现代 SOC
的 10 个基本功能

安全运营中心 (SOC)
中的数据到一切

splunk>
turn data into doing™

目录

安全运营中心 (SOC) 中的数据到一切

我们生活在一个空前创新的时代。技术正在重构整个行业，使我们的业务全球化，并提高我们的劳动力效率。但我们只触及了表面。随着创新的不断涌现，我们无法预测将会取得什么成就，以及我们随后可能面临的后果。

随着连接设备的数量迅速接近 800 亿台，自动化已经深入我们的日常生活，我们世界的变化只会加速，攻击面将不可避免地扩大。安全部门被迫应对来自多种来源、不同格式和速度更快的数据，这表明许多组织没有为今天和明天的数据挑战做好准备。

您的组织需要可见性来了解那里有什么，并需要上下文来更好地理解真正面临风险的是什么。在系统和使用系统的人周围有更多的数据，最终可以让我们更好地理解如何管理风险。

所以，组织不惜花费数十亿美元和数不清的时间来尝试挖掘其数据的价值，堵塞其基础设施整体视图暴露的安全漏洞。他们正在创建数据湖 - 集成和跨无数系统工作，创建大量数据，同时还在复杂的工具网络中导航，这些工具旨在聚合、监控和分析这些数据，以解决他们最大的安全挑战。

我们的方法：数据到一切

为我们组织提出的每一个问题、我们做出的每一个决定和我们采取的每一个行动提供数据至关重要。但是，在一个不断发展、联系日益紧密、产生越来越多数据的世界里，挑战不仅在于如何跟上这一切，还在于如何迅速将其转化为洞察力和行动。数据具有不同的形式，来源也不尽相同，许多组织还没有利用它们来更好地保护自己。

优化您的安全堆栈，使您的团队能够以最高性能运行，这需要一个单一的平台，让团队能够采取行动，从调查和监控到编排和补救。它必须是一个强大的平台，使整个组织能够通过单一的整体视角来利用数据的力量。这种方法意味着技术投资更少、更智能，复杂性更低，数据和行动之间的障碍更少。

我们将此称为**数据到一切平台**。它是任何现代安全运营中心 (SOC) 的基础，将数据从您的组织带到您最紧迫的安全用例中。

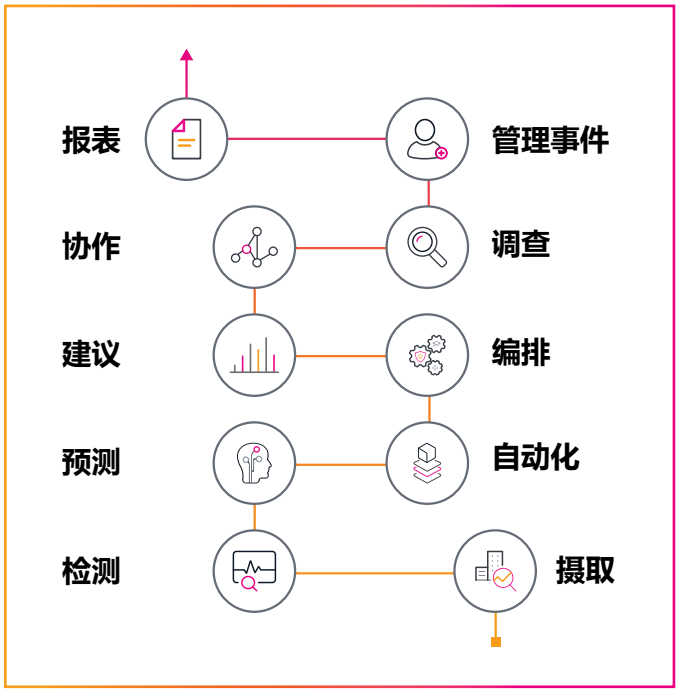
构建现代 SOC

安全团队在前线努力工作：识别、分析和减轻组织面临的威胁。虽然他们尽了最大努力，但每天积压的事件数量仍在继续增长。现实是，**没有足够的熟练专业人员**来分析大多数组织面临的大量事件。

但是，由数据到一切平台驱动并建立在此平台上的现代 SOC，具有跨整个企业的可见性，为每个团队成员创建了一个共同的工作表面。使用单一套件即可无缝集成其他供应商的解决方案以增强现有能力，这意味着，分析师可以将时间花在更高价值的活动上，消除了在几十种产品之间切换的需要，并为每个团队成员创建了一个共同的工作表面。

这不应该是一个临时拼凑的解决方案。安全套件应该具有强大的分析能力，可以提升中小型员工的工作能力，让他们深入了解潜在的威胁，避免将时间浪费在误报的警报上。最后一个关键的特性是套件能够利用先进的机器学习 (ML)、自动化和编排技术。

为了构建现代 SOC，组织需要一个可以支持以下 10 种功能的安全操作平台：



10 项功能

1.摄取

所有数据都是安全相关的。数据就好比 SOC 赖以存活的氧气。各种分析工具和算法可以呼吸它。同样重要的是，要能够大规模地从任何 (结构化或非结构化) 来源摄取数据。您还需要组织数据的能力，使其可由机器或人来操作。

2.检测

进入系统事件后，安全运营套件必须具备检测事件的能力。在这种情况下，检测的重点是事件，这与侧重于文件或网络流量的传统解决方案不同。安全运营套件可以利用关联规则、机器学习和分析案例等多种功能。

3.预测

假设您可以在发现安全事件前 30 分钟收到警报。想象一下，这对您的 SOC 来说将意味着什么。SOC 可以通过预测安全事件的能力将事件主动上报为相关人员，或使用预定义流程简化响应。一些新兴的预测技术有望为分析人员提供更大规模袭击的早期预警、先兆或指标，并在未知因素变成更大风险之前识别这些因素。

4.自动化

自动化是一种可以为 SOC 分析人员提供帮助的新技术。Splunk 最近收购的 Phantom 就是一个很好的例子。自动化工具采用标准操作程序，并可将其转化为数字化脚本，以加速调查、改进、搜寻、控制和补救。

具有自动化功能的 SOC 可以处理更多的事件，例如，过去需要 30 分钟的进程现在只需 40 秒就可以完成。在 SOC 的发展过程中，自动化不再是一种选择，它已经成为一种必备的工具。

5.编排

您购买多种产品来支持 SOC 是出于实际需要，而不仅仅是因为您有额外的预算。大多数这些工具都有着特定的用途，可以增加您的防御能力，但这些工具都不太可能发生变化。这就会出现问题，因为威胁是不断发展变化的，而捕捉威胁的产品也需要在 API 驱动的环境中跟上这种发展的步伐。

这就是编排的作用。您可以通过编排功能插入并连接 SOC 内部和外部的所有产品。您不再需要为每个产品打开新的浏览器选项卡或单独的单点解决方案登录，也不需要从不同的解决方案进行复制粘贴的操作。编排所有产品的能力可以消除开销，缓解不良情绪，并可以帮助分析人员将精力集中在更有意义的任务上。

6.建议

此时，事件已经通过机器。如果支持 SOC 的平台能够告诉分析人员下一步该做什么，那不是很好吗？现代 SOC 可以通过给出建议实现这一功能。这一过程可以通过独立操作或脚本的方式得以实现。该功能有两个好处：1) 对于新的分析人员来说，教他们当类似的威胁再次出现时该怎么做非常具有教育意义；2) 对于有经验的分析人员而言，它可以充当一种完整性检查，或者作为敦促他们了解他们应该掌握的情况的一种提醒。

7.调查

我们预计 90% 的第 1 层分析师的工作将在不久的将来实现自动化。但其他的工作将会怎样呢？完成最后一英里的工作当然还是需要细致、精确的人工分析。直观的安全工具有助于分析人员的人工工作效率，并可以帮助他们对需要调查的事项进行优先排序。

8.协作

安全是一项团队运动，需要协调、沟通和合作。在 SOC 环境中，所有环节都很重要，处理事件时必须全盘考虑，团队需要具有 ChatOps 能力，或者能够展开合作并将工具、人员、流程和自动化连接到透明的工作场所。

通过这种方式就可以围绕各种信息、想法和数据问题展开工作。这种方式可以让安全团队更好地展开合作，联合 SOC 之外的人员处理警报，与同行共享关键的时间敏感型详细信息，并最终促进行业合作。

9.管理事件

就算我们竭尽全力预防事故，事故还是会发生。重要的是，当发生事故时，要可以为安全团队提供管理响应流程所需的所有工具。团队需要确保他们制定了应对计划、工作流程、证据收集方式、沟通机制、记录方式和时间线。因此，事件管理已经成为现代 SOC 的核心功能。

10.报表

您无法管理自己无法衡量的东西。我们生活在一个数据驱动的世界，安全也不例外—因此，我们现在可以对安全过程的所有方面进行衡量。拥有适当的报表工具有助于我们了解任务执行内容，因此安全团队可以准确地衡量他们所处的情况和需要达到的目标。如今，SOC 面临的挑战是他们依赖于过多的平台，这使得他们不可能得到准确的报告。

进入 Splunk

Splunk® 平台，也称为 Splunk Cloud 或 Splunk Enterprise，是您的起点。Splunk 是一个可定制的数据分析平台，可以将机器数据转换为有形的业务成果。不像其他替代方案，Splunk Cloud 和 Splunk Enterprise 使您能够利用现有技术投资，以及由 IT、安全和业务系统、应用程序和设备生成的广泛的扩展数据，以便进行近乎实时的调查、监控、分析和操作。

但更具体地说，Splunk 安全操作套件汇集了领先的 SIEM、UEBA和 SOAR 技术，这些技术建立在一个共同的工作表面上，为现代 SOC 提供强大支持。

Splunk Enterprise Security (ES) 是一个分析驱动的 SIEM 解决方案，可提供实时安全监控，先进的威胁检测，事件调查和取证以及事件响应，以便进行有效的威胁管理。

通过 **Splunk ES**，安全团队可以获得更快的威胁检测、调查和响应能力。他们可以使用专门打造的框架和工作流来加速检测、调查和事件响应。他们还可以使用预构建的仪表板、报表、调查功能、用例分类、分析、关联性搜索和安全指示器来简化威胁管理和事件管理。然后，他们可以使用这些功能来关联软件即服务 (SaaS) 和内部资源，以发现和确定用户、网络、端点、访问和异常活动的范围。

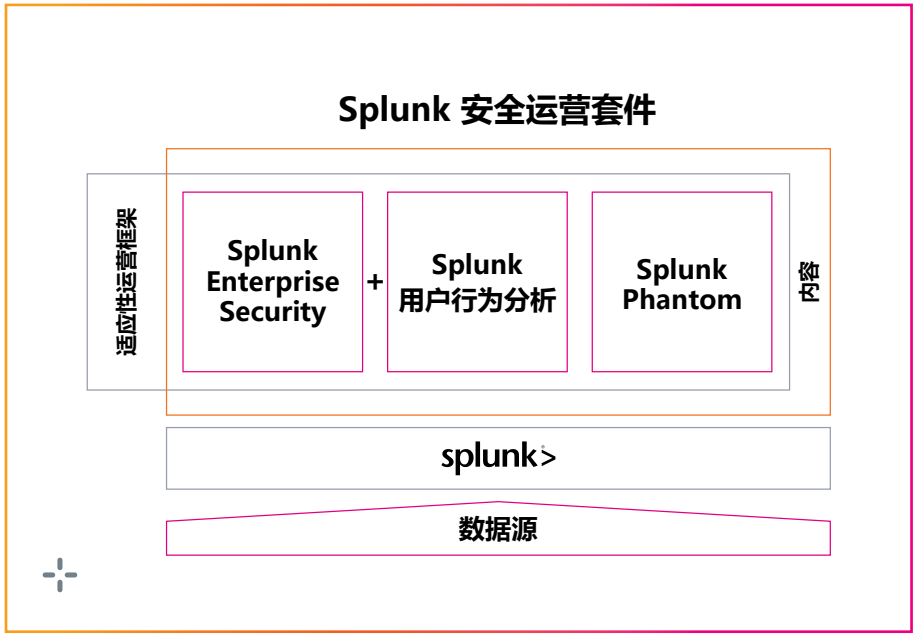
Splunk 用户行为分析 (UBA) 是一种以机器学习为支持的解决方案，可用于查找用户、端点设备和应用程序的未知威胁和异常行为。它可以强化您现有的安全团队，并通过发现由于缺乏人员、资源和时间而被遗漏的威胁来使他们更有成效。

安全团队可以使用 **Splunk UBA** 来增强可见性和威胁检测能力。值得一提的是，他们可以使用无人监管的 ML 算法检测内部和未知的威胁，这是传统安全产品无法提供的功能。他们可以使用复杂的杀死链可视化技术自动将异常行为关联到高保真度的威胁中。这一功能可以将团队解放出来，让他们可以花更多的时间来查找保真度更高的，基于行为的警报。他们还可以通过动态内容订阅更新在无需停止

业务运行的情况下识别最新的威胁，从而使安全团队能够主动保持最新的威胁检测技术。

Splunk Phantom 是一个可以将团队的流程和工具集成在一起的 SOAR（安全编排、自动化和响应）平台，使他们能够以更加智能的方式开展工作、更快地进行响应并提高他们的防御能力。

Phantom 可以帮助实现 SOC 安全运维工作的最大效率。安全团队可以实现重复任务的自动化，以优化工作效率，并更好地将注意力集中在真正需要人工输入的决策上。它们可以通过自动检测和调查减少驻留时间，并可以通过以机器速度执行的脚本缩短响应时间。Phantom 还可以帮助安全团队集成现有的安全基础设施，以便每个部分都积极参与到 SOC 的防御策略中。



开始使用。

详细了解 Splunk 的安全运营套件如何帮助您打造全新的 SOC。

10-Essential-Capabilities-of-a-Modern-SOC-106

splunk> turn data into doing™