网络检测 & 终端安全 & 邮件防护场景

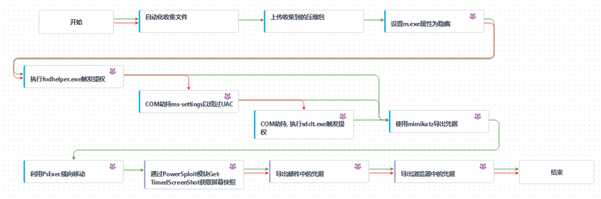
- 以评估对象部署位置进行归类分组，按照预置逻辑将 2000+ 评估用例进行场景归类；
- 适用于中级安全人员针对特定评估对象创建评估任务，实现定向评估分析。

云端内容推送

- 以通过云端升级服务器获得场景内容的持续更新。
- 针对不具备联网的设备，也提供离线内容更新服务。

知识云赋能可编排场景

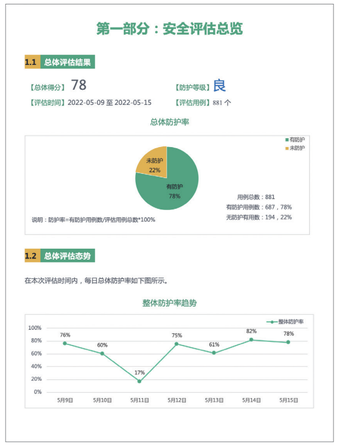
360 抗攻击能力评估系统提供场景编排功能，经过知识云赋能，丰富场景知识库，以图形化、流程化的方式展示一次攻击活动的上下文，不仅通过完整的攻击链呈现一次攻击活动中所使用的技战术；而且通过包含完整上下文的攻击场景，即可全面评估安全产品对完整攻击的防护情况。



安全工作汇报时如何体现成果

专业的评估报告

基于时间段、评估任务名称及评估对象自动生成、订阅评估报告，并优化了对安全设备优化建议，从而方便对安全设备有针对性的进行改进，并可以提供专家解读服务，进行差距分析。



联系我们
公司官网：www.360.net
客服热线：400-0309-360
售后邮箱：service-tech@360.cn

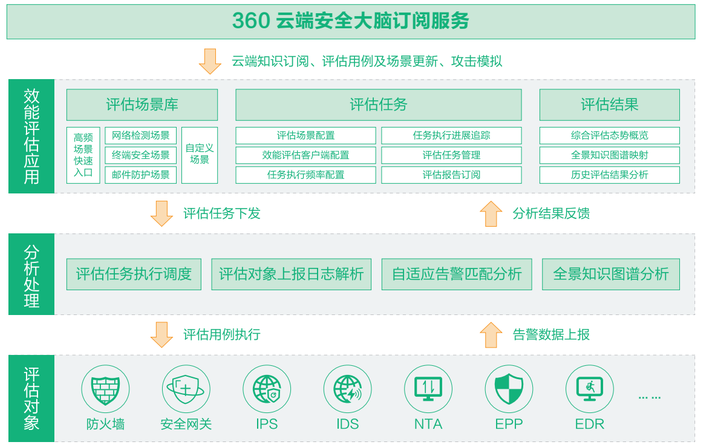
360数字安全
数 字 安 全 的 领 导 者

360抗攻击能力评估系统 V2.0

产品概述 01

360 抗攻击能力评估系统是一款智能量化评估并持续改进安全防御产品体系有效性的能力型产品，通过订阅 360 行业领先的实战攻防技战术知识库，形成一套完善成熟的自动化评估机制，对客户布防的安全产品构建的纵深防御体系进行全面覆盖测试，以度量其面向历史以及最新攻击的整体效能和差距，同时为客户提供针对性的改进建议，形成安全防御能力持续提升的闭环控制系统。

产品采用软件形态呈现，结合 360 云端安全大脑知识云数据订阅与安全专家服务赋能，采用定向可控的模拟真实攻击的方法进行安全产品有效性检验。产品在行业的定位是为已构建纵深防御体系或处于网络对抗最前沿的客户提供安全防御能力有效性评估的高端产品，产品基于云端攻击技战术的更新能够持续的为客户提供防御能力有效性评估。



能力介绍 02

南北向防护能力评估

边界安全防护类评估 防火墙、入侵防御系统、Web 应用防火墙、异常流量清洗等安全防护设备。

东西向防护能力评估

内网横向检测类评估 边界或关键网络节点的流量检测、入侵防御、APT 检测等安全防设备。

终端安全类评估

模拟终端侧攻击或模拟恶意样本运行，评估对象通常是部署在通常为部署于终端的安全防护产品，如 EDR、EPP、CWPP 等。

邮件安全类评估

模拟发送钓鱼邮件，评估对象主要为邮件安全网关，核心目的在于评估其对钓鱼邮件、恶意附件的识别能力。

核心价值 03

替管理层分忧

在 360 抗攻击能力评估系统的帮助下，管理层能够直观地了解网络安全防护能力，清晰认识到安全带来的价值和投资回报率，对公司当前的防护水平有量化的认知。

为 CISO 答疑解惑

360 抗攻击能力评估系统帮助 CISO 检验已采购的众多安全设备是否真的有效；安全设备是否发挥最大效能；从而有效认识安全建设规划及预期与实际效果之间的差距，为未来的规划、建设、优化等决策提供科学量化依据。

助力安全团队提升企业整体防御能力

在 360 抗攻击能力评估系统的赋能下，安全团队从边界、内网、终端、邮件等维度，全面评估防御能力；循环评测，促使安全防御能力不断提升，保障重大活动不失分；为安全设备选型提供可靠数据支撑，量化结果；自动生成薄弱攻击面及改进建议的书面报告，轻松搞定汇报材料，从而持续性地提升企业的安全防御能力，助力客户构建健壮的安全防御体系。

风险前移，预先防范

借助系统性攻击模拟评估用例发现潜在安全薄弱点，预先采取防范措施。

效能量化，有序规划

量化分析安全设施的风险抵御能力，为安全规划提供有的放矢的数据支撑。

主动防御，促进运营

以攻击者视角常态化开展系统性防御能力评估自查，同步进行能力补齐，螺旋式提升运营能力。

典型场景 04

我们现在的安全防护能力怎么样？

● 安全防护能力总览

结合网络安全纵深防御体系建设理念，分别从边界、内网、终端、邮件维度展示当前安全体系的风险识别能力。所有攻击模拟评估用例均经过无损处理并充分验证，不会对现网产生任何影响。

● 持续监控防护能力的变化

通过周期性地执行评估任务，集中统计分析同一任务在历史不同时间节点的评估结果，从而：

- ☑ 追踪安全能力补齐工作进展；
- ☑ 纵览防御能力历史变化趋势；
- ☑ 并支持下钻防御能力异常时间段的评估任务详情，结合原始日志排查异常原因。

我们可以在什么地方缩减预算，在什么地方增加预算，依据是什么？

● 评估结果分析可视化

360 抗攻击能力评估系统支持自动将评估用例的识别情况映射至技战术图谱；从全景技战术知识图谱视角呈现评估结果，从而：

- ☑ 快速判断当前安全体系在哪些攻击战术阶段；
- ☑ 哪些攻击技术防御能力存在缺陷；
- ☑ 有序规划下一阶段安全能力提升工作。

之前XX公司发生的攻击事件，我们能抵御么？

● 丰富的评估场景库

提供高频场景快速入口

- ☑ 归纳总结常见的高频、高危攻击行为，例如 APT 高级威胁评估、黑客工具模拟评估、OWASP 流行攻击评估等；
- ☑ 适用于基础安全人员利用预定义的高频场景快速开展整体性防御评估。