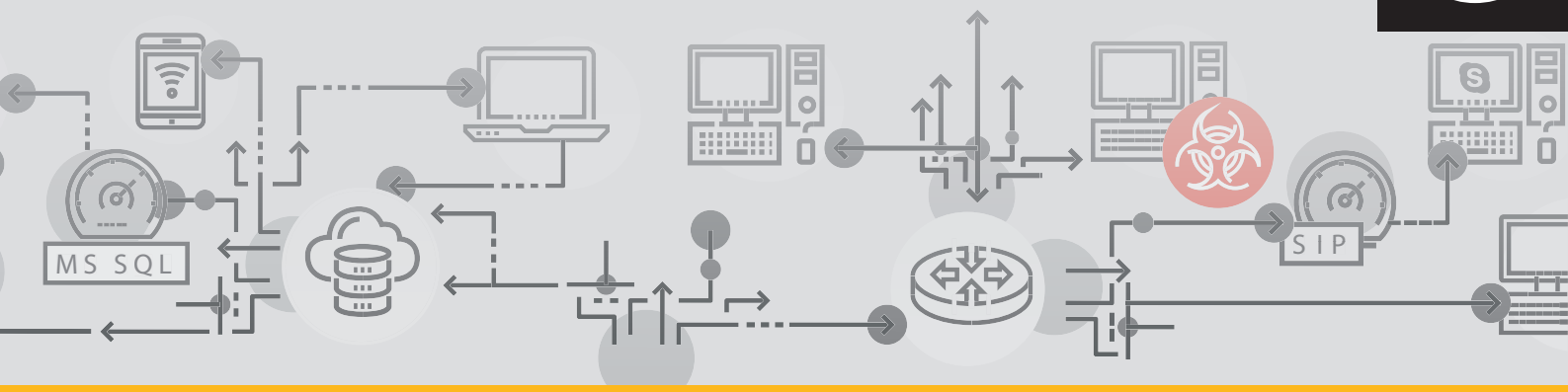


GREYCORTEX MENDEL

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。

高级攻击很常见但很难发现

每年8次
攻入企业网络

40%
的网络威胁未被发现

49天
仅使用当前工具检测所耗时

现有的安全工具是脆弱的

未知威胁

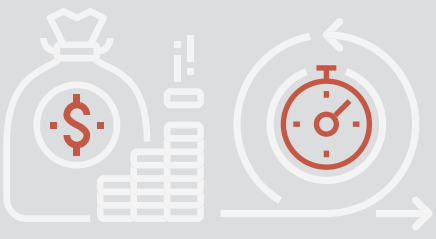
高级未知威胁，如恶意软件，特洛伊木马和勒索软件; 如果不及时发现，他们会导致：

- 敏感数据丢失
- 组织被攻击
- 商业损失
- 声誉丧失

缺乏可视性

缺乏网络可视性使得很难识别可疑设备和不良角色，以及：

- 严重延迟
- 未知装置
- 时间损失
- 浪费金钱



员工疏忽

员工和承包商有意或无意地违反了政策。 这产生：

- 敏感数据泄露
- 攻击其他组织
- 合规问题
- GDPR违规

商业风险是真实的

网络流量分析可防止违规

网络流量分析（NTA）结合了人工智能，机器学习和其他工具来检测可疑或异常的网络事件。GREYCORTEX MENDEL使用NTA来监视网络周边以及网络中的流量以实现全面覆盖。

GREYCORTEX MENDEL可检测整个网络中的威胁，包括BYOD/物联网设备，甚至还有其他解决方案漏掉的高级未知攻击。

65%
的客户失去信任

以超高速度进行强大的检测

高级未知威胁，包括在1分钟-6小时内检测到的恶意软件，木马，勒索软件，RAT和零日攻击，而不用花49天

23%
的商业机会损失

详细的网络可见性

- 每个主机
- 每个设备
- 每个子网
- 每一项服务
- 每一个应用
- 包括BYOD/物联网

5%
股价下跌

使用方便

- 在2分钟以内从警报到解决
- 完整的事件和流量过滤
- 完全可定制的仪表板
- 更容易的事件管理

来源：Ponemon Institute
Studies： 2011 - 2017

MENDEL包括

机器学习驱动检测

MENDEL先进的人工智能和机器学习功能比其他解决方案更有效地检测威胁：

- 区分人机交流
- 检测异常行为
- 发现隐藏的威胁

停止攻击

MENDEL会在检测到威胁时进一步切断攻击。

- 与您现有的防火墙集成
- 简单的界面允许常用或特定的拦截
- 时间很重要，在几秒钟内配置和阻断攻击

完全可视性，包括BYOD/IOT

MENDEL可识别进出网络的流量，以及网络内设备之间的通信：

- BYOD/IOT同样适用
- 可视化个别设备和应用程序，而不仅仅是网络层
- 快速过滤每一次通信

上下文可视性更快的解决方案

有效地检测攻击只是网络安全难题的一部分。MENDEL添加额外的上下文数据以加快事件解决。

- 整合GEOIP和黑名单
- 使用导入的私钥解密SSL/TLS流量
- 将MENDEL与Active Directory集成以识别网络中的用户

关联治疗检测准确

攻击可以采取许多似乎安全的步骤。 MENDEL将这些事件汇集在一起，以显示攻击的真实性质。

- 威胁无法隐藏在繁重的数据量中
- 从一个中心位置识别多个办事处的事件
- 在两分钟内解决问题

单独有效或作为附加数据源

不同的安全基础设施需要不同的配置。 MENDEL完善您现有的工具来填补空白。

- 类似SIEM的结果,但成本只要一半，时间只有十分之一
- 将数据导出到SIEM系统供大型安全团队使用
- 事件管理允许更高级的解决方案

MENDEL安全

中小企业和企业

政府

SCADA/ICS

基础设施

MENDEL部署

本地（虚拟或物理）

安全即服务

安全运营中心

MENDEL实施

30 分钟安装

自动学习您的网络

辅助机器学习~5分钟/天

体验MENDEL

免费的 30 天概念验证（POC）

识别网络中的严重问题 - 从攻击到性能问题。

即使在 “干净” 网络中也存在问题:

20%的网络设备对整个大网络构成威胁,包括病毒/恶意软件/特洛伊木马/RAT

零日攻击

移动恶意软件

易受攻击的物联网设备

无效的网络矩阵

未打补丁的应用程序

性能异常/问题

未经授权的数据访问

数据泄露

合规性问题（未来的GDPR问题）

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

GREYCORTEX