你的网络中有什么?

网络和应用程序性能漏洞使您受到威胁。
在攻击之前，恶意软件，勒索软件和特洛伊木马会隐藏在您的网络中。
您需要一款易用,且有完整网络可视性和威胁检测的工具。

GREYCORTEX

All-Seeing Network Security

GREYCORTEX MENDEL 使用先进的人工智能，机器学习和数据分析来发现威胁，识别漏洞并为您的IT团队提供全面的网络可视性，同时节省时间。

高级安全

MENDEL自动学习网络以发现异常现象，并将人类与机器行为区分开来，即使在物联网设备上也是如此。

全网络可视性

比Netflow或IPFIX更丰富的数据流。 可视化网络上的每个主机，子网，设备和应用程序。

轻松表现

功能强大且易于使用。 节省时间并提高生产率。 SaaS或内部部署都能满足团队需求。

检测

- 恶意软件，勒索软件（WannaCry等），零日和高级威胁
- 远程木马（RAT）
- 移动恶意软件
- 数据泄漏和隧道流量
- DoS, DDoS
- TOR 使用

鉴定

- 网络依赖性
- 易受攻击的应用程序
- 新的未知的 BYOD
- 网络配置错误
- 违反内部安全规则
- 网络和应用程序性能问题

部署

- 提高安全操作和网络管理员的生产力
- 节省1-2人的工资
- 部署仅需要几分钟
- 易于与SIEM，SOC或其他系统集成

传统工具能力不足

大多数组织都依赖传统预防技术，如防火墙和防病毒解决方案以及入侵防御。 但是，这些工具有不足之处，而且数据表明检测和信息反馈必须得到改进.....攻击者数月内未被发现，常常在环境中横向移动。

Gartner Research - 2016年检测和缓解APT的最佳实践

GDPR 合规性

GREYCORTEX MENDEL 可帮助您在几个关键领域满足GDPR要求：

内部数据保护管理

+ 跟踪网络中敏感数据的访问和传输
+ 检测敏感数据泄漏和未经授权的数据使用

发现受到损害之前发现攻击

+ 尽早检测高级攻击
+ 识别数据保护的风险

监测GDPR的遵守情况

+ 验证和执行安全政策
+ 不断监控安全基础设施
+ 准确报告数据保护漏洞

物联网设备兼容

MENDEL可以检测网络中对物联网设备的攻击，就像它检测“非物联网”设备中的攻击一样。

+ 物联网设备通常安全性较差
+ 即使在“安全网络”中，它们也可以轻松访问
+ 最小的设备也可能会发生攻击

早期威胁检测

GREYCORTEX MENDEL通过威胁的行为来检测未知威胁，而不是他们的名字，在很多情况下节省宝贵的时间。

+ 高级威胁导致数据窃取造成的损失超过400亿美元（2015年）
+ 攻击者经常隐藏在网络中，等待攻击
+ 快速反应对于阻止攻击造成损害至关重要

自2016年11月部署以来，GREYCORTEX为我们提供了巨大的帮助。 我们能够发现安全策略违规和性能问题，并将这些问题与以用户遇到的问题联系起来。 我们可以看到攻击的发展并采取行动。 我们确实加强了我们的安全态势，并对结果非常满意。

Kiwi.com IT运营经理JosefStaša

KIWI · COM

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，通过检测其它设备错过的敏感数据，网络，商业机密和声誉的网络威胁，帮助组织保护他们的未来。

Purkyňova 127, 612 00 Brno, Czech Republic, +420 511 205 216, info@greycortex.com, www.greycortex.com