聚铭铭察高级威胁检测系统

产品白皮书

聚铭网络科技有限公司

2024 年 04 月

目录

声明

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司和北京聚铭信安科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系聚铭网络技术服务部。

联系信息

北京总部：北京市海淀区丹棱街 18 号创富大厦 9 层

南京总部：南京市雨花台区软件大道 180 号南京大数据产业基地 7 栋 4 层

电　　话：025-52205520/52205570

传　　真：025-52205565

全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

聚铭网络技术服务以及营销网络覆盖全国，并在各地设有办事处和分支机构，为客户提供无微不至的解决方案和高效的服务支持。聚铭专家团队 7x24 小时全天候在线，确保在安全事件发生时提供分钟级应急响应。

1.产品概述

聚铭铭察高级威胁检测系统（iATD）结合失陷分析、威胁情报分析、入侵检测分析、异常行为分析、病毒木马分析、未知威胁检测等多种技术于一体，对网络中的南北流量/东西流量进行全面深度威胁检测与溯源分析。产品基于资产、威胁事件、网络会话、威胁情报等多源数据进行对全网流量实时进行威胁感知、可疑流量分析,为客户在高级威胁入侵时,及时察觉,及时止损。

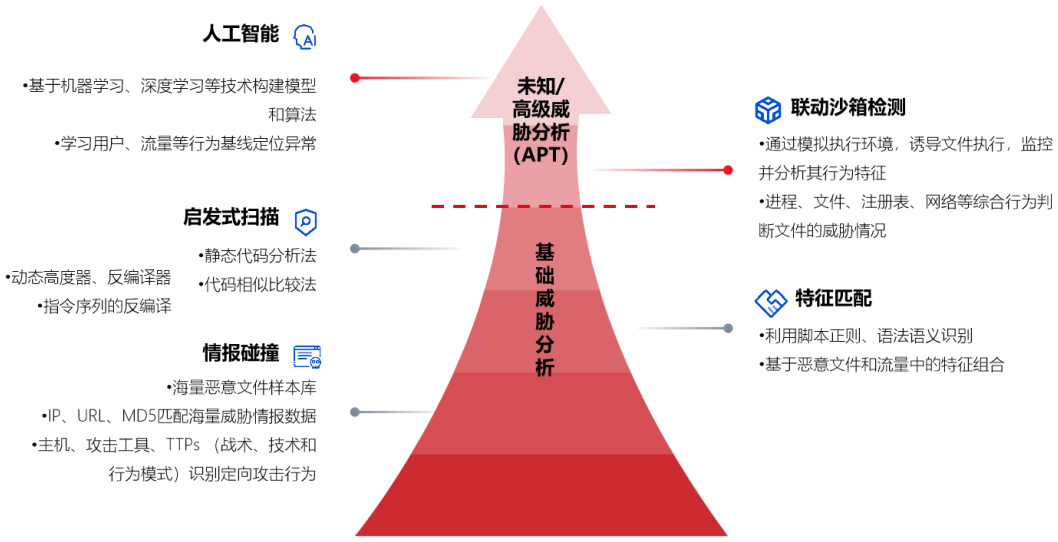

图 1.1 铭察高级威胁检测系统

产品除了具备常规的入侵检测功能外，还可以从网络流量中还原出文件（HTTP、SMTP、POP3、IMAP、FTP、SMB 等协议）并通过多病毒检测引擎有效识别出病毒、木马等已知威胁/未知威胁。系统采用零拷贝技术，实现高速流量接入。实时进行会话重建、协议识别、异常协议检测等功能。

产品结合失陷分析、网络攻击检测、威胁情报分析、异常流量行为挖掘、文件检测、隐蔽通道检测、域名异常检测等技术，对全网流量实时进行威胁感知、可疑流量分析。

2.产品架构

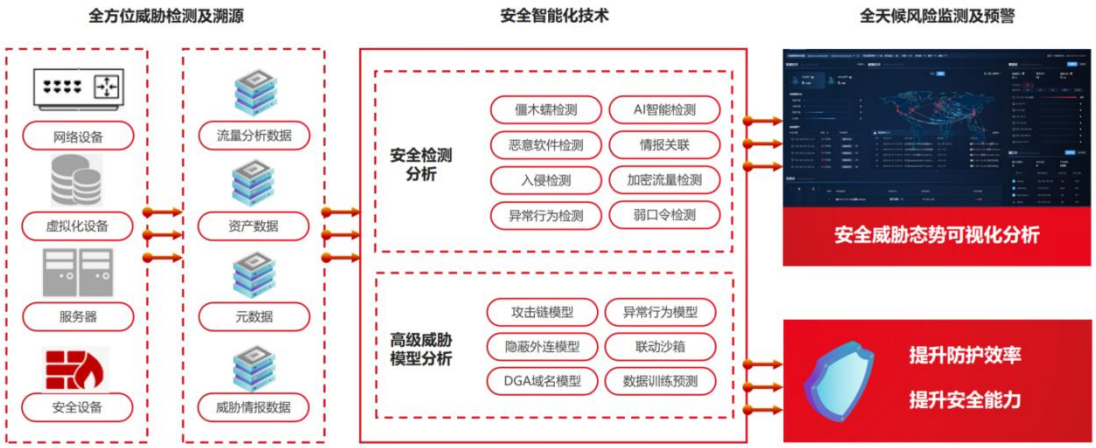

图 2.1 铭察高级威胁检测系统架构图

产品系统架构如图 2.1 所示，监听口接收镜像/分光流量，通过流量采集引擎对数据包进行快速处理以及硬件资源调度。通过筛选引擎过滤不关注的数据，将过滤后的数据进行二次处理，分别进行特征检测、元数据提取、文件提取、流量存储处理等。通过特征检测引擎检测基于特征的已知攻击，通过元数据、文件提取实现检测数据预处理，通过流量存储实现数据留存取证。之后通过将元数据和事件进行泛化处理，结合失陷分析、网络攻击检测、威胁情报分析、异常流量行为挖掘、文件检测、隐蔽通道检测、域名异常检测等技术，对全网流量实时进行威胁感知、可疑流量分析，并以大屏的方式展现。

3.产品功能

3.1.流量采集

产品通过旁路镜像、高性能采集网络流量，可将采集到的网络流量进行协议解析后并以元数据的形式存储，通过网络协议实时解码、元数据提取，建立完整的日志、协议、数据包全字段索引库，以便于快速提取多维度的网络元数据进行检测与分析，为后续异常数据挖掘、分析、取证建立牢靠的基础。

产品支持对 2-7 层协议进行识别和元数据提取，可解析还原 DNS、FTP、HTTP、IMAP、POP3、SMB、SMTP、ICMP 等协议并以元数据形式存储，用于威胁的溯源取证。

3.2.文件还原

产品支持识别网络流量中的 HTTP、SMTP、IMAP、POP3、FTP、SMB 等多种协议识别，并提取流量中的原始文件，如 DOC、DOCX、PPT、PPTX、XLS、PDF 等文件，通过多维度检测模块进行检测与分析。

3.3.威胁检测

3.3.1.下一代入侵检测

下一代入侵检测模块有效弥补目前安全设备（防火墙、IDS、IPS 等）对攻击识别能力的不足，针对暴力破解、反弹 Shell、本地提权、恶意命令执行、SQL 注入、XSS 注入、跨站请求伪造、Webshell 上传、文件包含漏洞、远程代码执行漏洞等行为进行监控，保证能够实时发现失陷主机，对入侵行为进行告警，精确识别应用、内容和环境等各层面攻击，帮助用户分析入侵行为的攻击链路和了解整体环境的入侵情况，从而让用户精准有效的发现威胁并解决问题。

3.3.2.网络异常行为检测

通过对网络流量双向会话行为的深入分析，发现网络中存在的 DoS/DDoS 攻击、扫描等异常行为、会话连接异常行为、反序列化攻击行为、远程命令执行行为、尝试提权成功行为、Struts2 攻击成功事件行为、成功权限提升行为、路由跟踪行为、密码猜测行为、密码暴力破解等行为，即刻发出告警，降低潜在的网络安全风险。

3.3.3.静态文件检测

静态文件检测指在不运行程序的情况下，对样本文件进行静态特征检测。产品内置多个反病毒引擎，支持多个反病毒引擎交叉检测，可检测包括 Shellcode、Webshell、后门程序、挖矿木马、间谍软件、蠕虫病毒、恶意软件、远程木马等，对已知威胁进行基于特征的静态检测和多检测模块交叉验证，最终给出检测结果。

3.3.4.联动沙箱检测

联动沙箱检测是一种通过文件的动态执行行为来识别恶意文件的检测技术，铭察高级威胁检测系统还原未知威胁文件，将文件传递到沙箱进行分析，其利用虚拟化技术仿真出组织常用的操作系统和应用环境，然后利用虚拟执行手段使文件运行并捕获其对系统产生的影响，如释放文件、加密文档、增加启动项、API 调用等，并对这些影响进行评估，识别对系统产生破坏的恶意文件；动态沙箱支持行为签名检测，根据主机或网络行为判断其是否为恶意文件，支持多种沙箱运行模式,包括 Windows、Android 和 Linux 等类型沙箱，单设备支持至少 10 个沙箱，支持对沙箱内样本的流量进行检测、支持反虚拟机和反调试行为检测、支持恶意代码及变种检测，最大限度发现 APT 等未知网络攻击。

联动沙箱检测是一种高效且可靠的恶意文件识别技术。通过结合铭察高级威胁检测系统和沙箱环境，它能够在不影响实际系统安全的前提下，准确识别并应对各种未知的威胁文件。

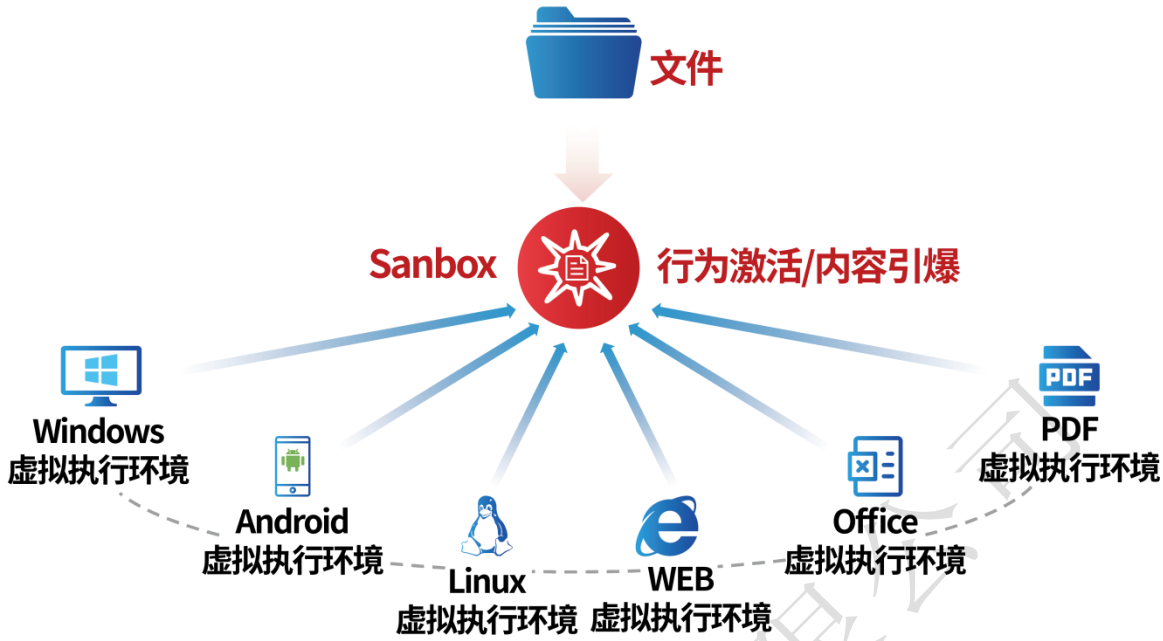

图 3.1 联动沙箱检测可“引爆”的内容

3.3.5.威胁情报检测

通过海量情报数据的采集、分析、验证及生命周期管理后生成威胁情报并内嵌于系统中形成情报中心，并将从流量中提取出的域名、IP、URL 等与系统内置情报进行关联比对，进一步确认网络威胁，辅助各行业安全运营人员进行运营决策。

3.3.6.人工智能检测

传统的基于特征的检测手段，如 IDS 或杀毒软件无法及时有效的应对新产生或手段高明的网络攻击，而人工智能具备对全新威胁的适应及预测能力，可以更加智能、精准地发现 APT 等未知威胁。

3.4.威胁分析

3.4.1.关联分析

产品基于 Kill Chain 框架，从多个攻击点位进行检测，同时不仅从流量层面

进行检测，也从文件层面进行检测，基于不同攻击阶段的检测模式，以实现对扫描探测、网络钓鱼、漏洞利用、木马下载、远程控制、横向渗透、行动收割等攻击阶段的全覆盖,可帮助用户发现更多的攻击威胁事件，减少盲点，更可将不同阶段的攻击事件进行串联，方便用户判断攻击进行到什么阶段以及溯源攻击的过程。

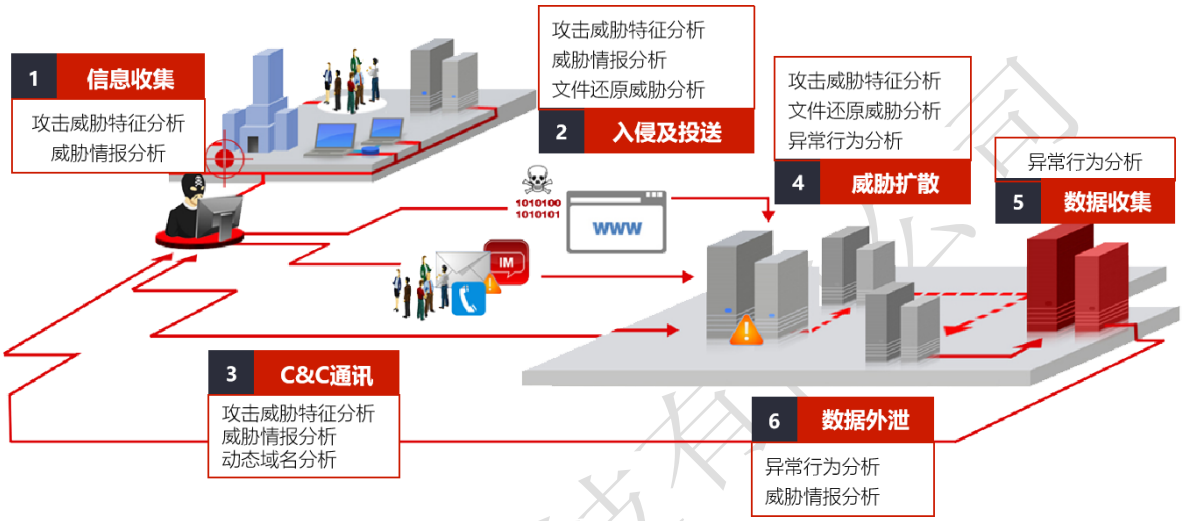

图 3.2 攻击链关联分析

3.4.2.资产风险分析

用户可利用系统对组织内资产进行标记，标记资产的类型、部门、重要程度、资产组、实现确信度、威胁等级、处理状态、风险主机（IP、MAC 地址、制造商、软件信息以及设备类型等）、设备类型等。重点资产监控功能对标记的资产进行分类统计，并将资产与告警策略关联，并对资产威胁精准分析，快速决策哪些重要资产需要及时处置，保护用户的资产。

3.5.溯源取证

3.5.1.事件追溯

事件追溯通过追溯攻击行为的整个过程，查找攻击源和被攻击目标，明确攻击阶段，查看攻击结果，详细了解攻击的整体情况。

针对溯源取证，系统一方面提供了多源威胁情报库，提供攻击和恶意代码家族相关的背景信息的检索和分析，另一方面从监控整体威胁事件态势，从内对内，外对内和内对外三个方向进行描述。

当发生新型、热点攻击等突发事件时，如近期的勒索病毒爆发，需要对攻击事件的详细信息进行溯源分析，对攻击源、攻击过程、攻击扩散面、被攻击的业务系统、攻击的恶意软件功能和危害等情况进行深入的分析，帮助用户更好的判定攻击的性质、手段和影响，从而确定合理的应对措施。追溯的目的是搞清楚真实情况后进行合理响应并制定相应的应对措施。

3.5.2.元数据追溯

文件系统中的数据分为数据和元数据。数据是指普通文件中的实际数据，而元数据指用来描述一个文件的特征的系统数据。产品支持网络流量协议元数据提取、解析、存储和检索展示。系统支持元数据追溯，可展示威胁主机的数量情况，可按照威胁主机威胁事件、威胁日志、文件检测数据、协议元数据进行检索、也可按照关注和可选字段进行相关检索。

3.5.3.流量采集存储

通过对网络流量采集存储、全数据分析，可用于对威胁的进一步溯源取证。系统支持抓包策略配置，并支持深度包解析、BPF 规则过滤功能，对关键网络流量进行原始 PCAP 留存，用于威胁溯源分析和网络攻击取证，追溯网络攻击的线索、攻击过程信息、发现威胁源头并留存攻击证据。

3.6.威胁态势

产品支持威胁态势大屏展示，包括综合态势感知、资产态势、威胁事件态势、攻击者态势、外联风险态势、横向威胁态势。综合安全态势展示用户最关心的告警层风险内容，包括告警分析和风险主机分析，支持风险威胁地图切换；资产态势监控资产整体态势，展示终端和服务器资产的风险情况和脆弱性；威胁事件态势监控整体威胁事件态势，从外对内、内对外、内对内三个方面来进行描述，对

内网中的威胁事件进行实时监控；攻击者态势监控外部对内部资产的攻击事件态势，直观展示外部攻击源（国家/城市)、攻击手段和被攻击的资产情况；外联风险态势监控内部资产的风险外联态势，直观展示外联的类型、趋势、影响的内部资产范围情况；横向攻击态势监控内部资产之间的威胁态势，发现内部威胁源以及影响的范围；利用不同的检测方法和威胁分析能力对网络流量进行分析挖掘，进而展示安全数据从接入流量、元数据/日志、威胁事件、告警 APT 几个层级的收敛和降噪的成果。

4.产品特点

4.1.人工智能检测技术

4.1.1.恶意加密流量检测

为了确保通信安全和隐私以及应对各种窃听和中间人攻击，HTTPS 逐渐全面普及，越来越多的网络流量也被加密，然而，攻击者也可以通过这种方式来隐藏自己的信息和行踪，通过给恶意流量封装上一层名为 TLS/SSL 的加密协议来将其伪装成正常流量进行传输，逃避传统安全设备的检测。

恶意加密流量及合法加密流量有不同的流量行为模式，根据对恶意加密流量的分析，提取恶意加密流量与合法加密流量的 SPL 数据（数据包长度与数据包到达间隔时间顺序）、流量相关的 DNS 元数据、TLS 元数据、HTTP 元数据，构造用于识别恶意加密流量模式的向量，采用集成学习算法学习流量向量建立相应的加密流量检测模型，实现对恶意加密流量的识别，有效发现高级威胁的相关线索。

4.1.2.隐蔽隧道检测

隐蔽隧道是绕过防火墙屏蔽的一种通信方式，防火墙两端的数据包，通过防火墙所允许的协议类型及端口进行封装，然后穿过防火墙，与对方进行通信，当被封装的数据包到达目的地后进行数据还原。

DNS Tunneling，是隐蔽隧道的一种，通过将其他协议或数据封装在 DNS 协议中传输建立隐蔽通信。产品支持 DNS 隐蔽隧道通信检测，基于隧道工具的 DNS 隐蔽隧道；DNS 直连隧道；APT32 利用 DNS 隧道通信；基于 DNS 隐蔽隧道关联分析发现受控主机;支持 ICMP 隐蔽隧道通信检测，利用 ICMP 隧道违规突破内网 WEB 访问，利用 ICMP 隧道传输数据，利用 ICMP 隧道进行远程控制；支持 HTTP 隐蔽隧道通信检测,采用基于 AI 的检测技术，可有效提升对网络隐蔽隧道流量中恶意通信行为的检出率和准确率。

4.1.3.DGA 域名检测

DGA (Domain Generation Algorithm)，域名生成算法，恶意代码里不写入域名字符串，而是使用一个私有的随机字符串生成算法，按照日期或者其他随机种子，每天生成一些随机字符串然后用其中的一些当作 C&C 域名。

产品支持 DGA 域名人工智能检测，通过建立针对 DGA 生成域名的集成学习模型，用海量 DGA 生成域名和正常域名样本通过集成学习模型进行训练，使集成学习模型具备识别 DGA 域名能力。在捕捉到网络流量中的域名信息后，将之输入深度学习模型进行识别，集成学习模型输出该域名是否为 DGA 生成的域名，进而准确定位受控主机。

4.1.4.WEB 攻击检测

在 WEB 应用攻击检测过程中，基本是依赖于规则的黑名单检测机制，无论是 WEB 应用防火墙或 IDS 等，主要依赖于检测引擎内置的正则规则，进行报文的匹配。

基于人工智能的 WEB 攻击检测技术支持 SQL 注入攻击检测，XSS 攻击检测；Webshell 攻击检测，包括 PHP/ASP/JSP 动态脚本的 Webshell 上传，检测冰蝎、蚁剑等加密 Webshell 通信，检测 Webshell 通信行为；基于机器学习的新一代 WEB 攻击检测技术弥补了传统规则集方法的不足，有效检测新型 WEB 攻击行为。

4.2.威胁情报检测技术

通过自有情报产出、商业情报购买、产品协同联动、开源情报获取等协作方式，输出可用于威胁检测的最新情报数据，系统内置威胁情报检测模块，包括：IP、域名、URL、文件 Hash 和漏洞等。

4.3.攻击链检测技术

Kill Chain 是由洛克希德-马丁公司提出的网络攻击模型，用于分析网络攻击

过程。产品基于模型将攻击分为七个阶段，包括从扫描探测、尝试攻击、漏洞利用、木马下载、远程控制、横向渗透、行动收割，通过这七个阶段可以掌握攻击者的攻击战术和攻击过程。

产品汇聚不同层次的攻击事件后，将所有的事件按 Kill Chain 的不同阶段进行主机事件关联，并展示到可视化的 Kill Chain 攻击链中，同时提供丰富的筛选条件，以便用户对各个阶段的数据进行深度分析,可帮助用户快速确认攻击阶段，并判断攻击是否成功。

4.4.综合溯源取证能力

溯源能力覆盖攻击链各阶段，可留存原始网络流量 PCAP。支持对网络攻击线索、攻击过程、攻击手段和主机威胁等信息进行溯源，发现威胁源头并留存攻击证据。通过对威胁事件、元数据、威胁情报以及原始会话数据包追溯，支撑安全运营人员威胁发现、威胁研判和威胁取证的全过程工作。

5.客户价值

5.1.高级威胁的精准检测

聚铭铭察高级威胁检测系统（iATD）可以快速并精准发现网络威胁攻击，准确率高，误报率低，具备检测已知威胁、未知威胁的全流程检测能力。

5.2.重大安全事件的快速响应

基于威胁情报的上下文，聚铭铭察高级威胁检测系统（iATD）可以帮助安全运营人员发现、研判重大安全事件，如：永恒之蓝、APT 事件。

5.3.网络攻击的回溯和分析

聚铭铭察高级威胁检测系统（iATD）还原和存储网络流量的元数据，可以帮助用户回溯已经发生网络攻击行为，分析攻击路径、受感染面和信息泄露状况。

5.4.满足新等保的合规要求

聚铭铭察高级威胁检测系统（iATD）满足了新等保 2.0 对网络攻击检测和分析要求，特别是针对新型网络攻击和 APT 攻击。