案例

Gigamon 深度可视化解决方案为实现博物馆数据完整性和安全性奠定标准化基础

Gigamon是上天赐给我们的礼物，它为我们所有的安全解决方案提供了基础。

MICHAEL TROFI
Trofi Security

挑战

- 无法实现对混合云环境的深度可视化
- 不断遭受来自恶意和受到国家支持的网络犯罪团伙的攻击
- 高流量噪音、事件日志存在错报情况以及流量重复

解决方案

- GigaVUE Cloud Suite for AWS (匹配AWS的GigaVUE云组件)
- GigaVUE HC系列
- GigaVUE-FM

产品优势

- 提升了对东/西向流量的可视化
- 减少了流入网络检测和响应系统(NDR)的流量规模
- 简化和净化了数据
- 可与已部署工具实现轻松集成，使用同一数据集，可提高完整性和预见性

关于客户

在保护1.7PB全世界种族大屠杀这些单一来源敏感性历史资料方面，美国大屠杀纪念馆 (United States Holocaust Memorial Museum)发挥着至关重要的作用。它是一座纪念大屠杀的活的纪念碑，激励着全球人民和领导人战胜仇恨，杜绝种族灭绝事件的再次发生，维护并增强人类尊严。纪念馆位于华盛顿特区的华盛顿国家广场之上，场地由联邦政府永久提供，其具有深远影响的教育项目和全球影响力则完全依赖于捐献者的慷慨帮助。

近十年来，Michael Trofi一直担任该馆CISO一职，负责保护这些珍贵资料的安全。Michael Trofi的公司Trofi Security，总部位于科罗拉多州 (Colorado) 拉斐特市 (Lafayette)，主要提供虚拟CISO和SOC服务。Trofi拥有40多年的信息技术和网络安全从业经验，先后涉猎多个行业。面对人才挑战，Trofi较早采用了人工智能 (AI) 和机器学习 (ML)技术，针对攻击采用了更加积极主动的防御方式，实现了日常网络安全防护的自动化执行，最大效率地发挥了团队力量。

业务挑战

除了保护敏感历史数据，纪念馆也负责向政府部门报告全球范围内正在发生的屠杀事件。也正是因为这个原因，纪念馆在世界范围内成为多个攻击来源的攻击目标。另外，纪念馆也肩负着最大化利用好这些数据的任务，正在不断加速向公有云迁移的进程，这也带来一系列安全挑战。通过云和复制节点处的数据，纪念馆提升了其在全球范围内接入教育服务的效率。根据Trofi的预测，纪念馆数据将在五年内全部迁移至混合云，本地数据中心规模将降至最低。

过去，Trofi和他的团队使用防火墙和点对点VPN来保护客户数据，但Trofi总感觉缺点什么。在进入混合办公模式之后，VPN已经不是实现远程连接的最佳方案，SASE解决方案正日益成为扩展安全周边的必需。更重要的是，在Trofi看来，指标、事件、系统日志以及追踪“并非答案”，因为每个应用都有自己的数据集，互相并不兼容。梳理所有噪音和重复流量需要投入大量时间，同时会伴随出现较多的错报现象。数据完整性的缺失使得团队无法向AWS安全产品提供流量。

那到底缺失了什么东西呢?这个东西就是深度可视化。Trofi希望能够更好实现对南/北向和东/西向流量的可视化，以便解决诸多问题，包括：数据发送至何处?接收方是谁?这些数据是合法的吗?而另外一个问题，正如Trofi指出，就是AWS安全所固有的一些限制，即AWS安全只专注事件而非流量。

Trofi表示，“将可视化扩展至流量水平，可为客户带来巨大优势。数据包、数据包、数据包，数据包不会撒谎。日志尽管重要，但它无法告诉你整个故事的来龙去脉，我们需要深入到数据包水平”。这也是我们引入Gigamon解决方案的原因，即Gigamon可以帮助我们快速定位流量中的异常之处，锁定背后的威胁活动。

解决方案

部署GigaVUE® Cloud Suite™ for AWS (匹配AWS的GigaVUE云组件) 后，Trofi及其团队获得了深入纪念馆AWS环境的更大可视化。Gigamon的数据包去重和流量映射功能显著降低了流量规模、提升了馈入NDR系统的流量质量。

数据集经过优化和梳理，可帮助团队有效整合安全工具。Trofi表示，“以前确实存在很多噪音，经过流量梳理后我们便能发现问题所在，所以，过滤噪音意义重大。”

也正因为Gigamon在流量分路、汇聚、去重等方面的卓越能力，美国大屠杀纪念馆才可以将其作为基础来服务其安全解决方案，这些方案来自Fortinet, Check Point, Armis以及 Forescout Technologies。在Trofi看来，数据完整性是Gigamon的最大优势，他表示，“Gigamon向客户提供唯一数据来源并将其发送至所有系统。”

Gigamon提升了数据完整性，赋予团队自动执行日常工作的能力，而这在以前是根本无法实现的。Trofi表示，“Gigamon深度可视化解决方案可以让我们充分享受AI和机器学习技术所具有的优势。”

Trofi还指出，在AI工具的帮助之下，大量日常工作实现了自动执行，专业人员可以将全部精力“聚焦于难题”之上。“比如，对于团队来说，当前最大的难题是消除全部未加密流量，如果采用日志这种老式方法，可能需要数年时间才能完成。Gigamon是上天赐给我们的礼物，它为我们的全部安全解决方案提供了基础”，Trofi表示。

方案优势

除了提升纪念馆的安全态势，Gigamon也可以提升网络性能。Gigamon让流量变得容易被观察到，助力网络运维团队消除恶意流量。

Trofi表示，“Gigamon给我们带来了一个全新的世界。我们可以借助可视化从流量角度来重新架构网络，而这在20年前是很难做到的。可视化让所有工作都变得轻松。借助可视化，我们可以分析应用接入情况，优化防火墙穿越路径，所以，可视化不仅可以帮助我们解决安全问题，也可以解决性能问题，这为我们继续开展工作提供了便利。”

团队在了解了什么才是有效路径之后，无需再对任何事物抱有敌意，可向用户提供更加卓越的体验。Trofi指出，Gigamon的这种经过提升的可视化解决方案 ，可为更多IT部门带来更多优势，助其实现工作协同，而这也是整个行业向前迈出的一大步。

关于 Gigamon

Gigamon致力于向业界提供深度可视化解决方案，助力客户获得可操作的网络情报智能，实现可视化工具效能的最大化。Gigamon功能强大的产品组合可赋能IT组织，助其实现安全合规运营，快速分析性能瓶颈并锁定根因。同时，实现对混合及多云IT基础设施的有效管理，降低运营费用，最终助力现代企业实现全面云端转型。Gigamon服务全球4200多家客户，其中包括超过80%的“财富百强企业”，10大移动网络提供商中的9家，以及全球数百个政府机构和教育组织。如欲了解更多Gigamon内容，敬请浏览公司官网 www.gigamon.com 。