解决方案

绿盟安全态势感知解决方案

业务挑战

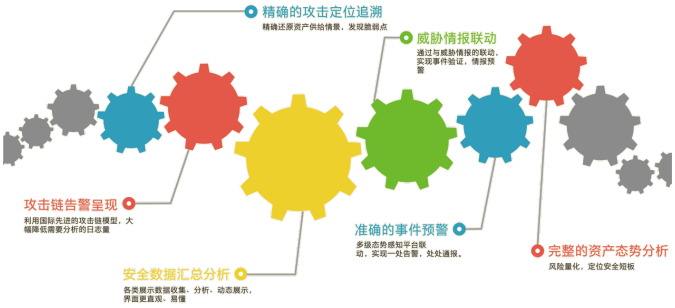
经过多年的信息安全建设，企业已投资部署了大量安全产品，特别是安全防护类别的产品，但随着攻击态势的不断演进，很多用户依然是安全事故频出，也让我们越来越清晰的认识到不论安全防护体系如何建设，也几乎不可能防止安全事件的产生，如何解决这些问题？需要将传统大量投资建设防护型体系，逐渐过渡到加强检测和响应维度，在安全事件发生的全过程进行监测与发现。但面对海量数据如何监测又带来了很多难题。

解决方案

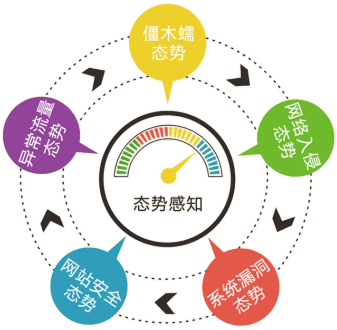
方案概述

绿盟安全态势感知解决方案，基于专业的安全分析模型和大数据管理工具，可准确、高效地感知整个网络的安全状态以及变化趋势，从而对外部的攻击与危害行为可以及时的发现，并采取相应的响应措施，保障信息系统安全。

关键功能



方案亮点



全面的安全感知能力

从外部威胁及系统自身脆弱性两个维度进行全面态势感知分析，站在威胁视角，以网络入侵、异常流量和僵木蠕为切入点，做到知彼；站在脆弱性视角，以系统漏洞和网站安全为切入点，做到知己，提供全方位、全天候的网络安全态势感知能力。

结合威胁情报的安全分析理念

通过企业本地部署绿盟态势感知平台，打通云端情报与本地设备的联动，形成情报触发预警，预警触发防护的闭环。

- 通过情报触发本地数据分析，形成预警
- 本地分析结果通过情报进行验证、并进一步关联分析
- 通过本地数据分析结果，结合绿盟企业安全中心配置防护策略并下发

完善的安全理论模型

利用事件理解模型实现多元数据关联分析，基于攻击链模型实现事件的正反双向推理，结合威胁情报模型实现威胁验证及预警，最终借助风险评估模型为安全防护决策提供有力支撑。

应用场景

安全运维监控

通过对安全数据集中收集、分析和呈现，大大减少告警日志数量，提高告警准确性，同时提供丰富详实的报表，满足各种安全检查需求，提升运维效率。

- 实时感知当前发生的各种攻击事件和资产威胁情况，通过溯源挖掘分析这些事件产生的原因，掌握黑客攻击路径，提供处置建议，提高运维质量和效率。
- 记录安全设备全部原始日志数据信息，可以灵活调取各个时间段数据，并按照需求自定义安全报表，定制记录表单，满足规范要求和安全检查需求。

安全风险监控
通过对核心业务系统持续的安全风险监控，做到业务系统薄弱环节的有效发现，并有针对性的进行安全防御能力建设，降低投资成本，提高建设质量。

- 实时呈现各个业务系统的安全现状，了解核心资产的遭受威胁情况，为后续投资与规划提供依据。
- 实时展示业务系统整体的安全威胁、安全漏洞同期比情况，为后续更好的开展运维工作提供依据。

典型案例
运营商行业典型案例
某运营商客户为了解决IDC入侵防护能力覆盖不完全，入侵防护产品告警日志量大且专业性较强，无法准确定位安全事件等问题。在IDC出口部署了240Gbps检测能力的入侵检测系统集群和态势感知平台，在全网流量检测的环境下帮助客户实现了日志关联、归并、整合，从而实现分钟级攻击事件响应、攻击预警、事件整合与集中呈现，满足合规要求。

政府行业典型案例
某政府行业为解决安全设备分散，无法进行统一分析、无法精确定位安全事件的问题，部署了绿盟安全态势感知平台，通过态势感知平台的部署，实现了海量数据的快速整合、关联分析。基于攻击链模型，快速定位安全事件，大幅度的降低了其运维复杂度，提升运维效率。