集成视图。
- 跨越 NetFlow 网络流量和日志事件中的安全事件关联进行行为分析。
- QRadar 模块化架构支持 IaaS 环境中的安全事件和日志监控，包括对于 AWS Cloud Trail 和 SoftLayer 的本机监控。
- 无论是作为一体化设备还是多层、多站点环境，QRadar 技术和架构的部署和维护都相对简洁。
- IBM Security App Exchange 具备提供安全框架，集成第三方技术功能至 SIEM 仪表盘以及调查和响应的工作流。

注意事项

- 终端监控的威胁检测和响应，基线文件完整性的需要利用第三方技术。
- Gartner 客户表示他们在集成 QRadar 的 IBM 漏洞管理插件方面成败不一。
- Gartner 客户表示 IBM 的销售流程比较复杂，而且需要耐心。

Intel Security

Intel Security 提供 McAfee 企业安全管理器 (ESM) 形态包括物理设备、虚拟或软件平台。 SIEM 产品的三种主要组件为 ESM、Event Receiver (ERC) 和 Enterprise Log Manager，这些组件可一同作为一个实例进行部署，或在分布式环境或大规模环境中单独部署。可选组件包括 Advanced Correlation Engine (ACE)、Database Event Monitor (DEM)、Application Data Monitor (ADM) 和 Global Threat Intelligence (GTI)。

过去一年里引入的增强功能包括：能够动态填充其它内部或外部来源的观察列表、与 Hadoop 进行更为深入的双向集成并支持以其它方式访问并管理威胁情报源。现在，与 McAfee Active Response 集成可为 ESM 提供更为强大的终端曝光度。McAfee Enterprise Security Manager 是采用其它 Intel Security 技术的企业以及那些希望找到包括响应功能的集成安全框架的企业的理想之选。

优势

- Intel Security 的 McAfee ePolicy Orchestrator (ePO) 客户对于 ESM 的深度集成给出了高度评价。
- Enterprise Security Manager 充分覆盖了运营技术（行业控系统[ICS]）、检测控制和数据采集 (SCADA) 设备。
- Intel Security 的 McAfee Data Exchange Layer (DXL) 能够在不使用 API 的条件下集成第三方技术。该方法能够将 ESM 作为一种 SIEM 平台。

注意事项

- Intel Security 在终端情报和自动响应等领域的很多高级 SIEM 功能都需要集成其它 Intel 组合产品或提高在其它 Intel 组合产品上的投资。
- Intel 具备的高级分析功能以及与第三方工具进行的集成较为有限。可通过 ACE 识别基线和变体并进行基于风险的分析。不过，Intel Security 不具备预测性分析功能，而且其它内置功能也不及那些领先的竞争对手强大。
- ESM 具有强大的工作流功能。不过，开箱即用的集成只对 Remedy 开放。对其它工作流产品的支持仅限于电子邮件或开发 ESM API。

- 在过去一年里，用户和 Gartner 客户一直反映 ESM 的稳定性和性能不佳。
- 用户还特别强调在技术支持方面感到不满意。
- 在过去的一年里，McAfee ESM 在 Gartner 客户查询方面的曝光度有所下滑，而且客户关于替代产品的讨论也增多了。

LogRhythm

LogRhythm 销售 SIEM 解决方案给大中型企业。LogRhythm 的 SIEM 可部署在设备、软件或虚拟实例格式中，而且可支持由 Platform Manager、AI Engine、Data Processors、Data Indexers 和 Data Collectors 组成的 n 层可扩展的分散化架构。此外，还可以进行统一的一体化部署。可部署 System Monitor 和 Network Monitor，进而提供终端和网络取证功能，如系统流程、文件完整性和 NetFlow 监控、DPI 和全数据包捕获。LogRhythm 可将事件、终端和网络监控功能与 UEBA 功能、集成式事件响应工作流和自动响应功能集成一体。

LogRhythm 已在去年拆分 SIEM 解决方案的日志处理和索引为两个独立的组件，进而添加了具备非结构化搜索功能的基于 Elasticsearch 的存储后端。此外还添加了集群全数据复制功能。其它增强功能包括改进了风险优先级 (RBP) 评分算法、增加了 Network Monitor 应用和协议的解析器、提供对于 AWS、Box 和 Okta 等云服务的支持，并集成了云访问安全代理 (CASB) 解决方案，包括 Microsoft 的 Cloud App Security 和 Zscaler（原 Adallom）。

LogRhythm 非常适合于需要集成式高级威胁监控功能以及 SIEM 的企业。那些安全团队需要高度自动化和开箱即用内容且资源有限的企业也可考虑采用 LogRhythm。

优势

- LogRhythm 可将 SIEM 功能与终端监控、网络取证、UEBA 和事件管理功能集成一体，进而支持安全运营和高级威胁监控使用实例。
- LogRhythm 可提供互动性强且可定制的用户体验、动态情境集成和安全监控工作流。
- LogRhythm 可提供新兴自动响应功能，能够在远程设备上执行动作。
- Gartner 收到了一致的用户反馈，这些用户普遍认为 LogRhythm 的解决方案易于部署和维护，而且提供了有效的开箱即用使用实例和工作流。
- LogRhythm 在 Gartner 客户的竞争性 SIEM 技术评估中一直非常引人注目。

注意事项

- 尽管 LogRhythm 的系统监控器和网络监控器等集成式安全功能有助于使来自 SIEM 的深度集成的 IT 实现协同，然而具备该领域的关键 IT 和网络运营需求的企业应针对相关局部解决方案进行评估。
- 客户反馈表明，自定义报告引擎是一项需要改进的功能。

- 与其它领先的 SIEM 供应商相比，LogRhythm 所具有的销售和渠道资源较少，而且北美以外地区的买家在转售商和服务合作伙伴方面的选择较少。

ManageEngine

ManageEngine 是隶属于 Zoho 的一家分公司，可利用 ManageEngine EventLog Analyzer 和 ADAudit Plus 产品提供 SIEM 功能。Log360 可将上述两种工具集成至单个产品。EventLog Analyzer 具备日志管理、监控、分析、关联和归档以及警报和报告功能。ManageEngine 具有两种版本 — 单一实例部署高级版，以及需要能够扩展至单一 EventLog Analyzer 实例之外的大型企业或 MSP 分布式版本。分布式版本可利用管理服务器来管理和提供个人托管服务器的单一视图。ADAudit Plus 专注于活动目录的监控、警报和审核，进而将用户情境提供给 EventLog Analyzer。ADAudit Plus 分为两种版本 — 标准版和专业版，具体取决于所需的功能。EventLog Analyzer 和 ADAudit Plus 都可作为能够利用 PostgreSQL 数据库进行存储的 VMware 镜像，而且都主要依赖于安全事件和日志收集的无代理方法。EventLog Analyzer 的许可以生成安全事件或事件日志的主机、设备或应用的数量为基础。

在 IT 服务和 IT 运营和管理领域，ManageEngine 是一家知名供应商。已经采用了其它 ManageEngine 工具以及正在寻找简单且顾虑成本效率，添加安全事件监控功能的企业应考虑采用 EventAnalyzer 或 Log360。

优势

- ManageEngine 可提供一种易于部署且能够通过 syslog 或日志导入快速集成的设备。
- 包括各种合规性报告在内的 1,000 多种预定义报告能够覆盖典型 IT 环境中的各种设备和应用。
- ADAudit Plus 可为仅利用活动目录来识别和访问控制的企业提供全面的记录和审计功能。

注意事项

- EventAnalyzer 具备基本的 SIEM 功能，但在一些关键领域落后于竞争对手，如安全运营和监控仪表盘、事件管理工作流、威胁情报源和平台支持、网络流量和 NetFlow 监控。
- 尽管 Log360 可集成 EventAnalyzer 和 ADAudit Plus，但分析师至少需要利用两种用户界面来执行各种活动，如监控新事件、调查和报告。
- 因为 ADAudit Plus 针对的是中小型企业，所以大型企业需要对于可扩展性、性能和支持方面的要求进行认真评估。
- SIEM 使用实例的 Gartner 客户极少关注 ManageEngine。

Micro Focus

NetIQ 于 2014 年被 Micro Focus 收购。Sentinel Enterprise 是 Micro Focus 的核心 SIEM 产品，而且通过 Change Guardian（用于主机监控和 FIM）和 Secure Configuration Manager（用于合规性使用实例）进行了补充。其它模块添加了包括威胁情报源、攻击检测和高可用性支持在内的一系列功能。NetIQ Identity Manager 和 Aegis 客户还可从与 Sentinel 进行的集成中获益，进而改善身份跟踪和工作流管理功能。日志管理可作为一款独立性产品 (Sentinel Log Manager)。Sentinel Enterprise 可作为软件和虚拟设备予以提供。

Micro Focus 在过去的一年里对 Sentinel 进行了适当改进，主要专注于可用性增强功能、平台运行状况和管理、虚拟化、简化部署以及改善威胁情报。

Sentinel 很适合于需要对高度分布的 IT 环境（如地理环境或云环境）进行大规模安全事件处理的企业或 MSSP，而且也非常适合于已经部署了 NetIQ IAM 和 IT 运营工具的企业，因为这些工具能够针对利用 Sentinel 检测的安全事件提供丰富情境。

优势

- Sentinel Enterprise 适合于专注于 SEM 和 SIM 威胁监控功能的大规模部署，因为可自动将情境信息添加至任何相关事件。
- 与其它 NetIQ 技术集成有助于支持用户监控、身份和终端监控和执行/响应使用实例。
- NetIQ 的架构是一种比较容易部署和管理的架构。扩展和分配只需要安装更多 Sentinel 实例。
- 除标准 Windows、Unix 和 Linux 平台以外，Sentinel 还支持主机平台监控。
- NetIQ 客户对于 Sentinel 的可扩展性和性能、定制现有报告模板的简易性和支持体验给出了中等以上水平或中等水平的评价。

注意事项

- NetFlow 数据只可用于为所提醒的事件提供额外情境，不可用于关联规则。
- Sentinel 的威胁情报功能仍落后于竞争对手。客户可从 NetIQ 购买威胁源。此外，Sentinel 对于一些开源来源来说具有基本支持，但第三方来源需要创建软件开发套件 (SDK) 插件，而且不支持 STIX、TAXII 等开放标准。
- 不能支持和集成 UEBA 工具，而且高级分析功能与竞争对手的产品相比也较为落后。
- 与部分竞争对手相比，重现关联规则的历史事件数据时，其结果的可用性和报告是有限的。
- NetIQ Sentinel 在 Gartner 客户的 SIEM 竞争性评估中的曝光度不高。

SolarWinds

SolarWinds Log & Event Manager (LEM) 软件可作为虚拟设备提供。具体架构包括 LEM Manager（可用于集中日志存储和管理）、LEM Console（可用于数据显示和搜索），以及多种可供选择的代理。LEM 可提供基本的防数据丢失 (DLP) 功能、FIM，以及面向 Windows 主机的自动响应功能。

2015 年，SolarWinds 添加了"零配置"威胁情报源，旨在针对有一定知名度的 IP 黑名单提供定期威胁情报更新。

SolarWinds 将 LEM 定位为一种易于部署和使用的 SIEM 产品，以便为资源受限且无大数据需求的安全团队提供高级分析工具或高级威胁检测功能。LEM 可与其它 SolarWinds 产品集成以实现运营监控，从而为变更检测、根本原因分析等操作提供支持。对于需要 SIEM 技术支持的企业来说，SolarWinds LEM 软件是非常理想的选择，它能够提供简便的架构，同时也十分适于希望结合运用 SIEM 技术和其它 SolarWinds IT 运营解决方案的用户。

优势

- SolarWinds LEM 采用简单的架构设计，可提供丰富的开箱即用内容，适于多种 SMB 合规性及安全运营使用实例。
- 此项技术非常适合已投资其它 SolarWinds 技术解决方案的组织，他们能够以集成方式实现这些解决方案的协同增效。
- 基于 Windows 终端代理的自动响应功能有助于控制威胁，同时也支持隔离控制功能。
- SolarWinds 可提供简化许可模式，具体依据资产统计情况而非资产消耗情况。
- 据 SolarWinds 客户反映，他们普遍对 LEM 较为满意，认为这款产品不仅功能强大，而且成本效益高。

注意事项

- SolarWinds LEM 只提供基础的统计数据和行为分析功能，并未集成用户行为分析功能或大数据平台。
- SolarWinds 不针对第三方的高级威胁防御技术提供专有支持。
- 如果客户需要更广泛的用户、应用或网络监控功能，那么他们必须使用其它 SolarWinds 产品来扩展 LEM 中的功能。
- 尽管 LEM 包含一个本地的流捕获和显示功能，但 LEM 无法实时关联流数据，亦不支持数据包捕获。
- SolarWinds 的 SIEM 架构支持 LEM 实例的水平扩展，但是不支持真正的分布式 n 层扩展。

Splunk

Splunk Security Intelligence Platform 由 Splunk Enterprise 和 Splunk Enterprise Security (ES) 组成，前者是 Splunk 的核心产品，能利用 Splunk 查询语言提供事件和日志记录、查询和可视化功能，后者则增加了安全特定的 SIEM 功能。数据分析是 Splunk Enterprise 提供的主要功能，用于 IT 运营、应用性能管理、商务智能，并且如果企业还实施了 Enterprise Security，那么企业就会越来越多地利用数据分析监控和分析安全事件。Splunk Enterprise Security 提供预定义的仪表盘、关联规则、搜索、可视化和报告功能，以支持实时安全监控和警报、事件响应，以及合规性报告等使用实例。Splunk Enterprise 和 Splunk Enterprise Security 提供多种部署选项，包括企业内部、公有云、私有云以及混合部署选项。此外，这两款产品都能以 SaaS 形式交付。Splunk 的架构包括流输入和 Forwarder（用于摄取数据），Indexer（能索引和存储原机器日志）和 Search Head（能通过网络 GUI 接口提供数据访问）。

2015 年年中，Splunk 收购了 Caspida 并借此增加了本地 UEBA 功能，而 Caspida 也改名为 Splunk UBA（Splunk 也能与多种其它 UEBA 产品协同运行）。2016 年年初，Splunk 进一步集成了 Enterprise Security 与 UBA 产品。同时，他们还改进了事件管理和工作流功能，并做出了改进以降低数据存储要求，提升可视化功能，以及扩展监控功能以覆盖其它 IaaS 和 SaaS 提供商。

Splunk 将继续关注安全事件监控和分析使用实例。Splunk base 中的威胁情报功能和安全产品特定应用则能带来更多上下文和功能。

如果您需要的是一个能灵活支持各类数据源和分析功能（比如机器学习和 UEBA）的 SIEM 平台，或者是一个覆盖整个企业的单一数据分析平台，那么您应该考虑 Splunk。

优势

- Splunk 在安全监控使用实例上的投资大大提高了其在 Gartner 客户中的曝光度。
- 其本地机器学习功能和集成的 Splunk UBA 都能提供高级安全分析功能用于更高级的方法，这样，客户就能获得所需的功能，用于实施高级威胁检测监控和内部威胁使用实例。
- 借助 Splunk 在 IT 运营监控解决方案领域投资推出的产品，安全团队能够基于他们的内部经验和现有基础架构与数据，实施安全监控功能。

注意事项

- 在满足用户的监控和报告需求时，Splunk Enterprise Security 只提供了基础的预定义关联，而领先的竞争对手则能为使用实例提供更丰富的内容。
- Splunk 的许可模式是基于每日索引 GB 级数据规模创建的。客户表示，该解决方案比其它 SIEM 产品更昂贵，因为它能处理海量数据，并且客户建议最好是做好数据源的规划和优先级排序，避免超量使用许可的数据规模。过去 12 个月，Splunk 推出了许可项目旨在满足海量数据用户的需求。
- 鉴于 Splunk UBA 需要单独的基础架构，并且其许可模式与 Splunk Enterprise 和 Enterprise Security 截然不同，因此，Splunk UBA 的潜在买家也需要制定合理规划。

Trustwave

Trustwave 提供多种安全产品，这些产品覆盖安全管理、网络、内容和数据、端点和应用安全等领域。Trustwave 的 SIEM 产品是 Security Management 产品组合的一部分。Trustwave 提供两种 SIEM 产品选项：SIEM Enterprise 和 Log Management Enterprise (LME)，两款产品都有实体和虚拟版本，LME 还可以通过 AWS 高级仪表基础架构 (AMI) 形式交付。Trustwave LME 和 SIEM Enterprise 提供了多种选项来满足中端市场和企业买家的需求。此外，Trustwave 还提供了各种联合托管或混合服务，用于增强其安全管理产品。

过去一年，Trustwave 改进了产品的核心功能，包括，改善存储选项、用户界面和搜索增强包，以及专注于托管和多租户部署的部署增强包。

如果买家已经购买了 Trustwave 产品组合中的产品和服务，或者如果中端市场买家希望寻找一款 SIEM 产品来补充其采用的各种 Trustwave 安全技术或需要通过联合托管服务获取支持，Trustwave 是他们的理想选择。

优势

- Trustwave 的 Security Management 产品提供各种部署和服务选项，包括联合托管或混合服务，这些服务能支持客户以有限的内部资源管理技术，监控和分析安全事件。
- 通过采用 Trustwave 的安全产品，客户还能从以下方面受益：Trustwave 安全产品中的许多技术能够实现更紧密的双向集成，从而支持自动响应功能（主动集成和响应），比如隔离端点或锁定账户。
- SIEM Enterprise 面向满足以下要求的客户提供关联、产能和定制化功能：有大规模事件监控和多租户需求，并且企业在多个地区运营。
- Trustwave 的架构更简单，能够减轻客户在部署阶段和未来扩展阶段的负担。

注意事项

- 在 Gartner 客户进行 SIEM 产品竞争性评估时，Trustwave 的曝光度非常低。
- 威胁情报的集成只限于 Trustwave SpiderLabs（包括一些第三方来源的数据）提供的数据源。如需将第三方来源的数据直接集成至 SIEM 中，您需要专业服务的支持。
- Trustwave SIEM Enterprise 没有本地用户行为分析功能，也没有与领先的 UEBA 供应商实现集成。
- 如果企业内部 SIEM Enterprise 买家需要集成大数据平台，那么他们就需要采用定制化方法，因为 Trustwave 的重心放在为联合托管 SIEM 客户提供大数据功能上。

增加和撤除的供应商

随着市场的变化，我们检查并调整了魔力象限 (Magic Quadrants) 的纳入标准。调整后，任何魔力象限的供应商组合将随时间推移而发生变化。供应商第二年未继续出现在魔力象限中并不意味着我们对该供应商的看法发生改变。这可能反映市场发生了变化，因此评估标准也发生了变化，或该供应商的重点也发生了变化。

增加

魔力象限中增加了一家供应商：ManageEngine。

撤除

去年入选魔力象限的供应商本年度依然在榜。

纳入和排除标准

满足了以下标准的供应商，才能入选 2016 SIEM 魔力象限：

- 产品必须提供 SIM 和 SEM 功能。
- 产品必须支持企业从异构数据源中捕获数据，包括网络设备、安全设备、安全程序和服务器等数据源。
- 供应商必须出现在最终用户组织的 SIEM 产品评估表中。
- 解决方案必须是以软件或设备，而非只以服务的形式交付给客户。

如果供应商仅满足以下条件，则该供应商将被排除在魔力象限外：

- 他们提供的 SIEM 功能主要面向的是他们自己产品中的数据。
- 他们将自己的产品定位为 SIEM 产品，但是最终用户组织却并未将他们的产品纳入最终候选名单。
- 2015 年，他们的 SIEM 产品收入少于 1350 万美元。
- 解决方案仅作为托管服务交付。

在排除供应商时，Gartner 会考虑市场上供应商的收入和相对曝光度。收入阈值设定为 2015 年 1350 万美元，这里的收入是指新增的许可收入加上维护收入。曝光度则是根据以下因素确定：入选 Gartner 客户最终候选名单（咨询客户得到的名单）的次数，同行洞察力报告，gartner.com 网站上的搜索和参考次数，出现在供应商提供的客户参考候选名单的次数，以及被其它 SIEM 供应商提名为竞争对手的次数。

评估标准

执行力

- **产品或服务：**评估供应商在以下领域提供产品功能的能力及其过往记录，包括实时安全监控、安全分析、事件管理和响应、报告，以及部署简化等领域。
- **整体可行性：**用于评估技术提供商的财务状况、整体公司的金融和实际的成功，以及业务单位持续投资于 SIEM 产品的可能性。
- **销售执行/定价：**用于评估技术提供商在 SIEM 市场的成功及其开展销售准备活动的能力。其中包括 SIEM 收入和现有客户群的规模，SIEM 收入和现有客户群的增长率，售前支持，以及销售渠道的整体有效性。此外，Gartner 客户的利率水平同样在考虑范围之内。
- **市场反应/过往记录：**评估 SIEM 产品与买家在求购时所述的功能需求的匹配程度，以及供应商在交付市场所需的新功能方面的过往记录。此外，我们还会评估供应商如何将自己的产品与大型竞争对手的产品区别开来。
- **营销执行：**评估供应商根据对客户需求的理解所制作的 SIEM 营销信息，与面向不同垂直行业或地区所制作的 SIEM 营销信息。
- **客户体验**：评估产品环境内的产品功能和服务体验。包括评估部署的便捷性、操作、管理、稳定性、可扩展性和供应商支持功能。此项标准主要通过以下方式评估：对供应商提供的样本客户进行的调查，通过咨询获得的客户反馈意见，同行洞察力报告，以及与正在使用 SIEM 产品或者已经完成了 SIEM 产品竞争性评估的 Gartner 客户进行的其它互动。
- **运营**：评估供应商的服务、支持和销售功能，包括在不同地区推出的服务、支持和销售功能。

表 1. 执行力评估标准

评估标准	加权
产品或服务	高
整体可行性	高
销售执行/定价	高
市场反应/过往记录	高
营销执行	中
客户体验	高
运营	高

来源：Gartner（2016 年 8 月）

前瞻性

- **市场理解力：**评估技术提供商理解新老买家需求并将这些需求转变为产品和服务的能力。市场理解力高的 SIEM 供应商能够一边满足合规性报告要求，一边响应各个领域的客户需求，比如有针对性的功能和漏洞的早期检测，以及简化的实施和运营等。
- **营销战略**：评估供应商能有效传播其 SIEM 产品的价值和差异化优势的能力。
- **销售战略：**用于评估供应商如何使用直接和间接销售、营销、服务和通信分公司来扩展市场覆盖的广度和深度。
- **产品/服务战略：**用于评估供应商开发和交付产品的方法，其强调的是映射至当前需求时的功能。未来 12 到 18 个月的开发计划也在评估范围内。因为 SIEM 市场已经相当成熟，大多数供应商已经很难在通用网络设备、安全设备、操作系统和整合型管理功能的支持上出奇出新。在本次评估中，我们对于供应商在这些领域的功能的相对评级保持中立态度，但是如果供应商在这些领域有缺陷，我们将给予一个严重的"前瞻性罚分"，也就是说，该供应商在前瞻性的评级上会变得更低。我们将继续增加用于检测有针对性攻击的功能的权重，包括：
  - 供应商的剖析和异常检测功能，用于增强现有的基于规则的关联功能。
  - 威胁情报和业务环境集成，包括自动更新、筛选、规则内的使用、警报和报告。
  - 用户监控功能，包括监控管理策略变更和与身份和访问管理 (IAM) 技术的集成，集成 IAM 技术是为了自动导入监控时使用的访问策略（用户环境）。同时，我们还会评估用于分析用户行为的预定义分析功能。

- 数据访问监控功能，包括数据库日志和与数据库审计和保护产品的集成的直接监控，DLP 集成，以及利用本地功能和集成的第三方产品的文件完整性监控。
- 应用层监控功能，包括，与第三方应用集成（比如，ERP 财务和 HR 应用，以及垂直行业应用），以便监控该应用层的用户活动和事务；用于定义企业内部开发的应用日志格式的外部事件源集成接口；以及从外部源获取应用上下文的能力。
- 分析功能，这是一个支持有针对性攻击和漏洞早期检测的重要功能。一直以来，SIEM 都是根据 SIEM 技术的主要存储层提供查询功能。为了让漏洞早期检测功能有效发挥作用，分析功能必须融合与用户、资产、威胁和网络活动有关的上下文，并提供查询性能来支持迭代式调查。有些 SIEM 供应商引入了单独的数据存储来保存大量的安全事件、内容和上下文数据，且这些数据存储针对高级分析进行了优化。还有很多供应商则构建了连接器来实现 SIEM 技术和行业标准大数据存储库的互联。
- 高级威胁检测、网络流量监控和数据包捕获功能的纳入，以及与提供这些功能的第三方技术进行集成，从而实现更有效的漏洞早期检测。

除了供应商对功能扩展的关注度外，我们依然很看重部署的便捷性和持续支持。相比基础使用实例覆盖范围的广度，用户，尤其是 IT 和安全资源有限的用户还是更看重这些特性。SIEM 产品很复杂，并且随着供应商不断扩展其功能，这些产品将变得越加复杂。如果用户能够用有限的资源成功部署、配置和管理供应商提供的有效产品，那么这些供应商必将成为 SIEM 市场的大赢家。

此外，我们还评估了 SIEM 技术的联合托管或混合部署选项与支持服务，因为越来越多的 Gartner 客户希望或者要求供应商提供持续服务支持，用于监控或管理他们部署的 SIEM 技术。

- **垂直/产业战略**：评估供应商为支持特定垂直行业的 SIEM 需求所制定的战略。
- **创新：**评估供应商开发和交付 SIEM 技术的方式，这种方式要有别于竞争对手，能够以独特方式满足关键的客户需求。此外，我们还会评估应用层监控、欺诈检测和基于身份的监控等领域的产品功能和客户使用情况，以及客户需要并且部署的其它产品特定功能。高级威胁检测和事件响应所需的功能也占了很大的权重，比如，用户、数据和应用监控、即席查询、可视化、为调查事件融合上下文，以及工作流/案例管理功能。同时，我们也会评估云的环境监控功能。
- **地区战略：**尽管北美洲和欧洲的 SIEM 市场创造的收入最多，但是拉丁美洲和亚太地区才是成长型 SIEM 市场，威胁管理是后两个市场的主要驱动因素，其次就是合规性要求。在整体评估魔力象限中的供应商时，我们会评估供应商在这些地区的销售和支持战略。

表 2. 前瞻性评估标准

评估标准	加权
对市场的了解	高
营销战略	中
销售战略	中
产品/服务战略	高
业务模型	未评估
垂直/产业战略	中
创新	高
地区战略	中

来源：Gartner（2016 年 8 月）

象限说明

领导者

入选 SIEM 领导者象限的供应商必须满足以下要求：提供的产品功能能够很好地匹配一般市场需求；在 SIEM 市场建立客户群和收入流最为成功；（得益于 SIEM 收入或与其它收入源结合的 SIEM 收入）可行性评级相对较高。除了提供与客户需求完美匹配的技术外，领导者还在满足新兴和预测的需求方面，拥有超凡的前瞻性和执行力。通常，他们拥有相对更高的市场份额和/或强劲的收入增长势头，并且在有效的 SIEM 功能及其相关的服务和支持方面，赢得了正面的客户反馈。

挑战者

入选 SIEM 挑战者象限的供应商必须满足以下要求：有多条产品和/或服务线、中等规模的 SIEM 客户群，以及能满足一系列一般市场需求的产品。随着 SIEM 市场日趋成熟，挑战者的数量开始萎缩。通常，该象限中的供应商的执行力很强（他们的财政资源可以证明这一点），销售业绩也很突出，并且整个企业或者其它因素让他们的品牌认知度变得很高。但是，挑战者尚未拥有一套完整的 SIEM 功能，或者他们的 SIEM 技术在与领导者的 SIEM 技术相比较时，还没有胜出的记录。

有远见者

入选 SIEM 有远见者象限的供应商必须满足以下要求：提供的产品功能能够很好地匹配一般市场需求，但是执行力比领导者逊色。这主要是因为他们在 SIEM 市场的份额要低于领导者，比如，他们的现有客户群或收入规模/增长势头要小于领导者，或者他们的整个企业规模或整体可行性比不上领导者。

特定领域者

入选 SIEM 特定领域者象限的供应商必须满足以下要求：提供的 SIEM 技术能够很好地匹配特定的 SIEM 使用实例需求或一部分 SIEM 功能需求。特定领域者重点关注某个特定的客户群体，比如，中端市场、服务提供商，或者某个特定地区或垂直行业。此外，受到一些因素的限制，根据 Gartner 的标准，该象限中的供应商只有一个小型或者有限的客户群。这些因素可能包括：有限的投资或功能，覆盖范围有限的足迹，或者在目前及未来 12 个月阻碍供应商向企业提供更广泛功能的因素。入选该象限并不会给供应商在更细化的市场或使用实例上的价值带来负面影响。

背景

SIEM 技术可提供：

- SIM - 日志管理、分析和合规性报告
- SEM — 实时监控和事件管理，面向网络和安全设备、系统及应用的安全相关事件

通常，企业部署 SIEM 技术是为了支持以下三大使用实例：

- 高级威胁检测 - 实时监控和报告用户行为、数据访问和应用行为，融合威胁情报和业务环境，并结合有效的即席查询功能
- 基础安全监控 - 日志管理、合规性报告和针对所选安全控制措施的基础实时监控
- 取证和事件响应 - 仪表盘和可视化功能，以及工作量和文档支持，用于实现有效的事件识别、调查和响应

尽管许多 SIEM 部署项目都获得了资金用于满足监管合规性报告要求，但是提升安全监控和早期漏洞检测功能已经成为了 SIEM 的主要推动因素。目前，SIEM 市场上的技术提供商基本都能支持这三个使用实例，但是，他们面向每个使用实例的功能的相对水平有所不同。本年度的评估依旧在高级威胁检测和响应的支持功能上投入了更多权重。在开展本研究时，我们还评估了入选魔力象限的供应商在上述三大使用实例领域的 SIEM 技术（参见"Critical Capabilities for Security Information and Event Management"）。

企业应该根据自身具体的功能需求和运营需求，考虑魔力象限中所有供应商的 SIEM 产品。他们应该根据以下领域的企业特定需求选择产品：基础功能与高级功能的相对重要性；部署规模；产品的复杂性（部署、运行、使用和支持）；IT 部门的项目部署和技术支持能力；以及与现有应用、数据监控和身份管理基础架构的集成（参见"Toolkit: Security Information and Event Management RFP"）。

负责考虑 SIEM 部署项目的安全经理首先应该定义企业的 SEM 和报告需求。需求定义应该囊括后续部署阶段所需的功能。其它团队输入的信息也能让项目受益匪浅，包括审计/合规团队、身份管理团队、IT 运营团队和应用所有者（参见"How to Deploy SIEM Technology"）。此外，企业还应该描述他们的网络和系统部署拓扑，并评估事件级别。这样，候选的 SIEM 供应商就能根据企业的特定部署场景，推荐解决方案。需求定义还需要包括初始使用实例之外的阶段部署。本魔力象限评估了技术提供商在最常见的技术选择场景中的表现，即，SIEM 项目获得资金，用于满足威胁监控/检测/响应需求和合规性报告需求。

市场概述

过去一年，市场对 SIEM 技术的需求依然相当强劲。SIEM 市场价值从 2014 年的 16.7 亿美元增长到了 2015 年的 17.3 亿美元（参见"Forecast Analysis: Information Security, Worldwide, 1Q16 Update"）。2015 年初的购买驱动因素到今天依然存在。其中，威胁管理是主要驱动因素，合规性次之。在北美洲，依然有许多小型企业会启动新部署项目，因为很多这类企业出于大型客户或业务合作伙伴的坚持，需要提升监控和漏洞检测能力。同样，合规性报告也依然是一项需求，但是与 Gartner 客户的讨论大多都是围绕安全开展的。在威胁管理和合规性需求的驱动下，欧洲和亚太地区对 SIEM 技术的需求依然保持稳定。而亚太地区和拉丁美洲这类不成熟的市场的增长率要高于北美洲和欧洲这类成熟市场。这种情况下，我们在对魔力象限中的供应商进行整体评估时，就会评估供应商在这些地区的销售和支持战略。

保守型选用 SIEM 技术的大型企业也会继续启动新部署项目。大型的后期采用者和小型企业非常重视部署和运营支持的简洁性。我们仍将看到大型企业重新评估 SIEM 供应商，以便替代不完整、无价值或者失败的部署项目中的 SIEM 技术。

SIEM 市场已经发展得相当成熟，并且竞争非常激烈。如今，客户有大量选择，也就是说，市场上有多家供应商能满足普通客户的基本需求。而最大的空白区域需求是有针对性的攻击和漏洞的有效检测。企业在早期漏洞检测方面做得不好，有漏洞的企业能够发现的漏洞不到 20%。而威胁情报、行为剖析和有效分析能够改善这一情况。我们在监控用户与实体行为分析 (UEBA) 的新兴领域，发现早期采用者能够用有限的部署资源，有效监测有针对性的攻击。2015 年， Splunk 收购了 UEBA 供应商 Caspida，HPE 则宣布推出一款包含 ArcSight 和 Securonix 的集成解决方案。我们预计，随着越来越多的企业开始基于行为开发使用实例，未来 18 个月，SIEM 供应商将继续增加对行为分析功能和第三方技术集成的本地支持。

大多数企业都会在三年内扩展他们一开始部署的 SIEM 项目，以便加入更多事件源，更有效地利用实时监控和调查来支持事件响应。大型 SIEM 供应商拥有一个庞大的现有客户群，他们将继续关注如何扩展现有客户的 SIEM 技术部署项目。总之，SIEM 供应商正不断逐步提升漏洞检测（威胁情报、异常检测和网络行为监控）和调查工作流与案例管理等领域的产品功能。

SIEM 供应商格局

在 2016 年的 SIEM 魔力象限评估中，共有 14 家供应商达到了 Gartner 的入选要求。其中 6 家为单点解决方案供应商，其它 8 家为销售其它安全或运营产品和服务的供应商。2016 年 6 月，Fortinet 宣布收购 AccelOps。AccelOps SIEM 产品将改名为 FortiSIEM。SIEM 市场依然被几家相比较大的供应商主导：HPE、IBM、Intel Security 和 Splunk，他们创造了超过 60% 的市场收入。LogRhythm 是表现依然亮眼的单点解决方案供应商之一。随着中小型企业开始寻求托管服务或 SIEM 即服务选项，来减少满足合规性或安全需求所需的内部资源，其它小型供应商面临的压力与日俱增。因此，我们发现，SIEM 供应商（包括大型供应商和小型供应商）都开始转向第三方服务提供商来为自己的 SIEM 产品和服务提供运营服务。

如今，各种各样的企业都部署了 SIEM 技术。而 SIEM 供应商则越来越关注如何支持更多使用实例，从而继续向现有客户群销售其它功能。有些企业在制定 SIEM 技术采购决策时可能不会进行竞争性评估，因为他们的 SIEM 技术是与相关的安全、网络或运营管理技术捆绑在一起，由一家大型供应商提供的。但是这只是特例，大多数企业还是会根据 SIEM 技术的优点来制定 SIEM 采购决策。

领先的 SIEM 供应商仍在继续关注有针对性攻击和漏洞的检测，他们采取的方式是在这种检测中融入威胁情报、分析、剖析和异常检测，以及网络行为监控。过去 18 个月，附带高级功能的专业 UEBA 产品正在涌现，并且开始逐渐被市场所了解和接受。一般供应商是将 UEBA 产品定位为 SIEM 的互补产品。因为相比 SIEM，UEBA 产品能更精准地找到高级攻击。实际上，UEBA 技术通常被部署用于支持单独的使用实例，而两种工具之间的辅助集成能让每款产品都获得分析结果和上下文。

领先的 SIEM 供应商都集成了大数据平台，比如自己的平台（如有的话）或 Hadoop 等开源平台。有些有内部安全研究功能的供应商，比如 IBM、HPE、Intel Security、RSA 和 Trustwave 还能集成专有的威胁情报内容。既有 SIEM 又有 MSSP 业务的供应商（EventTracker、HPE、IBM 和 Trustwave）则在推销联合托管的 SIEM 技术部署选项，其中包含各种监控服务。RSA 提供了一个面向日志管理和网络数据包捕获的通用平台，并且将 SIEM 技术与 IT GRC 技术集成一体。Intel Security 的战略则越来越关注其自身安全产品组合的技术集成，以及如何向使用其端点产品和其它安全产品的大型企业销售 SIEM。有些供应商由于关注的是特定的垂直市场和/或 SIEM 收入和竞争曝光度而没有入选魔力象限：

- FairWarning 致力于为医疗卫生市场提供隐私侵犯检测和预防解决方案，其中包括在应用层监控用户行为和资源访问。目前，该公司已经在其产品中加入了针对销售人员的安全监控功能。
- SIEM 供应商 Huntsman Security 是 Tier-3 旗下的一家子公司，主要业务区域是英国和澳大利亚。剖析和异常检测功能是该公司的技术亮点。但是，随着我们的收入和曝光度要求变得更严苛，该供应商没有达到我们的入选标准。
- Lookwise 是一家从 S21sec 剥离出来的 SIEM 供应商，主要业务区域是西班牙和南美洲。S21sec 提供的威胁情报资讯是 Lookwise 的独特优势，这些情报主要关注的是银行和关键基础设施行业。但是，随着我们的收入和曝光度要求变得更严苛，Lookwise 也没有达到我们的入选标准。
- Tango/04 致力于为欧洲和南美洲的客户提供运营事件关联、业务流程监控和 SIEM 解决方案。但是，随着我们的收入和曝光度要求变得更严苛，该供应商无法再达到我们的入选标准。
- Tripwire 的 Log Center 致力于增强 Tripwire 的功能，从而提供更优质的系统状态情报信息。
- Tenable 的 SecurityCenter Continuous View (SecurityCenter CV) 为 Tenable 的客户提供一个中央功能，用于分析安全漏洞数据和从 Tenable 技术集成合作伙伴的解决方案中获得的事件数据。

客户需求 - 针对系统、用户、数据和应用的安全监控和合规性报告

过去一年，部署了 SIEM 技术的 Gartner 客户的关注点依然是安全使用实例。有针对性攻击和漏洞的检测依然是主要驱动因素，合规性仍然次之。通常，安全部门想利用 SIEM，改进其内外部威胁发现和事件管理功能（参见《利用 SIEM，检测有针对性的攻击》）。因此，他们需要针对主机系统和应用的用户行为和资源访问进行监控（参见《有效的安全监控离不开情境》）。在本年度的 SIEM 魔力象限评估中，我们一如既往地增加了支持有针对性攻击检测的功能的权重，包括对以下功能的支持：用户行为监控、应用行为监控、剖析和异常检测、威胁情报、有效的分析，以及事件响应功能。

有些企业因为其安全项目有局限性，因此需要继续采用 SIEM 技术。他们需要能提供预定义内容（如关键规则、查询、仪表盘、报告和威胁反馈）的产品，来支持基础的安全监控和合规性报告功能，并且其部署和支持服务要非常简便。

SIEM 解决方案应该：

- 能够实时收集和分析从主系统、安全设备和网络设备收集的事件以及威胁、用户、资产和数据的情境信息。
- 提供长期事件和情境数据存储和分析。
- 提供能够轻松进行定制以满足企业特定需求的预定义功能。
- 部署和维护尽可能简单。

可扩展性

可扩展性是部署 SIEM 时的一个重大考虑因素。为了满足给定部署项目的要求，SIEM 技术必须能够收集、处理、存储和分析所有与安全相关的事件。如果事件需要实时监控，那么企业就必须尽可能减少该事件收集和处理的延迟。事件处理包括剖析、过滤、聚合、关联、警报、显示、索引和写入数据存储。可扩展性还包括（甚至在事件高峰期）在即席查询响应时间内可以访问分析和报告所需的数据，从而实现迭代式调查。即使事件存储会随着时间的增长越来越大，企业依然需要保持良好的查询性能。我们主要根据以下三个因素确定部署规模：

- 事件源数量
- 每秒持续的事件（过滤后收集的事件）
- 事件数据存储的规模

我们认为事件源主要是服务器，但是也包括防火墙、入侵检测传感器和网络设备。有些部署项目中事件源还包括电脑端点，但是这种情况并不多见。因此，我们并没有在事件源总数中计入电脑端点。大型、中型和小型部署项目之间没有明确的界限，因为有些部署项目可能有很多相对安静的事件源，而有些项目则可能有部分非常繁忙的事件源。比如，某个部署项目有几个日志源可能非常繁忙，超过了小型部署项目的每秒事件流 (EPS) 限值，但是从架构上来看，它依然属于小型部署项目。

Gartner 将满足以下条件的项目定义为小型部署项目：事件源不超过 300 个；持续 EPS 率不超过每秒 1500 个事件；以及后备存储规模不超过 800 GB。满足以下条件的项目为中型部署项目：事件源在 400 到 800 个之间；持续 EPS 率在每秒 2000 到 7000 个事件之间；以及后备存储规模在 4TB 到 8 TB 之间。满足以下条件的项目则为大型部署项目：事件源超过 900 个；持续 EPS 率超过每秒 15000 个事件；以及后备存储规模不低于 10TB。还有一些超大规模的部署项目由数千个事件源，持续 EPS 率超过 25000，后备存储超过 50TB。我们可能会得出某家供应商的 SIEM 技术非常适合小型、中型或大型部署项目。这意味着，该供应商一般或者经常成功部署这种规模的项目。当然，每家供应商都有异常值。

SIEM 服务

如今，越来越多的 Gartner 客户表示，他们在为其 SIEM 部署项目寻求外部服务支持，或者计划获取此类支持来辅助 SIEM 产品（参见《使用联合托管 SIEM 的方式和时机》）。外部服务的驱动因素包括：缺乏内部资源来管理 SIEM 部署项目，缺乏资源来实时监控警报（而非每天甚至更久才监控一次），或者缺乏专业知识来扩展部署项目、加入新使用实例（比如端点检测监控和响应）。预计，随着越来越多的客户出现全天候监控需求，并实施需要更深入的 SIEM 运营和分析专业知识的使用实例，SIEM 用户对此类服务的需求只会与日俱增。

SIEM 供应商可能会在内部员工、外包服务或合作伙伴的帮助下，利用托管服务满足这些需求。此外 SIEM 用户也可以选择托管安全服务提供商，他们能实时监控和分析事件，并收集日志用于报告和调查。如今有些客户选择放弃管理 SIEM 技术，而利用内部资源监控和调查 SIEM 技术，这种情况下，支持这类客户的托管 SIEM 或 SIEM 即服务产品（如 Splunk Cloud）越来越多（参见《有关 SIEM 即服务的创新性洞察力》）。在基础使用实例方面，资源严重不足的客户可能会选择 SaaS 类型的日志管理服务，Logentries、Loggly、Papertrail、Sumo Logic 等供应商能提供此类服务，他们不仅有安全程序，他们的服务还覆盖运营使用实例。但是，让外部服务提供商来满足客户特定需求，执行事件收集和存储、警报、调查和报告可能也会出现问题。因此，客户在寻找服务时，应该评估服务提供商是否满足当前及计划的使用实例。

SIEM 备选方案

因为 SIEM 技术很复杂并且成本高昂，同时市场上还涌现了一些安全分析技术，这种情况下，客户越来想采用其它方法来收集和分析事件数据，识别高级攻击。Elasticsearch、Logstash 和 Kibana (Elastic Stack)、OpenSOC、Apache Metron 以及其它的利用或在本地使用 Hadoop 等大数据平台的工具都能提供数据收集、管理和分析功能。如果企业有足够的资源来部署和管理这些服务，并开发和维护分析工具，以启用安全使用实例，那么他们可能就能获得一款用更少的成本满足更多需求的解决方案（与商务技术相比）。Gartner 正在跟踪该方法的开发，以及为这些技术提供 Elastic Stack 即服务（如 Elastic）或托管安全服务 (MSS) 的服务提供商。

如果企业缺乏资源和成熟的流程来部署和支持 SIEM 技术，并且他们不能或者选择不与托管安全服务提供商 (MSSP) 合作来实现监控，他们也可以用日志管理技术（或服务），比如 Graylog 或 Sumo Logic 等没有或只有少量现成使用实例的技术来满足基础的日志和审查需求。

目前市场上有很多提供商提供的托管检测和响应 (MDR) 服务与这些 MSSP 的产品不同，他们的服务一般是通过分析选定的网络和端点数据，发现和响应客户环境中的高级威胁（参见"Market Guide for Managed Detection and Response Services"）。通常，他们的服务和事件源范围要比 MSSP 或 SIEM 部署项目的范围要小。正因为此，他们一般不会与 SIEM 或 MSSP 直接竞争，因为后者的客户有更广泛的使用实例需求。但是，MDR 服务提供商也能提供有效的高级威胁检测功能，如果企业有充足的资源来支持这些使用实例，那么企业也可以考虑将 SIEM 预算投入在 MDR 服务上。Gartner 将继续关注该领域，评估 MSS、MDR、日志和 SIEM 之间的交互和交叉。

Gartner 推荐的文章

有些文档可能没有涵盖在您订阅的报告中。

《Gartner 魔力象限调查如何评估市场与供应商》

《利用 SIEM，检测有针对性的攻击》

《2016 年安全监控和运营入门》

《关键的安全信息和事件管理功能》

证据

在撰写本报告时，我们采纳了以下信息作为论据：简报中的信息，从供应商处收集的结构化数据，在咨询和其它互动中与 Gartner 客户的讨论内容，Gartner 客户在同行洞察力调查中提供的反馈，以及供应商的样板客户提供的数据。

[1] "2016 Verizon Data Breach Investigations Report (DBIR)". Verizon.第 11 页中的图 9 表明：2015 年，在内部检测方面负责泄露检测的相关方低于 20%。

评估标准定义

执行力

产品/服务：供应商为细分市场提供的核心产品和服务。这包括现有的产品/服务功能、质量、功能包、技能等，无论是本地提供还是通过市场定义及子标准中规定的 OEM 协议/合作伙伴关系提供。

整体可行性：可行性包括整个企业财务健康、业务部门财务及实践成功、个别业务部门继续进行产品投资、提供产品、在企业产品组合中保持领先水平的可能性等方面的评估。

销售执行/定价：供应商在所有销售准备活动中的功能以及为其提供支持的结构。这包括交易管理、定价和协商、售前支持以及销售渠道的总体效率。

市场反应/过往记录：随着机遇的发展、竞争对手的行动、客户需求的演化和市场动态的变化，做出反应、改变方向、灵活调整并取得竞争成功的能力。这种标准还应考虑供应商的响应历史。

营销执行：设计用于推广企业信息，以影响市场、提升品牌和业务、提高产品知名度、建立产品/品牌及企业在买家心目中的正面形象的计划，其清晰性、质量、创造性和功效。这种“思想份额”可通过广告宣传、促销活动、思维领导力、口碑和销售活动得以提高。

客户体验：促使客户通过所评估产品取得成功的关系、产品和服务/计划。具体而言，这包括客户接受技术支持或客户支持的方式。这也可包括辅助工具、客户支持计划（及其质量）、用户群可用性、服务级别协议等等。

运营：企业实现其目标和承诺的能力。具体因素包括企业结构的质量，如支持企业持续有效且高效运营的技能、经验、计划、系统和其它工具。

前瞻性

对市场的了解：供应商了解买家需求并转化为产品和服务的能力。具有高度愿景的供应商能听取和了解买家的需求，并通过提升愿景形成或提升需求。

营销战略：在企业范围内持续传达并通过网站、广告、客户计划和定位声明对外说明的明确、独特的信息。

销售战略：使用直接或间接的销售、营销、服务、通信的适当网络，拓宽、加深市场覆盖范围、技能、专业知识、技术、服务和客户群，以进行产品销售的战略。

产品/服务战略：供应商的产品开发及交付方法，侧重于可映射到当前及未来要求的差异化、功能、方法和功能包。

业务模型：供应商设定商业主张的有效性和逻辑性。

垂直/产业战略：供应商用于指导资源、技能、产品，以满足包括垂直市场在内的个别细分市场的具体需求的战略。

创新：出于投资、整合、防御或先发制人目的而对资源、专业知识或资本进行的直接、相关、补充和协同布局。

地区战略：供应商用于指导资源、技能、产品，以满足"国内"或本土之外的区域的具体要求，无论是直接指导还是通过适用于该区域和市场的合作伙伴、渠道、子公司间接指导。

GARTNER 总部

公司总部

56 Top Gallant Road

Stamford, CT 06902-7700

USA

+1 203 964 0096

区域性总部

澳大利亚

巴西

日本

英国

如需世界各地的完整位置列表，请点击 http://www.gartner.com/technology/about.jsp。