Kiwi.com 案例研究

Kiwi.com（前身是Skypicker）是一家发展迅速的在线旅行社。该公司成立于2012年，现已发展至1100多名员工，并且持续快速增长。它每年为数百万消费者提供服务，将不同路线的运营商的航班结合起来。Kiwi.com管理一个包含大约1,900台设备的多元化网络。GREYCORTEX MENDEL实施的目标是使Kiwi.com能够充分关注其核心业务，同时保持其不断增长的IT基础架构的安全可靠。

> “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，并将这些问题与用户遇到的问题联系起来,这是之前工具未见过的。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。“（IT运营经理Josef Stasa）

挑战

随着业务和团队发展迅速，Kiwi.com 的IT基础架构和网络发展速度更快。

Kiwi.com 部署 MENDEL 的主要原因是确保Kiwi.com的IT基础设施可靠和安全,以此维护商誉。整个公司的日常运作对于有效地完成这一点至关重要。 Kiwi.com需要能够从运营，性能和安全监控的角度监督其网络的技术基础架构和网络管理。

其他挑战包括：

- 保护客户数据
- 检测现代威胁并防范针对网络用户的攻击
- 提供以安全为重点的网络基础架构行为概述，包括对各个网段，设备和个人用户的正常行为进行自动分析
- 改进安全策略执行
- 监控Kiwi.com当前的安全基础架构配置和有效性
- 易于扩展

挑战

- 保护客户数据
- 检测未来的APT，RAT，零日攻击等
- 越来越多的IT基础设施
- 网络可视性
- 安全策略

优势

GREYCORTEX MENDEL 包含了几个可以让Kiwi.com的IT团队受益的重要功能。 最重要的是基于先进的机器学习和人工智能的行为检测引擎。 输出与每小时更新的黑名单IP和签名列表结合在一起。 由于这些工具是集成的，MENDEL不仅可以检测基于已知签名的威胁，还可以基于原子级别的攻击症状; 例如，APT 攻击处于休眠状态，但在仍与其控制台进行通信。 MENDEL 还包括应用程序性能监控功能，为团队提供关键业务事务处理的详细数据，并结合安全事件进行简单的根本原因分析; 所有这些都是实时的，不会减慢网络速度。 最后，MENDEL帮助执行了Kiwi.com现有的安全政策并保持其遵守政府法规。

优点

- 基于行为的高级未知威胁检测
- 基于签名的已知威胁检测
- 应用性能监控
- 网络可视性

结果

GREYCORTEX MENDEL 很快安装完毕，立即自动开始学习网络。Kiwi.com的原始安全架构虽然很强大，但与 GREYCORTEX MENDEL 相比有了很大的改进，现在已经为更高级的威胁做好了准备。

另外,MENDEL还帮助 Kiwi.com 实现以下目标：

- 更好地执行安全政策和更快的解决事件
- 完整的网络可视性
- 发现和分析网络和应用程序性能问题
- 取证分析

结果

- 有效的检测
- 安全策略得以实施
- 更高的知名度
- 取证分析

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