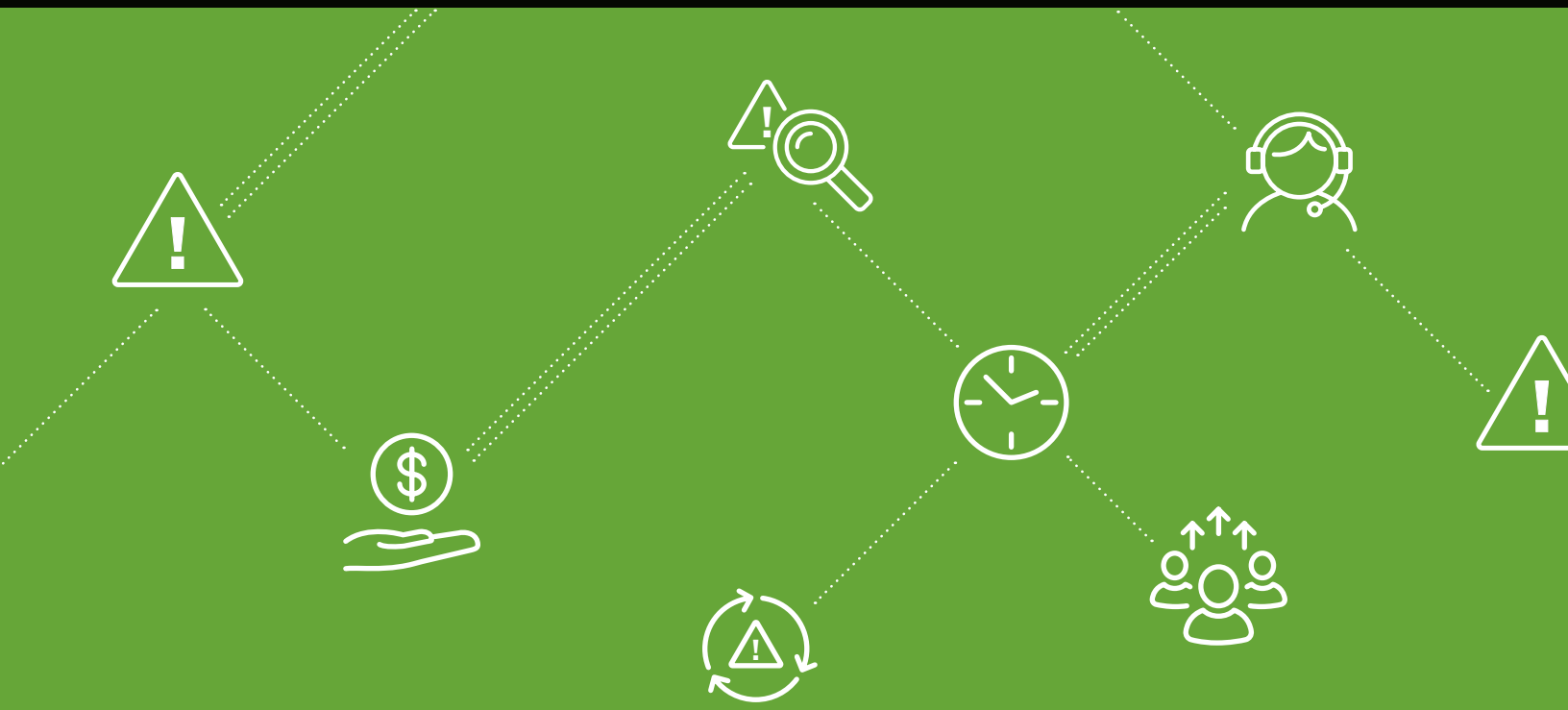
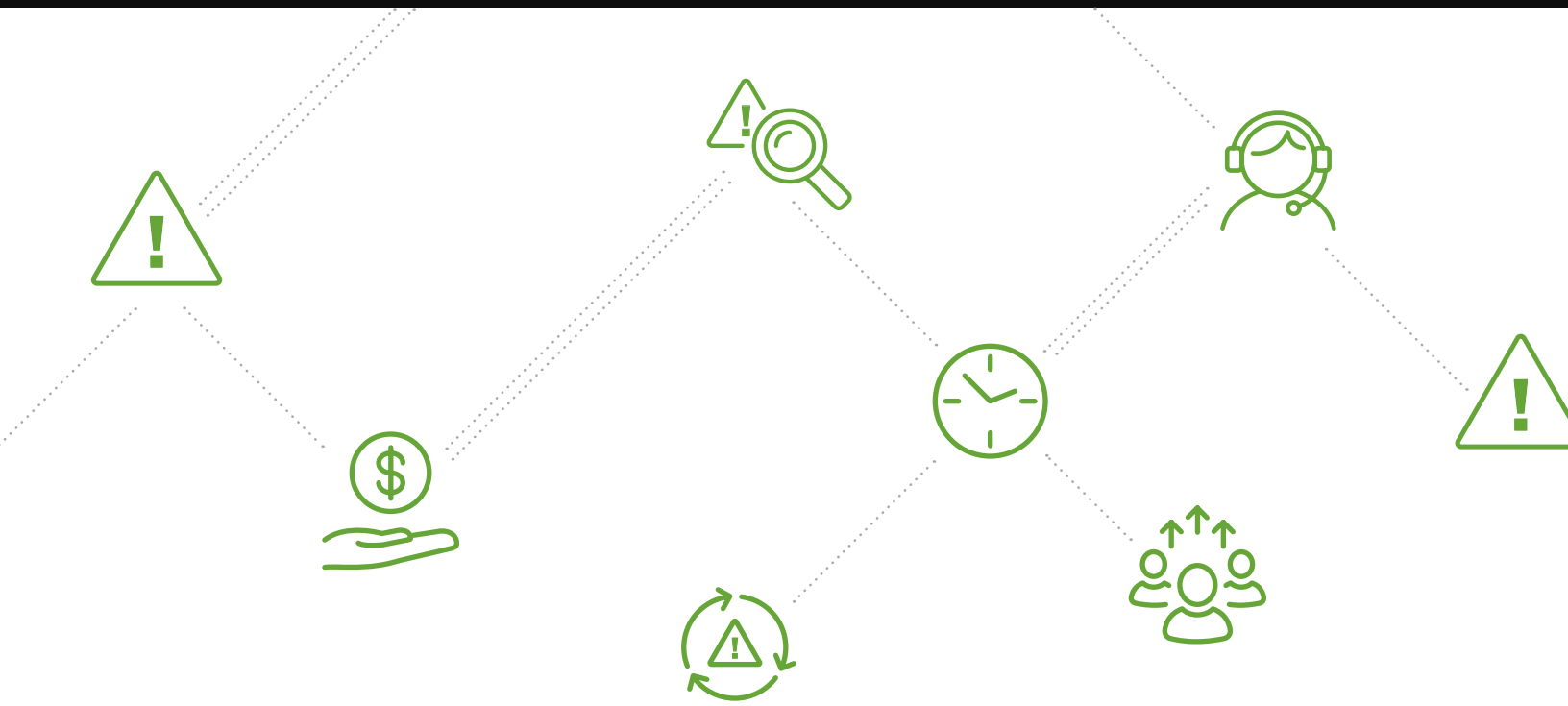


SIEM 买方指南

基于分析的安全解决方案的购买者是谁，以及购买的内容、地点和原因是什么

目录



1.SIEM 是什么

安全信息事件管理 (SIEM) 解决方案就像飞行员和空中交通管制员使用的雷达系统。如果没有 SIEM，企业 IT 部门无异于“盲飞”。虽然安全设备和系统软件擅长捕捉和记录孤立的攻击和异常行为，但是当今最严重的威胁是分布式的，跨多个系统协同工作，并使用先进的规避技术来避免检测。没有 SIEM，袭击就会发生并发展成为灾难性事件。

日益复杂的攻击和云服务的使用（增加了遭受漏洞攻击的机会）放大了 SIEM 解决方案对当今企业的重要性。

在本买方指南中，我们旨在解释什么是 SIEM 解决方案、它不是什么、它的演变、它的作用以及如何确定它是否是适合您的组织的正确安全解决方案。

那么，SIEM 是什么?

Gartner 将 SIEM 定义为“通过对来自各种事件和上下文数据源的安全事件进行实时收集和历史分析来支持威胁检测和安全事件响应的技术。”

简单英语里的意思是什么?

简而言之，SIEM 是一个安全平台，可以提取事件日志，并提供对这些数据的单一视图和更多见解。

SIEM 的演变

SIEM 不是一项新技术。该平台的基本功能已经以某种形式存在了将近 15 年。

随着时间的推移，SIEM 解决方案变成了具有更多内容的信息平台 - 它的使用范围扩大到包括合规性报告，汇总来自防火墙和其他设备的日志。但是 SIEM 技术往往很复杂，难以调整，并且要识别攻击，IT 专业人员必须知道他们在寻找什么。但是，该技术变得困难并且不可扩展。

这促使 SIEM 解决方案发展得更灵活，更易于使用。这一点在今天尤为重要，因为组织已经将云解决方案和数字化转型应用到了我们生活的每个方面。

因此，理解传统 SIEM 和现代基于分析的 SIEM 解决方案之间的区别很重要，我们将在后面介绍这一点。

但了解与 SIEM 相关的使用案例以及您的组织是否真的需要 SIEM 解决方案或其他内容也很重要。

这需要明确传统 SIEM 与现代基于分析的 SIEM 解决方案之间的区别。

传统的 SIEM 被困在过去

寻找用于收集、存储和分析纯安全数据的机制相对简单。存储数据的选项并不缺乏。然而，收集所有与安全相关的数据并将所有数据转化为可执行的情报是另一回事。

许多投资 SIEM 平台的企业 IT 组织都在艰难的发展中发现了这个基本事实。在花费大量时间和金钱记录安全事件之后，麻烦在于，不仅需要很长时间来获取所有数据，而且用于创建 SIEM 的底层数据系统往往是静态的。

更糟的是，可供分析的数据仅基于安全事件。这使得难以将安全事件与其他 IT 环境中发生的事情相关联。出现问题时，调查安全事件需要花费大部分 IT 组织承担不起的宝贵时间。此外，传统的 SIEM 解决方案无法跟上需要调查的安全事件的速度。云服务的继续采用扩大了威胁载体，企业需要监控用户活动、行为、跨关键云和软件即服务 (SaaS) 以及内部部署服务的应用程序访问，以确定潜在威胁和攻击的全部范围。

下图解释了传统 SIEM 解决方案的一些关键限制。

传统 SIEM - 问题和特征

问题	问题
无法使用所需的数据	限制检测、调查和响应
难以维护和操作	复杂性和熟练的工作人员
漏报和误报程度高	SecOps 负担
不稳定	中断史
不灵活的数据	无法适应重要情况
静态工作流程	有限和受到限制
无法检测现代威胁	业务风险

替代方案：基于分析的 SIEM

企业 IT 需要的是一种简单的方法，将所有安全相关数据中的信息关联起来。一种使 IT 能够管理其安全状况的解决方案。IT 组织不应该仅仅在事件发生后观察事件，而应该能够预测事件的发生并实施措施以实时限制其漏洞。为此，企业需要一个基于分析的 SIEM 平台。

以下是传统 SIEM 和现代解决方案之间的区别。Gartner表示，区别在于**“现代 SIEM 的工作原理不仅仅是记录数据，而且不仅仅应用数据分析的简单关联规则。”**

在这种背景下，一种特定类型的现代 SIEM 应运而生，我们喜欢称之为基于分析的 SIEM 解决方案。这种现代化的解决方案使 IT 部门能够实时监控威胁并快速响应事件，从而避免或限制损害。但并非所有的攻击都是外部的，IT 部门需要一种监控用户活动的方式，以便将内部威胁或意外危害的风险降到最低。威胁情报对于理解更广泛的威胁环境的性质以及将这些威胁纳入组织环境至关重要。

基于分析的 SIEM 必须擅长安全分析，让 IT 团队有能力使用复杂的定量方法来深入了解并确定工作的优先顺序。最后，今天的 SIEM 必须包括作为核心平台的一部分来打击高级威胁所需的专用工具。

基于分析的 SIEM 与传统 SIEM 之间的另一个主要区别在于现代化解决方案的灵活性，它可以将解决方案部署在本地、云中或混合环境中。

下图解释了组织应该选择基于分析的 SIEM 解决方案而不是传统 SIEM 的七大理由。

取代传统 SIEM 的七大理由

组织通常与传统 SIEM 过时的体系结构相关联，传统 SIEM 通常使用具有固定模式的 SQL 数据库。这些数据库可能会成为单点故障或受到规模和性能限制。

1. 有限的安全类型	通过限制摄入的数据类型，检测、调查和响应时间有限。
2. 无法有效地获取数据	使用传统 SIEM，数据的摄入可能是一个极其繁琐的过程，或者非常昂贵。
3. 调查速度缓慢	使用传统 SIEM，基本操作（例如原始日志搜索）可能需要大量时间 - 通常需要几个小时和几天时间才能完成。
4. 不稳定性和可扩展性	基于 SQL 的数据库越大，它们的稳定性就越差。客户经常遭受性能差或者大量中断，因为事件中的峰值会导致服务器停机。
5. 使用寿命终止或路线图不确定	随着传统 SIEM 供应商改变所有权，研发速度缓慢。没有持续的投资和创新，安全解决方案就无法跟上不断增长的威胁环境。
6. 封闭的生态系统	传统 SIEM 供应商往往缺乏与市场上其他工具集成的能力。客户不得不使用 SIEM 中包含的内容，或在定制开发和专业服务上花费更多。
7. 限于本地	传统 SIEM 通常仅限于本地部署。安全专业人员必须能够使用云、本地和混合工作负载。

将您的 SIEM 带到云端

在云中运行 SIEM 或 SaaS 可以帮助解决许多组织使用安全情报的问题，但许多 IT 领导仍然不信任云安全性和可靠性。在消除基于云的 SIEM 解决方案之前，要知道大多数大型云服务的安全实践和技术可能比典型企业的安全实践和技术要复杂得多。

SaaS 已经广泛用于 CRM、HR、ERP 和业务分析等业务关键型系统。SaaS 对企业应用程序有意义的相同原因 - 快速、方便的部署、低开销操作、自动更新、基于使用情况的计费和可扩展的、强化的基础架构 - 使云非常适合 SIEM。

基于云的解决方案可灵活使用来自本地和云端的各种数据集。随着越来越多的企业工作负载转移到基础架构即服务 (IaaS)、平台即服务 (PaaS) 和 SaaS，轻松与第三方系统集成表明 SIEM 在云中更具有意义。将 SIEM 带到云端的主要优势包括混合架构的灵活性、自动软件更新和简化配置，即时、可扩展的基础架构以及强大的控制和高可用性。

SIEM 在企业中的使用案例

既然您已经了解 SIEM 的演变，以及可区分现代基于分析的 SIEM 解决方案和传统 SIEM 的特点，现在是时候解释该技术实际解决哪些安全使用案例了。

早期检测、快速响应和协作以减轻高级威胁，这对当今企业安全团队提出了重大要求。报告并监控日志和安全事件已经不够。安全从业人员需要从 IT、业务和云中的整个组织范围内的所有数据源获得更广泛的见解。为了领先于外部攻击和恶意内部人员，公司需要一种高级安全解决方案，可用于快速响应检测、事件调查和 CSIRT 违规情景的协调。此外，公司还需要能够检测并响应已知、未知和高级威胁。

企业安全团队必须使用 SIEM 解决方案，该解决方案不仅可以解决常见的安全使用案例，还可以解决高级使用案例。为了跟上动态威胁情况，现代 SIEM 需要能够：

- 集中并汇总所有安全相关事件，因为它们是从它们的源生成的
- 支持各种接收、收集机制，包括系统日志、文件传输、文件收集等。
- 将上下文和威胁情报添加到安全事件中
- 关联并警示一系列数据
- 检测高级和未知威胁
- 描绘整个组织中的行为
- 获取所有数据（用户、应用程序）并使其可用于监视、警报、调查和临时搜索
- 从数据中提供临时搜索和报告以进行高级违规分析
- 调查事件并进行取证调查，以便进行详细的事件分析
- 评估并报告合规情况
- 使用安全状况分析和报告
- 通过简化的临时分析和事件排序来跟踪攻击者的行为

虽然主要从服务器和网络设备日志中收集，但 SIEM 数据也可能来自端点安全、网络安全设备、应用程序、云服务、身份验证和授权系统以及现有漏洞和威胁的在线数据库。

但数据聚合只是整个过程的一半。然后，SIEM 软件将生成的存储库关联起来，并查找异常行为、系统异常情况和安全事件的其他指标。此信息不仅用于实时事件通知，还用于合规性审计和报告、性能仪表板、历史趋势分析和事后事件取证。

鉴于安全威胁的数量和复杂程度不断上升，以及每个组织中数字资产的价值不断上升，采用基于分析的 SIEM 解决方案作为整个 IT 安全生态系统的一部分不断发展并不让人感觉奇怪。

您是否真的需要 SIEM?

您已经了解 SIEM 是用来做什么的，现在是进行更广泛对话的时候了。您的组织是否需要 SIEM 或其他东西?

您的组织可能尚未对高级安全使用案例做好准备，而只需要一种解决方案（例如中央日志管理 (CLM)）来提供对机器数据的深入了解。无耻插件：有关安全和日志管理的信息，请参阅 **Splunk Enterprise**。

那么，什么是中央日志管理解决方案？CLM 被简单地定义为一种解决方案，可以集中查看日志数据。

为了了解更进一步的内容，我们向您提出下面的问题：什么是日志数据?

日志数据日志数据是由计算机生成的日志消息，是每个公司、组织或机构运营情况的明确记录，通常是查明故障原因和支持更多业务目标的未使用的手段。

我们回到 CLM。日志管理的目的是收集这些计算机生成的日志，并使其可用于搜索和报告。在安全方面，这意味着 CLM 可以帮助进行事件调查和警报分类等事情。

自从 SIEM 出现以来，日志管理一直是 SIEM 能力的核心功能。但是，如果您所需要的仅仅是日志数据的见解，那么基于分析的 SIEM 解决方案是否适合您？让我们转向**著名的 SIEM 分析师 Anton Chuvakin** 寻找答案：

总之，这意味着如果您使用 SIEM 解决方案进行日志聚合，则您付出的代价太大。这里的关键是您可以使用 SIEM 来解决基本和高级使用案例。

在成熟线的另一端，还有 **Gartner 创造的术语**用户和实体行为分析 (UEBA)。此类别还有其他名称，例如 **Forrester** 首选的安全用户行为分析和 **Splunk 首选用户行为分析 (UBA)** - 后者是我们将在本报告中坚持使用的术语。它们都是用不同的方式来指代相同的技术。

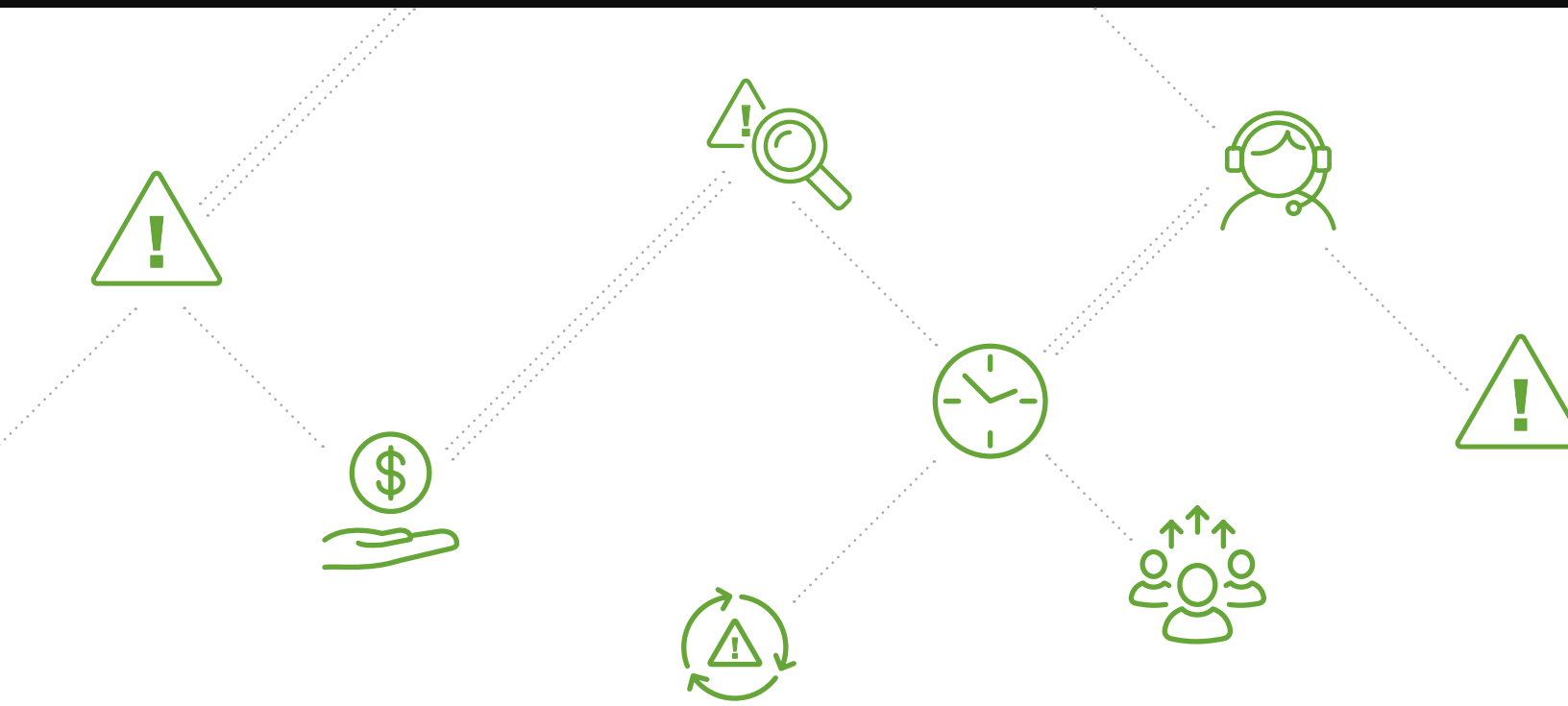
UBA 用于威胁检测以发现和修复内部和外部威胁。作为一个例子，UBA 通常被视为更高级的安全使用案例，部分原因是它能够学习和设置用户的正常习惯基准，然后在超出正常范围时发送警报。

坚持这个例子，为了建立基线，UBA 解决方案将跟踪此类活动的习惯，例如：

- 用户通常从哪里登录
- 用户拥有什么权限
- 用户访问什么文件、服务器和应用程序
- 用户通常使用什么设备登录

就上下文而言，一些 UBA 供应商正试图在 SIEM 市场上竞争。这些是 SIEM 领域的新进入者。UBA 是一种有用的解决方案，但仅凭 UBA 解决方案无法取代 SIEM 解决方案。UBA 不是 SIEM 的新类别。它是一项独立的安全技术。理想情况下，UBA 解决方案应该能够与基于分析的 SIEM 解决方案配合使用。

更清楚的是：就像 CLM 解决方案不是 SIEM，UBA 解决方案也不是 SIEM。现在，只有Chuvakin 博士发送了**关于这方面的推文**。



2.SIEM 要点

现在，我们深入了解基于分析的 SIEM 解决方案的构成内容。基于分析的 SIEM 的六项基本功能：

实时监控	威胁可以快速移动，IT 部门需要能够实时监控威胁并关联事件以发现和制止威胁。
事件响应	IT 部门需要采取有组织的方式来解决和管理潜在漏洞，以及安全漏洞或攻击的后果，以便限制损害并缩短恢复时间和成本。
用户监控	使用上下文监控用户活动对查明违规行为并发现滥用行为至关重要。对特权用户进行监控是合规性报告的共同要求。
威胁情报	威胁情报可以帮助 IT 部门识别异常活动，评估业务风险并优先处理响应。
高级分析	分析是从海量数据中获得见解的关键，机器学习可以自动执行此分析以识别隐藏的威胁。
高级威胁检测	安全专业人员需要专门的工具来监控、分析和检测杀伤链中的威胁。

这些功能使组织能够将他们的 SIEM 用于广泛的安全使用案例以及合规性。它们也是基于能力定义现代 SIEM 的一种方式。让我们深入了解构成基于分析的 SIEM 的每个基本功能。

实时监控

发现威胁所需的时间越长，它可能造成的损害就越大。IT 组织需要一个 SIEM，其中包含可以实时应用于任何数据集的监控功能，无论它位于本地还是云中。此外，该监控功能需要能够检索上下文数据源（例如资产数据和身份数据）以及可用于生成警报的威胁情报源。

基于分析的 SIEM 需要能够识别 IT 环境中的所有实体，包括用户、设备和应用程序以及任何不特定附加到身份的活动。SIEM 应该能够实时使用这些数据来识别范围广泛的不同类型和类别的异常行为。识别后，需要将这些数据轻松地输入到已设置的工作流中，以评估此异常可能代表的潜在业务风险。

应该有可自定义的预定义关联规则库，可提供安全事件和活动实时演示的安全事件控制台，以及可提供持续威胁活动实时可视化的仪表板。

最后，所有这些功能都应该增加开箱即用的相关搜索功能，可以实时调用或计划在特定时间定期运行。同样重要的是，应通过直观的用户界面提供这些搜索，以免 IT 管理员需要掌握搜索语言。

最后，基于分析的 SIEM 需要提供在本地搜索实时数据和历史数据的能力，这种方式可以减少访问搜索数据所产生的网络流量。

Autodesk 使用 AWS 上的 Splunk 节省时间和资本性支出成本

制造、建筑和媒体娱乐行业的客户（包括最近获得最佳视觉效果的 20 个奥斯卡奖获得者）使用 Autodesk 软件来设计、可视化和模拟他们的想法。鉴于 Autodesk 在全球的庞大规模，Autodesk 面临着两个截然不同的挑战：需要在多个内部团队的全球范围内获得业务、运营和安全洞察力，并需要选择合适的基础设施来部署运营智能软件。在部署 Splunk 平台后，该公司具有的优势包括：

- 节省数十万美元
- 关键的运营和安全相关见解
- 实时了解产品性能

为什么选择 Splunk

Splunk 于 2007 年首次在 Autodesk 中找到了一个家，作为利用机器数据进行操作故障排除的一种方式。如今，这种用法已经扩展到包括三个 Autodesk 部门的实时监控、详细的安全洞察力和执行相关的业务分析，其中包括：

- 企业信息服务 (EIS) - 负责全球企业 IT 管理，包括信息安全和信息管理。
- Autodesk 消费者团队 (ACG) — 负责所有 Autodesk 面向消费者的产品。
- 信息建模和平台产品 (IPG) - 负责为商业客户提供 Autodesk 解决方案，包括所有行业的设计师和工程师。

Autodesk 正在使用 Splunk Enterprise Security (Splunk ES) 来缩短识别和解决安全问题的时间。该公司还使用 Splunk App for AWS 为 Splunk Enterprise 和其他关键应用程序交付和管理灵活的资源。

增强数据驱动的决策

Splunk Enterprise、Splunk App for AWS、Splunk Enterprise Security 和其他 Splunk 解决方案使 Autodesk 获得对操作、安全和产品性能的重要实时洞察。Splunk 灵活的数据驱动分析和基于 AWS 的平台节省了 Autodesk 时间，降低了资本成本，并增强了关键决策的范围和深度。**阅读更多**。

事件响应

任何有效事件响应策略的核心都应是强大的 SIEM 平台，它不仅可以识别不同的事件，还可以提供跟踪和重新分配以及添加注释的方法。

IT 部门应该能够根据其角色为组织中的其他成员提供不同级别的访问权限。其他关键功能包括手动或自动聚合事件的能力，支持可用于从第三方系统提取数据或将信息推送到第三方系统的应用程序编程接口 (API)，收集法律许可的取证证据的能力，以及就如何应对特定类型事件为组织提供指导的手册。

最重要的是，基于分析的 SIEM 需要包含自动响应功能，这些功能可以中断正在进行的网络攻击。

实际上，SIEM 平台需要成为枢纽，可以围绕着它制定用于管理事件的可定制工作流程。当然，并非每件事情都有与其紧密相连的相同紧急程度。基于分析的 SIEM 平台为 IT 组织提供了通过仪表板分类任何潜在威胁的严重性的方法，该仪表板可用于分类新的重要事件，将事件分配给分析师进行审查，并检查用于调查线索的详细事件详情，基于分析的 SIEM 能够为 IT 组织提供所需的上下文洞察力，以确定对任何事件的适当响应。

这些响应能力应包括识别显著事件及其状态、指出事件严重性、启动修复过程以及围绕事件对整个过程进行审计的能力。

最后，IT 团队应该有一个仪表板，他们可以在调查过程中直观地将筛选器应用到任何字段，只需点击几下鼠标即可扩展或缩小分析范围。最终目标应该不过是让任何安全团队成员都能够将事件、操作和注释放入时间表中，以便团队的其他成员能够轻松理解正在发生的事情。这些时间表可以包含在日志中，使得审阅攻击和实施可重复杀伤链方法来处理特定类型事件变得简单。

PagerDuty 使用 Splunk Cloud 和 Amazon Web Services 确保端到端的可视性

客户转而寻求企业事件响应服务 PagerDuty，以便快速有效地管理和解决他们的 IT 事件。当云本地公司需要解决方案来满足其运营分析和分类需求时，它采用了在 Amazon Web Services (AWS) 上运行的 Splunk Cloud。借助 Splunk Cloud 和 AWS，PagerDuty 可确保其服务的高可用性，并可扩展以满足客户需求。自从部署 Splunk Cloud 后，PagerDuty 具备下列优势：

- 确保客户满意度和高度可用的云服务
- 比以前的服务节省 30% 的成本
- 缩短 IT 和安全事件解决时间 - 从数十分钟到几分钟或几秒钟

为什么选择 Splunk

Arup Chakrabarti 是 PagerDuty 的基础架构工程总监，负责现场可靠性、内部平台和安全工程。他的组织章程旨在提升公司整个工程组织的生产力和效率，包括公司产品开发组织内的多个工程团队。

在采用 Splunk Cloud 之前，PagerDuty 依靠日志记录解决方案，该解决方案无法扩展，因为该公司每天都在开始索引数百 GB 的日志。更重要的是，该团队发现很难从数据中获得可操作的信息来做出决策并迅速解决问题。在与以前的服务和 Splunk Cloud 并肩运行之后，该团队确定 Splunk Cloud 提供了快速解决问题并确保客户高可用性所需的速度。几天后，工程师们迁移到 Splunk Cloud。

“使用以前的解决方案时，有些查询需要花费 30 分钟时间来处理数据，并向我们提供需要的信息，这实在令人无法接受。” Chakrabarti 说。 “从客户影响的角度来看，我们最终使用 Splunk Cloud 将时间从几十分钟缩短到了几分钟或几秒钟。”

Chakrabarti 指出，尽管成本并非选择 Splunk Cloud 的主要动力， **“当我向会计团队宣布这个消息时，他们非常欣喜若狂， ‘我们将得到最好的解决方案，顺便说一句，与我们目前使用的相比，它便宜 30%’ ”** **阅读更多**。

用户监控

用户活动监控至少需要能够分析访问权限和身份验证数据，建立用户环境并提供与可疑行为和违反公司和监管政策相关的警报。

至关重要的是，能够将用户监控扩展到最常成为攻击目标的特权用户，并在受到威胁时，最大限度地减少损失。事实上，由于这种风险，特权用户监控是大多数受监管行业合规报告的共同要求。

实现这些目标需要实时视图和报告功能，能够利用各种身份机制，这些机制可以扩展为包括任意数量的第三方应用程序和服务。

Travis Perkins PLC 采用基于分析的 SIEM 来实现混合云转换

Travis Perkins PLC 是英国建筑商的商户和家庭装修零售商，拥有 2000 家分店和 28000 名员工。2014 年，该组织开始了“云优先”旅程；但是，其现有的安全信息和事件管理解决方案无法为混合环境提供必要的安全洞察力。Travis Perkins PLC 在审查了可用的备选方案后，选择了 Splunk Cloud、Splunk Enterprise 和 Splunk Enterprise Security (ES) 作为其 SIEM。在部署 Splunk 平台后，Travis Perkins PLC 具有的优势包括：

- 提高了混合基础架构的可视性
- 获得了检测和应对复杂网络威胁的能力
- 由于更有效的资源配置，降低了 IT 成本

为什么选择 Splunk

面对经济衰退期间充满挑战的市场形势，Travis Perkins PLC 不再将技术投资作为优先事项。最近，随着业务条件的改善，该公司对所有技术基础架构进行了战略审查，并采用了云优先方法来降低成本并提高灵活性。由于 Travis Perkins PLC 推出了大量云服务，包括来自 Google Cloud、Amazon Web Services 和 Infor CloudSuite 的 G Suite，很快就显而易见，其现有的 SIEM 无法提供对复杂混合环境中安全事件的必要见解。在审查了 HP、IBM 和 LogRhythm 等替代产品后，Travis Perkins PLC 选择了 Splunk Cloud、Splunk Enterprise 和 Splunk ES 来提供与安全相关的活动的单一视图。

从头开始建立安全

Travis Perkins PLC 利用 Splunk ES 实施提供的机会提高所有 IT 人员的安全意识，而不是只关注安全团队。IT 运营团队的员工现在可以访问特定的仪表板和警报，以便他们可以充当潜在威胁的第一响应者，并在必要时在上报给专门的安全团队之前立即采取行动。因此，Travis Perkins PLC 开发了一个高效、精益的安全运营中心 (SOC)，而不需要投入可能通常需要的大量资源。

自动化威胁防御

由于遍布英国的 24000 名员工使用各种设备访问企业数据，Travis Perkins PLC 实现大部分网络安全自动化至关重要。借助 Splunk ES，Travis Perkins PLC 现在可根据之前相关的数据或公司现有安全解决方案的警报计算不同威胁活动的风险评分。由于业务面临网络钓鱼邮件的特定问题，如果通过 Splunk 平台中的相关搜索识别出受感染客户端，它会生成自动警报。然后相关团队使用预设的手册响应进行反应。Splunk ES 中的泳道为资产或用户提供了全面的视图，并大大缩短了安全事件调查和解决所花费的时间。**阅读更多**。

威胁情报

基于分析的 SIEM 必须提供两种不同形式的威胁情报。第一个涉及利用威胁情报服务，提供关于损害指标、对手策略、技术和程序的最新信息，以及各种类型事件和活动的附加环境。该情报使得识别此类异常活动变得更加容易，例如识别到已知为活动命令和控制服务器的外部 IP 地址的出站连接。利用这该级别的威胁情报，分析人员可获得评估攻击的风险、影响和目标所需的信息 - 这对优先考虑适当的响应至关重要。

情报的第二种形式涉及评估资产的关键性、使用情况、连通性、所有权以及用户的角色、责任和就业状况。当涉及评估和分析事件的风险和潜在影响时，这种额外的上下文常常是至关重要的。例如，基于分析的 SIEM 应该能够提取员工徽章信息，然后将该数据与 VPN 身份验证日志相关联，以提供公司网络上员工位置的上下文。为了提供更深层次的分析和操作情报，SIEM 还应该能够利用 REST API 通过工作流操作或脚本来检索，以将其引入系统，并将关系数据库的结构化数据与机器数据结合起来。

理想情况下，威胁情报数据应与各种类型的 IT 基础架构和应用程序生成的机器数据集成，以创建观察列表、关联规则和查询，从而提高早期违规检测的成功率。这些信息应该与事件数据自动关联，并添加到仪表板视图和报告中，或者转发给防火墙或入侵防御系统等设备，然后修复相关漏洞。

SIEM 提供的仪表板应该能够跟踪部署在 IT 环境中的漏洞检测产品的状态和活动，包括提供扫描系统的运行状况检查以及识别不再被扫描漏洞的系统的能力。

简而言之，全面的威胁情报覆盖需要为任何威胁列表提供支持，自动识别冗余情报，识别并优先考虑多个威胁列表中列出的威胁，并为各种威胁分配权重以识别它们代表的真实商业风险。

洛杉矶市整合 40 多个城市机构的实时安全情报分享

为了保护其数字基础架构，洛杉矶市要求对其部门和利益相关者的安全态势和威胁情报进行态势感知。过去，该市 40 多家机构采取了不同的安全措施，使数据整合和分析变得复杂。洛杉矶寻求可扩展的 SaaS 安全信息和事件管理解决方案，以识别威胁、确定优先顺序并减轻威胁，获取可疑活动的可见性并评估整个城市的风险。在部署 Splunk Cloud 和 Splunk Enterprise Security 后，该城市具有的优势包括：

- 创建全市范围的安全运营中心 (SOC)
- 实时威胁情报
- 降低运营成本

实时态势感知

Splunk Cloud 为洛杉矶提供了其安全状态的整体视图。Splunk 转发器将来自该城市部门的原始日志和其他数据发送到 Splunk Cloud，在那里它们被标准化并返回到集成的 SOC，然后在 Splunk 仪表板中进行分析和可视化。

在 Splunk ES 中使用预先构建的、可轻松定制的仪表板，管理人员和分析人员可以随时随地了解整个城市网络基础架构中的安全事件。将所有安全数据保存在一个不断更新的数据库中，Lee 的团队可以查看和比较任何机器生成的数据，包括不同的日志以及结构化数据和非结构化数据，以提取包容性强、可操作的安全情报。

及时威胁情报

该市的集成 SOC 不仅仅收集信息；它还提供信息。它将 Splunk Cloud 的数据转化为及时的威胁情报。该市与其机构以及 FBI、国土安全部、特勤局和其他执法机构等外部利益相关者共享其调查结果。有了这些信息，该市可以与联邦机构合作识别风险并制定战略来阻止未来的网络入侵。

“有了态势感知能力，我们可以了解自己的情况”李说。“但凭借威胁情报，我们可以知道我们的敌人。我们现在正在运行集成的威胁情报项目，我们的 Splunk SIEM 是我们在集成安全运营中心（ISOC）部署的集中式信息管理平台的关键解决方案之一。”
阅读更多。

高级分析

基于分析的 SIEM 可以通过采用复杂的定量方法（例如统计、描述性和预测性数据挖掘、机器学习、模拟和优化）应用高级分析，以产生额外的重要见解。关键的高级分析方法包括异常检测、同行组分析和实体关系建模。

同样重要的是，基于分析的 SIEM 需要提供工具，例如，通过将分类后的事件映射到杀伤链或创建热图以更好地支持事件调查，使数据可视化和关联成为可能。

尽一切可能要求使用 SIEM 平台，该平台使用机器学习算法，能够自行学习代表正常行为与实际异常的内容。

然后，可以使用该级别的行为分析来构建、验证和部署预测模型。甚至可以在 SIEM 平台上采用使用第三方工具创建的模型。

基于云的创新型 SIEM 部署为 Equinix 提供可操作的安全情报

Equinix 公司将世界领先的业务连接到遍布五大洲的 33 个市场的客户、员工和合作伙伴。在 Equinix，安全性至关重要，因为全球数千家公司都依赖 Equinix 数据中心和互连服务。为了获得统一的安全基础架构视图，Equinix 需要具有集中可见性和 SIEM 功能的云解决方案，这些解决方案可以轻松、快速地实施，无需大量的操作工作。在部署 Splunk Cloud 和 Splunk Enterprise Security (ES) 后，Equinix 具有的优势包括：

- 全面的操作可视性
- 增强安全态势
- 节省时间和成本

通过 Splunk Cloud 和 Splunk Enterprise Security 全面了解基础架构

在实施 Splunk Cloud 之前，Equinix 每个月都会产生超过 300 亿次的原始安全事件，导致不堪重负。借助 Splunk ES 和 Splunk Cloud，安全团队现在可以将 300 亿原始安全事件减少至约 12000 个相关事件，然后再减少至 20 个可操作警报，从而为专用 SOC 提供可操作的安全智能和基础。

借助 Splunk 平台中汇总的所有数据，安全团队可以在系统之间交叉引用数据，使他们能够比以前快 30 % 的速度研究、调查和响应事件。“我们的最终目标是保护我们的客户、员工和数据。借助 ES 和 Splunk Cloud 作为我们的 SIEM 平台，我们所需的信息始终处于我们的指尖。” Equinix CISO 的 George Do 说。

“无论何时我们需要调查事件，我们只需在 Splunk 仪表板中显示相关数据，以便我们的安全团队以及我们的 C 级管理人员都可以访问这些信息。与部署基于本地的传统 SIEM 相比，节省的时间和精力非常大，总拥有成本 (TCO) 可节省 50%。”

多亏了 Splunk ES，Equinix 现在拥有全面的安全分析功能。例如，只要用户账户显示可疑活动迹象，例如本地员工意外从另一个大陆登录，高优先级警报就会立即触发并发送给安全团队。此外，将 Splunk Cloud 与 ES 结合使用可帮助 Equinix 防止敏感业务信息的泄露。特别是，管理员使用相关性来确定离职员工是否可能试图窃取机密数据。**阅读更多**。

高级威胁检测

安全威胁不断演变。通过实施网络安全监控、端点检测和响应沙盒以及行为分析相结合，基于分析的 SIEM 可以适应新的高级威胁，以识别和隔离新的潜在威胁。大多数防火墙和入侵防护系统无法单独提供这些功能。

目标不仅应该是检测威胁，还应该确定威胁的范围，方法是确定特定的先行威胁在最初发现后可能迁移到哪里，应该如何控制威胁以及如何共享信息。

SAIC 获得可见性和威胁检测

Science Applications International Corp.(SAIC)是一家领先的技术集成商，专门从事技术、工程和企业信息市场。凭借在科学研究、计划管理和 IT 服务等领域的专业知识，SAIC 从美国政府获得大部分收入。该公司需要建立强大的安全运营中心 (SOC) 和计算机事件响应团队 (CIRT) 来抵御网络攻击。在部署 Splunk 平台后，该公司具有的优势包括：

- 改进安全状态和操作成熟度
- 事件检测和修复时间减少 80% 以上
- 全面的企业环境可视性

为什么选择 Splunk

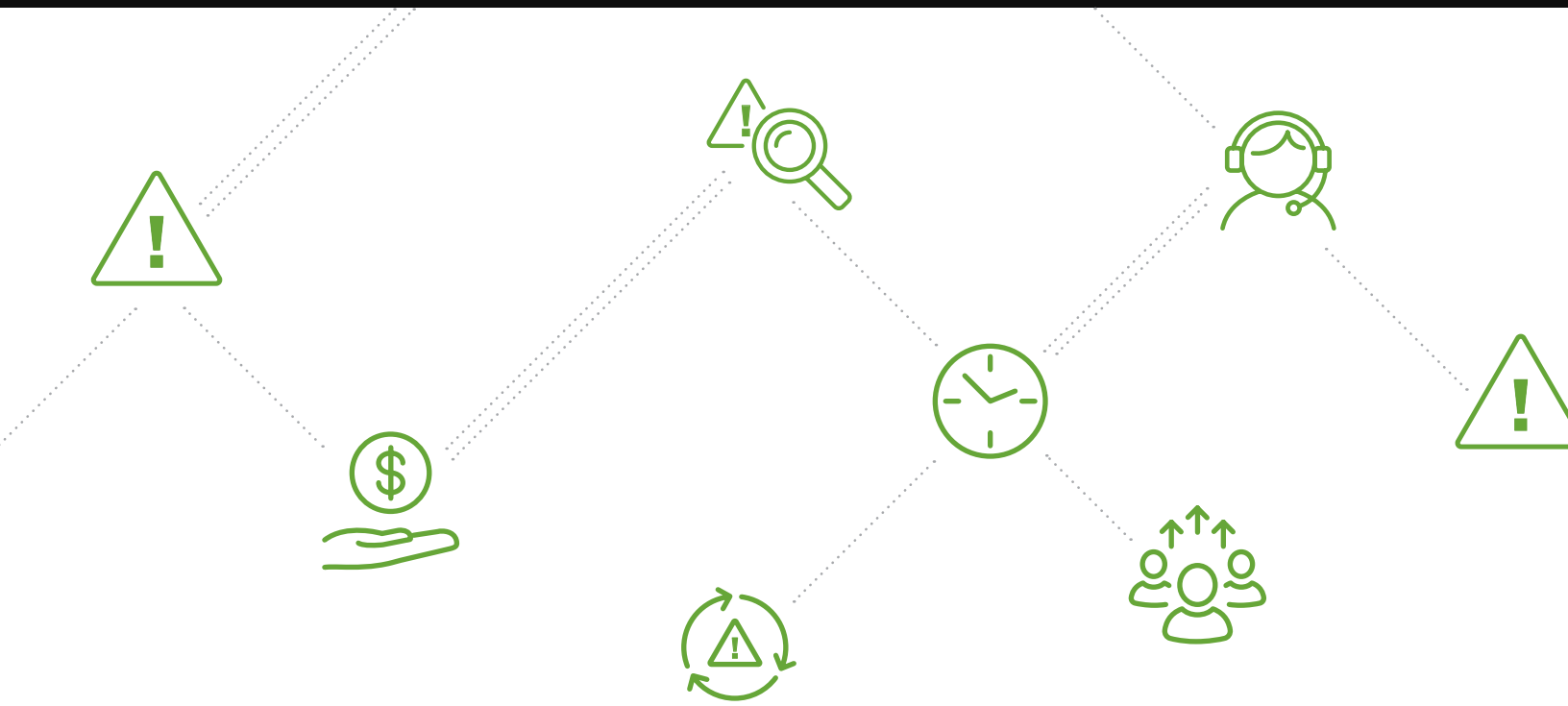
原 SAIC 于 2013 年分裂为两家公司后，为了避免组织利益冲突，SAIC 需要建立一个 SOC 作为其新安全计划的一部分。虽然它拥有大部分所需的安全工具，但 SAIC 缺乏安全信息和事件管理解决方案来确定其防御。原公司作为其安全调查的核心工具使用的传统 SIEM 存在局限性。SAIC 向 SIEM 补充了 Splunk Enterprise，使用该平台通过相关搜索以及事件调查进行事件检测。SAIC 的 IT 运营人员现在也在使用 Splunk 解决方案进行网络监控、绩效管理、应用分析和报告。

SAIC 开始构建新的 SOC 之后，公司决定依靠 Splunk 作为其所有类 SIEM 需求的单一安全智能平台，包括事件检测、调查和报告以实现持续监控、警报和分析。

对环境的全面可视性和威胁检测

SAIC 现在使用 Splunk 软件监控其环境是否存在任何威胁。在 SOC 中，分析师可以监控自定义 Splunk 仪表板，以发现异常或未授权行为的警报和迹象。他们现在可以立即知道已知的基于签名的威胁（例如由 IDS 或恶意软件解决方案记录的威胁）以及未知威胁（例如具有非典型活动的特权账户）。

传统 SIEM 通常使用预先构建的严格搜索进行搜索，但无法捕捉到高级威胁并产生大量误报。借助 Splunk平台，SAIC 分析人员已经建立了新的高度准确的相关搜索，以检测 SAIC 特有的威胁和损害指标，从而使团队能够高度评估和管理风险。包括 CISO 在内的高级管理人员现在可以查看与威胁活动有关的关键指标，包括趋势、合计源位置以及新近发现的损害指标。**阅读更多**。



3. 现代 SIEM 的九项技术功能

您已经了解**基于分析的 SIEM 的六大基本功能**，我们现在深入了解构成基于分析的 SIEM 解决方案的技术，以帮助您进一步区分现代 SIEM 与传统 SIEM、开源 SIEM 以及 SIEM 市场中的新进入者，例如 UBA 供应商。

对于任何探索 SIEM 市场的人员，推荐阅读 Gartner 年度安全信息和事件管理魔力象限报告。随着报告的发展，它已经发展到包括开源 SIEM 供应商和新技术，例如 UEBA 供应商。

该分析公司还提供了补充 SIEM 报告，并且在另一份研究报告中突出强调了将现代 SIEM（例如 Splunk 可提供的内容）与其他类别区分开来的九种技术能力。

将现代 SIEM 解决方案与更广泛的类别区分开来的九种技术能力是：

	SPLUNK	传统 SIEM	开源	新进入者
1. 收集日志和事件	是	是	是	是
2. 实时应用关联规则	是	是	DIY	是
3. 实时应用高级分析和机器学习	是	有限	DIY	是
4. 长期的历史分析和机器学习	是	有限	DIY	有限
5. 长期事件存储	是	有限	是	有限
6. 搜索并报告规范化的数据	是	是	是	是
7. 搜索并报告原始数据	是	复杂	是	复杂
8. 摄取上下文数据以进行其他关联和分析	是	有限	是	有限
9 解决非安全使用案例	是	否	DIY	否

1. 收集日志和事件

基于分析的 SIEM 解决方案应该能够收集、使用和分析所有事件日志并实时提供统一的视图。这使 IT 和安全团队能够从一个中心位置管理事件日志，将多个机器上的不同事件或多个日期关联起来，将其他数据源（例如注册表更改和 ISA 代理日志）与完整图像绑定。安全从业人员还可以从一个地方审计和报告所有事件日志。

2. 实时应用关联规则

事件关联是一种理解大量安全事件的方法，然后通过将多个事件链接在一起以获取洞察力，深入研究那些实际重要的事件。

3. 高级分析和机器学习的实时应用，以及 (4.) 长期历史分析和机器学习

有一种基本的分析形式，在 SIEM 的背景下提供数据背后的见解来揭示模式。这使得安全分析师能够深入挖掘并在威胁发生之前发现威胁或进行事故取证。

Forrester 最近的一项调查发现，74% “的全球企业安全技术决策者将安全监控作为一项高或重要的优先事项进行评估”，并且“供应商正在将安全分析功能添加到现有解决方案中，而新的供应商正在构建（安全分析）解决方案，以利用更新的技术，而不需要传统解决方案的支持。”

机器学习 (ML) 进一步进行数据分析。ML 通过基于分析的 SIEM 解决方案使组织能够使用从历史数据中变得更加智能的预测分析。这有利于安全从业人员检测事件，预测甚至防止攻击等等。

5.长期事件存储

基于分析的 SIEM 解决方案能够长期存储历史日志数据。这可以使数据随时间推移相关，也有助于满足合规要求。

为什么这在安全方面具有重要意义？例如，长期的机器数据保留使安全分析师能够执行安全取证来追溯网络违规的攻击路线。

6.搜索并报告规范化的数据

根据 SIEM 搜索和报告，用户可以搜索他们的数据，创建数据模型和枢纽，保存搜索和作为报告枢纽，配置警报以及创建可共享的仪表板。

7.搜索并报告原始数据

就 SIEM 而言，搜索和报告原始数据是来自各种来源的数据收集，并由基于分析的 SIEM 解决方案集中。与传统系统不同，基于分析的 SIEM 解决方案可以从几乎任何来源获取原始数据。这些数据可以转化为可操作的情报，而且，它可以变成易于理解的报告，从 SIEM 平台直接发布给合适的人员。

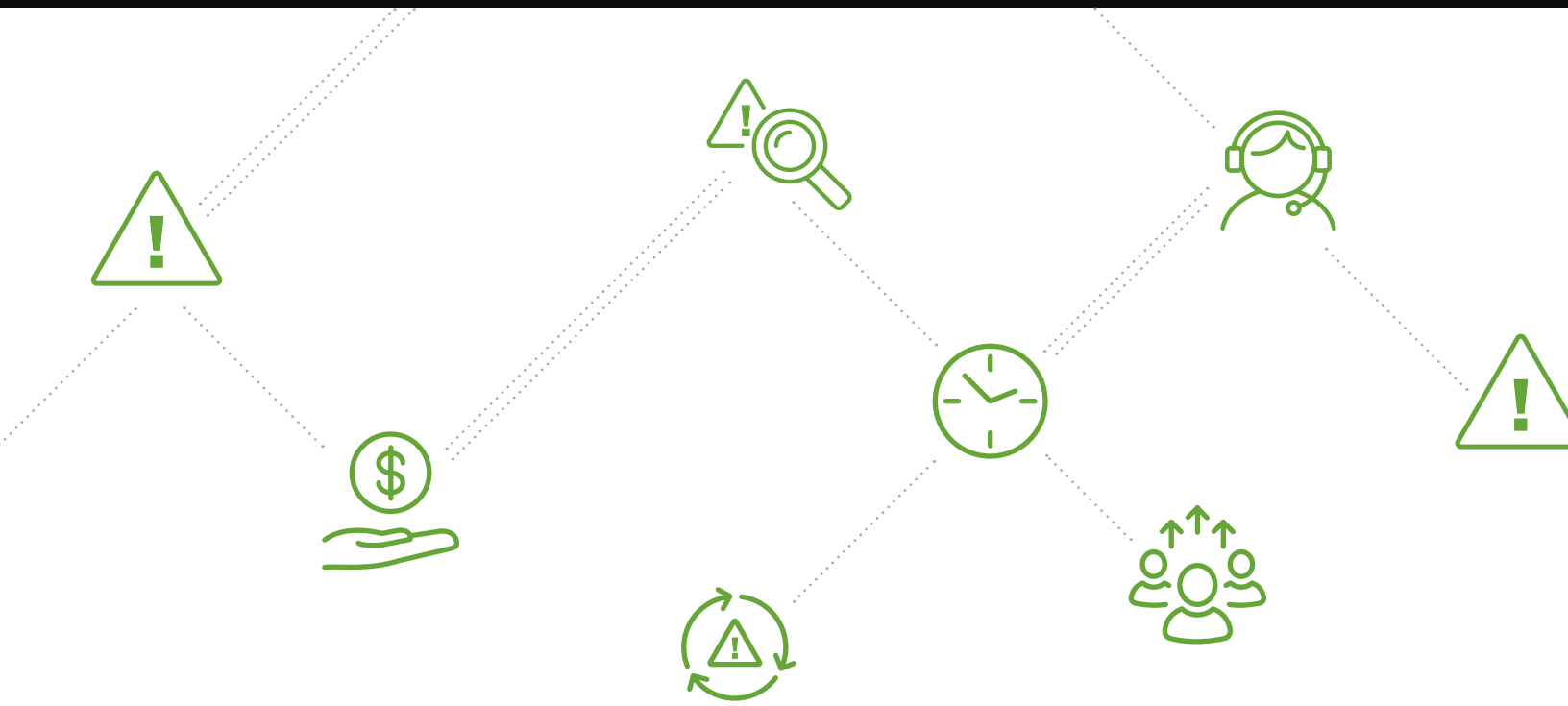
8.摄取上下文数据以进行其他关联和分析

在基于分析的 SIEM 解决方案收集数据后，用户需要额外的上下文来了解如何处理数据及其含义。这对于区分真正的威胁和虚假警报以及能够有效检测和应对真正的威胁至关重要。

基于分析的 SIEM 解决方案能够为外部威胁情报、内部 IT 操作和事件模式添加上下文。这允许用户实时进一步钻取并响应威胁。

9.解决非安全使用案例

基于分析的 SIEM 解决方案与传统 SIEM 解决方案之间的另一个区别是它可以用于多种使用案例，包括非安全用途，例如 IT 运营。



4.进入 SPLUNK

机器数据是一类增长速度最快、最复杂的大数据。也是最具价值的部分，包含明确的所有用户交易、客户行为、机器行为、安全威胁和欺诈活动等记录。不论您现在从事何种行业，Splunk 均能将计算机数据转化为有价值的真知灼见，这就是我们所说的运维智能。

Splunk Enterprise 可以从任何来源监控和分析机器数据，以提供操作智能，从而优化您的 IT、安全和业务绩效。Splunk Enterprise 具有直观的分析功能、机器学习、打包应用程序和开放式 API，是一个灵活的平台，可从重点用例扩展到企业范围的分析主干。Splunk Enterprise：

- 收集来自任何来源的日志和机器数据，并为其建立索引
- 强有力的搜索、分析和可视化能力可从整个组织提供支持
- 庞大的 Splunkbase 应用程序生态系统为安全性、IT 运营、业务分析等提供解决方案
- 可用作本地软件或云服务

运维智能让您实时了解到您的 IT 系统以及技术架构正在发生什么，这样您可以做知情决定。由 Splunk 平台启用，这是所有 Splunk 产品、高级解决方案、应用与加载项的基础。

Splunk 作为您的 SIEM

Splunk 安全解决方案不仅符合当今 SIEM 的新标准，而且还提供安全分析功能，提供有价值的上下文和视觉洞察力，帮助安全团队做出更快更明智的安全决策。

Splunk 为希望部署 SIEM 或从其传统 SIEM 迁移的企业提供多种选择，并提供本地部署、云部署或混合部署选项的选择。

客户可以使用 Splunk Enterprise 或 Splunk Cloud 解决他们的基本 SIEM 使用案例。Splunk Enterprise 和 Splunk Cloud 是核心 Splunk 平台，提供收集、索引、搜索和报告功能或 CLM。许多 Splunk 安全客户使用 Splunk Enterprise 或 Splunk Cloud 来构建自己的实时关联搜索和仪表板，以实现基本的 SIEM 体验。

Splunk 提供了一个高级解决方案 Splunk Enterprise Security (ES)，该解决方案通过即用型仪表板、相关搜索和报告来支持高级 SIEM 使用案例。Splunk ES 可在 Splunk Enterprise、Splunk Cloud 或两者上运行。除预先构建的关联规则和警报外，Splunk ES 还包含事件审查、工作流功能和第三方威胁情报源，帮助您进行调查。此外，Splunkbase 上还有 300 多个与安全相关的其他应用程序，其中包含针对特定第三方安全供应商的预建搜索、报告和可视化。这些即用型应用程序、实用程序和附加组件提供了监视安全性、下一代防火墙、高级威胁管理等多种功能。这些功能提高了安全覆盖范围，由 Splunk、Splunk 合作伙伴和其他第三方提供商提供。

Splunk ES 还是一个由五个不同框架组成的基于分析的 SIEM，可独立使用，以满足广泛的安全使用案例，包括合规性、应用程序安全性、事件管理、高级威胁检测、实时监控等等。基于分析的 SIEM 平台将机器学习、异常检测和基于标准的关联结合到一个单一的安全分析解决方案。

Splunk ES 可让您在视觉上随时间关联事件，并传递多堆栈攻击的详细信息。

该平台还可以让组织实时发现、监控和报告所有安全相关数据与业务环境中的威胁、攻击和其他异常活动。借助高级分析功能，客户可以在整个安全生态系统中实现加速威胁检测和快速事件响应。

Splunk ES 是更广泛的安全产品组合的一部分，通过 Splunk Enterprise 用户行为分析 (UBA) 向 CLM 提供 Splunk Enterprise 和高级 UBA 功能。

什么使 Splunk 作为 SIEM 工作?

- Splunk 软件可用于运行任何规模（大、中、小）的安全操作中心 (SOC)
- 支持全面的信息安全操作 - 包括状态评估、监控、警报和事件处理、CSIRT、违规分析和响应以及事件关联
- 对 SIEM 和安全使用案例的开箱即用支持
- 检测已知和未知的威胁，调查威胁，确定合规性并使用高级安全分析获取详细洞察
- 经过验证的集成式大数据安全智能平台
- 使用临时搜索进行高级违规分析
- 本地部署、云和混合本地部署和云部署选项。

Splunk UBA

Splunk UBA 是一种以机器学习为支持的解决方案，提供您需要的答案，以查找用户、端点设备和应用程序的未知威胁和异常行为。它不仅关注外部攻击，而且侧重于内部威胁。它的机器学习算法产生具有风险评级的可操作结果，并提供证据表明增强安全运营中心 (SOC) 分析师现有技术以加快行动。此外，它为安全分析师和威胁寻找员提供视觉枢纽点，以便主动调查异常行为。

Splunk UBA 一览:

- 使用以行为为中心的专用和可配置的机器学习框架，利用无监督的算法来增强检测足迹
- 通过将数百个异常自动拼接为单一威胁，增强 SOC 分析师 UEBA 功能
- 通过在攻击的多个阶段可视化威胁来提供增强的上下文
- 支持与 Splunk Enterprise 进行双向集成，以进行数据采集和关联，并使用 Splunk Enterprise Security 进行事件范围界定、调查和自动响应

Infotek 和 Splunk 为公共部门提供安全智能平台

许多组织依靠 SIEM 软件来监视、调查和响应安全威胁。但是，在美国一家政府机构中，当其传统的 HP ArcSight SIEM 软件无法达到预期时，其任务受到阻碍。该机构转向领先的网络安全、软件和系统工程公司 InfoTeK 取代其 SIEM 工具。在部署 Splunk 平台后，该客户具有的优势包括:

- 在一个周末部署并在第二天停止攻击
- 减少 75% 的成本以支持其 SIEM
- 减少所需工具的数量，包括日志聚合器和端点解决方案

借助 Splunk Enterprise 和 Splunk ES，该机构获得了基于分析的 SIEM，以合理的成本为 IT 团队提供可操作的安全情报。InfoTeK 在一个周末为客户部署了 Splunk 软件。

从第二天开始，该软件证明了它的价值。IT 团队能够搜索安全事件，并立即阻止攻击媒介。

“使用 Splunk 可以在几秒钟、几分钟或几小时内完成其他产品需要花费数小时、数天甚至数周才能完成的工作。” InfoTeK 高级事件处理和安全工程师 Jonathan Fair 说。 “我们能够在产品甚至被完全购买之前提供 ROI，因为客户已经成功地阻止了需要完全重建网络的威胁。” 阅读更多。

单击此处，了解 InfoTek 如何将 SIEM 成本降低 75%。

监控 报告	检测 警报	分析 调查	响应 合作	SIEM
预定义的视图和规则	相关规则，阈值	分析调查和上下文丰富	整个企业的协调和响应	安全运营管理警报和事件管理，基于策略的规则，开箱即用的安全规则和分析

美国政府内阁级别部门在传统软件维护方面节省 900,000 美元

公民期望政府机构不仅要明智地花纳税人的钱，而且要尽一切努力确保通过弹性运营来有效提供服务。美国一家大型内阁级部门之前拥有 HP ArcSight，这是一种缓慢而昂贵的安全信息和事件管理工具，无法满足该机构的需求。出于安全和合规性原因而使用 Splunk Enterprise 替换它之后，该部门具有下列优势：

- 每年在软件维护上节省 900,000 美元
- 改进安全检测、响应和修复
- 将安全调查从几小时减少到几分钟

主动安全方法

Margulies 和他的团队支持该部门的 SOC，包括使用 Splunk Enterprise 调查安全事件的 40 位分析师以及依赖该软件进行故障排除和报告的大型企业 IT 团队。其他客户包括必须确保该部门符合安全法规的人员。

Heartland Automotive 通过 Splunk 平台保护品牌声誉，确保数据安全

Heartland Automotive Services, Inc., dba Jiffy Lube 是美国快速润滑油零售服务商店最大的加盟商，因其著名的换油而闻名。Heartland Automotive 需要一个网络安全平台来保护其品牌及其最重要的资源 - 数据。自从将 Splunk ES 和 Splunk UBA 部署为其集成的 SIEM 平台以来，Heartland Automotive 已经看到了诸多益处，其中包括：

- 通过在三周内实施 SIEM 和内部威胁防护解决方案，在短时间内实现价值
- 获得了推动创新的平台，总体拥有成本降低 25%
- 建立实时安全调查和内部威胁保护

SIEM 的实施通常很复杂，因为大型组织有很多数据源，并且可能需要数周时间来配置警报。根据 Alams 的说法，Splunk 专业服务团队完成了识别公司数据源的整个过程，充实了 SIEM 设计并无缝配置警报。

“快速实现价值是一切 - 我们能够在三周内实施 SIEM 和内部威胁检测解决方案，而在之前，这通常需要三个月的时间。” Heartland Automotive Services 的 IT 和信息安全主管 Chidi Alams 说。 “快速实现价值给首席财务官和我们高级领导团队的其他成员留下了深刻的印象 - 仅一天就能完成部署，几乎在第二天便可实施 - 增加了他们对我们快速交付的信心。” **阅读更多。**

单击此处，了解 Heartland Automotive 如何利用 Splunk 实现创新，并将总体拥有成本降低 25%。

Splunk ROI 故事

基于分析的 SIEM 解决方案往往因昂贵的投资而受到批评。但这只是旁观者眼中的花费。

基于分析的安全解决方案在您的组织成为内部人员攻击的受害者之后似乎有多昂贵？或者窃取头条的勒索软件攻击。

所以，没有违反即时投资回报 (ROI)，并主动保护您的组织免受内部和外部恶意行为人的侵害。

但这不是 SIEM 投资回报结束的地方。

基于分析的 SIEM 解决方案支持常见的 IT 使用案例，例如合规、欺诈、盗窃和滥用检测、IT 运营、服务情报、应用程序交付和业务分析

随着安全团队与其他 IT 职能一起工作，其他使用案例的可见性将导致跨组织的集中式视图，实现跨部门协作和更高的 ROI。

若要了解基于分析的 SIEM 解决方案的真正 ROI，最好的方法是听取使用过的人员的意见。

SIEM 的未来

驱动 SIEM 发展的基本技术可能已经存在多年，但这并不意味着所有 SIEM 都是过时的技术。

事实上，正如本买方指南中指出的那样，并非所有的 SIEM 都具有相同的效果。通过了解传统 SIEM 解决方案与现代基于分析的解决方案之间的差异，可以很好地展示这一点。

正是这些基于分析的 SIEM 为市场的未来提供了最明亮的亮点。这些现代化的安全解决方案对于威胁检测、修复、警报和合规报告仍然非常有用，同时提供了可证明的投资回报。

随着现代威胁形势的不断发展，基于分析的 SIEM 解决方案已经证明它们能够适应并领先于这些威胁。

您是否想详细了解 Splunk 基于分析的 SIEM 解决方案以及它如何帮助改善组织安全状况？
立即与 Splunk 专家交谈。

splunk>

了解更多：**www.splunk.com/asksales**　　**www.splunk.com**