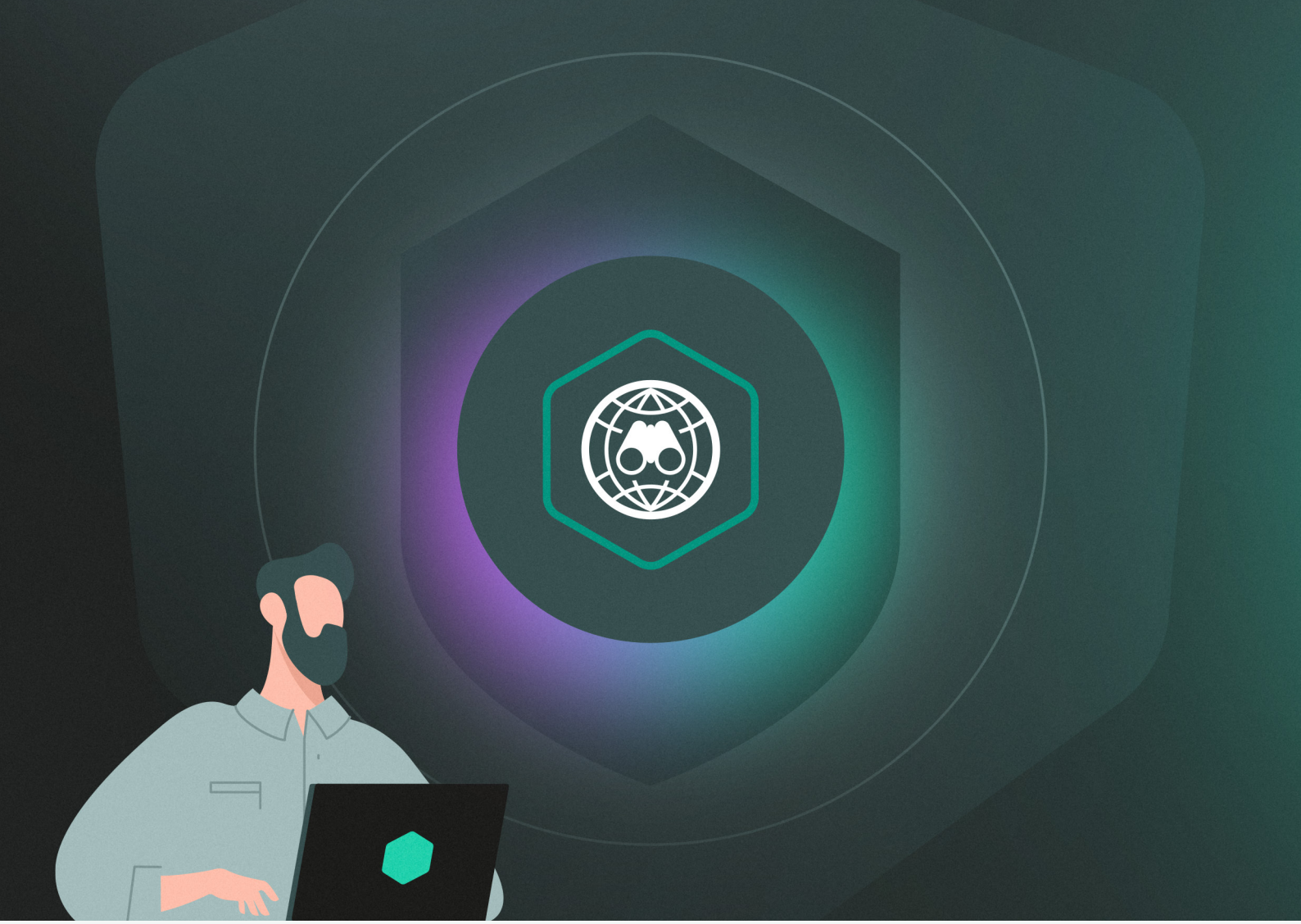

卡巴斯基威胁情报

评估威胁情报来源

kaspersky 引领未来

如需了解更多信息，请访问 kaspersky.com，并关注 #引领未来# 话题标签

简介

随着攻击面逐渐扩大和威胁日益复杂，仅对事件作出响应是不够的。越来越复杂的环境为攻击者提供了许多机会。每个行业和每个组织都有自己独特的数据需要保护，并使用自己的一组应用程序和技术，等等。所有这些因素都为可能的攻击方法引入了大量变量，每天都有新的攻击方法出现。

在过去的几年里，我们观察到不同类型的威胁和不同类型的攻击者之间的界限越来越模糊。以前只对有限的组织构成威胁的方法和工具已经扩散到更广泛的市场。这方面的一个示例是“影子经纪人”组织开展的代码倾销，它将先进的漏洞提供给犯罪集团使用，这些犯罪集团本来无法通过其他途径获得这种复杂的代码。另一个示例是高级持续性威胁 (APT) 活动的出现，这种攻击的重点不是网络间谍，而是盗窃 - 窃取金钱以资助 APT 集团所参与的其他活动。这样的威胁还在不断增多。

需要一种新方法

以前只对有限的组织构成威胁的方法和工具已经扩散到更广泛的市场。

随着企业越来越多地成为高级定向攻击的受害者，很明显，成功的防御需要新的方法。为了保护自身，企业需要采取积极主动的方法，不断调整其安全控制措施，以适应不断变化的威胁环境。要跟上这些变化，唯一的办法是建立一个有效的威胁情报计划。

威胁情报已经成为所有行业和地域的不同规模的公司建立的安全运营体系的一个关键组成部分。以人类可读和机器可读的格式提供的威胁情报可以在整个事件管理周期内为安全团队提供有意义的信息，并为战略决策提供依据 (图 1) 。

尽管如此，对外部威胁情报的需求在不断增长，大量威胁情报供应商应此而生，而每家供应商都提供多种不同的服务。面对这样一个广泛而又竞争激烈的市场，以及其中不计其数的繁杂选择，您的组织在选择正确解决方案时可能无所适从，倍感沮丧。

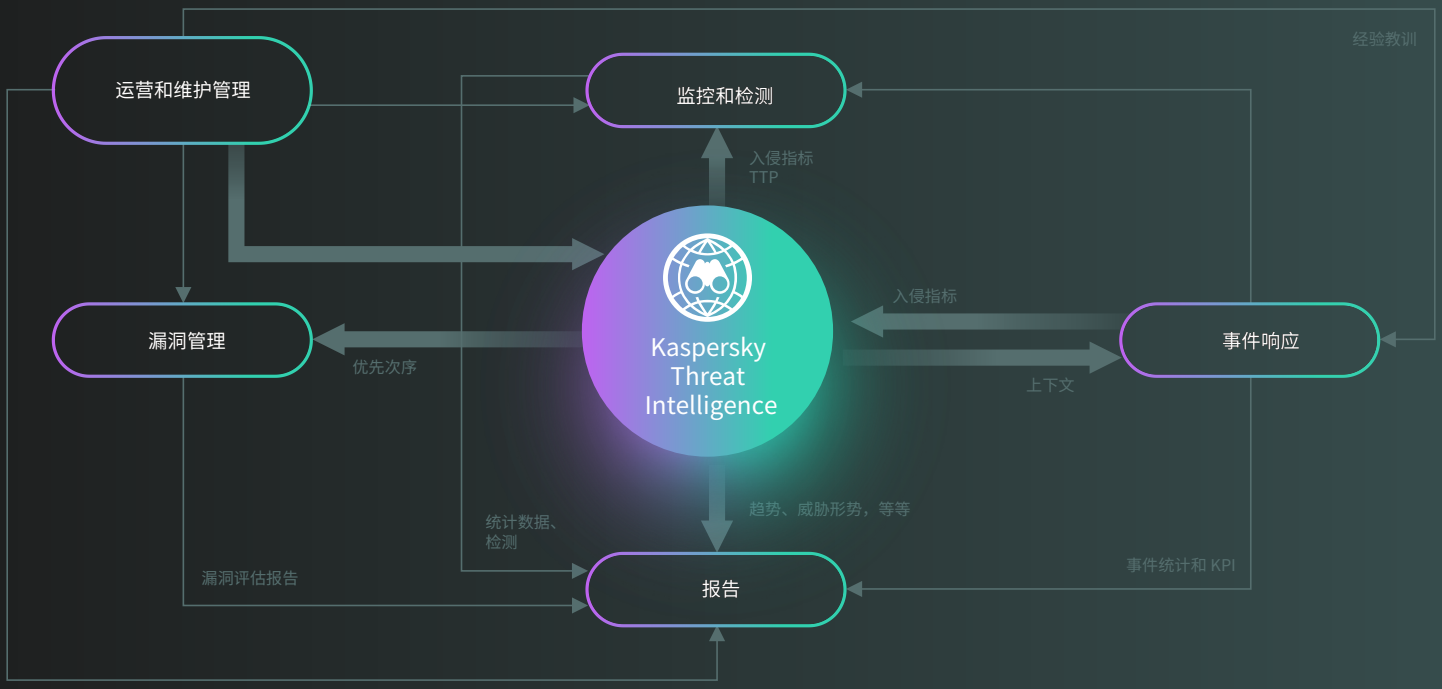

图 1

威胁情报驱动的安全运营

如果威胁情报并非针对您的企业的具体情况进行定制，结果可能只是雪上加霜。在如今的许多公司中，安全分析师有一半以上的工作时间都用来筛查误报，而不是主动搜寻威胁和做出响应，导致检测时间大大增加。向您的安全运营提供不相关或不准确的情报将使错误警报的数量增多，并对您的响应能力以及您的公司的整体安全产生严重负面影响。

最出色的情报在哪里...

那么，您如何评估众多的威胁情报来源，确定与您的组织最相关的情报来源，并有效地将其付诸实施？几乎每一家供应商都声称其情报最为优秀，在此情况下，您如何在大量无意义的营销中辨明真相？

这些问题虽然有效，但绝对不是您应该首先询问的问题。许多组织被华而不实的宣传文案和的浮夸的承诺所吸引，认为某些外部供应商能为自己提供某种无比强大的洞见，却完全忽视了一个事实：最有价值的情报存在于他们自己的企业网络边界中...

来自入侵检测和预防系统、防火墙、应用程序日志和其他安全控制系统日志的数据可以揭示公司网络内部发生的很多事情。它可以识别特定于组织的恶意活动模式。它可以区分正常用户和网络行为，并有助于保留数据访问活动的追踪痕迹。

图 2
实施外部威胁情报

像攻击者一样思考

为了建立一个有效的威胁情报计划，公司（包括那些建立了安全运营中心的公司）必须像攻击者一样思考，从而识别和保护最可能的目标。要从威胁情报项目中获得真正的价值，需要非常清楚地了解什么是关键资产，以及哪些数据集和业务流程对完成组织的目标至关重要。识别这些“皇冠上的明珠”使公司能够围绕它们建立数据收集点，以进一步将收集的数据与外部可用的威胁信息进行映射。考虑到信息安全部门拥有的资源通常是有限的，对整个组织进行分析是一项庞大的工程。解决方案是采取基于风险的方法，从而首先关注最易受影响的目标。

一旦定义并实施内部威胁情报源，公司就可以开始考虑将外部信息加入到现有的工作流程中。

这是一个关于信任的问题

外部威胁情报源的可信程度参差不齐：

公开情报源可以免费获得，但它们往往缺乏上下文，并会返回大量误报

在开始时，一个不错的方案是访问行业特定的情报共享社区，比如金融服务信息共享和分析中心(FS-ISAC)。这些社区提供了极有价值的信息，但它们通常是有门槛的，往往需要会员资格才能访问

商业威胁情报来源更为可靠，但购买这些情报的费用可能很高

选择外部威胁情报来源的指导原则应该是“质量高于数量”。一些组织可能认为，他们能集成的威胁情报源越多，可以获得的监测能力就越强。这在某些情况下可能是对的 - 例如，涉及到高度可信的来源（包括商业来源）时，提供针对组织的特定威胁概况的威胁情报。但在其他情况下，会有很大的风险：无意义的信息让您的安全运营团队不堪重负。

专业威胁情报供应商提供的信息的重叠程度可能非常小。由于他们的情报来源和收集方法各不相同，他们提供的见解在某些方面将是独一无二的。例如，一家供应商由于主要在某个特定地区开展业务，因此提供了与来自该地区的威胁有关的更多细节，而另一加供应商则提供了关于特定类型威胁的更多细节。因此，获得这两个来源的访问权限可能是有益的 - 如果结合使用，它们可能有助于揭示更全面的情况，并指导更有效的威胁搜寻和事件响应任务。但请记住，这类可信来源也需要事先经过仔细评估，以确保提供的情报适合您的组织的具体需求和用例，比如安全运营、事件响应、风险管理、漏洞管理、红队判研，等等。

评估商业威胁情报产品时需要考虑的问题

在评估各种商业威胁情报产品方面，迄今仍然没有统一的标准，但在评估时应该谨记一些要点：

假设您的公司已经实施了一些安全控制措施，并确定了相关的流程，并且对您来说，将威胁情报与当前使用并了解的工具相结合非常重要。那么您应该寻找能够将威胁情报顺利集成到现有安全运营中的交付方法、集成机制和格式

您应该寻找具有全球覆盖的情报。攻击没有边界 - 针对拉丁美洲公司的攻击可以从欧洲发起，反之亦然。供应商是否在全球范围内获取信息，并将看似不相干的活动整合成内在关联的活动？这种情报将帮助您采取适当的行动

如果您正在寻找更具战略意义的内容，以便为您的长期安全规划提供参考，比如：

- 攻击趋势的高层次视图
- 攻击者使用的技术和方法
- 动机
- 归因，等等，

那么您应该关注一家在持续发现和调查您所在地区、行业的复杂威胁方面具有良好记录的威胁情报供应商。供应商根据您的公司的具体情况定制其研究功能的能力同样至关重要

情报与普通数据的区别就在于上下文。没有上下文的威胁指标是没有价值的 - 您应该寻找能够帮助您回答“为什么这很重要”这类重要问题的供应商。关系上下文（比如与检测到的 IP 地址相关的域或下载特定文件的 URL，等等）提供了额外的价值，可以通过发现网络中新获得的相关入侵指标，促进事件调查并支持更好的事件“范围界定”

结论

二十余年来，卡巴斯基一直专注于威胁研究。借助数 PB 的丰富威胁数据、先进的机器学习技术和独特的全球专家库，我们致力于为您提供来自全球的最新威胁情报，帮助您即使在面对从未见过的网络攻击时，也能从容应对。