# 绿盟关键信息基础设施安全态势感知平台

# 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 | V1.0 | ■ 日期 | 2019-3-27 |
| ■ 撰写人 | | ■ 批准人 | |

# 目录

# 一. 现状及挑战

## 1.1 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，勒索病毒会给政府、医疗和教育各领域的业务体系造成巨大打击，影响人民生活的稳定运行；0day 漏洞被利用频发，会给信息化时代人们的数据安全造成影响；黑客组织针对机关单位的攻击，在网页上挂上反共标语会对政府的公众形象带来负面影响。所以网络安全问题是和社会、国家和人民群众息息相关的重大问题。

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。自 2016 年国家网信办发布《国家网络空间安全战略》以后，国家加强法律法规的建设，也加大了对网络安全的监管和检查力度。

1）2015 年刑法修正案明确网络服务供应者的责任和义务。

2）2016 年网络安全法明确对关键基础设施单位的建立监测预警与应急处置机制，在监管上采取更主动的方式对互联网威胁和风险进行管控。

3）2017 年 CII 保护条例明确要对基础设施进行定期检查和设置应急响应预案，要求企业采取措施对关键信息基础设施进行风险管理。

4）2018 年等保 2.0 明确云计算、大数据、物联网和移动互联等新技术纳入监管，对安全运营的范围进行补充说明。

5）在监管上，主观机关加大网络安全检查的力度，检查的频率从几年前的两年一检提升到一年多次检查和整改。

在客观上，国家对互联网空间及关键基础设施单位的安全管理的要求从合规及事件管理要求上升的风险管理，需要企业、安全产业乃至整个社会积极响应。在过去，我们关注合规要求和安全事件响应及处置，在未来，我们需要合规和事件管理的基础上做到安全风险治理，做到防患于未然。

## 1.2 当前挑战

1. 辖区内被监管单位中已经部署了各种不同类型的安全设备、各类设备的安全呈现都非常分散，缺乏宏观层面的态势把控和整体评估。
2. 网络安全监管与等保备案信息没有充分结合，缺少对关键信息基础设施的精准防护。

3. 传统安全设备产生海量的安全日志，且误报高，缺少对海量安全告警中高危信息的有效识别，以及对告警有效性的准确性把关。
4. 缺乏安全事件发现后对责任单位的有效通报手段。
5. 针对 APT 等高级威胁缺少防御手段，尤其是需要对监管行业关心的重点事件、重点规则进行单独监测。
6. 安全事件的追踪溯源能力较弱，缺乏对黑客、黑客组织的回溯。

# 二. 平台介绍

## 2.1 方案概述

绿盟关键信息基础设施安全态势感知平台(Critical Information Infrastructure Platform，CIIP)，是一款面向监管行业客户，专注于安全风险的分析、发现、评估、可视化的平台。通过采集互联网及 CII 系统相关数据，再利用大数据存储、分析技术，对各类安全数据进行关联分析和深入挖掘，可以及时发现被监管单位网络中的各类威胁事件行为、系统脆弱性，并对安全事件进行通报预警及可视化呈现，及时预警大规模网络攻击和病毒传播，保障关键信息基础设施的网络安全，有效辅助监管单位开展网络安全业务工作。

平台定位如下：

1. 面向关键信息基础设施进行精细化拦截阻断、动态协同防御和协助调查，保障关键信息基础设施免受攻击、入侵、干扰和破坏。
2. 全方位感知网络安全态势，监测、防御、处置境内外网络安全风险和威胁，实现对系统安全的整体展示、态势感知、攻击事件溯源、及对潜在威胁的预警功能。
3. 协助监管单位组织开展等级保护、监督管理、信息通报、重大活动安保工作与应急指挥调度。

按照平台建设目标和实际业务需求，CIIP 目前包括的主要功能主要有 10 个方面，主要包括：等保管理、安全监测、态势感知、通报预警、快速处置、侦查调查、追踪溯源、情报信息、指挥调度和攻防演练，CIIP 业务架构如图 1 所示。

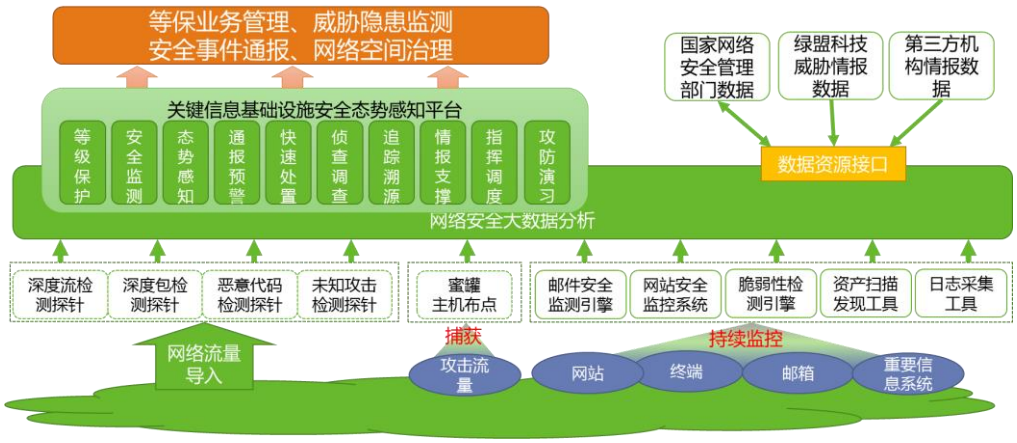


图 1 关键信息安全态势感知平台业务架构

## 2.2 方案内容

### 2.2.1 等级保护

等级保护子系统是一套用于支撑网络安全等级保护业务工作开展、数据监管与分析、安全状况评价、态势呈现及日常工作管理支撑的等级保护综合管理平台，落实网络安全法对公安监管部门开展等级保护工作提出的责任要求，支持网络安全等级保护条例及等级保护 2.0 系列政策标准提出的工作要求、工作流程的落地实施，支持对国家关键信息基础设施和重要信息系统重点监管，是公安机关开展等级保护工作的抓手平台，同时，作为等级保护数据汇聚平台，与公安部列装设备信息安全等级保护检查工具箱、即将列装的工控系统安全等级保护检查工具及用于等级保护专项工作开展的数据采集与填报工具等进行对接，实现数据的集中存储、分析和应用。

### 2.2.2 实时监测

实时监测子系统能够及时发现、识别、阻断网络攻击威胁，监测恐怖组织、黑客组织、不法分子等攻击活动、攻击行为及攻击方法手段。实时监测子系统监测重点保护对象所受的攻击、威胁、破坏、窃密、渗透等情况，以及重点保护对象的网络、系统、大数据等安全状况、存在的漏洞、隐患等，为快速处置、通报预警提供支撑。同时实时监测子系统结合情报信息的输入，向 CIIP 平台提供威胁监测的技术手段，目的是及时发现、识别、阻断网络攻击威胁，为快速处置、通报预警提供支撑，同时，它也是态势感知模块的输入。

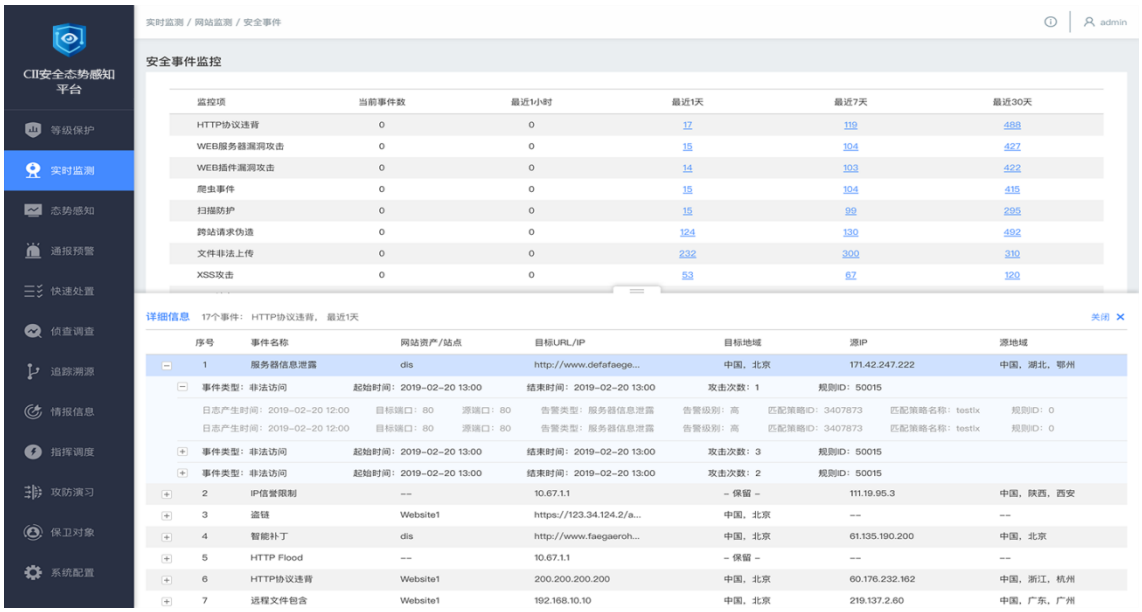


图 2 关键信息安全态势感知平台实时监测子系统

## 2.2.3 态势感知

态势感知子系统专注于系统风险的分析、发现、评估、可视化的子平台。态势感知子系统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。

态势感知子系统，专注于从入侵威胁、异常流量、僵木蠕、系统脆弱性、网站安全、APT攻击六大部分进行安全态势感知，能够覆盖各种安全运营场景。


图 3 关键信息安全态势感知平台态势感知子系统

## 2.2.4 通报预警

通报预警子系统接收来自实时监测、态势感知、情报信息等子系统发送的安全威胁信息、安全隐患信息、安全事件数据等，当数据涉及到监管单位及被监管单位的安全运维部门时，通报预警子系统及时将相关信息和处置建议发送到相关部门。

通报预警子系统通过各个相关系统的数据分析和阈值设定，自动或人工产生通报预警漏洞挖掘、分析、防御能力。系统可以定时发布安全态势、威胁情报等信息；也可在出现高危漏洞和突发重要事件时，提供相应的安全通告和处置建议。

通报预警子系统支持各类通用通报的创建、审批、签发、跟踪功能，支持对单一通报的签收、反馈情况的统计跟踪，支持通报发送对象的定制化，支持与 CIIP 平台其他业务子系统进行数据对接与协同联动。

### 2.2.5 快速处置

快速处置子系统的安全事件识别、分析、处置，根据“攻防技术跟踪”研究主流安全攻防技术并识别各种攻击的特征，这些数据通过“场景建模”过程形成计算模型；从“情报获取”、“数据采集”来的漏洞情报与监控数据在计算模型中进行“安全分析”，分析后形成的告警信息再经“告警分析”过程识别出安全事件，确认的安全事件由“事件处置”过程处理；事件处置完毕后还将进行“根因分析”，分析发现的问题在“调查核实”后进行“违规处置”。

快速处置子系统支持网络安全事件的资源调配与快速处置功能，支持事件的分级与研判，支持处置任务的下发、跟踪、关闭、评价，支持事件原因分析以及与测评结果数据的对比功能。

### 2.2.6 侦查调查

侦查调查子系统主要功能是为案件侦查提供相关服务，在案件发生（报案）后，对案件本身提供辅助调查、取证、立案等功能，并对侦查调查的流程进行管理。。

侦查调查子系统也具备可疑案事件的推送能力，协助监管单位缩小侦查范围，并未侦查结果提供证据支撑。

### 2.2.7 追踪溯源

追踪溯源子系统为案件侦查服务，在发生网络攻击案件或有线索的情况下，依托情报信息、工具等对攻击者及其手段进行溯源，为案件侦查提供线索和证据。

追踪溯源子系统通过大数据和 DFI 深度流检测技术，通过 DFI 机器学习自主发现，态势感知和威胁情报联动发现溯源，交互式分析溯源 3 大核心能力，针对 APT 安全事件、DDOS 攻击、僵木蠕传播、业务流量分析、企业网内路径分析等需求，以低成本提供超过 3 个月或者更长时间的流量回溯及取证能力。

### 2.2.8 情报信息

公网资产漏洞被通报、数据泄露、木马病毒等安全事件频发，带来安全风险和不良影响，一方面公网资产可能沦为攻击者入侵内网的跳板，另一方面公网资产安全事件被公开或通报也对名誉或社会公信力造成不良影响。

威胁情报子系统通过借助云端和互联网资源来主动获取来自各方的威胁情报信息，通过大数据平台的信息整合和关联分析形成针对自身暴露问题的具体可读化信息，并能够最大化降低对互联网的脆弱性暴露从而大幅降低来自互联网的威胁。

### 2.2.9 指挥调度

指挥调度子系统是实现等级保护、实时监测、通报预警、快速处置等业务功能的数据联动，支持重大任务安保任务的创建、调度功能，支持时间信息的上报、下发，支持安全应急人员、资源的调度，对当前网络安全管理与攻防态势进行实时跟踪与展示。

在重大安保活动期间，协助安保作战指挥，有效组织、利用本地专家、安全厂商、电信基础运营商、团体，加强本地安全支撑。当发生安全事件时，应急组通过平台进行通报预警，专家组确认信息，分析决断后，指挥技术组现场分析、取证、处置，协调单位及时消除影响，保障系统恢复正常运行。

### 2.2.10 攻防演习

攻防演习子系统可以提供一套可实施的、闭环的演练场景用以模拟安全事件，可以辅助客户通过模拟演练的方式亲身参与到安全事件攻防之中，进而充分了解安全事件中攻、防双方的思路及实践方法

攻防演练的最终目的即是完善安全事件的应急机制。通过一次模拟的安全事件可以让安全团队以低成本实施一次有效的应急响应，同时也可有效识别出当前安全处理机制的不足或缺陷。

同时，绿盟提供专业的红蓝对抗团队和业务流程，帮助技术人员全面提升攻击技术分析、临时防御措施、日志分析及事件识别等安全能力。并通过攻防演练的组织和实践，可以优化 IT 技术组织结构，为 IT 部门的协调发展做好基础建设。

# 三. 方案创新与价值

## 3.1 安全大数据分析能力

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。

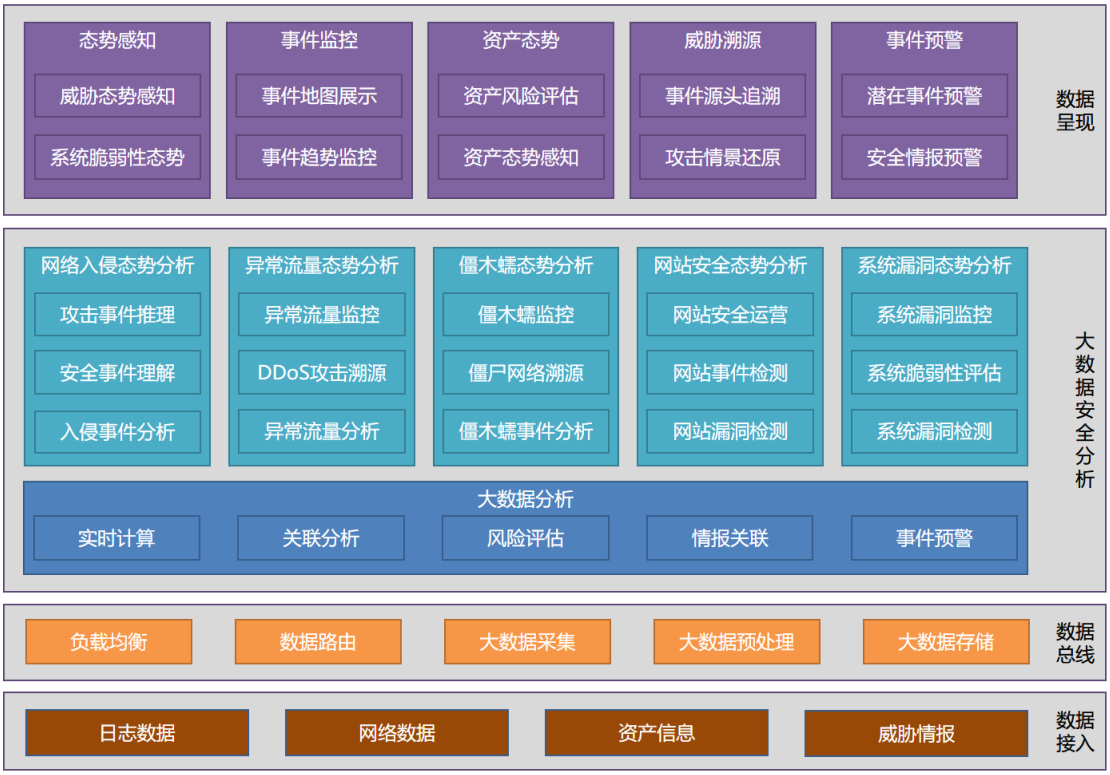


图 4 态势感知数据分析架构

## 3.2 态势感知能力

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。

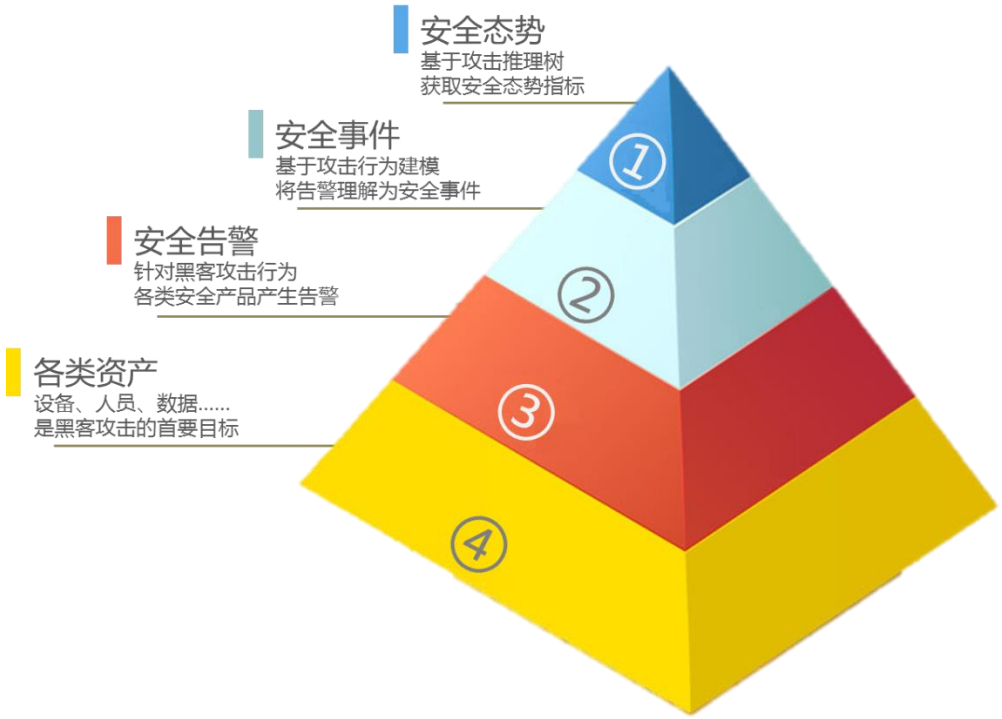


图 5 态势感知能力

## 3.3 威胁情报关联分析能力

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。

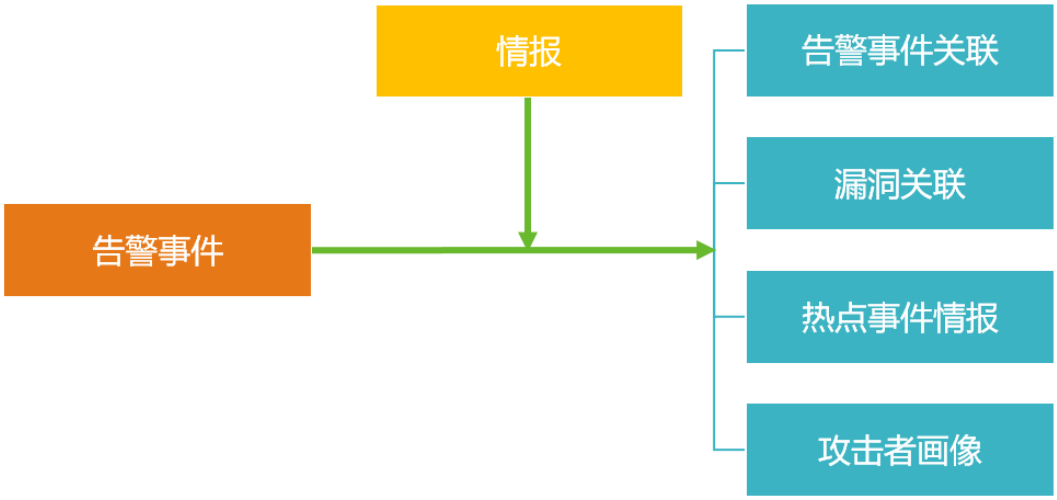


图 6 威胁情报的应用

## 3.4 安全事件追踪溯源能力

攻击溯源流程首先是基于攻击目标和构建的推理方法库，在理解引擎生成的安全事件基础之上进行推理，将独立的安全事件进行串联，生成完整的攻击链。并针对同一攻击者利用不同手段对一个目标进行攻击的情况，对攻击链进行整合，以生成更加准确的攻击链信息

然后对安全事件进行前两个阶段的推理之后，会生成完整的攻击防御树，并提供攻击和防御两个角度的信息呈现

最后在生成的攻击防御树基础之上挖掘攻击目标和攻击者的信息并进行可视化呈现且从攻击者资料库当中匹配攻击者的情报信息，用以完善攻击者的画像，以及预判攻击者可能采取的行动，同时支持生成溯源报告书。

## 3.5 统一威胁探针

统一威胁探针采用深度流检测技术及深度包检测技术对各类应用进行深入分析，搭建应用协议识别框架，准确识别大部分主流应用协议，可以对基于应用识别的应用进行精细粒度的管理，能够很好的对这些应用安全漏洞和利用这些漏洞的攻击进行检测和防御。支持在 WEB 界面和安全中心上配置应用管理策略，可根据应用管理策略控制应用的使用，并支持在对象中搜索名称，提高了策略配置的效率和产品易用性。对缓冲区溢出、SQL 注入、暴力猜测、DOS 攻击、扫描探测、蠕虫病毒、木马后门、间谍软件等各类黑客攻击和恶意流量进行实时检测及报警，并通过与防火墙联动、TCP Killer、发送邮件、安全中心显示、日志数据库记录、运行用户自定义命令等方式进行动态防御。

统一威胁探针不仅仅采用深度包检测，还包括深度流检测，通过多种检测技术的并行检测，不仅可以通过专家模式检测已知僵木儒威胁的同时，还能检测 0day 攻击和未知攻击，进而能够有效地监测反向型、加壳型隐匿性木马，恶意蠕虫，僵尸主机通信等。主要目标是掌握用户重要 IDC 系统、党政机关和重要企事业单位是否有僵尸网络、恶意蠕虫、木马文件等类型的事件传播。

**具备多项能力：**

1. IDS入侵检测能力
2. WEB深度检测能力
3. 恶意文件检测能力
4. NTI威胁情报能力
5. Webshell专项检测能力


图 7 统一威胁探针