思科主动威胁分析

一个安全的网络是实现增长和保持稳定的强大后盾。保护您的业务数据和客户数据对于在基于信任的环境中保护您的员工、客户和信誉具有至关重要的作用。然而，随着您不断拓展功能，保持您的网络的完整性可谓困难重重。此外，改变围绕移动和云资源设计的业务模式会额外增加公司网络的复杂性。威胁形势因此而不断变化，各种威胁快速演变，企图发现防护漏洞。信息安全市场的复杂性与日俱增，安全工作也因之变得支离破碎。为实现创新和突破，企业需要的安全解决方案应能够在主动保护和灵活扩展两个方面达到平衡。

迅速：检测时间和针对性缓解时间缩短，意味着平均响应时间缩短。

重点：更高的保真度可减少误报并确保提供适当的遏制和切实可行的补救建议。

准确：持续监控和调查加上完整数据包捕获可消除安全盲点。

简介

思科主动威胁分析 (ATA) 将深厚的专业知识与前沿技术、领先的智能功能和高级分析相集成，从而以超快的速度、超高的准确性和超强的针对性来检测和调查威胁。作为一个全面的安全解决方案，我们的专家调查员会运用我们一流的全球安全运营中心网络全天候监控客户网络，提供不间断的警戒和深入分析。

功能

	增强版	高级版
全天候威胁分析和事件监控	✓	✓
思科综合安全情报增强功能	✓	✓
日志和遥感勘测数据收集	✓	✓
客户门户	✓	✓
元数据提取	✓	✓
基于规则的分析	✓	✓
高级分析	✓	✓
人性化事件支持	✓	✓
完整数据包捕获		✓
主动威胁搜索		✓
安全设备管理（思科和第三方）	附件	附件

人员

全天候威胁分析和事件监控：拥有全球安全运营中心网络，其技术精湛的认证专家可为您的网络提供不间断的警戒和按需分析

人性化事件支持：指定具有深入事件分析和调查技能的专属调查管理员，实时监控您的环境和特定网络目标，以便针对您的特定需求提供事件管理

主动威胁搜索：相关活动包括找出传统警报机制无法识别的恶意活动。搜索方法记录在可随威胁和恶意攻击活动的演变而持续更新的实时脚本中。

智能

思科综合安全情报
增强功能：利用思科专有威胁信息和第三方威胁信息来提供针对最新威胁的情景和环境感知能力

邮件 + 终端 + Web + 网络 + IPS + 设备

主动威胁分析利用思科 Talos 的安全知识和思科综合安全情报来提供多个层面的洞察力和情景信息

技术

元数据提取：从网络分路器提取数据包报头和关键负载信息并进行存储，以便在事件调查过程中提供额外的数据和情景信息，从而提高事件保真度

完整数据包捕获：收集和存储完整的原始数据包信息，以便执行深入分析和调查，从而能够确认攻击行为并弄清相关问题，例如：谁是真正的攻击者，执行了哪些恶意活动，以及哪些数据遭到泄露

日志和遥感勘测数据收集：从各种网络元素收集遥感勘测数据，以便确定数据之间的关系，从而在事件调查过程中实现快速分析

分析

基于规则的分析：分析方法基于预定的规则匹配，检测已知的攻击模式或行为

高级分析：根据模式和统计异常，利用机器学习技术和专有算法来检测恶意行为。这一切都依赖于可扩展的大数据架构，对大量非结构化安全遥感勘测数据进行处理、存储和分析，从而获得更好的可视性和情景信息

www.cisco.com/go/securityservices