文献引用格式：赵阳 . 绿盟威胁情报解决方案 [J]. 信息安全与通信保密 ,2020( 增刊 1):23-28.
ZHAO Yang.NSFOCUS Threat Intelligence Solution[J].Information Security and Communications Privacy,2020(S1):23-28.

# 绿盟威胁情报解决方案 *

赵　阳
（北京神州绿盟科技有限公司，北京 100089）

**摘　要：**绿盟威胁情报解决方案，基于多源多类型情报，利用多源情报清洗与归并技术、互联网资产画像技术、大数据关联分析技术和机器学习技术，结合威胁预警、设备联动智能防御、热点事件应急处理、追踪溯源、攻击者画像、定位反制等手段，通过云地结合，构建下一代预警、检测、响应、追溯一体化的立体协同防御生态，应用前景非常广阔。

**关键词：**网络安全；威胁情报；应急响应；追踪溯源；攻击者画像；定位反制
**中图分类号：**TN915.08　　**文献标志码：**B　　**文章编号：**1009-8054(2020)S1-0023-06

# NSFOCUS Threat Intelligence Solution

ZHAO Yang
（NSFOCUS, Beijing 100089, China）

**Abstract:** Built upon multi-source intelligence cleaning and merging, Internet asset profiling, correlative analysis of big data, and machine learning, the NSFOCUS Threat Intelligence (NTI) solution that comes with a wide variety of intelligence from multiple sources, is capable of threat alerting, intelligent defense via device collaboration, emergency response of topical incidents, traceback, attacker profiling, attribution and countermeasures. By integrating the cloud and on-premises devices, the NTI solution forms the next-generation all-around coordinated defense ecology that features alerting, detection, response, and traceback, thus having a broad application prospect.

**Key words:** cyber security; threat intelligence; incident response; traceback; attacker profiling; attribution and countermeasures

* 收稿日期：2020-08-21；修回日期：2020-08-27　Received date:2020-08-21; Revised date:2020-08-27

## 0 引 言

随着全球网络空间安全攻防对抗的快速升级，基于已有防御规则的被动防护已成为网络安全防护的瓶颈，威胁情报则是解决该问题的关键。

## 1 传统防御体系的弊端

当传统网络安全防护手段应对当前全球网络空间安全攻防对抗时，存在以下弊端：

（1）防御体系方面。传统攻击检测和防御体系依赖静态、被动和孤立的已知签名和规则，无法有效应对当前以规模化、自动化、0day 高级持续性攻击为特征的各种复杂安全威胁。

（2）检测和追踪能力方面。随着黑客攻击的专业化和组织化，传统的安全控制措施无法检测和应对高级威胁不断升级和变动的战术、技术手段和过程，对未知威胁或高级威胁的检测往往力不从心。

（3）安全威胁响应方面。当前的黑客攻击越来越规模化、自动化，从漏洞挖掘到规模化攻击的时间间隔正急剧减小，但客户不同组织间或同一组织内部的大多安全防护控制手段和技术设备是各自孤立的，无法在全网内共享。

## 2 解决方案概述以及核心价值

绿盟威胁情报解决方案通过情报数据的协同与联动，为网络空间安全作战与指挥的开展提供平台级支撑，是及时发现、迅速研判、快速响应、协同侦办的网络安全监察业务工作开展的重要且必要手段，如图 1 所示。

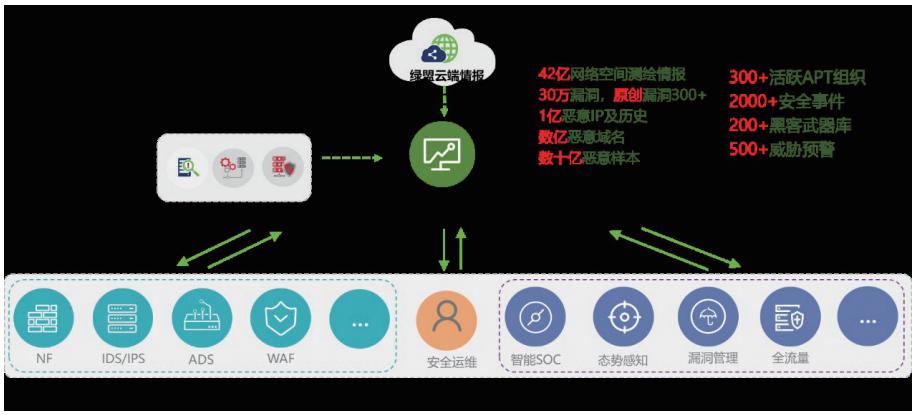


图 1 绿盟威胁情报解决方案全景

其核心价值包括：

（1）威胁情报驱动网络安全防御体系全面转型

威胁情报的诞生源于攻防的不对等。随着黑客攻击的规模化、自动化、多样化、灵活化，传统的基于签名和规则的防御体系捉襟见肘，传统的基于“已知”规则的检测在遇到 0Day、APT 等“未知”威胁时，完全无法感知和防御。威胁情报的出现驱动了网络安全防御体系全面转型，从基于静态的规则向动态的自适应的防

御体系转变。

（2）使攻防不对等的局面完全扭转

绿盟威胁情报帮助防守方了解攻击者，包括攻击者的背景、思维方式、能力、动机、使用的攻击工具、攻击手法、攻击模式等。对攻击者了解越多，就能越好的识别威胁以便快速的做出响应。

（3）大幅缩减应急响应时间

在应急响应中，应用威胁情报为安全防御产品赋能，可以大大缩短安全产品对最新威胁的响应和处置时间，达到“单点感知，全网防御”的效果。

## 3 关键技术

### 3.1 基于知识图谱建模的威胁推理技术

威胁情报知识图谱的构建是决定攻防效果的关键基础因素。根据知识图谱进行威胁推理，能够使威胁情报数据转化为态势感知、威胁预警、证据链等威胁防御方法，这些方法将构成防御方的一个关键体系。

### 3.2 威胁自适应诱捕与追踪技术

为了能对网络空间中具有随机性和不固定性的事件进行捕获、追踪、分析与预警，云端通过使用 IDC、云环境等多种平台在全球范围内部署了基于威胁情报的威胁自适应诱捕与追踪技术的系统。

### 3.3 大数据关联分析与威胁挖掘技术

首先对输入数据进行大数据关联分析，提取网络行为关联关系、指向关系、从属关系、时频关联性和相似性关联性等，然后再将关联关系输入到分析引擎并使用多种机器学习模型对已知关联数据，层层深入挖掘，发现高价值数据，包括未知威胁数据。

## 4 应用实践与优势

### 4.1 应用场景

绿盟威胁情报解决方案，适用于如图 2 所示的 8 大场景 [1]。


图 2 绿盟威胁情报方案适用场景

### 4.2 实际应用效果

在云端，绿盟拥有丰富的威胁情报，包括 42 亿的网络空间测绘情报、30 万的高质量漏洞情报、1 亿的恶意 IP 情报、数亿的恶意域名情

报和数十亿的恶意样本情报，跟踪到了 300 余个活跃 APT 组织，2000 余个安全事件，发现了黑客利用的 200 余个武器库，共发布了 500 余篇威胁预警。

在地面，用户基于客户本地威胁情报平台，将云端威胁情报和客户本地的专属情报相结合，对本地的安全设备和安全平台进行赋能，便于客户的安全运维人员及时进行威胁响应和处置。具体的应用效果包括：

（1）威胁预警，防患未然

基于威胁情报进行漏洞和威胁事件预警，发布预警报告 500 余篇。

（2）威胁态势，实时监控

高精度威胁捕获，全球威胁态势尽在掌握，捕获实时威胁数亿次。

（3）攻击溯源，锁定元凶

还原攻击过程，通过威胁情报提供“证据”，攻击溯源到 APT 组织 300 余个。

（4）单点感知，全网联防

单点发现威胁，通过威胁情报共享进行全网联防，威胁情报共享数万次。

### 4.3 方案特色

（1）基于知识图谱的数据平台构建方案，多维度支撑数据的态势分析、呈现和事件预警。

①知识图谱的数据建模

基于知识图谱的异构数据融合共享环境平台，利用知识图谱强大的特征表达能力、属性抽象能力、复杂关系关联能力、语义分析能力对整个平台的异构数据提供一个丰富的知识网络。不仅有利于对各种平台的异构数据进行基于业务场景的数据共享，也有利于对结构化数据和非结构化数据进行数据分析和数据挖掘，生成知识、智慧。对未来的威胁预警、预判、防护等安全治理有重要的意义。

②基于知识图谱的数据挖掘与分析产生威胁事件

通过对漏洞、行为、知识、事件多张图的组织，经过数据挖掘、分析、关联，将隐藏在其中的威胁事件抽取出来，形成威胁事件告警与威胁态势，高效的提供威胁事件发现能力和威胁预警能力。

（2）分层数据处理模型方案，支持输出从情报到外部数据源的溯源。

参考 DIKW 数据模型，对平台数据进行分层数据模型构建。模型根据数据的处理阶段划分为五类：外部数据、原始数据、标准数据、知识和威胁信息。

基于 DIKW 的数据模型，将平台中繁杂的异构数据通过数据转化为信息、数据转化为知识、数据转化为威胁信息等多个关键步骤，构建数据金字塔。在处理模型的过程中融入了多种数据建模思想，包括基于知识图谱的图构建对异构数据的元数据描述，对整个数据体系形成完整的图描述，为平台的数据融合、数据搜索、威胁信息生成、数据和事件共享架构了一个完美的框架。多层数据处理模型，在使用威胁事件态势和预警的过程中可以对每层数据提取元数据描述的证据，通过这些证据内容可以根据数据层级关系进行数据源溯源。

（3）基于多标准扩展的数据体系方案，规范化数据格式标准体系。

基于 STIX[2] 扩展的数据描述体系，结合大

数据平台对各种资产数据、漏洞数据、补丁数据、样本数据等数据进行多维度关联分析，引入 CWE、CPE、CAPEC、ATT&CK、MAEC 等知识体系，达到威胁信息发现、预警的效果。

（4）高可扩展的数据接入方案，灵活高效扩展数据接入系统。

①插件化的数据源接入技术方案

基于插件的数据源接入方案，插件框架提供多种数据传输协议接口、数据压缩与解压缩算法、数据加密与解密算法、数据库连接方法。可以应对未来日益增加的数据源接入需求。数据源的接口变化对应的数据源接入插件很容易即可适配，大大降低了增加新功能的成本。每个数据源接入插件都是一个独立的应用，不仅易于维护，也提高了平台的稳定性。

②插件化的数据清洗与标准化技术方案

基于插件的数据清洗与标准化方案，插件框架提供多种数据清洗方法、结构化数据处理方法、非结构化数据处理方法、数据校验方法等多种数据接口支持。未来随着业务发展，接入的数据源越来越多，错综复杂的异构数据不通过修改系统功能而通过编写插件进行数据清洗和数据标准化功能，极大的降低了维护成本。独立的插件作为平台中独立的应用运行。使平台的可维护性和稳定性得到了极大的提高。

（5）业务场景支持事件维度的态势分析、呈现和事件预警。

①基于样本的漏洞利用态势分析

漏洞数据、样本数据根据样本对漏洞利用情况进行挖掘分析，获取漏洞从公布到爆发再到利用的威胁态势。然后根据资产数据和漏洞数据的关联关系分析出漏洞的影响范围。从而跟踪漏洞的影响范围、利用情况、利用程度等态势信息。

②样本家族事件态势跟踪

使用知识图谱对样本数据和样本利用漏洞数据特征，通过聚类算法将样本抽象归类，获取样本家族信息。结合资产信息和设备日志、流量信息、威胁情报对样本家族的威胁事件进行追踪。使用威胁预警算法针对样本家族的威胁事件进行预警。

### 4.4 主要优势

（1）获得了 23 项已授权技术专利；

（2）参与威胁情报领域的国家标准《信息安全技术网络安全威胁信息格式规范》制定；

（3）获得多项国家级奖项；

（4）获得 Gartner、IDC 等多家权威机构推荐。

## 5 经济效益与社会效益

### 5.1 经济效益

在绿盟科技的客户中，已经使用了威胁情报的客户超过了 60%，威胁情报已经成为新一代安全的必备品，应用前景广阔。2017—2019 年，绿盟威胁情报连续 3 年销售额平均增长率超过 60%。

### 5.2 社会效益

通过情报赋能，大幅缩减威胁响应时间，新型威胁可达小时级甚至分钟级防御，通过情报，尤其是暗网 [3] 和黑客论坛监控，为数千家客户发现黑客攻击和敏感信息泄露等问题。向 8 家国家主管机构进行威胁情报上报，上报情报

总数超过 4 万条，累计上报原创漏洞 300 余个，获得 9 项优秀单位支撑奖项。

## 6 结 语

绿盟威胁情报解决方案已经在政府、运营商、金融、互联网、交通、教育医疗等行业得到广泛应用，威胁情报已经成为下一代安全的必备品。绿盟威胁情报解决方案极大扩展了威胁防御的时空边界，驱动了网络安全防御体系的全面升级。

**参考文献：**

[1] 斯科特·罗伯茨，利百加·布朗．情报驱动应急响应 [M]. 李柏松，李燕宏，译．北京：机械工业出版社，2018:13-14.

[2] Cyber Threat Intelligence Technical Committee. Structured Threat Information Expression (STIX™)[EB/OL].(2020-08-08)[2020-08-17].https://oasis-open.github.io/cti-documentation/stix/intro.

[3] Enterprise Risk Management Research Team.Market Guide for Security Threat Intelligence Products and Services[R].USA:Gartner,2020.

**作者简介：**

**赵 阳**（1983—），女，硕士，绿盟科技威胁情报产品经理，主要研究方向为威胁情报、应急响应。