案例研究：IBM® QRadar® 助力网络取证

行业痛点

恶意攻击的平均识别时间是 229 天。对应阻断攻击的平均时间是 82 天*。这些统计数据明确说明了快速、确凿的威胁检测的重要性，并且检测活动要求始终保证总流量的可视化。但是，由于大多数安全解决方案的设计都旨在实时地发现攻击，但是无法保留这些攻击产生的证据，尤其是那些发生在数月乃至数年前的攻击。许多企业痛苦地意识到这一后果可能是毁灭性的。

为了解决这一问题，IBM® 推出了 QRadar® SIEM，这是一款先进的安全信息和事件管理平台，能够帮助企业检测异常并发现高级威胁。

客户挑战

在开发 QRadar® SIEM 时，IBM® 需要确保该平台能够完整捕获并存储所有网络数据，一旦发生攻击，即可为最终用户提供完整、真实的证据。

为实现这一目标，IBM® 正在寻找行业合作伙伴，从而确保：1) 绝对实时地捕获所有数据，2) 发生漏洞攻击事件时，可及时检索选择的数据以进行事件取证。

IBM®的合作伙伴需要拥有良好的背景知识和对行业深刻的洞察力，并具备一流的技术。Napatech 是必然选择，它是唯一能够满足所有要求的候选者。

“使用 Napatech 产品让我们从此高枕无忧。他们优秀的工程团队和技术完整性，让我们有绝对的信心相信他们有能力制造出世界水平的产品。”

Russell Couturier 博士，检定分析 CTO
IBM 安全部门

挑战

IBM® 需要确保其 QRadar® SIEM 平台 100% 地捕获和检索网络数据，从而在发生网络漏洞攻击时为最终用户提供完整、真实的证据。

解决方案

作为既定战略合作伙伴，Napatech 提供了我们需要的先进技术。这确保了：
1) 完全实时地捕获所有数据，
2) 发生漏洞攻击事件时，可及时检索选择的数据以进行事件取证。

优势

- 确保所有证据的可用性
- 超快的数据提取
- 超长的保留时间
- 全方位和智能的流量洞察

* 波耐蒙研究所

我们的解决方案

IBM® 已部署了 Napatech 技术来加速其分析系统，从而确保 100% 地实时捕获网络数据。为了确保在需要时可提供完整的网络历史记录，集成了来自 Napatech 的 Capture-to-Disk 技术。这确保了以纳秒级的精度记录所有数据包，同时还允许快速方便地进行数据提取。这使 QRadar® SIEM 能够及时重建指定事件的全貌，而不仅限于大致轮廓。

优势

凭借此解决方案，IBM® 可提供数据完整性等级极高的领先安全平台，为最终用户提供安心保障，在需要时可随时提供所有数据。主要优势包括：

- 数据包零丢失 – 确保所有证据的可用性
- 超快速提取关键信息
- 全方位和智能的流量洞察

附加优势

为了优化系统性能并确保跨平台无缝集成，开发了一些定制的增强功能，包括：

- **双倍性能提升**
  通过物理方式将流量进行划分，并将数据流直接传输至恰当的 CPU 内核，从而实现性能的双倍提升。这将有助于进行取证调查所需的大量数据分析。

- **唯一的会话 ID**
  通过设计唯一会话 ID 机制将来自多个 SIEM 组件的所有信息整合在一起，从而在网络数据包和重建信息之间提供智能链接。通过将来自指定通信会话的每个数据包与唯一的 ID 相关联，可以立即检索特定数据包。

- **延长保留时间**
  通过在一个网络中组合多个捕获到磁盘设备，我们成功延长了保留时间，并且不会影响搜索性能。这延长了取证调查的时间窗口，同时也为最终用户提供了完全可扩展的存储解决方案。

Napatech Pandion

在数据过载时，相关性意味着一切。Pandion 网络记录器可使您实时获取所有流量，并可根据需要只检索相关数据。

Napatech Pandion 基于 Napatech SmartNIC，可用于一系列以太网接口选件，带有可配置存储和 Napatech Pandion 软件。

Pandion 以十多年经业界认可的 Napatech FPGA 技术为基础，针对主要安全分析和合规应用实现了 100% 捕获到磁盘。

了解更多信息，请访问：
www.napatech.com/products/napatech-pandion/

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

DN-1111 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