绿盟全流量威胁分析解决方案

产品白皮书

■ 文档编号		■ 密级	完全公开
■ 版本编号	V1.0	■ 日期	2019-05-08

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，建立网络安全全流量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全流量监测通报平台。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。

2017 年 1 月，中央网络安全和信息化领导小组办公室下发关于印发《国家网络安全事件应急预案》的通知。通知指出编制目的是为了建立健全国家网络安全事件应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序。

2017 年 6 月，《中华人民共和国网络安全法》正式施行，它顺应了网络空间安全化、法制化的发展趋势，不仅对国内网络空间治理有重要的作用，也意味着建设网络强国、维护和保障我国国家网络安全的战略任务正在转化为一种可执行、可操作的制度性安排，标志着我国网络空间领域的发展和现代化治理迈出了坚实的一步。

1.2 当前挑战

1. 客户期望能够在原始流量分光/镜像场景下，通过部署单套设备即可发现网络中存在的各类安全问题；

2. 客户期望能够增加对安全场景的分析能力，以应对传统安全设备处理不了的 0day、APT 攻击等行为；

3. 当网络攻击事件发生后，客户期望能对攻击者进行分析，能够快速感知事件的影响范围；

4. 当事件发生后，客户期望可以溯源历史流量数据和 pcap 文件，从而分析还原黑客攻击的具体行为及过程。

5. 针对安全热点事件，客户期望能够快速感应现网系统中是否存在同类安全问题，并提供预防手段。

二. 绿盟全流量威胁分析解决方案

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，充分利用网络全流量、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。

关于未来的安全分析体系建设，Gartner 在 2017 年 6 月份举办的第 23 届 Gartner 安全与风险管理峰会上发布了十一大信息安全技术，其中一项就是网络流量分析技术，Gartner 对其的定义为：“网络流量分析解决方案融合了传统的基于规则的检测技术，以及机器学习和其他高级分析技术，它通过监控网络流量、连接和对象，找出恶意的行为迹象，尤其是失陷后的痕迹。”这充分说明了网络流量分析技术在应对安全威胁方面的重要性。

绿盟全流量威胁分析解决方案针对原始流量进行采集和监控，对流量信息进行深度还原、存储、查询和分析，可以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，保障重要信息系统的网络安全。

图 1 绿盟全流量威胁分析解决方案架构示意图

2.2 方案架构

绿盟全流量威胁分析解决方案整体架构分为四层，最底层是平台接入的各类数据源，这里主要包括实时的网络流量数据以及绿盟威胁情报中心（NTI）提供的威胁情报数据；数据中心层通过探针设备对镜像流量数据进行全流量采集及解析，并将采集到的原始流量数据及解析后的协议日志进行分类存储；数据分析层可以基于规则引擎、威胁情报能力来检测已知威胁，基于沙箱检测引擎、机器学习引擎来检测未知威胁，然后通过攻击链引擎对黑客的整个攻击环节进行关联，实现对高级威胁事件的全方位分析；最终，平台通过用户视角，将各类威胁事件与情报信息进行可视化呈现，主要包括威胁监控、业务监控、自定义场景、挖掘检索和情报分析等功能。

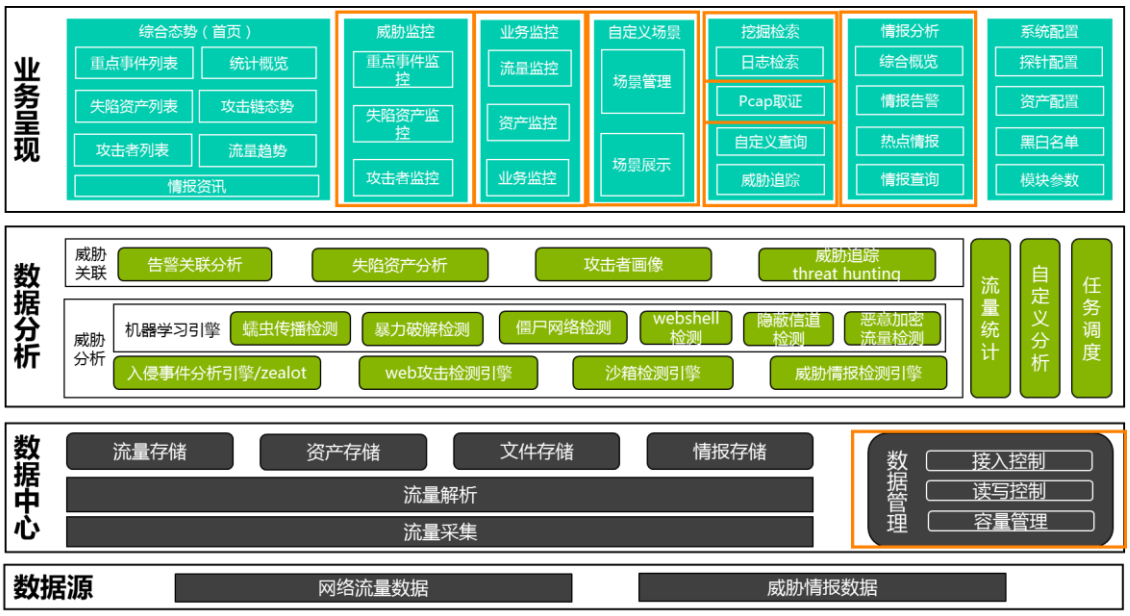

图 2 绿盟全流量威胁分析解决方案整体架构

2.3 方案组成

绿盟全流量威胁分析解决方案主要由四部分组成，分别是全流量分析探针（UTS）、高级威胁检测系统（TAC）、威胁情报系统（NTI）和全流量存储分析平台（TAM）。

图 3 绿盟全流量威胁分析解决方案组成部分

统一威胁探针（UTS）主要完成流量数据的采集、解析以及 pcap 数据的存储功能，并将解析完成后的元数据信息发送至 TAM 进行集中处理和分析。

威胁分析系统（TAC）提供恶意文件检测功能，基于沙箱检测引擎，可以动态虚拟执行各类文件及应用程序，并将检测结果上报至 TAM 进行进一步处理和分析。

威胁情报中心（NTI）提供威胁情报功能，通过与情报的有效结合，可以实时获取全球最新的热点事件和信息，大幅提升安全威胁事件的可信程度。

全流量威胁分析平台（TAM）是绿盟全流量威胁分析解决方案的核心，用于大数据分析。通过 TAM 平台可以对流量元数据进行加工和整理，利用其强大的大数据分析能力及各类机器学习算法，快速发现各类安全威胁及事件，也可以对历史事件进行回溯，准确把握事件发生的过程及影响。为了便于系统部署与集成，TAM 平台同时也向用户提供北向接口，可与绿盟云/第三方平台进行集成。

2.3.1 统一威胁探针（UTS）

统一威胁探针（UTS）主要实现流量数据的采集和解析工作，可以对流量数据进行逐层解码，将解析后的流量元数据上传至大数据平台，将原始流量 pcap 数据留存在本地硬盘。同

事，UTS 上也包含入侵检测、病毒检测及吸星等各类安全探针，可以提供安全威胁的检测能力。

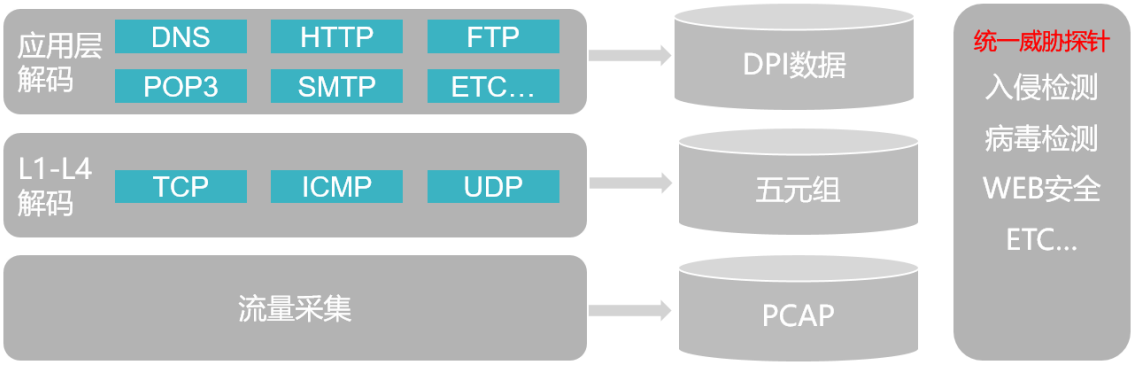

图 4 绿盟全流量威胁分析解决方案组成部分

1. 数据采集

数据采集模块通过千兆/万兆数据输入接口可以对原始分光/镜像流量进行实时采集，同时利用零拷贝、轮询、大页缓存、无锁执行等技术对数据包的捕获效能进行优化，以达到在高带宽网络中对流量数据高速稳定捕获的性能要求。

2. 数据解析

1）L1-L4 层协议解析

L1-L4 层协议解析模块可以对网络流量进行逐层解析，将传输层协议数据剥离出来，使其在会话重组过程中按照数据流的形式进行处理与管理。会话重组过程利用四元组区分会话，采用高并发会话重组技术，通过会话链接池以负载均衡的方式高效管理高并发会话，保证了数据的并发处理速度与效率。

2）应用层协议解析

应用层协议解析模块采用基于多模匹配的协议识别技术、基于解析模板的智能提取技术、基于流量特征的流识别技术等关键技术，对流量数据进行高效、完整、准确的协议类型识别与解析。通过全流量特征识别，针对接入的全部会话流，系统可以进行元数据解析及会话流相关统计，输出网络元数据及会话流统计信息。

3. pcap 数据存储

全量 pcap 包的存储功能是平台进行数据分析、数据回溯的基础。UTS 探针共输出两类数据，一类是流量元数据，一类是全量 pcap 包。流量元数据记录流量中的主要信息，主要用于威胁分析、流量监控、挖掘检索等功能，是后续大数据分析的主要输入，以 http 访问为例，流量元数据主要记录会话中的时间戳、五元组、http 头部等关键字段。全量 pcap 包则是记录原始流量中的全部信息，会将整个包的内容 1:1 地存储下来，主要用于 pcap 包取证。

2.3.2 威胁分析系统（TAC）

绿盟威胁分析系统（TAC）可以精确检测通过网页、电子邮件或文件共享方式试图进入内部网络的恶意软件，包括 0day 攻击及具有抗检测能力的高级恶意软件。当前的恶意软件大多具备强大的抗逃避能力，而 APT 攻击还可能使用 0day 攻击的方式，传统的防病毒引擎很难发现它们。TAC 通过新型的虚拟执行检测技术可以有效发现这些攻击行为，帮助客户有效的遏制由此带来的风险，如敏感信息泄露、业务中断等。同时，TAC 将虚拟执行的结果上报至 TAM 进行进一步分关联的分析。

TAC 产品具有如下特点：

1. 检测已知和 0day 攻击，抗逃避能力强：基于不依赖已知攻击特征的虚拟执行技术，可以检测利用 0day 漏洞以及其它传统防病毒引擎无法检测的高级恶意软件。不同于沙箱技术仅在行为层面进行检测，可以通过内存指令级分析，在漏洞利用阶段发现攻击，对抗针对沙箱技术的逃避技术。

2. 检测恶意软件全生命周期活动：对恶意软件在终端的整个活动进行分析，跟踪漏洞利用、软件下载、回连命令控制服务器外传数据等恶意软件各阶段的活动行为，并输出详细的入侵行为报告。

3. 分析应用协议及文件类型全面：覆盖主要的传输协议：http、smtp、pop3、ftp 等，同时可以对黑客利用的主要文件类型全面检测，包括 Office 文档、PDF、Flash 等，并可对压缩文件进行检测。

4. 检测精确：基于恶意软件在模拟环境下运行的真实行为做判断，误报的几率可以忽略不计，使安全专家聚焦响应真正的威胁，保障安全运维的效率和效果。

5. 多引擎集成，提供事件响应的优先排序：集成多种传统检测引擎，可以通过报警比对等方式了解威胁的严重程度，确定事件响应的优先级。并同时面对传统恶意软件提供更高的检测能力。

6. 提供闭环的纵深解决方案：通过二级信誉系统（企业本地信誉库、全球信誉库）联动 IPS，自动化阻截恶意软件的下载及回连活动，保障防御的及时性。同时提供事件的关联分析、攻击的地理位置视图等先进的可视化能力，更直观的了解威胁态势。

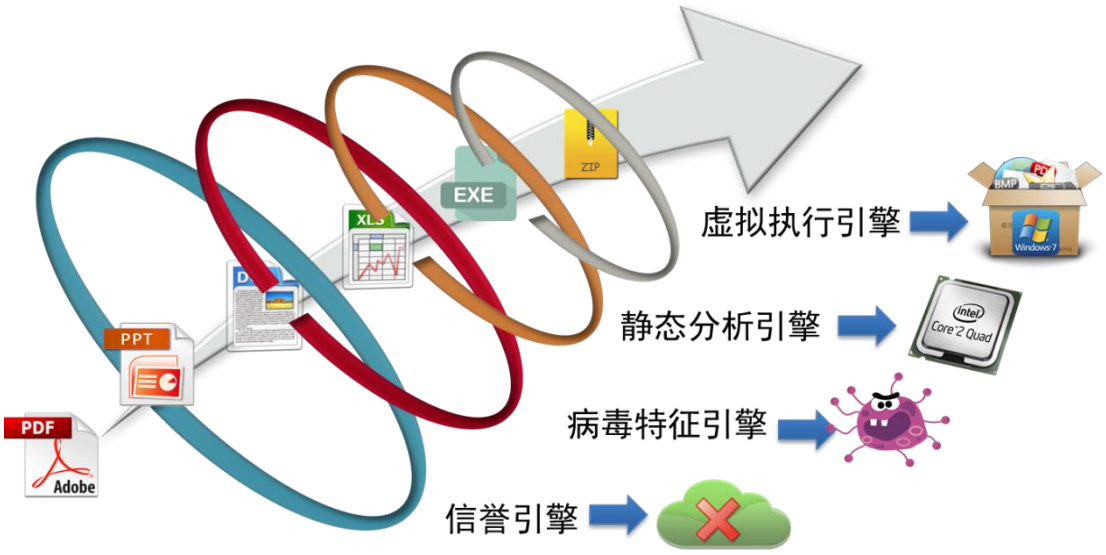

图 5 威胁分析系统多重检测引擎

2.3.3 威胁情报中心（NTI）

威胁情报中心（NTI）为 TAM 平台提供全球威胁情报信息支持，情报类型包括 C2 情报、热点事件、恶意样本、恶意 URL、恶意 IP、恶意域名等，也支持用户自定义的情报信息的导入。TAM 接入流量信息后，会匹配威胁情报进行威胁检测，命中情报信息后，可以跳转到 NTI portal 查询情报的详情，例如恶意度评分、端口开放、历史恶意行为以及关联的 ip、样本等。

NTI 依托绿盟在安全领域的长期积累，已经建立了比较完善的威胁情报生产和应用体系。在情报源上，不仅包含绿盟高质量的漏洞等安全数据库和安全设备脱密数据，还包括互联网数据的全面采集和第三方安全企业、情报机构的广泛合作和情报共享；在情报处理上，基于绿盟大数据分析平台对数据和情报进行深度挖掘，同时也结合情报专家和安全专家的丰富经验进行高级情报的分析；输出的威胁情报不仅包括网络资产的基础信息、指纹、漏洞、信誉等基础情报，也包括 TTP、高级威胁分析、资产威胁分析、行业威胁分析等高级情报；在情报的输出使用上，采用 Portal 查询、API 接口、邮件推送等多种方式共享威胁情报，支撑客户的安全预警、资产监控、产品联动、威胁响应、安全运营等核心业务。

2.3.4 全流量数据分析系统（TAM）

绿盟全流量高级威胁分析系统（TAM）是一套基于大数据技术，采集用户原始流量，并实现应用层流量还原、安全场景分析，为高级威胁分析提供数据支撑的平台系统，目的是为客户提供尽可能准确的“结果”。

TAM 具备全流量分析功能，利用其机器学习引擎和规则检测能力，可以及时发现网络安全事件线索，及时检测病毒木马、网络攻击等安全事件情况；TAM 具备全流量关联和取证功能，能够从多维度多角度进行长时间跨度的关联分析，同时系统提供渐进式安全事件分析和取证；TAM 具备特定安全场景分析能力，能够快速实现客户提出的一些安全场景并进行场景分析。

1. 事件场景分析

1）重点事件分析

系统可以对事件告警进行关联分析并输出用户关注的重点事件，如热点事件、apt 攻击事件、Botnet 事件、恶意样本传播事件或是单次高危攻击事件等（webshell、隐蔽信道）。同时，用户也可以根据自身业务特点自定义事件类型进行输出，帮助用户从海量告警中快速发现需要处理的重点事件。

2）失陷资产分析

平台可以结合攻击方向、攻击类型等维度对失陷资产进行判断，从资产角度出发，结合攻击链模型向用户展示失陷资产的总体情况，帮助客户从海量告警事件中，快速定位需要关注和处理的资产。

3）攻击者画像

系统可以从攻击者的角度出发，为客户梳理出对网络最具威胁的攻击者，通过情报关联功能，追溯攻击者的相关信息，聚合攻击者在客户网络中的攻击行为和通信行为，增加攻击事件可信度，客户可以通过攻击者画像分析，回溯事件源头，从根本上处置类似攻击事件的发生。

2. 数据回溯及 pcap 包取证

当系统检测规则落后于攻击行为，特别是 0day 攻击发生后，用户需要通过数据回溯分析，来检测出以往系统漏检的一些重要攻击行为信息。系统通过情报或用户自定义规则作为输入，可以对历史流量数据进行回溯，并将回溯检测结果保存在单独的存储空间中，打上特定的标签，以便和实时检测结果进行区分。

基于数据回溯功能，系统提供 pcap 包取证能力。用户可以通过查看流量日志进行 pcap 包取证，也支持以事件下钻的方式，自动关联出攻击告警相关的 pcap 包信息。用户还可以手动设置条件，查询自己关心的流量，对历史流量进行精确下载。

三. 方案创新与价值

3.1 全流量数据采集能力

该方案在全流量数据采集方面应用了一系列关键机制来提高数据采集能力，最大限度地优化了数据捕获方式和数据包处理性能，使之既能满足大流量安全场景下各类数据采集的完整性，又能有效提升设备的使用效率。

3.2 全流量数据存储能力

影响全流量数据存储的最大问题是性能和空间。该方案在数据采集后，通过白名单、多通道、数据压缩、反序列化等方法，最大程度地提高了数据的存储效率。由于流量元数据和全量 pcap 包的使用场景不同，所以在存储过程中对上述两种数据也进行了分开存储。流量元数据信息通过 UTS 解码之后，直接发送到 TAM 平台侧进行存储和后续利用；而全量 pcap 包平时只保存在 UTS 探针内部，当用户进行 pcap 取证时，TAM 会按照规则调取 UTS 中的 pcap 数据到自身平台中，供用户下载使用。

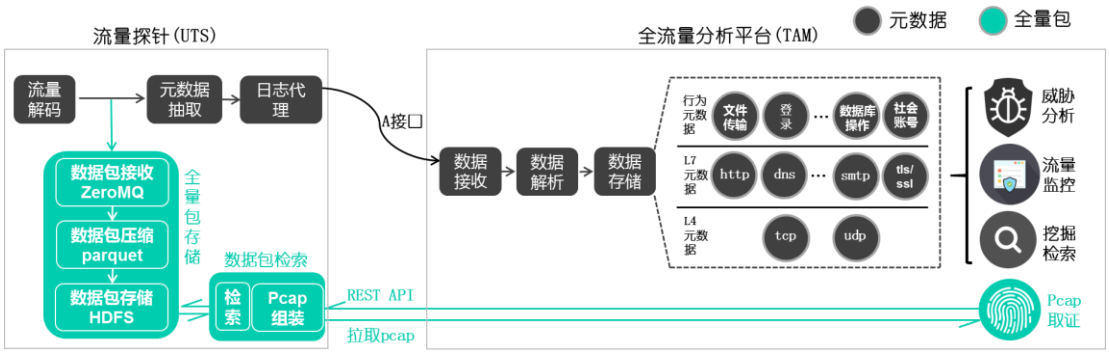

图 10 元数据与全量包的数据存储方式

3.3 安全大数据分析能力

在海量安全数据中，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。但是面对海量的网络流量、安全日志、威胁情报、环境信息等，按照传统方式利用数据库进行数据挖掘、安全分析将变得极端困难，更无法形成有效的安全态势感知能力。

该方案利用绿盟科技多年来在网络安全方面的研究和积累，提出了多种适用于流量场景下的安全分析模型，同时利用绿盟科技在大数据分析方面的技术能力，合力形成了安全大数据分析技术，使得绿盟科技能够将自身的安全业务能力充分落地到平台建设中。

3.4 热点事件回溯能力

热点事件细分为漏洞披露和样本披露两种场景。漏洞披露之后，对安全厂商和攻击者来说都是可见的，此时双方存在“时间赛跑”，使用传统方案，在检测规则出来之前，很有可能出现攻击漏检的问题。而对样本披露来说，对安全厂商和攻击者也都是可见的，此时容易打草惊蛇，攻击者会做出应对，使用传统方案，检测规则可能失效，或者攻击者切断样本通信，使得事件影响无法深入调查。

该方案中，基于全流量数据存储，其对热点事件的回溯能力可以很好的解决传统方案的局限性。在重大漏洞应急时可以排查资产漏洞利用情况，做到“零时间风险窗口”的快速响应；在样本披露发生时，可以提供抵御攻击者的应变手段，并且基于恶意样本历史通信流量，做事件的深入调查。

3.5 威胁情报关联分析能力

绿盟威胁情报中心依赖多年的安全经验和情报数据积累，可为用户提供及时准确的威胁情报数据。通过威胁情报关联分析，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。