napatech

案例研究：助力高级威胁检测平台缩短响应时间

ROHDE&SCHWARZ
Cybersecurity

行业痛点

在软件定义一切的世界中，上万亿的终端和海量数据在网络中涌出，在这种情况下，企业对于资产和资源的保护需求比以往任何时候都要迫切。根据 Cybersecurity Ventures 统计，在过去短短两年间，企业遭受的攻击提升了 15 倍，预计导致的损失仅在 2017 年就超过 50 亿美元，而在 2015 年还只有 3.25 亿美元。

威胁情报平台和安全信息事件管理 (SIEM) 系统为安全运维 (SecOps) 团队提供了处理攻击所需的重要支持。但是，尽管这些工具收集了大量的攻击数据，它们仍无法提供网络上所收发数据包的完整历史记录。因为这需要更深入的探查，才能证实所有疑似攻击事件，对他们进行排序，并依次加以解决。

挑战

Splunk 是目前市面上最多样化的 SIEM，广泛用于从整个企业基础设施的安全、网络和服务器资产中收集数据。但是，为了深入剖析网络安全及其性能，任何在 Splunk 中登记过的异常活动都必须按优先次序排序，并加以分析。此任务涉及到对数十亿条记录进行压缩和排序，这让 SecOps 团队不堪重负，从而大大延长了事件处理时间。

“93% 的安全人员都忙于处理警报数据，跟本无暇对所有的潜在威胁进行分类。”

Intel 安全

解决方案

为了应对这一挑战，Rohde & Schwarz Cybersecurity 与 Napatech 联合创建了一个高级网络威胁检测平台，该平台利用 Splunk 和其他 SIEM系统。该平台通过捕获和记录每个数据包，提供 100% 的数据可见性及数据粒度，为 SecOps 团队提供了快速确定可疑事件和深入调查这些事件的工具。

挑战

任何经 Splunk 或类似威胁情报平台登记过的异常活动都必须按优先次序排序并分析。这涉及到对数十亿条记录的处理，导致 SecOps 团队不堪重负，而且大大延长了事件响应时间。

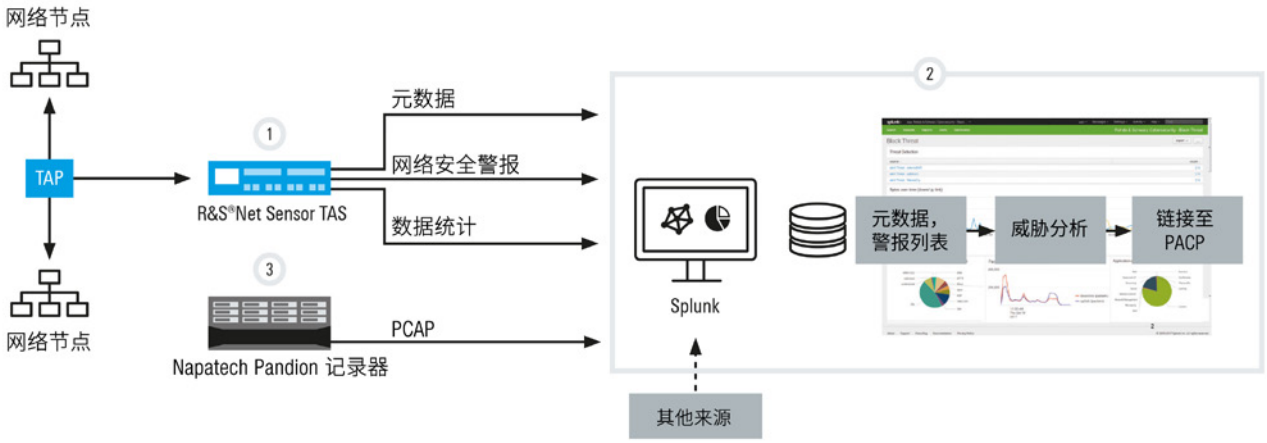
解决方案

Rohde & Schwarz Cybersecurity 与 Napatech 联合创建了一个高级网络威胁检测平台，其利用 Splunk，使得 SecOps 团队得以快速以粒度级别按优先次序对选定事件进行排序并进行调查。

优势

- 完整流量可见性
- 即时访问详细的数据包历史记录
- 缩短响应时间
- 与现有 Splunk 或类似威胁情报平台无缝融合

Rohde & Schwarz Cybersecurity 和 Napatech 解决方案实现了最深入的威胁检测



该解决方案需要采取三管齐下的方式：

1. **R&S Net Sensor TAS（威胁分析系统）**对流量执行深入的数据包检查 (DPI)，提取元数据和流量统计数据，并将这些数据与已知的入侵检测系统 (IDS) 规则匹配起来。随后，TAS 将这些发现结果发送给分析平台，比如 Splunk。

2. **Splunk** 显示从 TAS 获取的数据，根据流量元数据，在需要之时执行其他威胁分析。

3. **Napatech Pandion Recorder** 以高达 40Gbps 的速度实时捕获和记录每个数据包。大型 PCAP 存储库可以长时间存取信息供 Splunk 随时提取所需数据以进行进一步调查。

案例

考虑这一特定场景：安全工程师正在调查 Splunk 事件，该事件是通过 TAS 发送的一个可疑域名。来自防火墙的对应事件显示，一链接曾试图攻击解析地址。

为了进一步调查这一事件，工程师在 Splunk 中单击该事件，然后使用 Pandion 工作流程，在短短几秒钟时间内，便可以看到与该域名解析和后续连接对应的完整数据包记录。

如果没有这些数据包记录，我们就只能通过推测来决定是报告还是忽略该事件了。通过分析数据包数据，工程师就可以清楚地确定从可疑地址接收和发送的信息内容、是否下载了有害文件、是否有信息被泄露到基础设施之外。

优势

基于这些信息，安全工程师可以快速根据严重程度和影响解决 Splunk 事件，确定事件的整个范围，快速提供所需的补救措施。

通过结合传统的 IDS、完整的 DPI 和深入的鉴定功能，该平台可让企业检测已知威胁并记录检测，以及检测在传统安全工具中难以发现的新异常情况。这不仅增加了可见性，也极大提高了事件响应速度。

主要增值表现包括：

- 完整流量可见性
- 即时访问详细的数据包历史记录
- 缩短响应时间
- 与现有SIEM 无缝融合

DN-1137 Rev. 1-ZH

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
ntjapansales@napatech.com