SIEM解析

SIEM(安全信息和事件管理)是一个由不同的监视和分析组件组成的安全和审计系统。最近网络攻击的增加，加上组织要求更严格的安全法规，使SIEM成为越来越多的组织正在采用的标准安全方法。

但是SIEM实际上涉及到什么呢?它由哪些不同的部分组成?SIEM实际上如何帮助减轻攻击?本文试图提供一种SIEM 101。后续文章将深入探讨一些可用于实际实现SIEM的解决方案。

1、为什么我们需要SIEM?

毫无疑问，对计算机系统的攻击不断增加。Coinmining, DDoS, ransomware，恶意软件，僵尸网络，网络钓鱼——这只是今天那些正义之战所面临的威胁的一部分。

有趣的是，正如赛门铁克(Symantec)在其2018年互联网安全威胁报告中所指出的那样，不仅攻击数量在上升，使用的途径和方法也在上升:

"从WannaCry和Petya/NotPetya的突然传播，到造币商的迅速增长，2017年再次提醒我们，数字安全威胁可能来自新的和意想不到的来源。"随着时间的推移，不仅威胁的数量在不断增加，而且威胁的范围也变得更加多样化，攻击者会更加努力地寻找新的攻击途径，并在此过程中隐藏自己的踪迹。

系统和网络监控在帮助组织保护自己免受这些攻击方面一直发挥着关键作用，多年来已经发展了一些相关的方法和技术。然而，网络犯罪性质的变化意味着一些攻击往往会被忽视，这一点很快就变得显而易见。数据融合，即来自多个数据源的数据的聚合和不同事件之间的相关性，以及长时间保留这些数据的能力变得至关重要。

网络攻击的增长导致合规要求更加严格。健康保险流通与责任法案(HIPAA),支付卡行业数据安全标准(PCI DSS),萨班斯-奥克斯利法案(SOX),和一般的数据保护监管(GDPR)——所有的这些都需要组织来实现一组全面的安全控制,包括监测、审计和报告,所有这些都促进了SIEM系统。

2、定义与演变

简单地说，SIEM是一个由多个监视和分析组件组成的安全系统，旨在帮助组织检测和减轻威胁。

如上所述，SIEM将许多其他安全规程和工具结合在一个综合的框架下:

日志管理(LMS)——用于传统日志收集和存储的工具。

安全信息管理(SIM)——集中于从多个数据源收集和管理与安全相关的数据的工具或系统。例如，这些数据源可以是防火墙、DNS服务器、路由器和防病毒应用程序。

安全事件管理(SEM)——基于主动监视和分析的系统，包括数据可视化、事件相关性和警报。

SIEM是今天的术语管理系统,所有上述合并到一个层,知道如何从分布式自动收集和处理信息的来源,将它存储在一个集中位置,不同事件之间的关联,并根据这些信息生成警报和报告。

3、SIEM组件

SIEM不是一个单独的工具或应用程序(尽管有一些工具可以帮助部署SIEM系统，见下文)，而是一组不同的构建块，它们都是系统的一部分。没有标准的SIEM协议或已建立的方法，但是大多数SIEM系统将包含本节中描述的大部分(如果不是全部的话)元素。

3.1聚合

日志表示在数字环境中运行的进程的原始输出，是提供实时发生的事情的准确图像的最佳来源，因此是SIEM系统的主要数据源。

无论是防火墙日志、服务器日志、数据库日志，还是在您的环境中生成的任何其他类型的日志，SIEM系统都能够收集这些数据并将其存储在一个中心位置以进行扩展的保留。此收集过程通常由代理或应用程序执行，部署在监视的系统上，并配置为将数据转发到SIEM系统的中央数据存储。

3.2处理和标准化

在SIEM上下文中收集数据的最大挑战是克服各种日志格式。从本质上说，SIEM系统将从大量层(服务器、防火墙、网络路由器、数据库)中提取数据，每种记录的格式都不同。

看看下面的例子:

这两个日志消息报告的是同一个事件——特定用户(您的真实用户)和客户机IP的身份验证失败。注意时间戳字段的格式、用户的日志记录方式和实际消息的不同。

为了能够跨不同源和事件相关性高效地解释数据，SIEM系统能够规范化日志。这个规范化过程包括将日志处理为可读的结构化格式，从日志中提取重要数据，并映射日志中包含的不同字段。

3.3关联

一旦收集、解析和存储，SIEM系统中的下一步将负责连接这些点并关联来自不同数据源的事件。这种关联工作基于各种SIEM工具提供的规则、为不同的攻击场景预定义的规则，或者由分析人员创建和调整的规则。

简单地说，关联规则定义了一个特定的事件序列，该序列可能表示安全性受到了破坏。例如，可以创建一个规则来确定在一段时间内从特定IP范围和端口发送的请求数量何时超过x。

环境中记录的数据量非常大。即使是中小型组织也很可能每天发送数十gb的数据。实际上，规则通过消除干扰并指向可能有意义的事件，帮助将数据压缩为更易于管理的数据集。

大多数SIEM系统还提供生成报告的内置机制。这些报告可以用于管理、审计或合规性原因。例如，可以将详细描述触发警报或规则的每日报告嵌入到仪表板中。

3.4呈现

可视化数据和事件的能力是SIEM系统中的另一个关键组件，因为它允许分析人员方便地查看数据。包含多个可视化或视图的仪表板有助于识别趋势、异常情况，并监控环境的总体健康或安全状态。一些SIEM工具将附带预先制作的仪表板，而另一些工具将允许用户创建和调整自己的仪表板。

3.5缓解和修复

一旦相关规则就位，并监视构建的仪表板以提供系统的全面概述，SIEM系统的最后一个关键组件就是一旦识别事件如何处理。

大多数SIEM系统支持自动包含和减轻安全事件的机制。例如，根据相关规则，可以将SIEM系统配置为自动启动内部升级流程——执行脚本，这些脚本通过触发警报、打开票证等来启动包含进程并将球传递到组织中的正确资源。

4、那么，SIEM如何提供帮助呢?

我们已经定义了什么是SIEM，并且对组成SIEM系统的主要组件有了大致的了解。但是SIEM系统实际上是如何帮助安全分析人员识别和阻止攻击的呢?

4.1可见性

对于安全分析人员来说，SIEM系统是他们所保护的IT环境的焦点。SIEM系统集中收集来自所有相关数据源的安全数据，存储大量信息，可以使用这些信息了解实时发生的事件和流程。

获得的可见性程度直接受到作为SIEM系统一部分的日志聚合和收集过程的影响。如上所述，如果没有适当的处理和解析，日志数据将缺乏结构，因此将更加难于分析。

SIEM系统的另一个主要优点是能够将事件关联起来并在仪表盘中可视化数据，这为分析人员提供了一种获得实时可见性的方法。

4.2事件检测和缓解

许多事件不会被第一行安全设备注意到，因为它们没有更广泛的上下文。SIEM相关规则以及围绕它们构建的报告机制可以帮助组织在发生这些事件时得到通知。

在DDoS攻击的例子中，防火墙很可能报告异常的网络流量，而web服务器请求则报告来自特定ip组的请求的404响应。

在这种情况下，缓解可能只是指示防火墙阻止来自这些ip的通信，可以将SIEM规则配置为在这两个事件之间进行关联，并向相关资源发出警报，以便在早期阻止攻击。

4.3合规

当今大多数合规性类型，如HIPAA、PCI DSS、SOX和GDPR，都要求组织遵守一系列的安全控制。这些控制包括:日志收集、监视、审计和警报。

不用说，从上面的描述中已经很清楚，SIEM系统为所有这些文章提供了支持，这也是SIEM成为实现安全性和合规性的行业标准的原因之一。

5、下一个什么?

这篇文章更多的是理论，而不是实践。组织正在实现SIEM，以保护其环境，并遵从越来越多的合规类型。一旦组织将SIEM的需求内在化，下一个自然阶段就是规划技术实现。