napatech

案例研究：利用 Splunk 实现完整且无缝的网络可见性

Splunk 简介

Splunk 是用于处理机器数据的领先软件平台，可让客户实现实时的智能运作。他们的使命，是对机器生成的海量数据进行机会和挑战的管理。

挑战：

处理数以亿计的日志

作为市场上最全面的事件管理工具之一，Splunk 被各行各业广泛采用，用于收集整个企业架构中事关安全性、网络和服务器资产的数据。为了提供网络安全和性能所需的必要信息，必须对任何 Splunk 记录的不寻常活动进行分析并优先处理。

此任务通常由安全和网络运营中心（SOC 和 NOC）管理，将数十亿条日志通知压缩提炼为最高优先级的可操作事件。然而，虽然 Splunk 可收集海量的事件数据，它并不提供网络上已发送和接收内容的完整记录。正因如此，SOC 和 NOC 需要一种方式来印证并解决任何看上去可疑的事件。

“在响应不准确和错误的信息方面，浪费的平均时间成本每年可高达 127 万美元。”

Ponemon Institute 调查

解决方案：

Splunk / Pandion 集成

这时，Napatech Pandion 将大显身手。Pandion 提供完整而持续的数据包捕获，这些数据包进而可与 Splunk 事件或任何其他观测到的异常事件进行匹配。任何信息都将存储在磁盘，操作人员随后可使用这些数据展开进一步的调查，我们将在下面作进一步讲解。

案例 1

在我们的第一个案例研究中，一位就职于金融服务机构的 SOC 安全工程师正在调查一则由 Suricata 发送的 Splunk 事件，其存在可疑的域名。

挑战

虽然 Splunk 收集海量的事件数据，它并不提供网络上已发送和接收内容的完整记录。因此，安全和网络运营中心需要一种能够用于调查可疑事件的工具。

解决方案

凭借 Splunk / Pandion 的集成程序，可将一切信息记录并存储在磁盘中，从而可以直接访问数据以作进一步研究。

优势

凭借其行业领先的搜索速度，Pandion 可在数秒钟内提供有用的信息，让 Splunk 用户确定事件的完整情况并提供补救措施。Pandion 可与任何现有的 Splunk 解决方案无缝集成，让企业可以尽早收回投资。

DN-1038 Rev. 1

napatech
pandion

Splunk

来自防火墙的相应事件表明，所涉及的地址曾有一次连接尝试。为进一步调查此操作，SOC 工程师在 Splunk 中单击此事件并使用 Pandion 工作流程，在几秒钟之内他们便看到了与名称解析和后续连接对应的完整数据包记录。

如果没有此信息，只能通过假设来决定是上报还是忽略该事件。但是通过分析数据包的数据，无论是否下载了有害的文档，SOC 工程师都能够准确地确定发送至或从可疑地址接收到的内容，也能够判断是否实际从设施中发送了任何信息。由此，Splunk 事件的严重性和造成的影响便可明确界定，无需再根据不完整的信息凭空猜测。

案例 2

在我们的第二个案例研究中，一位在社交媒体机构工作的 NOC 分析师在 Splunk 中看到了一则应用警报，提示响应慢/无响应，因此他需要确定应采取措施的具体环节；而要弄清楚这一点可能非常耗时而复杂。但凭借 Pandion / Splunk 集成解决方案，NOC 分析师只需单击事件，搜索数据包，即可快速确定架构中的哪一部分可能存在问题：是网络、服务器还是数据库。通常，架构中各领域的利益相关者只能够了解到各自域内的信息，并倾向于认为“未发现任何问题”，这一点很难避免。但有了这一解决方案，原始数据包内的数据将结论性地显示出组织中的哪个部分需要对事件采取措施，并提供根因分析信息。

案例 3

在我们的第三个案例研究中，一名就职于一家大型国防承包商的事件响应者注意到，网络安全设备向 Splunk 发送了一则警报，表明有可疑的 SSL 流量产生。在这种情况下，服务器可能更易遭受“心脏出血 Heartbleed”漏洞的攻击，而这一漏洞将泄露来自近期网页交易记忆库中的各类信息，包括明文用户名和密码。事件响应者在 Splunk 中单击事件，对数据包进行分析后，他可直接确定：

1. 漏洞是否已被成功利用
2. 通过此安全隐患所获取的确切信息

“一家企业通常在一周内平均可接收到将近 17000 次恶意程序警报。花费在响应这些警报上的时间对于企业的财务资源和 IT 安全人员来说都是极大的消耗。”

Ponemon Institute 调查

优势

正如我们所见，Pandion 提供了简单易用的工作流程。通过在 Splunk 中单击任何事件，操作用户可立即获取 Splunk 事件相应的完整网络数据包踪迹。凭借其行业领先的搜索速度，Pandion 只需短短数秒即可提供答案，让 Splunk 用户了解事件的完整情况并立即提供所需的补救措施。

Pandion 可与任何现有的 Splunk 解决方案无缝集成，让企业可以尽早回收投资，节约大量成本。

如需更多案例研究，请访问：
www.napatech.com/resources/case-studies

欧洲、中东、非洲
Napatech A/S
丹麦，哥本哈根

Tel. +45 4596 1500
info@napatech.com
www.napatech.com

北美
Napatech Inc.
马萨诸塞州，波士顿
加利福尼亚州，洛斯阿图斯
华盛顿，哥伦比亚特区

Tel. +1 888 318 8288
info@napatech.com
www.napatech.com

亚太地区
Napatech 大中国区、南亚
台湾，台北市
Tel. +886 2 28164533 Ext. 319

Napatech 日本株式会社
日本，东京
Tel. +81 3 5326 3374

Napatech 韩国分公司
韩国，首尔
Tel. +82 2 6001 3545

ntapacsales@napatech.com
www.napatech.com