浅谈SIEM

一、概念
SIEM (Security Information Event Management，安全信息与事件管理)

Gartner的定义：SIEM为来自企业和组织中所有IT资产（包括网络、系统和应用)产生的安全信息(包括日志、告警等）进行统一的实时监控、历史分析，对来自外部的入侵和内部的违规、误操作行为进行监控、审计分析、调查取证、出具各种报表报告，实现IT资源合规性管理的目标，同时提升企业和组织的安全运营、威胁管理和应急响应能力。

SIEM技术已经存在了十多年，是从日志管理学科发展而来的。最初是基于传统的日志收集和管理，引入了对日志数据的长期存储，分析和报告，并将日志与威胁情报结合起来（SIM）；后来具备可以解决系统安全事件的能力：通过对防病毒系统、防火墙和入侵检测等事件的聚合、关联，实时分析日志和事件数据，提供威胁监控和事件响应（SEM）。SIEM 作为SOC平台的基础支撑技术，主要是用来收集、监测和分析网络资产和安全设备的日志和事件。高级的SIEM已经发展到包括用户行为分析（UEBA）以及安全编排自动响应（SOAR），近几年也出现了SIEM和SOAR之争。SOAR解决方案可以作为SIEM解决方案的一种补充，因为SIEM偏“记录”，SOAR偏“行动”。

二、作用
1、数据聚合
聚合来自网络，服务器，数据库，应用程序和其他安全系统（如防火墙，防病毒和入侵检测系统（IDS））的数据。

2、威胁情报提供
将内部数据与包含漏洞，威胁参与者和攻击模式数据的威胁情报源相结合。

3、关联
将事件和相关数据链接到有意义的捆绑包中，这些捆绑包代表真正的安全事件，威胁，漏洞或取证发现。

4、Analytics（分析）
使用统计模型和机器学习来识别数据元素之间更深层次的关系，以及与已知趋势相比的异常，并将它们与安全问题联系起来。

5、警报
分析事件并发出警报，通过电子邮件或其他方式，比如安全仪表板即时告知安全人员。

6、仪表板和可视化
创建可视化，以允许员工查看事件数据，识别不符合标准模式的活动

7、合规
自动收集合规性数据，生成适应HIPAA，PCI / DSS，HITECH，SOX和GDPR等标准的安全性、治理和审计流程的报告。

8、存储
长期存储历史数据，以便为合规性要求、追踪取证等提供数据。

9、威胁发现
允许安全人员对SIEM数据运行查询，过滤和透视数据，以主动发现威胁或漏洞。

10、事件响应
提供围绕安全事件的案例管理，协作和知识共享，使安全团队能够快速同步基本数据并及时响应威胁。

11、SOC自动化
使用API与其他安全解决方案集成，并允许安全人员定义应执行以响应特定事件的自动化手册和工作流。

以下是评估SIEM产品时要审核的一些最重要的功能：

•与其他控件集成 - 系统是否可以向其他企业安全控件发出命令以防止或阻止正在进行的攻击？

• 人工智能 - 系统能否通过机器和深度学习提高自身的准确性？

•威胁情报源 - 系统是否支持组织选择的威胁情报源，或者是否强制要求使用特定的源？

•强大的合规性报告 - 系统是否包含针对常见合规性需求的内置报告，以及是否为组织提供定制或创建新合规性报告的能力？

• 取证功能 - 系统是否可以通过记录感兴趣的数据包的标头和内容来捕获有关安全事件的其他信息？

三、工作原理
SIEM软件的工作原理是收集整个组织基础架构中的主机系统，安全设备和应用程序生成的日志以及事件数据，并在集中平台上进行整理。从防病毒事件到防火墙日志，SIEM软件可识别此数据并将其分类，例如恶意软件活动，失败和成功登录以及其他潜在的恶意活动。

安全信息和事件管理过程可以分解如下：

数据收集 - 所有网络安全信息源（例如服务器，操作系统，防火墙，防病毒软件和入侵防御系统）都配置为将事件数据提供给SIEM工具。大多数现代SIEM工具使用代理从企业系统收集事件日志，然后处理，过滤并将它们发送到SIEM。一些SIEM允许无代理数据收集。例如，Splunk使用WMI（Windows Manage Instrumentation，windows管理规范）在Windows中提供无代理数据收集。

策略 - 配置文件由SIEM管理员创建，该管理员在正常情况下和预定义的安全事件期间定义企业系统的行为。SIEM提供默认规则，警报，报告和仪表板，可以进行调整和自定义以满足特定的安全需求。

数据整合和关联 - SIEM解决方案整合，解析和分析日志文件。然后根据原始数据对事件进行分类，并应用将各个数据事件组合成有意义的安全问题的关联规则。

通知 - 如果事件或事件集触发SIEM规则，系统会通知安全人员

当软件识别出可能对组织构成威胁的活动时，会生成警报以指示潜在的安全问题。可以使用一组预定义规则将这些警报设置为低优先级或高优先级。例如，如果用户帐户在20分钟内生成20次失败登录尝试，则可能会将其标记为可疑活动，但设置为较低优先级，因为它最有可能是忘记其登录详细信息的用户。但是，如果帐户在5分钟内遇到120次登录尝试失败，则更有可能是正在进行的暴力攻击并被标记为高严重性事件。

四、日志管理流程
SIEM服务器的根源是日志管理平台。日志管理涉及收集数据，对其进行管理以启用分析以及保留历史数据。

哪些组织系统将其日志提供给SIEM？SIEM对哪些其他业务数据感兴趣呢，下图大致描绘了SIEM的数据源。

1、数据采集
SIEM从数百个组织系统收集日志和事件（有关部分列表，请参阅下面的日志源）。每次设备发生时，每个设备都会生成一个事件，并将事件收集到平面日志文件或数据库中。SIEM可以通过四种方式收集数据：

通过安装在设备上的代理（最常用的方法）

通过使用网络协议或API调用直接连接到设备

通过直接从存储访问日志文件，通常采用Syslog格式

通过SNMP，Netflow或IPFIX等事件流协议

SIEM的任务是从设备中收集数据，对其进行标准化并将其保存为能够进行分析的格式。下一代SIEM预先集成了通用云系统和数据源，允许直接提取日志数据。

2、数据管理
在大型组织中，SIEM可以存储大量数据。这些数据或存储在本地或存储在云端，基于Amazon S3，Hadoop或ElasticSearch等技术实现数据的高效存储和检索。

3、记录保留
PCI DSS，HIPAA和SOX等行业标准要求将日志保留1到7年，大型企业每天都会从IT系统中创建大量日

志，SIEM需要了解他们保留哪些日志以满足合规性和取证要求，SIEM使用以下策略来减少日志量：

Syslog服务器 - syslog是一种标准化日志的标准，仅保留标准格式的基本信息。Syslog允许您压缩日志并保留大量历史数据。

删除计划 - SIEM会自动清除不再需要的旧日志，通过从Syslog格式访问日志文件。

日志过滤 - 并非所有日志都是组织面临的合规性要求或法医目的所需的。可以按源系统，时间或SIEM管理员定义的其他规则过滤日志。

汇总 - log数据可以汇总为仅维护重要的数据元素，例如事件计数，唯一IP等。

历史日志不仅对合规性和取证有用，还可用于深度行为分析。如用户行为分析（UEBA）技术，该技术使用机器学习和行为分析来智能地识别异常或趋势。

下一代SIEM利用低成本的分布式存储，允许组织保留完整的源数据。这样可以对历史数据进行深入的行为分析，以捕获更广泛的异常和安全问题。

六、SOAR的介入
1、概念
SOAR（security orchestration, automation and response，安全编排自动化响应）

安全编排自动化响应（SOAR，Security Orchestration and Automation Response）是Gartner 2018年在安全领域定义的最新前沿技术，与UEBA、EDR等侧重于威胁识别发现的技术不同，SOAR集中在识别后的威胁处理，强调用户可以通过事件编排以编码实现任意的威胁处理逻辑。

2、作用
大部分传统安全厂商只关注识别，忽略了处理，支持简单的阻断/通知/放行的处理方式，另一方面，企业对于威胁的处理又有复杂的逻辑编排需求，希望通过和已有的安全产品联动起来，形成威胁处理的闭环。SIEM虽然可以对可疑行为发出警报，但真正的目标是尽可能快速有效地对可疑行为采取行动。SOAR整合数据源，使用威胁情报源提供的信息，并自动响应以提高效率和效果。SIEM可以“说”某些东西，但那些包含SOAR的东西可以“做”某些东西。

SOAR通过更丰富，更高质量的数据和日常安全任务的自动化的聚合和关联，帮助组织增强威胁检测和响应。SOAR影响SIEM的另一个关键方法是帮助标准化事件分析和响应程序。这里的目标是部分或完全自动化一系列活动，以便安全人员有更多时间来寻找威胁而不是响应威胁。通过自动执行响应操作，例如阻止防火墙或入侵检测系统上的IP地址，暂停用户帐户或将受感染的端点与网络隔离，SOAR可以帮助促进更快的事件响应，从而减少潜在的破坏和破坏原因。

最后
购买和运行SIEM产品的复杂性和成本，以及其他安全分析技术的出现，引起了人们对收集和分析事件数据以识别和响应高级攻击的替代方法的兴趣。Elasticsearch，Logstash和Kibana（又名ELK堆栈或Elastic Stack）的组合就是一个很好的例子。还出现了替代基础广泛的SIEM解决方案的替代方案，这些解决方案主要集中在日志收集和安全分析元素上。在这个领域竞争的厂商包括Elastic，Cybraics，Empow，Elysium，Jask（由Sumo Logic收购），MistNet，PatternEx，Qomplx，Rank Software和Seceon。
与商业技术相比，拥有足够资源来部署和管理这些资源以及开发和维护分析的组织，也许能够获得一种满足其需求的解决方案，从而以更低的成本获得解决方案。然而，对研发和安全能力不足的客户来说，尽管这些软件是免费的，但为这些解决方案进行规模化设计所涉及的工作量以及支持所需事件源和分析所需的开发工作仍然是巨大的，从投入产出比来说，有可能购买商业版解决方案或许是更好的选择。