绿盟安全态势感知平台

产品白皮书

【产品管理中心】

■ 文档编号		■ 密级	完全公开
■ 版本编号	V2.0	■ 日期	2017-10-21
■ 撰写人		■ 批准人	

目录

一. 安全现状及挑战

1.1 安全现状

随着信息技术不断发展，信息安全给安全监管部门提出新的挑战，而且我国目前信息系统安全产业和信息安全法律法规和标准不完善，导致国内信息安全保障工作滞后于信息技术发展。

为提高国家信息安全保障能力，2015 年 1 月，公安部颁布了《关于加快推进网络与信息安全通报机制建设的通知》（公信安[2015]21 号）文件。《关于加快推进网络与信息安全通报机制建设的通知》要求建立省市两级网络与信息安全信息通报机制，积极推动专门机构建设，建立网络安全态势感知监测通报手段和信息通报预警及应急处置体系。明确要求建设网络安全态势感知监测通报平台。实现对重要网站和网上重要信息系统的安全监测、网上计算机病毒木马传播监测、通报预警、应急处置、态势分析、安全事件（事故）管理、督促整改等功能，为开展相关工作提供技术保障。

2015 年 6 月，第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法(草案)》，中明确提出建立网络安全监测预警和信息通报制度，将网络安全监测预警和信息通报法制化。 •

1.2 当前挑战

1. 企业中已经部署了各种不同类型的安全设备、各种设备的安全呈现都非常分散，运维难度大。
2. 传统安全设备产生海量的安全日志，且误报高，需要靠人工甄别。
3. 传统安全设备只能分析过去或现在正在发生的问题，但是无法告诉客户未来会发生什么。
4. 传统安全设备不会存储原始数据信息，事件一旦发生，追溯难。
5. 客户购买了很多安全设备，但缺乏专业的运营人员对数据进行分析处理，来保障企业安全。

二. 绿盟安全态势感知平台

2.1 方案概述

随着“互联网+”的全面推进，信息技术在国家社会经济建设中的应用也越来越广泛，新型的网络安全威胁也更加突出，传统以“防护”为主的安全体系将面临极大挑战。未来网络安全防御体系将更加看重网络安全的监测和响应能力，充分利用网络态势感知、大数据分析及预测技术，大幅提高安全事件监测预警和快速响应能力，应对大量未知安全威胁。

绿盟安全态势感知解决方案对骨干网络出口和重要网络节点进行严密监控，及时预警大规模网络攻击和病毒传播，保障重要系统的信息系统的网络安全。

通过绿盟安全态势感知平台，可以有效支撑安全监控部门开展网络安全工作，实时掌握网络安全态势，及时掌握重要信息系统相关网络安全威胁风险，及时检测漏洞、病毒木马、网络攻击情况，及时发现网络安全事件线索，及时通报预警重大网络安全威胁，调查、防范和打击网络攻击等恶意行为。

宏观层面，绿盟安全态势感知平台严密监控、切实防范大规模病毒攻击和网络攻击。微观层面，绿盟安全态势感知平台监控保障重点信息系统的网络安全，实现安全事件的预警、检测、响应、取证。按照“统一规划、分级部署、协同共享”的原则，建设形成多级互联互通的通报平台，构建覆盖全网的网络安全态势感知、安全监测和通报预警体系。

运营服务方面，态势感知解决方案提供可管理的威胁检测和响应服务，为企业提供集安全威胁检测设备，安全威胁分析平台及安全服务专家于一体的安全运营服务。

2.2 方案内容

2.2.1 绿盟安全态势感知平台简介

绿盟安全态势感知平台(Threat Situation Awareness，TSA)是一款面向运营商、政府、金融、能源、大型企业等客户，专注于系统风险的分析、发现、评估、可视化的平台。态势感知平台可以收集各种安全数据，利用大数据技术结合威胁情报进行集中处理、关联分析，再利用可视化技术，将各种安全事件进行可视化呈现，为安全运营提供可靠的信息数据支撑。

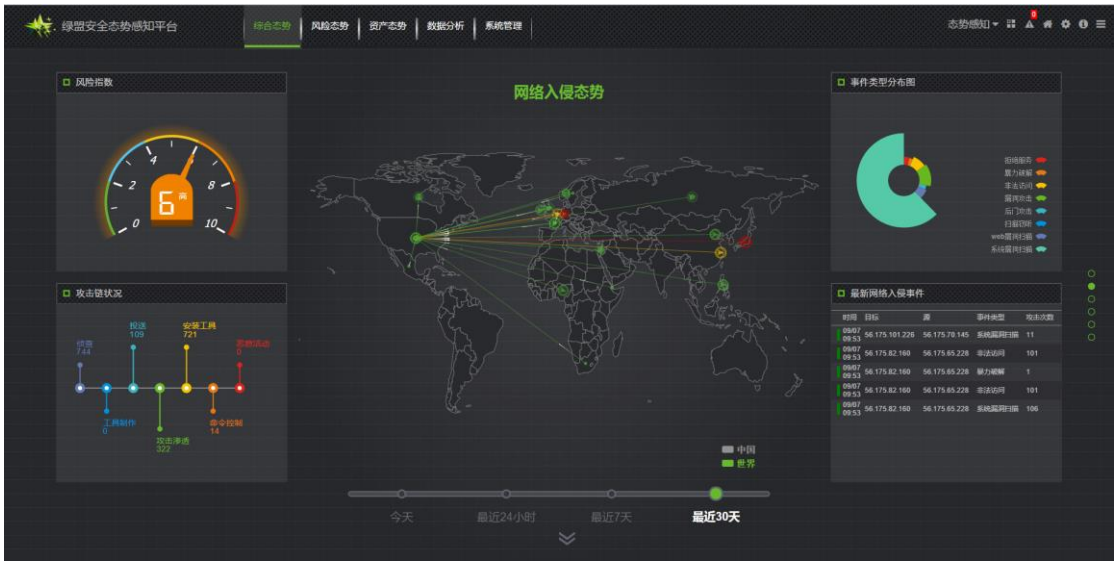
绿盟安全态势感知平台，专注于从网络入侵、异常流量、系统漏洞、网站安全、僵木蠕五大部分进行安全态势感知，能够覆盖各种安全运营场景。

2.2.2 网络入侵态势感知

绿盟科技经过多年的研究，提出“基于对抗的智能态势感知预警模型”，形成“入侵攻击推理引擎”，取得较好的网络入侵态势感知效果。

尤其是对“基于对抗的智能态势感知预警模型”的相关研究，绿盟科技研究团队吸收了“杀伤链”（Kill Chain）和“攻击树”（Attack Tree）等相关理论，形成了独有的推理决策引擎，借助大数据安全分析系统的分布式数据库，可以实现网络入侵态势感知。

经过实际测试，在网络带宽 1Gbps 的典型环境中，入侵检测系统每日的日志在 20 万条左右，经过“入侵威胁感知引擎”分析处理后，形成 500 个左右的威胁事件，再经过“APT 攻击推理引擎”分析处理后，仅仅形成 10-20 个攻击成功的事件。数据压缩率达到万分之一，大幅节省数据处理的时间成本和人工成本。



2.2.3 异常流量态势感知

目前，DDoS 攻击越来越频繁，尤其针对发达地区和重点业务。在 2016 年第一季度，全球范围内的 DDoS 攻击事件频发。从重大攻击事件分析，追逐利益仍然是黑客攻击的主要动机，“黑客主义”事件也在不断挑战政府的网站。

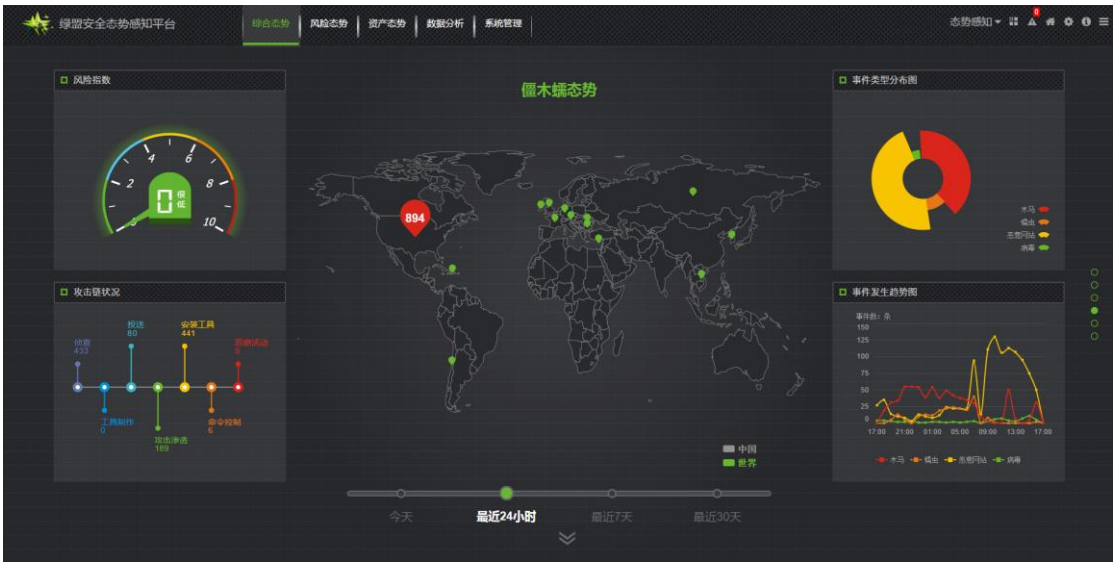
在抗拒绝服务攻击方面，绿盟进行了超过十年的研究。可以对全网流量进行深度流检测，具有网络流量自学习功能，与同类产品相比误报率降低 80%以上。绿盟网络流量分析系统可以准确发现 DDoS 攻击事件并掌握攻击源、攻击目的、攻击总流量和峰值流量，协助客户准确掌握网络 DDoS 攻击态势。

2.2.4 僵木蠕态势感知

僵尸网络、木马、蠕虫病毒三者合称“僵木蠕”。

僵木蠕对互联网和企业内部网络危害非常巨大。僵木蠕消耗大量网络带宽，引起 ARP 攻击等问题，造成骨干网络瘫痪。同时受到僵木蠕传染的主机受到命令控制服务器的控制，成为 DDoS 攻击的帮凶。更为严重的是，目前大多数僵木蠕的命令控制服务器位于海外，对国家网络安全造成严重的威胁。

绿盟科技针对僵木蠕的传播特点，对网络上传播的僵木蠕进行识别，并追踪溯源僵木蠕的传播路径、控制命令路径，最终追踪溯源发现命令控制服务器。通过发现的命令控制服务器，再反查受控主机，最终实现对僵木蠕网络态势的感知，为后续采取行动打击僵木蠕创造条件。



2.2.5 系统漏洞态势感知

黑客攻击本质上是利用系统存在的安全漏洞对系统进行危害。因此要避免黑客攻击，一个重要的安全防护手段就是在黑客之前发现重要信息系统存在的脆弱性问题，并进行修补，做到防患于未然。

绿盟科技研发了国内领先的远程安全评估系统（NSFOCUS RSAS）、web 应用漏洞扫描系统（NSFOCUS WVSS），其中远程安全评估产品连续 4 年国内市场占有率排名第一，是国内监管测评机构首选的漏洞扫描和风险评估工具。依托于这些产品，可以发现网络信息系统脆弱性，形成脆弱性态势感知。

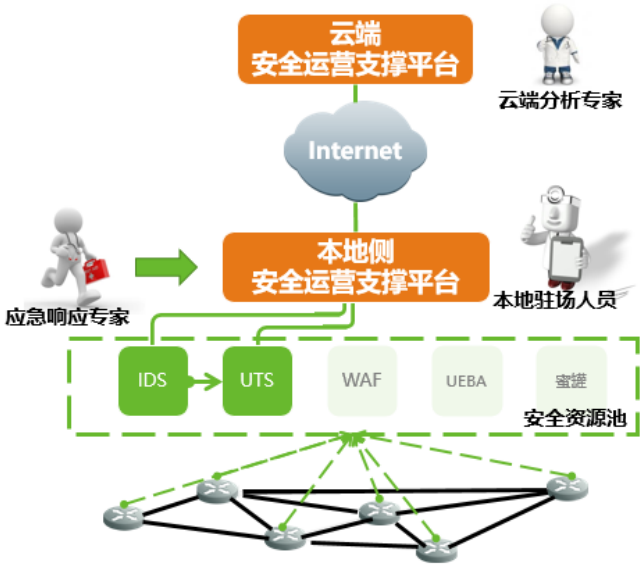
2.2.6 网站安全态势感知

网站作为网络信息系统对外提供服务的重要窗口，面临的安全威胁也是最多的。对重要网站信息系统的黑客攻击，不仅会对网站造成严重破坏，还会让黑客能够利用被黑网站对网站浏览者进行攻击，造成更为恶劣的影响。因此，需要对网站的安全态势进行监控，及时发现网站安全问题。

网站安全态势感知，可以及时监控到网站漏洞情况，发现网站挂马、网页篡改、域名劫持等黑客攻击行为，对网站平稳度、网站敏感内容等进行持续监控，并有效进行运维管理，从而避免因为网站出现问题导致公众问题。

2.2.7 安全运营服务简介

企业已经购买了很多安全检测防护类设备和安全运营分析的平台，但是苦于缺乏专业的安全人才来管理运营分析这些设备和平台上的日志数据，无法真正发挥出设备和平台的能力来保障企业安全，态势感知解决方案融合了安全运营服务，可将客户本地的运营平台跟绿盟科技云端安全运营支撑平台对接，由绿盟云端专家给客户提供 7x24 小时的运营服务，并跟客户本地测的驻场运营人员配合，实现热点事件的预警与防护、高危访问源的检测与封杀、可疑安全事件的发现与确认等系列闭环的安全运营服务，帮助企业降低整体的安全运营投入成本和风险、减轻客户的安全运营负担，保障企业网络安全。

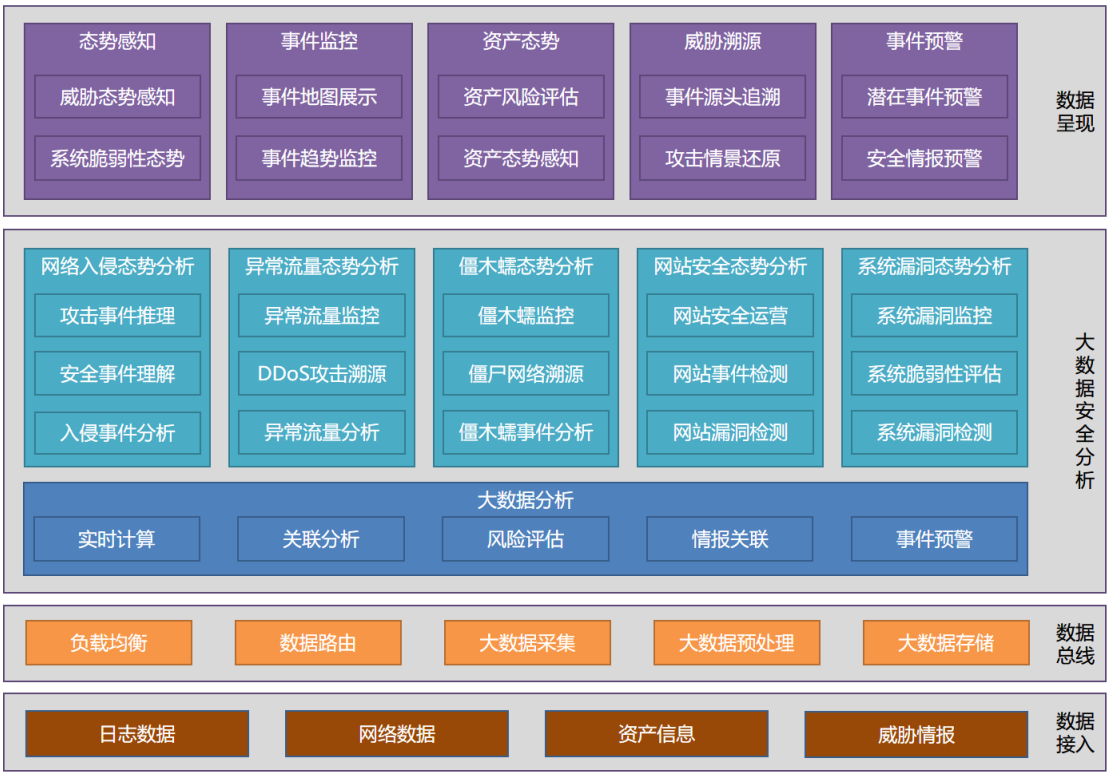


三. 方案创新与价值

3.1 安全大数据分析技术

安全从业者早已知道，在海量的安全数据中，各类数据之间有千丝万缕的联系，通过对这些联系的分析，可以发现很多靠传统手段无法发现的安全问题。但是面对海量的安全日志、网络流量、威胁情报、环境信息……传统的利用数据库进行安全分析、数据挖掘变得极端困难，更无法形成有效的安全态势感知。

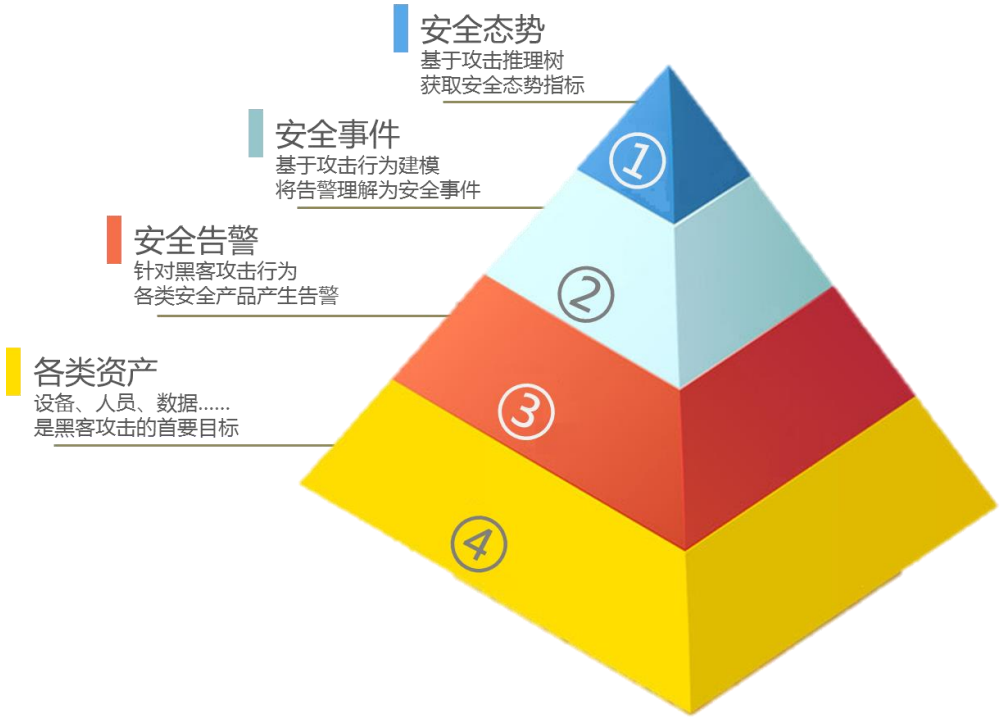
绿盟科技经过多年的研究，和安全事件分析经验积累，提出了多种安全分析模型。同时绿盟科技利用在大数据分析方面的技术积累，形成了安全大数据分析技术。二者结合将以往不可能的安全大数据分析变为可能。



3.2 安全态势感知技术

绿盟科技在态势感知、早期预警方面持续进行安全研究，持续跟踪了美国安全防护预警体系建设思路，对美国的“爱因斯坦计划”、“可信互联网连接（TIC）计划”以及后续的“持续监控计划”都进行了深入的研究。

在此基础上，绿盟科技形成了自己的态势感知和安全预警理论，利用安全大数据分析技术，结合多种安全分析模型和安全产品实现了强大的态势感知能力。能够提供包括顶层设计、平台建设、子系统建设全套解决方案实施能力。



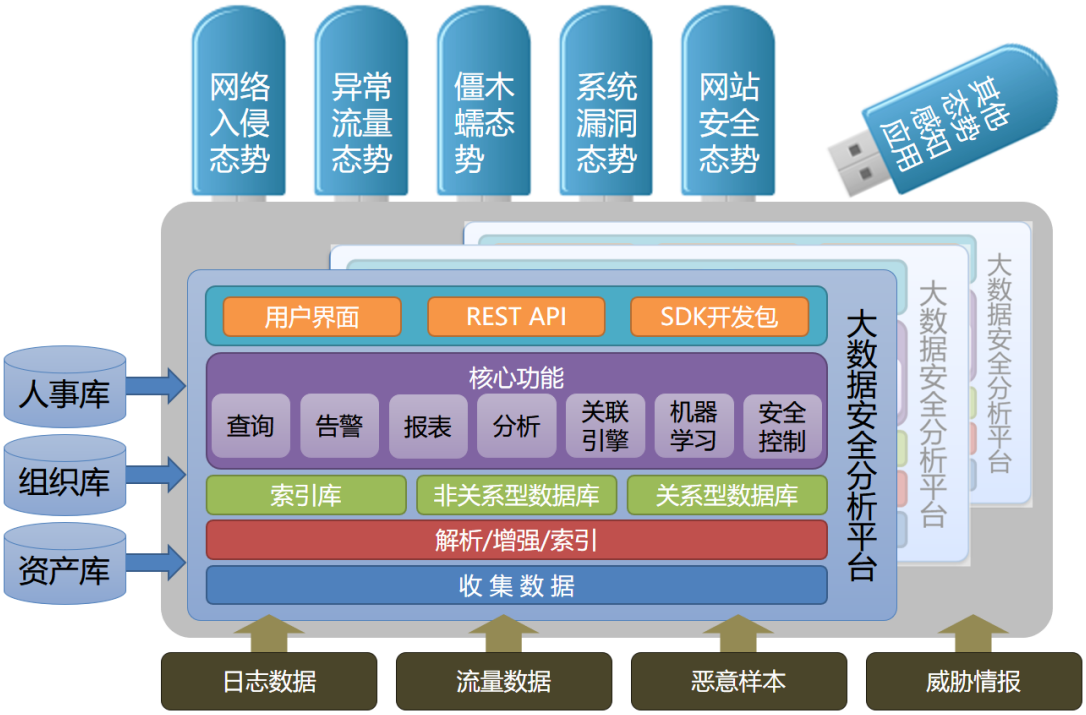
3.3 柔性平台灵活扩展

绿盟安全态势感知平台采用灵活先进的柔性平设计，可以满足各种不同规模的部署场景，支持快速扩展。

平台采用模块化设计，分为网络入侵态势、异常流量态势、僵木蠕态势、系统漏洞态势、网站安全态势。每一个子系统均可以独立上线运行或下线停运。不同的子系统组合可以实现不同的态势感知目标，随业务目标变化支持灵活扩展。

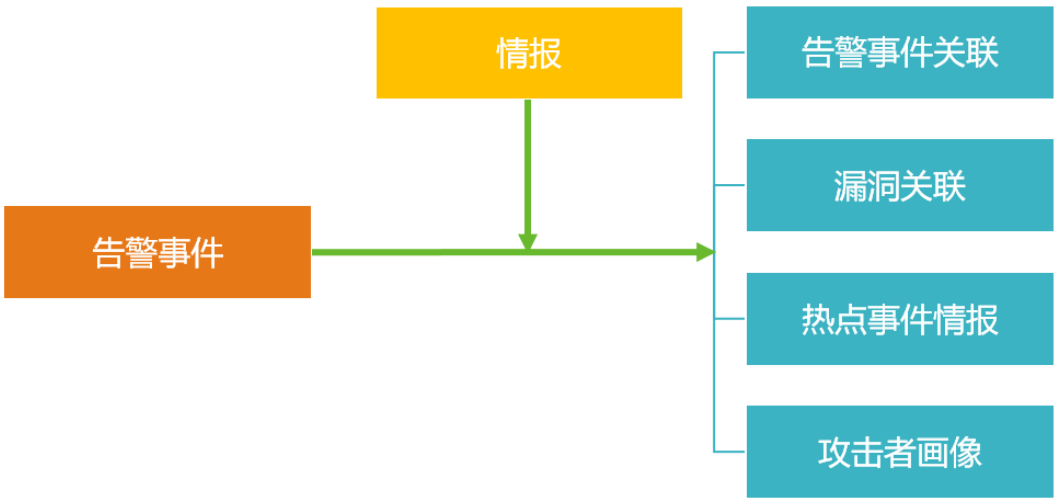
在平台监控性能不足时可以通过集群技术对平台计算资源、存储资源、监控采集设备进行灵活扩充，整个平台所有模块部件都可以通过设备扩容实现态势感知能力扩充。

平台提供 SDK、开放 API 接口等方式，能够满足监控业务可扩展性需求，能够根据安全业务需求的变化进行平台功能的调整。



3.4 威胁情报关联分析

绿盟威胁情报中心（NSFOCUS Threat Intelligence center, NTI）是绿盟科技依赖多年的安全经验和情报数据积累推出的一款威胁情报分析和共享平台，可为用户提供及时准确的威胁情报数据。借助 NTI 的威胁情报支撑，用户可及时洞悉资产面临的安全威胁进行准确预警，了解最新的威胁动态，实施积极主动的威胁防御和快速响应策略，结合安全数据的深度分析全面掌握安全威胁态势，并准确地进行威胁追踪和攻击溯源。



3.5 融合安全运营服务

MDR 服务（Managed Detection and Response Service）,是国际知名咨询机构 Garnter 在 2016 年 5 月提出的概念，后续逐步被发达国家或地区的企业客户所接受。绿盟科技此次将安全运营服务融于到态势感知整体解决方案中，与传统的运维服务不同，安全运营服务是采用一体化集成的方式为企业提供端到端的服务。借助这种新的服务模式，企业可以规避信息安全建设项目人员、技术、流程和管理的风险，有效避免投资浪费。另外一方面，企业无需为安全运营投入大量精力进行规划、设计、部署和运维，可大幅度降低安全运营带来的负担，使企业可以集中资源和精力再自有业务上创造价值。