欧盟金融公司案例研究

该客户是一家欧洲金融公司，为欧洲和亚洲10多个国家近1000万个人客户提供多种金融产品。 该公司管理着一个复杂多样的网络基础设施，为超过1000个物理位置的50,000多名员工提供服务。

复杂网络中的高级安全监控

在GREYCORTEX MENDEL实施之前，该公司面临的主要挑战：

- 网络边界内的网络威胁检测不足
- 内部安全策略的监控不足以及可疑网络行为的检测不足
- 缺乏取证鉴定工具

网络在设备类型和网段数量方面高度多样化。它还在快速扩张，用户数量波动很大，有数百台新设备由公司子公司拥有和管理，更重要的是拥有非常多元化的业务合作伙伴组合（从个体户到企业)。

该公司曾实施过相对强大的IT安全架构，事实证明无法为以上挑战提供最佳的解决方案。

- 边界防火墙和基于签名的入侵检测无法检测到由已感染设备接入内部网络而带来的威胁。而且，基于签名的检测仅限于检测已知的威胁。
- 已经部署了简单的网络流量收集和分析设备，但它仅提供了有限的异常检测功能，这些功能对于网络管理而言或许足够，但对于IT部门来说则不足（例如检测到不正常的用户行为和违反安全策略行为。
- 这些技术与SIEM和流量处理器一起提供了一个非常强大的网络安全洞察力（例如，什么数据在流动，使用什么应用程序）。然而，该网络缺少强大的网络行为分析能力，这将使SIEM的能力缺失。
- 对于NetFlow或SIEM是否为取证分析提供了足够的上下文，以及安全事件调查（证明其不灵活和耗时）所需的上下文数据，该公司面临着不确定性的挑战。

该公司经过考虑，然后拒绝了几项技术

- 考虑了基于沙箱行为分析的网络威胁检测。鉴于该公司对网络带宽的要求以及其复杂的网络拓扑结构，该选项的价格将非常昂贵。
- 排除了基于记录所有网络数据包（TCP转储）的专用取证分析工具，因为它不符合欧盟流量拦截规则。
- 其他几种用于取证分析的专用工具也被考虑，但被证明仅能提供很低的价值。

大的行为分析和其他优势

GREYCORTEX MENDEL为公司的挑战提供了最佳答案：

- MENDEL的行为分析引擎对于先进的未知威胁以及检测可疑网络行为特别有效，同时降低运营成本。 与绝大多数其他行为分析工具相比，它不依赖手动规则集（阈值）。它能自动生成一组特定规则，并根据正常网络行为（整个网络，每个子网，主机和服务）自动生成并不断调整。
- 多种独特的专用检测算法用于检测远程访问木马（RAT）和其他高级威胁。 这种检测基于类似的行为特征（例如，与人类行为不同的机器行为）。
- MENDEL的基于签名的引擎可以检测网络内部和网络边界的威胁，为主IDS提供额外的安全层。
- 除NetFlow之外，MENDEL还分析网络通信元数据并将其存储六到九个月（存储空间够可以更久）。这提供了对取证分析至关重要的背景和内容（同时避免与非法监视相关的法律问题以及对存储容量的要求相对较低）。

部署GREYCORTEX MENDEL是为了分析总部和周边网段的所有可用流量（部署了三个探测器和一个采集器）。 此外，安全部门利用此机会为子公司和业务合作伙伴的网络管理员提供了基于角色的访问控制。这让管理员对其网段有更多的安全透视。

挑战

- 网络边界内部的网络威胁检测不足
- 内部安全策略的监控不足以及可疑网络行为的检测不足
- 缺乏取证鉴定工具
- 高度多样化和复杂的网络

无法应对当前挑战的IT安全基础设施：

- 防火墙和边界的入侵检测系统
- 简单的NetFlow收集和分析
- SIEM和流量处理器

有几项技术被证明价格过高或几乎没有附加值：

- 沙箱行为分析
- 专用的取证工具

部署

- 行为分析引擎，基于正常网络行为自动生成和修改规则
- 用于检测RAT的独特算法
- 基于签名的检测引擎在网络内部和外围提供了额外的安全层
- 存储NetFlow和网络流量元数据用于取证分析

更好的检测和更快的事件响应

GREYCORTEX MENDEL在多个方面提供了高附加值。

- MENDEL的风险评估能力帮助该部门更专注并大大改善其运作，既节省时间，又执行一系列重要任务，并产生更好更快的事件响应。
- 凭借其强大而轻松的浏览和过滤功能，安全事件的分析占时很少。
- GREYCORTEX MENDEL很快证明了它的有效性和能力。 它报告了几个严重的安全事件（见下表），无论是在网络边界还是网络内部，这些事件都很容易被调查，并得到了公司IT团队的快速响应。

除了客户的主要需求之外，让下级管理员访问MENDEL界面还有助于大大改善公司内部和子公司及其合作伙伴的网络管理员和安全部门之间的通信。 这些网络管理员可以被纳入事件的调查和回应，从而大大提高工作效率。

结果

MENDEL的附加值：

- IT安全部门更专注和高效的工作
- 及早发现并轻松调查严重安全事件（参见下表）
- 由于与下级网络管理员进行更轻松的沟通，改善了调查和事件响应

按方法检测出的威胁总结

安全事件	基于签名的检测（IDS）	使用行为分析进行检测（NBA）
未知的恶意软件 远程访问木马	--	疑是机器行为 可预测到通讯模式
违反内部安全政策 P2P数据共享	--	行为异常 通信端点的数量比平常高，而且端口数据量比平常要高
网络侦察 针对HTTPS应用程序	--	Web攻击算法 更多因素
违反内部安全政策 （第三方应用程序将数据发送到外网）	--	行为异常 与外部主机的异常通信
已知的恶意软件Conficker的变种	已知的数据签名 （与主IDS使用的签名不同）	疑是机器行为 定期通讯
已知恶意软件Troj / VB-GXP的变种		--

GREYCORTEX

GREYCORTEX使用先进的人工智能，机器学习和数据挖掘方法帮助企业实现IT运营的安全性和可靠性。 MENDEL，GREYCORTEX的网络流量分析解决方案，通过检测对敏感数据，网络，商业机密和名誉的网络威胁，帮助企业，政府和关键基础设施部门保护他们的未来，而其他网络安全产品则忽视了这些威胁。

Purkyňova 127, 612 00 捷克布尔诺，+420 511 205 389, info@greycortex.com, www.greycortex.com