建设更好 SOC 的基本指导

splunk>
turn data into doing™

要领先于手段高超的网络威胁非常困难。检测未知或隐藏的威胁更是难上加难，特别是当现有的点和陈旧安全工具无法解决高级安全威胁的复杂性和数量时。

过时的解决方案很难检测到内部威胁、横向移动的恶意软件和受到感染的帐户带来的风险，部分原因是它们无法应对当今的网络威胁，另一方面的原因是为传统安全运维中心 (SOC) 提供支持的软件解决方案会向分析人员发出大量警报，但很多都是误报。

无论您的安全团队工作多么努力，或者多么有天赋，都会有大量的安全事件积压 — 而且这种情况不可避免。现实的情况是，我们根本没有足够的熟练安全人才 (事实上，这一缺口高达 350 万人)，而且，即使有可以满足要求的人员，他们的成本也十分高昂。

他们的工作实际上因为他们使用的工具而变得更加困难。在今天的 SOC 中使用的过时工具不仅会消耗预算，而且这些工具由无法很好地工作协作的不同供应商构建。如果不同的供应商无法很好地协作，流程就会变慢，数据也会丢失。

因此，分析人员常常无法看到整个企业内部发生的所有状况。实际上，平均而言，业务和 IT 决策者估计，在他们拥有的数据中，暗数据 (未知或未开发) 的比例达到 55%。那么，如果一开始就无法看到大部分可用数据，安全专业人员该如何保证那些看不到的数据的安全呢？毕竟，安全性对所有数据而言都非常重要。

这就是理解 SOC 的起源对于处理今天的问题至关重要的原因。SOC 最初作为物理和虚拟安全操作的新重心出现。它们需要不断的维护、扩展和前所未有的速度，以产生价值。

SOC 分析人员一天的工作很快集中在对警报进行分类和后续处理。他们有太多的事情要处理，第 1 层分析人员很快就会不堪重负，只能任凭自己沉浸在不断落后的无力挣扎中。

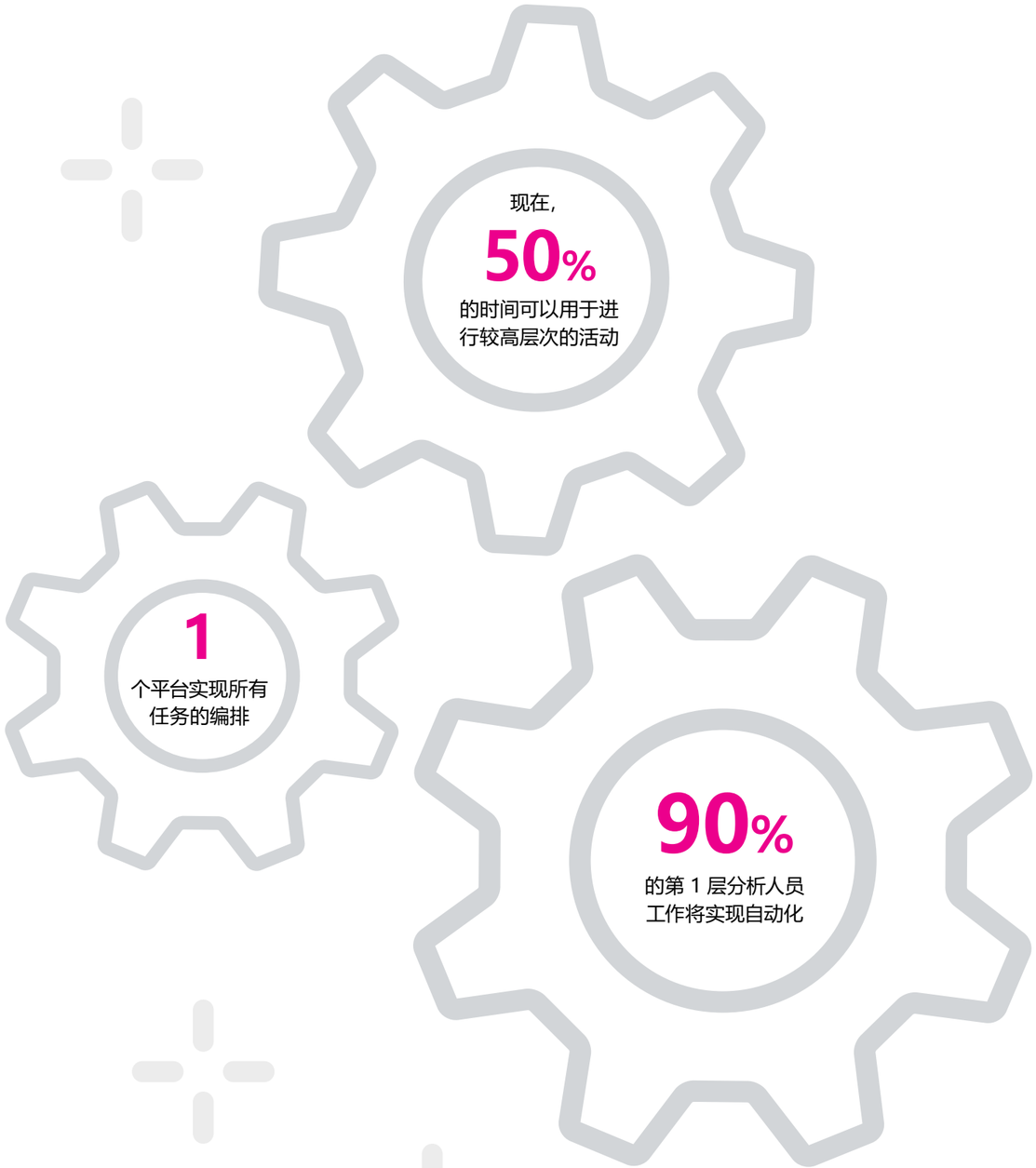
他们的工作变得更加困难，因为 80% 的 SOC 建立在相互独立、互相割裂的系统之上。

我们都需要接受这样一个新的事实：他们根本没有足够的专业技术人员来分析他们所面临的数量如此庞大的事故，而且大多数分析人员也没有适当的工具来弥补不足。

那么，依赖于陈旧技术方案的公司应该怎么做呢？除了克隆他们所有的 SOC 分析人员，并争取到他们梦寐以求的资金支持以外，还要看公司用来为其分析人员应对各种威胁所采用的技术方案。

安全团队需要在 SOC 中添加新的分析功能来应对新的威胁，在它们发展为可怕的网络怪物之前，让他们对潜在的威胁具有更深入的了解。他们需要允许安全专业人员实现某些流程自动化的工具，这样他们就可以专注于真正的警报—也就是真正的威胁。

现在，是时候构建一个更好的 SOC 了。是时候构建下一代的 SOC 了。



在当下构建可以满足未来需求的 SOC

未来，90% 的第 1 层分析人员工作将实现自动化。他们的大部分工作都是单调的、重复性的，而自动化则可以让分析人员专注于真正重要的任务。

其次，我们预计他们的工作将从花费时间筛查警报转向对检测和响应逻辑进行细微的调整，进而创建关联规则和脚本，以推进自动化过程。我们预计分析人员 50% 的时间将花在具有更高价值的活动上。

最后，我们希望像 Splunk 这样的平台可以接入网络并创建用于监控和调查事件的单个平台，这样就不需要在几十种产品之间来回切换。

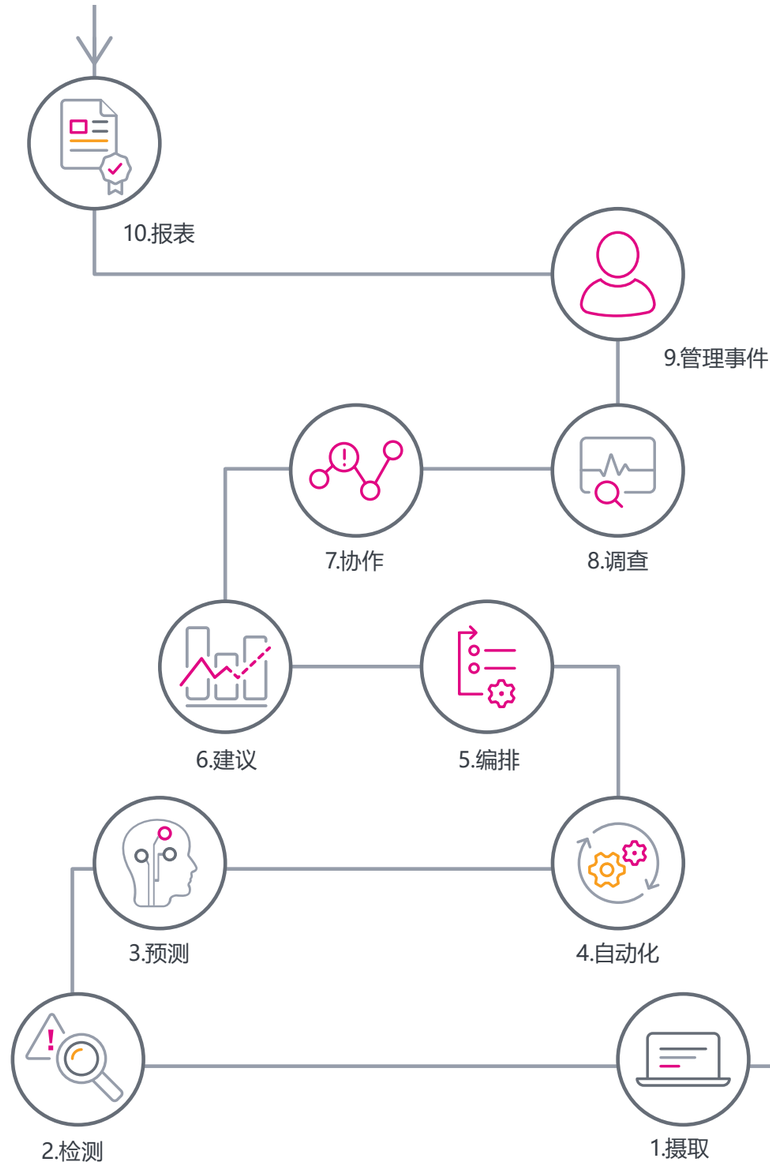
组织不需要等到未来才能得到他们今天需要的技术。

事实上，构建可以满足未来需求的 SOC 真正开始于接受这样一种理念，也就是可以采用一种精心构建的平台为 SOC 提供支持，然后插入必要的自动化和机器学习工具。而这就需要支持这样一种理念，我们可以成为 SOC 的领导者。

下一代 SOC 构建在一个单独的套件上，它可以无缝集成来自其他供应商的解决方案，以增强现有的功能。但这并非临时拼凑起来的解决方案。

安全套件还应该具有强大的分析能力，可以提升一小部分员工的工作能力，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。

具体来说，为了构建可以满足未来需求的 SOC，组织需要一个支持 10 种功能的安全运维平台：



1.摄取

所有任务均始于数据。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

假设您可以在实际发现安全事件前 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，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？下一代 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

我们之前提到过，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。那么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，并可以帮助他或她对需要实际调查的事项进行优先排序。

8.协作

实现安全性需要团队协作和沟通。换句话说，也就是：团队合作。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，事件管理已经成为下一代 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

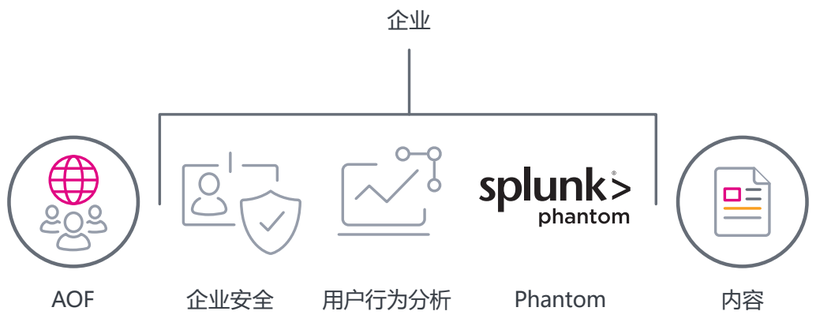
Splunk 安全运营套件集领先的 SIEM、UEBA 和 SOAR 技术于一身，这些技术构建在单个平台上，可为下一代 SOC 提供强大支持。没有一个 Splunk 的竞争对手敢说他们可以在一个平台上集成所有解决方案。

Splunk 不仅可以本地支持这些功能，而且还支持以下用例：

实时监控	Splunk Enterprise 或 Splunk Cloud 或 Splunk Enterprise Security
调查	Splunk Enterprise 或 Splunk Cloud 或 Splunk Enterprise Security
自动化和编排	Splunk Phantom
高级威胁和内部威胁检测	Splunk 用户行为分析或 Splunk Enterprise Security
事件响应	Splunk Phantom 或 Splunk Enterprise Security
合规性	Splunk Enterprise 或 Splunk Cloud 或 Splunk Enterprise Security

Splunk 平台，也称为 Splunk Cloud 或 Splunk Enterprise，是您的起点。这里是您摄取数据的地方。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 SaaS 和其他开源替代方案，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。

Splunk 安全运营套件



但更具体地说，Splunk 安全运营套件由以下部分组成：

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。之后，他们可以使用这些功能在 SaaS 和本地数据源之间进行关联，以发现并确定用户活动、网络活动、端点活动、访问活动和异常活动的范围。

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 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将现有的安全基础设施集成在一起，以便每个部分都积极参与到 SOC 的防御策略中。

关于 Splunk。

Splunk Inc. 使所有人都可以访问和使用数据，使其更具价值。

详细了解 Splunk 的安全运营套件如何帮助您打造全新的 SOC。

Splunk、Splunk>、Data-to-Everything、D2E 和 Turn Data Into Doing 是 Splunk Inc. 在美国和其他国家/地区的商标和注册商标。
所有其他品牌名称、产品名称或商标均属于其各自所有者。© 2020 Splunk Inc.版权所有。

2020-Splunk-SEC-Fundamental-Guide-to-Building-a-Better-Security-Operations-Center-110-EM

splunk>
turn data into doing™