GREYCORTEX MENDEL

产品数据表

GREYCORTEX MENDEL是针对企业，政府和关键基础设施的高级网络流量分析，性能监控，威胁检测和深度网络可视性解决方案。MENDEL采用人工智能和机器学习来分析和监控网络流量，从而检测组织内部和外部的新型和未知攻击; 包括数据泄露，操作异常，以及其他技术无法看到的其他高级威胁。MENDEL的部署仅需要数分钟时间，并填补了传统安全工具留下的空白，减少了使网络操作安全可靠所需的时间和资源。

检测方法

MENDEL 持续监控网络流量，并采用多种高级方法来检测恶意，异常和可疑行为：

预测分析	根据提前学习的每个主机上的所有子网，主机和服务的网络行为，GREYCORTEX MENDEL可以预测预期的通信行为。不符合学习行为模式的流量被报告为异常。异常情况的例子包括：数据传输，通信伙伴数量，通信端口数量，流量数量等。
发现分析	MENDEL维护最新的活动网络服务和主机列表。如果受监控网段中出现新主机（例如BYOD）或服务，则会报告发现事件。如果服务或主机停止通信，更改MAC地址或DNS名称也会同样报告。此方法还根据预设策略报告允许或拒绝的服务之间的通信。
流量分析	检测网络中已知和不需要的行为模式，如端口扫描，强力和字典攻击，大量流量等。
重复性分析	不同于不可预测的人类行为模式,机器的行为模式是可预测的。此功能基于存储数据的长期数据处理，使MENDEL能够检测受RAT，C&C，APT等攻击的被感染主机的通信。此方法可检测恶意软件通信使用的各种协议，包括HTTP/S，DNS或ICMP。
性能分析	网络性能监控和应用性能监控模块可分析HTTP/S，MS-SQL或SIP等各种协议的数据传输效率。性能指标也是建模的，所以如果任何服务器开始出现性能问题，它发出异常警报，例如应用程序响应时间.而且不需要设置任何阈值。性能指标是自动学习的。
基于规则的分析	根据用户定义的规则报告事件，如数据传输，流量，数据包吞吐量，子网上的阈值，主机，服务，允许或拒绝的通信向量（防火墙审计）等。
基于签名的分析	通过检测常见或可预测的威胁，恶意软件以及C&C，P2P，恶意软件，特洛伊木马，聊天，Web，漏洞攻击，TOR，扫描，政策违规等多个类别中的攻击来报告事件。

流量处理和分析

网络行为分析

基于流量和数据包的网络流量分析以及机器学习，智能误报消除和多种检测方式（参见上文）。

检测能力：

- 恶意软件活动 - 传播，下载，垃圾邮件等
- 攻击者活动 - 扫描，蛮力攻击，漏洞等。
- C&C活动 - RAT，APT，AVT，机器人，蠕虫，rootkit等
- 数据泄露

深度包检测

按需和数据包捕获/流量记录；涵盖源IP和目的IP，MAC，子网，协议，端口，IP族（IPv4，IPv6）。DPI丰富了流程中的L7应用程序元数据。

基于签名的检测

基于签名的入侵检测引擎：

- 内部网络监控
- 多线程处理
- 多签名来源
- 检测已知的恶意软件，攻击和其他活动
- 规则分析和性能异常值的自定义规则

性能监控

基于流量和数据包的网络和应用性能分析（NPM，APM）：

- 应用觉察
- 监控当前和平均带宽，响应时间，往返时间，用户体验时间，服务器应用程序响应时间等。
- 自动异常检测

历史元数据

GREYCORTEX MENDEL的高级安全网络指标（ASNM）协议是一种安全和性能方面的协议，它提供比NetFlow协议更丰富的分析。

功能包括：

- 双向流量记录和重复数据删除
- 适用于HTTP/S，SSL，TLS，SMB，SMB2，SMTP，FTP，SSH，DNS，XMPP，SIP，SSH，MS-SQL，DHCP，Modbus，DNP3等协议。
- 完整的ASNM记录可能包含900多个参数
- 数据可以存储几个月到几年（取决于存储容量）

主要优点

有效和高效

- 更敏感和可靠
- 降低运营和集成成本

比NetFlow更多

- 比NetFlow（以及类似协议）更敏感的行为检测
- 通过安全参数和性能分析增强NetFlow/IPFIX记录
- 基于分组的检测，改进基于流量的检测（用于安全和性能监控）

强大的检测

- 零日和高级威胁（APT等）
- 远程访问木马（RAT）
- 数据泄漏（滥用DNS，SSH，HTTP/S，ICMP等）
- 隧道流量（DNS，SSH，HTTP/S，ICMP等）
- 协议异常
- 耗时的端口扫描
- 字典和暴力攻击
- 准备盗窃内部数据和其他内部问题，如违反内部安全规则
- 网络配置错误
- DoS, DDoS
- 自动数据收集（例如eshop）

详细的网络可见性

- 有关子网，主机，服务，端点和数据流的详细信息
- 元数据提供了关于网络行为的充分信息，用于取证调查，法规遵从等。
- 几个月的历史数据被编入索引并且可以快速访问

风险评估

- 强大的风险评估能力

报告

- 广泛的可定制报告（包括粒度报告，警报等）
- 直观的网页图形用户界面
- 事件管理
- SIEM以系统日志，CEF和IPFIX格式集成
- 防火墙整合
- 编排工具和其他整合

输出

图形用户界面

Web用户界面（IE，Firefox，Chrome，Opera，Safari，Edge等）
- 完全细化的访问
- 易于定制的仪表板
- 无限过滤和排序

报告和警报

- 条件报告（警报）
- 事件管理
- 可定制的输出格式
- 可读格式：电子邮件（html），pdf，docx，自定义链接到GUI

集成

- SIEM：基于CEF（通用事件格式）格式或IDEA报告协议
- 可定制的输出格式
- 以IPFIX格式导出
- 与业务流程工具和其他基础设施集成

输入

网络数据

- 镜像流量（TAP，SPAN或其他类型的镜像数据端口）
- IP层支持：TCP/IP的L2至L4层，包括 IPv6协议
- 基于流的协议（NetFlow系列，IPFIX）

威胁情报

- IDS签名的各种来源（Proofpoint ETPro）
- 其他数据库（IP声誉，域名声誉，GEO IP，WHOIS等）

网络觉察

- 功能网段/子网的定义（共享相同的网络行为模式，例如管理，销售，服务器，WiFi，VoIP，打印机，DMZ等）
- IP到主机名（使用DNS和DHCP记录）

用户觉察

- IP到域用户（使用域控制器事件日志，LDAP）

设备

		网络吞吐量Gbps							
		0.2	0.5	1	2	4	10	20	40
HW	一体式（传感器+收集器）	✓	✓	✓	✓	✓	✓	✓	✓
	收集器				✓	✓	✓	✓	✓
	传感器	✓	✓	✓	✓	✓	✓	✓	✓
VA	一体式（传感器+收集器）	✓	✓	✓					
	收集器			✓	✓	✓	✓	✓	✓
	传感器	✓	✓	✓					
	中央收集器	最多50个的收集器集群或一体机（最高2Tbps）							

优质服务

	远程管理	定期威胁情报报告	当日威胁报告	安全咨询	全天候专业支持
MENDEL Analyst	o	o	o	o	o
MENDEL SaaS	✓	o	o	o	o

✓ standard　o optional

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

GREYCORTEX