kaspersky 引领未来

XDR、SIEM 与 SOAR 的对比

太多的缩写词让人晕头转向？让我们看看这些词都代表什么

简介

SIEM、SOAR、MDR、EDR、EPP、XDR 等等都是有关网络安全的缩写词，您是不是已经摸不着头脑了？这可以理解——所以我们准备了这份实用指南来帮您厘清三个主要术语的区别：SIEM、SOAR 和 XDR。这些缩写词的背后有什么样的故事？这些容易混淆、有部分字母相同的术语是怎么在这个行业里形成的呢？它们是真的有不同的含义，还是只是营销噱头？有哪些相同点和不同点？它们是互为补充，还是存在竞争关系？让我们一起来探究吧！让我们利用知识的力量，拨开缩写词和专业术语的重重迷障，让一切都豁然开朗！

SIEM

安全信息与事件管理 (SIEM) 是一套将安全事件管理 (SEM) 和安全信息管理 (SIM) 结合在一个平台上的工具和服务。SIEM 收集、汇总、分析并存储来自整个 IT 基础设施的日志数据，以用于各种用例，包括治理和合规，以及基于规则的可疑活动相关性匹配。

SIEM 的运作方式是什么？

第一款 SIEM 服务诞生于 2005 年，原本用于汇总并存储来自组织的整个 IT 基础设施（包括端点、应用程序和网络设备）的日志和事件，以便用于合规性报告。SIEM 在此数据集上运行相关性分析，寻找可能表明可疑行为的任何模式或事件，并为安全运营中心 (SOC) 生成警报。不久之后，安全分析人员发现这些警报不仅可以用于合规和治理任务，而且能够更主动地识别和阻止生态系统中的任何恶意活动的进行。

SIEM 的局限性

SIEM 服务的问题在于并非专为事件检测和响应而设计的。因此使用起来有点困难，原因如下：

- 警报过多 — SIEM 提供的庞大数据集必须手动过滤、处理和分析，这对于试图在迅速变化的威胁环境中阻止攻击的安全分析师来说不太方便。
- 缺少上下文 — 为应对新的、复杂且棘手的攻击，安全分析师需要通过连贯的上下文信息来了解组织的威胁环境，而不是 SIEM 提供的毫无关联的数据流。
- 过于被动 — 阻止可疑进程、隔离文件和其他响应能力不在其功能范围内；它基本上是一种被动的分析工具。

安全专业人员试图通过在 SIEM 之上分层设置附加工具或使用机器学习和行为分析插件来开发新一代的技术，从而解决这些问题。但仍然需要一种工具来提供更高质量的警报以及支持更迅速的自动化流程。

安全编排、自动化和响应

安全编排和自动响应 (SOAR) 工具于 2015 年问世，用于解决 SIEM 系统的上述某些缺陷。SOAR 平台通过整个基础设施中的各种来源（包括管理系统和威胁情报平台）获取数据，并提供优先级分析。然后，安全团队可以利用 SOAR 平台与通过 API 连接的安全工具生态系统的集成，配置对于传入威胁的多阶段、跨解决方案的自动化响应。

SOAR 的运作方式是什么？

这个工具的用处很大！原因如下：
SOAR 工具可以实现自动化。虽然这些工具最为人熟知的能力是自动事件响应流程，但它们实际上可以将各类工作流程自动化，包括漏洞扫描、日志分析、用户访问管理和威胁分类等。
在这个过程中要用到“攻略手册”，即由特定事件触发的一组预配置规则，这些规则告诉系统在特定工作流程中的下一步应该执行哪些步骤。大多数 SOAR 解决方案都附带数百个随时可用的“攻略手册”，涵盖需要 SOC 团队处理的最常见任务。团队可以配置自己的“攻略手册”，将其他更多特定的重复流程自动化。

其次，SOAR 工具提供编排功能。自动化是指用机器驱动的方式执行单个工作流程中的各项任务，而编排是指将多个不同的工具和流程协调到一个更大的工作流程中，将所有相关数据整理到一个平台上，以形成统一的、可据此采取行动的信息。

SIEM 与 SOAR 的关系

SIEM 与 SOAR 这两种工具通常配合使用，类似于助理和经理的关系：SIEM 收集所有日志，将它们关联起来以查找警报，并将此信息提供给 SOAR，再由 SOAR 带头采取响应行动。

SOAR 的局限性

一切听起来都很棒，对吧？问题是，维护一个配置完善且与合作伙伴工具相集成的 SOAR 平台需要由配备先进技术且成熟的 SOC 持续提供保障。鉴于当前在网络安全技能方面的不足，许多组织目前还无法建立这样的 SOC。

如果没有熟练技能和警惕能力来维护 SOAR 平台，SOAR 分析人员最终可能会收到过多的低优先级警报、误报和基本不连贯的数据集，原因是平台上的各种工具都是孤立的，而这正是他们想要避免的情况。

扩展检测与响应

XDR 是一种本地或基于云的安全解决方案，大致分为两类：原生和混合。原生 XDR 是由一家供应商统一提供的一套工具，而混合 XDR 是将其他第三方解决方案集成到您的生态系统中。“XDR”一词最早出现在 2018 年，其中“X”代表“eXtended”（扩展）：XDR 通过收集来自多个安全层（包括电子邮件、云和网络）的数据并关联在一起，将防护范围“扩展”到传统的端点检测、响应和保护工具（EDR 和 EPP）之外，为整个 IT 基础设施提供全面保护。

所以，它是一个让一系列工具能够协同工作的平台，并使用机器学习和自动化技术来帮助安全团队保护整个安全生态系统……听起来有点类似于 SOAR，不是吗？但这两者存在一些本质上的区别。让我们来具体看一看……

XDR 与 SOAR：有什么区别？

1. XDR 解决方案针对的是端点数据和优化 — 这意味着事件检测和响应是一项核心设计功能，因此能够提供 SOAR 工具通常不具备的高级分析功能。XDR 工具擅长检测未知威胁和零日攻击威胁，利用强大的人工智能、机器学习算法和威胁情报来帮助组织扩大防护范围。另一方面，SOAR 工具的应用场景更为广泛，因为它们可以对整个基础设施内的任何流程进行编排和自动化，而不仅仅局限于事件响应。

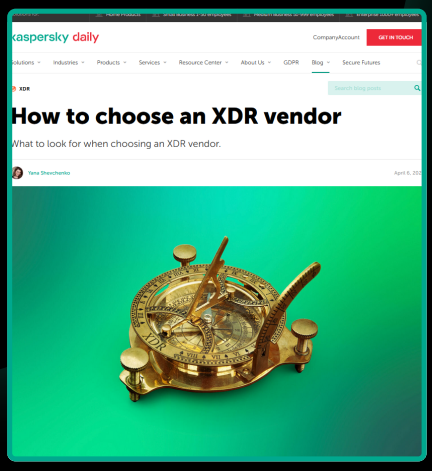
2. XDR 可以看作是 SOAR 的精简版 — 通过一种简化的界面，可对传入的威胁和警报执行一键式自动响应。对于没有资源来维护复杂且配置完善的 SOAR 平台的组织来说，使用 XDR 可能要方便得多。

3. XDR 支持跨产品无缝集成 — 无论是跨单个供应商的多个工具，还是跨第三方产品，XDR 在实现无缝互操作性方面都有很出色的表现。SOAR 工具在尝试将所有不同的、孤立的工具集成到他们的堆栈中时常常面临困难；而 XDR 将这些孤立的工具融合到一起，从而实现了高效的一站式威胁响应。

如何选择 XDR 供应商？

很多网络安全产品供应商紧跟潮流，推出了自己的 XDR 解决方案。如何选择一款适合自己的产品呢？查看我们的帮助指南：

https://www.kaspersky.com/blog/choosing-xdr-vendor/44063/



那么，XDR 会取代 SIEM 和 SOAR 吗?

这个问题还没有定论，因为 XDR 是相对较新的技术，还在不断发展。从当下来看，大多数专家推荐使用整合的方法，因为这些解决方案各具优势，与其他解决方案相辅相成：

- SIEM — SIEM 的应用场景不只是威胁检测，还包括日志管理、合规性和分析非威胁相关数据等。
- SOAR — SOAR 攻略手册的高度可定制性有助于对整个组织基础设施的流程进行编排和自动化。
- XDR — 在威胁检测和响应方面，XDR 解决方案凭借高级分析功能，提供首屈一指的增强防护。

正在为您的安全专家寻找一款久经考验、适合广泛场景的解决方案?

卡巴斯基专家安全是一款基于云原生 EDR 解决方案的 XDR，为您的组织提供增强的可见性和功能，用于跨所有端点和网络的基于 AI 的检测和自动响应逻辑，促进各种事件的自动化响应。该平台内置先进的检测和分析技术，与世界领先的威胁情报形成有效互补。卡巴斯基的 XDR 解决方案采用统一架构，通过单一 Web 控制台进行集中管理。详情请访问 go.kaspersky.com/expert。

www.kaspersky.com.cn