2022

技术白皮书

天阗高级持续性威胁检测与管理系统 V2.0

威胁分析一体机

（TAR-AIO）

启明星辰 领航信息安全 Venus

目录

一. 引言

1.1 背景

1.1.1 网络安全法制化建设稳步推进，数据安全逐渐成为焦点

习近平总书记指出：“安全是发展的前提，发展是安全的保障”。这表明在塑造数字化发展这个新“动力系统”的同时，也要注重实现网络和数据安全的“制动系统”。唯有如此，才能形成健康、良性、高质量的数字化发展新格局。

网络安全法的正式施行，标志着我国网络安全纳入法制化轨道。等级保护 2.0 相关标准的正式实施，构成了国家网络安全保障的基本制度、基本策略和基本方法。2021 年 7 月，国家互联网信息办公室发布《网络安全审查办法（修订草案征求意见稿）》，从关键信息基础设施到供应链安全等多角度维护国家安全。同月，工业和信息化部、国家互联网信息办公室、公安部联合印发了《网络产品安全漏洞管理规定》，自 2021 年 9 月 1 日起施行。该规定的施行将推动网络产品安全漏洞管理工作的制度化、规范化、法治化，引导建设规范有序、充满活力的漏洞收集和发布渠道，防范网络安全重大风险，保障国家网络安全。特别值得一提的是 2021 年 9 月 1 日即将施行的《中华人民共和国数据安全法》，它的颁布和实施为规范数据处理活动、保障数据安全、促进数据开发利用提供了法律依据。同时标志着数据安全正逐渐成为焦点，并已经成为国家战略层面的重要考量。经过近几年的发展，针对数据安全的各项保障工作逐渐取得成效。

我们相信，随着相关法律法规的不断落地以及相关技术的不断成熟，我国网络安全治理能力和数据安全保障水平将会不断迈上新的台阶。

1.1.2 威胁框架进入“攻防兼备”新阶段，并逐渐成为网络安全行业的风向标

过去一年多，以 ATT&CK 为代表的威胁框架热度不减，并逐渐进入“攻防兼备”的新阶段。

2020 年 1 月 7 日，MITRE 发布 ATT&CK For ICS 知识库。ATT&CK For ICS 首次成功描绘了针对工控系统的攻击所涉及的技术，为关键信息基础设施和其他使用工业控制系统的组织评估网络风险提供了重要参考。

2020 年 10 月，MITRE 发布 ATT&CK v8 版本，将 PRE-ATT&CK 替代为新的侦察和资源开发两个战术，较上一版本更加完整地描绘了攻击者针对传统 IT 系统的攻击过程。

2021 年 4 月，MITRE 发布 ATT&CK v9 版本，新增了 ATT&CK for Containers，首次描绘出针对 Kubernetes 和 Docker 的攻击技术。

随着近几年的发展，以红方视角为主的威胁框架逐渐完善，但网络安全防护领域的知识库始终缺失。2014 年 NIST 发布的网络安全框架 CSF 提供了用于管理网络安全风险的通用语言和系统方法，但其更像一个面向合规的方法论，缺乏真正可落地实践的基础。

在此背景下，2020 年 8 月，MITRE 发布了用于主动防御的实战型指导框架：MITRE Shield。该框架是基于对真实攻防对抗环境所涉及的主动防御战术、技术提炼而成的知识库，包括了引导、收集、控制、检测、破坏、促进、合法化、测试 8 大战术和 33 种技术。Shield 提供了针对 ATT&CK 攻击技术对应防御技术的映射，防御者可以利用 ATT&CK 威胁框架分析攻击者的技战术，同时利用 Shield 知识库部署网络防御设施。MITRE Shield 知识库虽然较 CSF 网络安全框架显得更“接地气”，但其每个具体防御技术仍然不够具体细化，缺乏可落地性。

2021 年 6 月，NSA 协助 MITRE 发布了 D3FEND 框架，D3FEND 作为 ATT&CK 的重要补充提供了对抗常见攻击技术的方法模型，并将每一项防御技

术与 ATT&CK 模型中的攻击技术相对应。与 MITRE Shield 不同的是，D3FEND 以数字工件本体作为概念化与实例化关系的基础，建立攻击技术和防御技术之间的关联。以 DNS 网络流量数字工件为例，其关联的防御技术（左侧）与关联的攻击技术（右侧）如下：

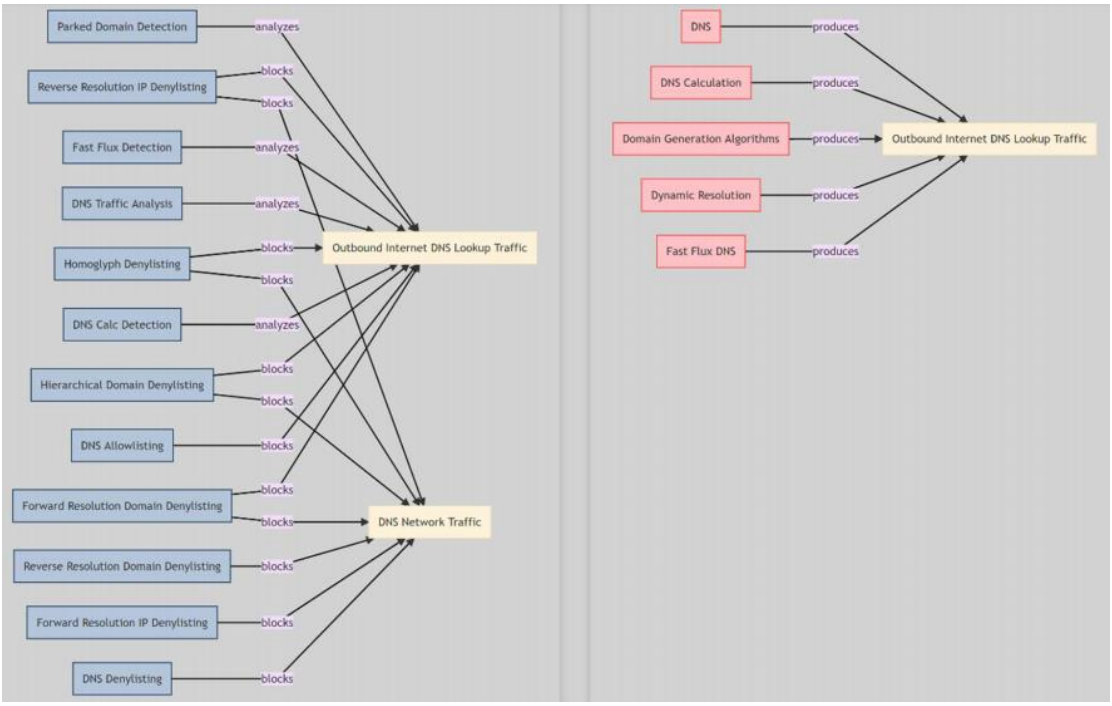


图 1_ D3Fend 框架 DNS 网络流量数字工件

1.1.3 Log4j2 远程代码执行漏洞扩散，供应链安全脆弱性受广泛关注

同往年相比，2021 年漏洞数量增长放缓，但并不意味着来自互联网的危害因此而降低，相反，漏洞公开的数量放缓某种程度上意味着更多的漏洞有可能选择被武器化，而选择不进行公开。

年底披露的 Log4j2 漏洞一经发布，震动整个国内外的安全行业，甚至整个国内外的 IT 界，使用该组件的应用极为广泛，导致无数引用该组件的系统和开源组件受到波及。随着 Log4j2 远程代码执行漏洞的扩散，供应链安全的脆弱性再次受到广大厂商们的关注。在整个供应链中，大批供应商在开发程序时选择引入第三方库，有的项目甚至引入上百个之多，而这些第三方库一旦某一个存在安

全问题，就会让企业暴露在安全风险之下，有可能导致企业重要系统被植入勒索病毒、服务器崩溃、用户数据及员工个人信息泄露，甚至是企业商业机密泄露等风险，从而引发无穷的隐患。

此漏洞对整个互联网带来极大安全威胁，直接动摇了以 Java 技术栈为重要组成部分的网络应用安全基础，堪比 2017 年核弹级漏洞“永恒之蓝”，大量的恶意代码已经将其纳入攻击传播的手段之一。

如果把 2017 年 5 月 12 日的“永恒之蓝”漏洞所导致的“WannaCry”勒索蠕虫事件比作一次互联网核爆攻击，那么，由于 Log4j 在基础设施和应用程序中的大量使用，2021 年 12 月 9 日由 Log4Shell 漏洞引发的一大波网络攻击则可以比作是一次脏弹攻击，不仅在攻击的当时造成严重杀伤，还会在未来相当长的时间（以十年计）持续地对我们的网络安全形成威胁。

减少漏洞是避免安全事件发生的根源，这就要求开发人员在掌握编程能力的同时，还应具备安全开发意识。开发人员不仅需要熟悉 CWE TOP25（MITRE 公布的前 25 个最危险软件安全缺陷知识库）漏洞的成因及危害，还应将安全性测试环节添加到软件的开发过程中，使得项目具备 DevSecOps 能力，至少应在软件开发过程中增加代码审计工程师或代码审计工具对代码进行审计。只有提升漏洞管理效率，才是高效的安全处理法则。

1.1.4 网络犯罪产业链逐渐成型，地下黑产技术“深度融合”

随着 RaaS（勒索软件即服务）、MaaS（恶意软件即服务）等模式的发展，网络犯罪产业链逐渐成型。网络犯罪过程中的任何环节都能找到相应的服务，网络犯罪团伙俨然已经成为一个协作有序、相互匿名的项目团队。在日益成熟的网络犯罪产业链下，地下黑产技术“深度融合”。

以 RaaS 模式为例，各成员通过暗网相互提供服务，管理者作为“项目经理”统筹资源的调配，赚得的勒索金额会根据不同工种的工作量给予一定的利润分成。勒索团伙通常包含资源服务团队，技术服务团队和业务服务团队。

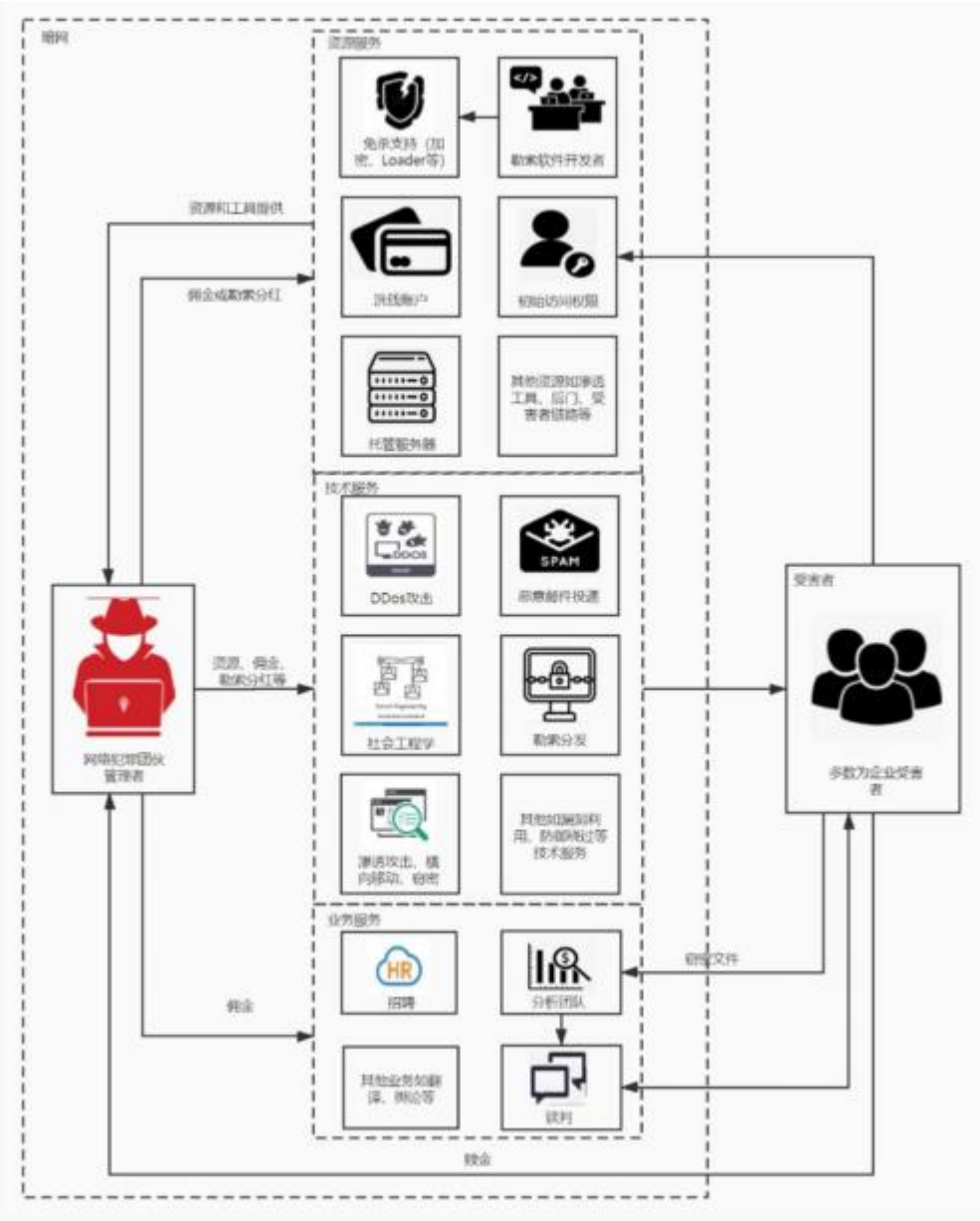


图 2_ D3Fend 框架 DNS 网络流量数字工件

在日渐成熟的网络犯罪产业链下，各类僵尸网络、勒索软件、加载器、商业木马“深度融合”，许多网络犯罪分子在产业链内发展关系，从而获得使团队运作或利润最大化的必要技术。以下是过去一年多我们观察到的不同攻击活动中常见的恶意软件投递关系图：

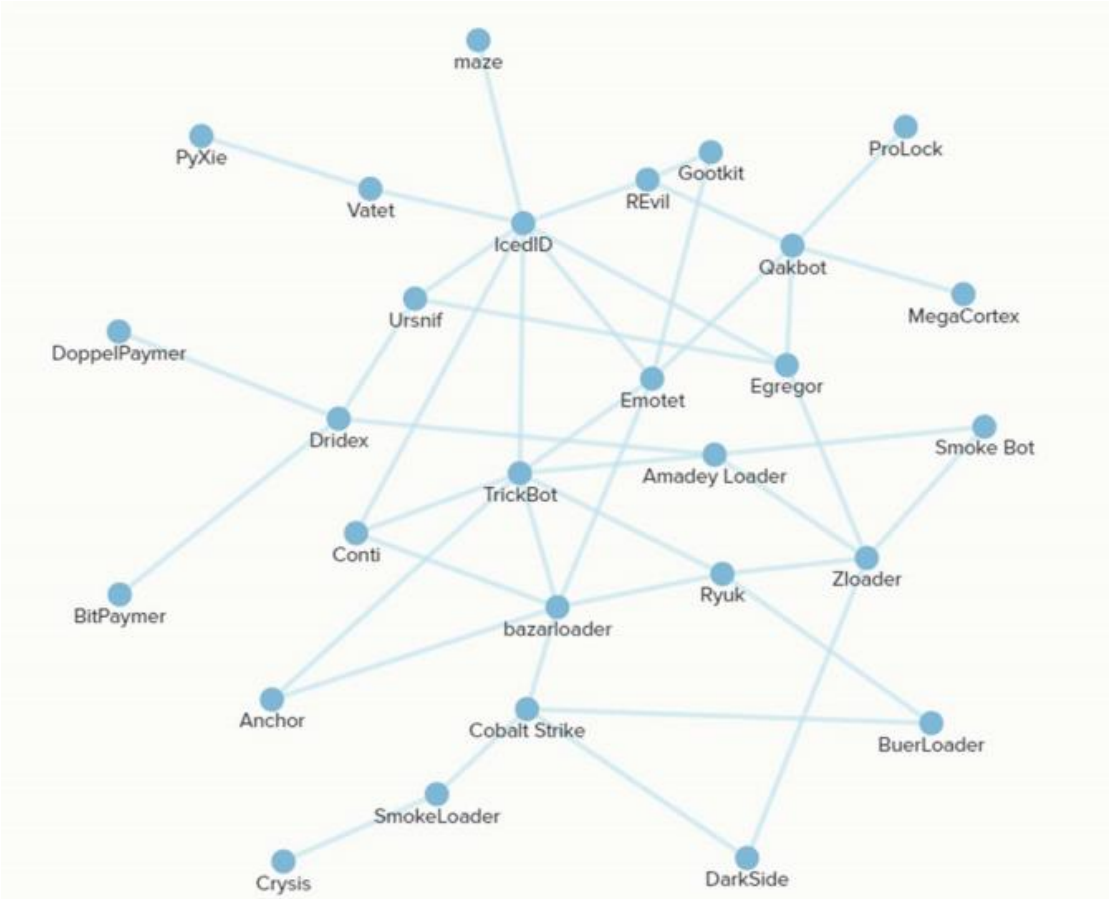


图 3_常见恶意软件投递关系图

1.1.5 勒索攻击已成为全球公敌，“多重勒索”、“APT 化”成为勒索攻击标配

过去一年多，平均每 11 秒就有一家企业成为勒索病毒攻击的目标，勒索攻击或在 2020 年造成高达数千亿美元的损失。据不完全统计，2020 年全球勒索攻击次数较 2019 年同比增长了 150%以上，每次勒索的平均赎金达到了 31 万美元；2021 年“勒索攻击产业”年收入将达到数千亿美元。勒索软件的威胁堪比“911”事件后全球恐怖主义所面临的挑战，并逐渐成为全球公敌。

在“RaaS（勒索软件即服务）”、“APT 化”攻击模式以及“Big Game Hunting（大型狩猎游戏）”盛行的大背景下，勒索攻击的参与者越来越多，勒索攻击的事后追查越来越困难，勒索入侵的过程越来越复杂，勒索攻击的目标越来越有针对性。勒索组织管理者通过招募相关领域的“人才”组成松散的“团队”。

“团队”构建完毕后，通过价值目标选择、攻击方案选择等完成前期准备，再通过弱口令爆破、僵尸网络、鱼叉攻击、水坑攻击、供应链攻击或者 0day/Nday 漏洞等方式进入受害者的网络环境，进而通过凭证窃取、权限提升、横向移动等找到受害者的重要资产，将数据打包后上传到攻击者的服务器，最后投放勒索软件进行精准勒索。一般一次完整的勒索攻击会持续数周甚至数月时间，攻击者在受害者网络中长期潜伏，甚至会在攻击过程中随时根据受害者的网络防护情况调整自己的策略，所做的一切都只为寻找最有价值的数据并在最后一刻“一招毙命”。同时，勒索攻击者已经普遍不满足于依靠单一勒索方式达到目的，而是采取泄露攻击目标重要数据，对攻击目标发动 DDoS 攻击甚至威胁与受害企业相关的客户等“多重勒索”方式达成最终的目的。

此外，以往勒索攻击主要针对传统 IT 系统，近年来随着云计算、物联网、移动互联网等技术的快速发展，勒索已经逐渐瞄准云上资源、IoT 设备、工控系统以及移动终端设备，这类本来自身安全性就较薄弱的系统在面对勒索攻击时更加不堪一击，轻则造成企业生产停滞，重则危害社会乃至国家安全。

未来，除了针对价值目标的“APT 化”勒索攻击外，类似 Dark Side 组织以摧毁重要基础设施为目的的高级勒索攻击将会屡见不鲜，勒索攻击将成为危害网络安全的首要威胁。

图 4_ APT 组织惯用技术矩阵

2021 年 5 月 7 日，全美最大油气输送管道运营商 Colonial Pipeline 遭到勒索软件定向攻击，此次勒索攻击由于涉及到国家级关键基础设施，故而引起了全球的震动和广泛关注。此次攻击的幕后黑手确认为 Dark Side 勒索团伙，该公司不得不向黑客支付了 440 万美元的赎金，以恢复被攻击的系统。

图 5_ Colonial Pipeline 输油管线

1.1.6 国家层面局势升级，必然伴随相应网络攻击

近日乌克兰局势不断升级，直到今天，发展成为全面的战争行为，除了目前牵动世界神经的战争局势发展态势，还有伴随在战争之下频繁的网络战争。网络攻击一直伴随着本次冲突的发展而不断出现，成为本次战争的先行战场。根据目前的威胁情报信息来看，除了之前针对乌克兰国防部、外交部、教育部、内政部、能源部、武装部队等机构的大规模分布式拒绝服务攻击外，近日一款用于攻击乌克兰的数据擦除恶意软件被部署在了乌克兰数百台重要机器上，造成了这些机器无法工作。

但从对战争的影响来看，这些攻击或许只能在战前给对方一定的威慑作用，并不会对战争产生多少影响，但是从 11 点开始的定点清除行动，需要事先对目标的重要设施和人员有精确的了解，这让我们想到去年追踪到的一系列针对乌克兰边防局和乌克兰国防部网络间谍活动，间谍活动以“COVID-19Vaccine”、“向 ATO 退伍军人付款”、“紧急更新！！！”、“乌克兰总统令 №186_2021”等内容诱饵进行攻击，这一系列网络间谍活动或许也是战前准备所做的重要的一步。

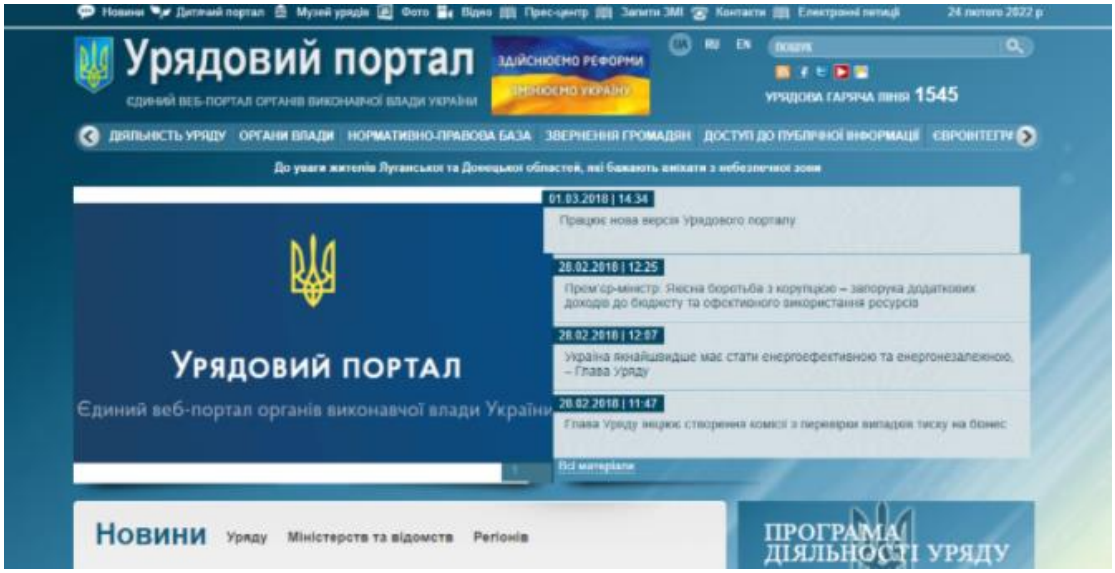


图 6_受攻击的乌克兰政府新闻网站（old.kmu.gov.ua）

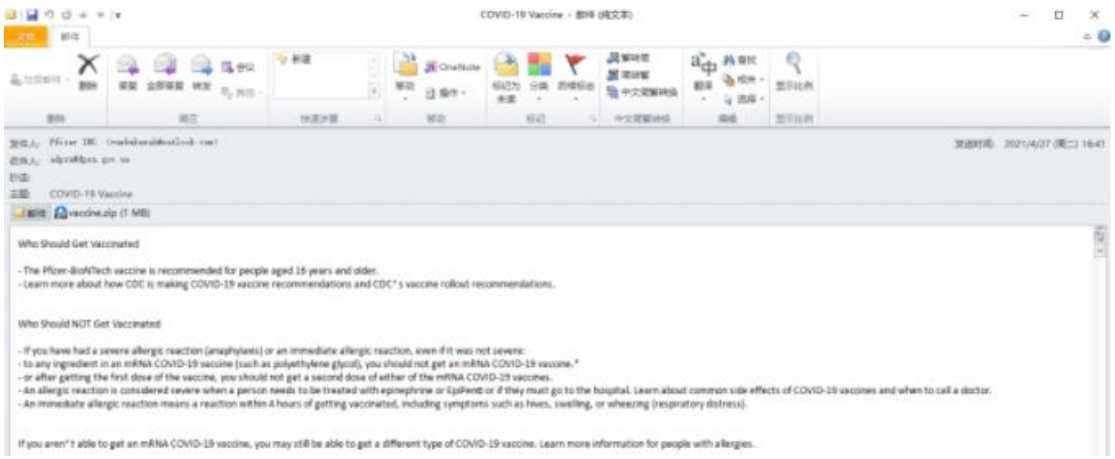


图 7_钓鱼邮件“COVID-19 Vaccine.eml”

从近期的观察来看，在战争发生之前，乌克兰和俄罗斯局势的升级都会伴随着相应的网络攻击，可以说，网络攻击似乎成为冲突背后用于压制对方的一种重要手段，除了可以破坏对手的网络基础设施外，还能对对手政府起到一定的威慑作用。

1.1.7 就地取材，LOLBins、攻击性安全工具滥用成趋势

对于攻击者来说，利用各种现成的工具来实现其最终目的无疑是最佳选择。一是，利用现成的工具可以更大地降低成本，攻击者只需要付出一定的学习成本便可轻松达到目的；二是，有些工具并非是真正的恶意软件，安全软件一般不会检测或者会被管理者当作白名单，大大提高了这类工具在使用过程中的“免杀”

能力。三是，使用现成工具往往会更进一步隐藏攻击者的真实身份，使得基于工具进行攻击者身份鉴别的手段失效。

在“Living off the land”热度不减的同时，攻击性安全工具（Offensive Security Tools，简称 OST）越来越受到攻击者的关注。“Living off the land”通常指攻击者使用目标主机上已安装的工具或功能进行攻击的方式，被利用的工具通常叫做“LOLBin”。在真实攻击中，LOLBin 一般以操作系统自带的具有一定功能（如网络访问，命令执行等）的系统文件为主。虽然“Living off the land”可以最大限度地避免攻击被发现的可能，但仅利用系统提供的有限功能“拼凑”出整个攻击过程并非易事，攻击性安全工具便进入了攻击者的视野。攻击性安全工具是指在不利用软件自身缺陷或漏洞的情况下，以合法身份实施入侵或规避安全防御机制的软件代码库。攻击性安全工具一般由信息安全专业人士开发，目的是促进网络安全相关技术的发展。通俗地讲，攻击性安全工具就是开源代码共享网站可以下载到的渗透工具或者较为知名的商业渗透攻击套件的集合。

1.1.8 新挖矿木马如雨后春笋般涌现，容器成为挖矿攻击重要目标

与普遍“APT”化的勒索攻击不同，为了获得更多的计算资源，挖矿攻击仍然以不断扩大感染面为主要目标。

过去一年多，随着以比特币为代表的数字加密货币的暴涨，挖矿木马也随之更加活跃。甚至一些知名 APT 组织也加入挖矿阵营。在这一年里，老的挖矿木马持续活跃，如永恒之蓝下载器木马以及 H2Miner 挖矿家族都在不断扩充漏洞攻击武器库；新的挖矿木马层出不穷，如 PGMiner、KingMiner 等新挖矿木马。

除了使用弱口令爆破、常见的漏洞利用外，挖矿攻击逐渐瞄准容器等云上资源。Docker 容器作为一种有效的软件应用程序打包方式，在过去几年越来越受欢迎，Docker 容器在各个公有云大量部署运行。这些容器由于天生具有计算资源丰富、难以监控等原因成为黑客垂涎的目标。一方面，黑客通过在 Docker Hub 发布带有挖矿木马的恶意镜像进行攻击；另一方面，黑客通过 Docker 的未授权访问漏洞或使用者在认证上的不安全设置入侵 Docker 容器并进行感染。

1.1.9 Web 攻击工具逐渐自动化、加密化，办公系统、安全设备漏洞威胁愈发严重

近年来，Web 攻击工具呈现逐渐自动化、加密化的趋势。以冰蝎、哥斯拉为代表的新型 Webshell 管理工具正逐渐往流量加密的趋势发展。传统的以特征串匹配为基础的流量检测手段已逐渐失效，以流量行为特征、机器学习、威胁狩猎为基础的检测方式正逐渐走上舞台。以 Goby、Xray 为代表的漏扫工具方兴未艾，它们普遍都集成了各类系统及应用的漏洞 EXP，并且支持自定义 EXP，通过丰富漏洞 EXP 资源库方便使用者快速获取权限。再配合各脚本、工具间实现高效联动，提升了漏洞的探测能力与利用效率。这些漏扫工具功能越来越强大，使用越来越方便，即使是入门级的新手也能依靠这些工具自动化完成大部分渗透工作。

此外，仍有不少 0day 漏洞被曝光，这其中大部分都是办公系统及安全设备本身的漏洞。这类漏洞具有覆盖范围广、危害大，利用难度较低的特点。由于 OA 系统通常位于 DMZ 区或内网，安全设备通常位于内网，加之国内部分企业网络环境相对复杂，访问控制策略不规范，时常会有内外网或 DMZ 区互通的现象出现。此时 OA 系统或办公设备的漏洞就会成为攻击者的绝佳入口，攻击者可利用 OA 系统挂马或当作跳板直达核心办公网，甚至利用安全设备漏洞直接关闭告警信息让攻击者畅通无阻。

1.1.10 IoT 僵尸网络变得更加隐蔽，NAS 设备成为 IoT 攻击新宠

传统的 IoT 僵尸网络由连接到命令与控制（C&C）服务器的众多受感染设备（Bot）组成，犯罪分子使用 C&C 服务器控制着整个僵尸网络。这意味着只要关闭 C&C 服务器，就会使僵尸网络无法工作。但是过去一年多，我们发现越来越多的僵尸网络引入了 P2P 和 Tor 网络技术，这使得僵尸网络变得越来越隐蔽，更加难以关闭。老牌僵尸网络 Mirai、Gafgyt 等都已引入 TOR 技术，Wifatch、Hide'N Seek、Hajime、Mozi、HEH 等也都纷纷引入了 P2P 技术。

由于 IoT 类设备一般无重要数据存储，所以勒索软件一直以 PC、服务器等

IT 类资产为目标。近年来随着 NAS 设备的普及，勒索软件已开始瞄准 IoT 设备进行攻击。2020 年下半年到 2021 年上半年，我们分别观察到 eCh0raix、Qlocker、AgeLocker、Muhstik 等勒索家族专门利用 QNAP NAS 设备漏洞进行传播，2021 年 6 月出现的 Ruyk 家族新变种也开始针对 NAS 设备进行攻击。我们预计，未来会有更多的勒索软件以 IoT 设备为目标进行攻击。由于附加在 IoT 设备上的安全能力普遍偏弱，其危害将会明显大于 Windows/Linux 系统下的勒索攻击。

1.1.11 人工智能技术距离实用仍存在距离

近两年，人工智能技术的研究继续维持高热度，以 GPT-3、AlphaFold2 等成果为代表，继续展现出强大的建模能力与应用潜力。而在人工智能赋能网络安全方面，在近年来从炒作到务实的整体发展趋势下，进一步呈现出以安全能力提升为核心目标而稳步发展的状态。

随着对人工智能技术原理及特性的理解逐步深入，网络安全业界对人工智能技术采用的针对性日趋增强，并更多尝试将其与已有技术结合使用（而非替代），从而更好地发挥技术综合优势。

鉴于网络安全领域数据的标注率低且类别分布严重不平衡等特点，无监督、自监督或半监督的方法或将有更广应用前景，以异常检测为典型代表。由于这类方法的准确性难以达到很高水平，通常作为一种安全威胁的（弱）信号形式来呈现，但对于未知威胁的发现有积极意义。

在恶意代码检测等数据样本资源较丰富的部分应用场景中，有监督的方法能够取得更高的检测准确率，在未来几年内将成为传统的基于签名特征方法的重要补充。

在加密数据（流量、文件等）检测方向，人工智能方法获得较多关注，主要基于元信息、统计信息及行为信息的特征来构建检测模型，能在有限的测试数据集上达到很好的效果，但其在更大规模、更一般性的数据集上的有效性较难保证，方法背后的原理仍存在争议。

人工智能的可解释性在网络安全领域的受关注程度正逐渐上升，但目前仍属于前沿科学问题，暂无一般性的高效、可靠技术可用，可解释性方法带来的价值也仍需深入评估，距离实用仍存在距离。

1.1.12 “以攻促防、以矛强盾”，漏洞攻防研究日益受到重视

漏洞是网络安全最重要的命门，不法网络攻击者不断在硬件、软件、协议的具体实现或系统安全策略上寻找存在的缺陷，从而能够在未授权的情况下访问或破坏系统。漏洞一旦被利用后果不堪设想，它能直接突破未授权的系统，进而在系统中进行拓展和控守。因此，漏洞研究与挖掘能力成为守护网络安全命门的关键武器。其发展趋势主要包括以下几个方面：

1、专业化定制化漏洞挖掘需求强烈

随着用户对采取高强度安全防护措施的目标网络侦察和了解的深入，网络攻防技术呈现出细分化和专业化的趋势，面向用户需求的定制化漏洞挖掘项目也越来越多。大而全的漏洞扫描设备被认为是安全防御和检测的基本形态，大多用来初步检测和发现安全漏洞，客观评估网络风险等级，而针对性的定制化漏洞挖掘和网络漏洞突破解决方案更受用户欢迎。

2、自动化渗透测试平台更紧密结合实战型漏洞

自动化渗透测试是目前比较热门的网络攻防领域，主要是利用了众多的已公开或未公开漏洞对目标资产和系统进行自动化检测，发现并利用这些弱点，从而降低人工检测强度，辅助渗透测试人员后渗透。很多自动化渗透测试平台局限于通过技术手段提供覆盖子域名探测、域名解析、端口、服务、Web 页面路径等网络资产探测、突破和利用，离实战化还有一定距离。而实战型漏洞拓展到网络渗透测试活动中遇到的各种安全防护系统、设备以及通信链路，这些漏洞不仅仅局限于 Web 跨站、数据库撞库等常见授权渗透测试场景，因此，实战型漏洞发现和自动化渗透测试平台是网络攻防对抗领域未来发展的重要方向。

3、政府、企业和院校加强漏洞挖掘人才培养

“网络空间的竞争，归根到底是人才的竞争”，如何培养高素质的网络安全队伍，引发网络安全行业乃至国家的高度关注。近年来，政府、企业和院校加强漏洞挖掘人才培养力度，以赛促学、以赛代练的漏洞挖掘大赛此起彼伏，例如“天府杯”、GeekPwn“极棒”、各种 CTF、“红帽杯”等等。从目前来看，国内的安全人才（尤其是漏洞挖掘人才）缺口高达百万，现有高校一年能够输出的信息安全专业毕业生只有不到 3 万人，即便再加上社会培训机构培养的人才，一年也超不过十万人，很难在短期内满足大量用户对安全人才的需求。虽然政府积极推动网络安全教育和人才培养，高校设立安全一级学科输出相关人才，企业等举办安全赛事选培相关人才。但是，总体增速仍然比不上网络发展，只要有新技术就会带来新网络安全的问题，对人才的需求也将会越来越大。

我们相信，在《网络产品安全漏洞管理规定》等法律法规的规范下，针对漏洞这一网络安全命门的研究会更加深入，并进一步合规化、法制化，成为增强网络安全防护能力的重要法宝。

1.2 面对新威胁的应对措施

过去几年中，网络攻击的数量呈指数级增长影响各种规模、行业的企业网络。而传统的基于黑白名单、签名和规则特征的安全威胁发现手段，已经不能应对不断发展的网络威胁和 IT 环境。

在这些威胁中，尤其是以高级持续性恶意攻击（APT 攻击）为代表的新威胁，更是让企业防不胜防。现有的任何防御手段在 APT 攻击这种定向攻击面前都显得苍白无力。

针对高级威胁，传统的头痛医头脚痛医脚的安全防御并无法解决问题，反而还带来了割裂的安全，缺乏全过程的防护。同时多异构设备的叠加带来了安全的碎片化，缺乏统一的视角和关联能力，无法打破数据孤岛，协同防御。

1.2.1 传统防御手段难以为继

网络安全检测分析是攻与防的持续对抗过程，传统的网络威胁分析存在很多的关键技术问题亟需解决：

1. **安全产品各自为战，难以形成合力**

现在网络里面部署了大量的安全产品，终端杀毒软件产品、网络边界防护防火墙，IPS 产品、网络检测 IDS，沙箱产品等。这些安全产品都是为了解决特定的安全问题部署进去的，相互之间没有联系，各自为战，对于稍微复杂的安全威胁问题是没有办法的，比如越来越多的恶意软件加入了反终端检测的功能，会使用多种静动态免杀手段躲避终端杀毒软件，甚至直接讲终端杀毒软件关闭，这就导致终端安全检测失效，恶意软件在突破终端杀毒软件后，继续进行破坏活动，往往伴随网络行为，比如与 C&C 远控服务器连接，横向发包探测等，这些行为是可以通过网络检测产品检测到的。但是网络检测产品仅仅发现了一次远控或探测的安全攻击行为，如果能够与终端系统的日志进行关联，就能够发现完整的一次恶软件攻击行为，还原出整个过程。

2. **海量安全事件无法运维，漏掉确定性的攻击线索**

目前网络威胁检测的技术方案还是以特征检测为主，通过报文头特征或载荷特征进行检测，每天产生的安全事件数量是非常大的，超过上万条。安全运维人员的处理基线是每天不到 100 条安全事件，同时运维人员在处理这些安全事件的时候，大多数安全事件都是“误报”的。造成目前网络流量检测技术方案误报多的现象主要有以下几个原因：一是类似于 PING 这类的“误报”，其本质并非误报。而是缺少上下文关联导致大量的报警淹没了关键攻击行为。这类“误报”必须和其他失陷的确定性报警结合起来作为攻击前奏来看，而不能单纯看作是确定性攻击。二是提取的攻击关键特征与正常协议冲突，攻击特征是在威胁发生时流量里面提取到的，这些特征大都是靠安全专家的经验总结提炼的，在面对现网错综复杂的业务应用流时，会出现攻击特征与正常的业务流特征冲突。三是网络流量引擎特征大都是单向特征，本质上缺乏对于攻击确定性的判定依据，现在大

多数安全事件是网络探测或攻击尝试行为产生的。这些安全事件无法给出确定性的攻击成功与否判定，对于用户的主观感受就是误报很多。

3. **未知威胁检测能力有限，APT 攻击检测缺乏有效手段**

这些年 APT 组织在攻击隐匿性方面越来越强，钓鱼手段更加精细化，针对性和迷惑性更强，利用开源代码，改进攻击工具，降低攻击成本。这些对于传统的基于特征和规则的网络安全检测产品来说都是严峻挑战。另外随着网络应用逐步向加密传输方式演进，边界网关产品对于加密隧道采取放通策略，攻击组织也利用这点，将 SSH 隧道等传输方式作为恶意软件通信的基本能力，直接通过边界网关产品进入内网。

4. **安全事件缺乏事后快速处置、追踪溯源、攻击路径还原的工具支撑**

网络安全产品检测出安全事件，因为缺乏关联分析，只能根据各自产品安全威胁事件的危害程度进行处置，对于危害程度更高的组合型 APT 高级威胁就无法及时处置了，需要有经验的安全运维人员到多个安全产品、系统里面进行事件、告警日志等分析，找到确定的失陷主机，然后追踪溯源，还原出攻击路径，最后去切断路径，实现完整的闭环。这些工作都需要统一的系统工具进行支撑，固化运维经验和提高效率。

1.2.2 新技术、新应对

早在 2013 年以前，APT 攻击对于我们来说还是个只闻其声未见其面的“奢侈品”，曾经名噪一时的“震网”攻击、“极光”攻击似乎离我们非常遥远。但是近年来，随着黑产团队的组织化、攻击技能的不断泛化，攻击目标的定向化、攻击工具的商品化，APT 攻击技术早已从高深不可得的“阳春白雪”，变成了技术小白都能尝试一下的“下里巴人”。

过去，造成较大影响力的攻击事件普遍存在着影响范围广、持续时间短等特点。而现代攻击中除了挖矿等少数需要大规模算力才能达成目标的攻击类型外，大多数攻击都在向“APT 化”发展。“A”即高级，主要体现在攻击者通常会采

取加密、混淆、0day 的方法绕过防御策略，甚至会针对被攻击者的特点单独制定攻击路线；“P”即持续，主要体现在攻击从前期的踩点、武器准备到载荷投递、定植，再到权限提升、内网横向移动直至最终的命令回传、加密文件等一般都需要经历较长的过程。

面对越来越多的“APT 化”攻击，迫切需要构建“主动防御、协同防御”的新型防御体系，其原因主要有以下几点：一是由于“APT 化”攻击的“高级性”特点，传统的基于已知特征或模型的被动检测模式完全无法应对新型攻击，攻击者 100%会突破防线进入受害者网络，“守不住，看不见”成为正常现象。但“雁过必留痕”，只要确保终端、边界、内网的流量、日志、告警记录都能充分记录下来，当未知攻击被有效识别后，具有丰富经验的安全专家就可以从历史数据中挖掘出失陷主机并还原出攻击链，从而实现攻击“找得着”；二是由于“APT 化”攻击的“持续性”特点，攻击者会长期潜伏在受害者内网中，从 DMZ 区到办公区再到核心区可能都会遍布攻击者的足迹，这就需要在网络边界、内网、终端等任何需要监控的环节都部署有相应的安全产品，同时通过产品之间的协同联动完成对全攻击过程的监控和防御。三是由于不同类型攻击特点的不同，表现为在终端或网络侧检测的难易度也不尽相同。类似“永恒之蓝”之类的 RPC 漏洞更适合在网络侧检测，而横向移动等攻击场景由于协议的加密问题更适合在终端侧检测。这就需要不同类别的安全产品互相配合，弥补自身在某一个检测方向上的短板。

基于上述现状，近年来，以“威胁狩猎、XDR”为代表的”主动防御、协同防御”技术或方法应运而生。威胁狩猎是指采用人工分析和机器辅助的方法，针对网络、终端等的日志或告警数据进行主动搜索、关联和分析，从而检测出以往被动检测无法察觉的威胁。威胁狩猎一般分为四个过程：首先，安全专家需要结合资产信息、威胁情报对网络中可能存在的高风险点进行预判；其次，利用已收集的数据，使用可视化、数据统计分析等方法对数据集进行挖掘与分析，查找已知或未知的攻击线索；之后，结合威胁模型对已发现攻击者的攻击工具和攻击技术进一步挖掘，发现攻击者的 TTP；最后尝试对上述威胁发现过程进行标准化或

自动化。要实现威胁狩猎的落地，必须依托于足够强大的协同防御体系，XDR 就是包括威胁狩猎以及各种其他检测防御技术的重要承载者之一。XDR（Extended detection and response）即扩展检测和响应系统，是 Gartner 2020 年《Top Security and Risk Management Trends》报告中提到的第一项技术和解决方案。通俗的讲，XDR 中的“X”有无限可能无限扩展的含义，即可以叠加 NDR、EDR 以及其它未来可能的“X”DR 检测能力，同时结合自动化编排和响应（SOAR），威胁狩猎，跨安全产品的威胁情报等方法和技术，全面有效增强检测和响应能力，形成完整的协同防御体系。

面对越来越多的“APT 化”攻击，只有融合被动检测、主动狩猎等各种技术的协同防御体系，才能有效监控攻击的各个阶段，真正让攻击“看得见，防得住，找得着”成为现实。

二. 定位与价值

2.1 产品定位

通过上述背景分析调查结果，我们发现攻防不对等的原因较多，包括传统防御绕过、高级威胁技术的使用、攻击工具化自动化等，而这些安全现状会让大部分的运维人员越来越担忧：

“部署很多安全设备，但还是不知道到底是否安全？

如果不安全，哪里不安全？

每天上报的攻击有很多，到底哪些攻击成功了？

越来越多的 APT 化攻击，威胁从哪里来，到哪里去？

是什么类型的攻击？造成了哪些损失？

我该怎么处理？”

结合启明星辰多年的网络安全运维经验，认为上述现状为当前业界对内部网络安全均存在的共性问题。

传统的网络安全建设方案，容易导致割裂的安全防御，无法协同作战，提供有效的整体安全防护，甚至导致安全运维复杂化。基于割裂的安全防御所产生的安全现状数据也将成为一座座安全孤岛，难以协同共享，导致碎片化的安全认知，只能看见碎片化的局部安全，无法形成统一的整体可视。

因此，安全需要如同一个统帅，协同指挥各个部队，形成一套完整的协同指挥作战中心。

结合理念，天阗威胁分析一体机（Threat Analysis and Response-All In One）的产品定位为：

以攻防研究为核心，配合场景分析、资产构建、自动响应、协同防御能力，构建下一代一体化高级威胁检测与响应体系，意在为客户提供一套集检测、分析、可视、闭环响应为一体的本地网络安全分析中心，让安全可感知、易运营。

2.2 产品价值

1. 采用 ATT&CK 知识体系构建全局安全可视

ATT&CK 知识体系构建了一套更细粒度、更易共享的知识模型和框架，可以认为是 Kill Chain 的扩展，网络安全检测能力可以根据 ATT&CK 体系进行覆盖和演进。天阗威胁分析一体机（TAR-AIO）是一整套网络安全检测和处置的产品，采用分析中心和检测引擎结合的架构。分析中心类似安全大脑，完成安全告警事件的集中收集、存储、分析以及联动处置等能力，检测引擎负责网络流量和文件的处理，完成安全检测的工作。

通过全流量分析、多维度的有效数据采集和智能分析能力，实时监控全网的安全态势、内部横向威胁态势、业务外连风险和服务器风险漏洞等，让管理员可

以看清全网威胁，从而辅助决策。

2. 大数据分析、检索能力

TAR-AIO 基于流行的大数据架构，具备 PB 级别的海量数据存储、高性能搜索与关联分析能力，并可通过集群等方式进行扩充。

网络里面的网络检测产品和网络边界防护产品的告警日志、系统日志、流信息等数据，都可以送到网络威胁分析处理系统里面进行存储、关联分析和展示。

3. 智能分析能力，应对未知威胁

随着黑客的技术发展以及变种、逃逸技术的不断改进，传统安全设备的静态规则防御手段已经捉襟见肘，依靠规则仅能防御小部分已知威胁，已无法检测最新攻击、未知威胁。

TAR-AIO 对于未知攻击威胁的解决思路是通过基于沙箱的恶意代码检测技术，与具体的安全攻击场景结合，发现隐藏的威胁。基于沙箱的恶意代码检测技术构造一个模拟的执行环境，让可疑文件在这个模拟环境中运行，通过可疑文件触发的外在行为来判定是否是恶意代码。具备对各类设备网络文件传输异常行为、漏洞利用行为、未知木马、隐蔽信道传输等多样性、组合性和持续性攻击的检测能力，其中漏洞利用行为可以通过恶意代码的静态检测与动态检测相结合的方式来监测；设备网络文件传输异常行为、未知木马检测等可通过间歇性连接分析以及可以加密传输等方式来进行监测；隐蔽信道传输则有专门的隐蔽信道分析技术来进行监测。

4. 高效协同响应，阻断风险扩散，辅助闭环

TAR-AIO 可联动启明星辰自有设备，不仅作为安全数据采集，当发生重要安全事件或风险在内部传播时，亦可通过联动进行阻断、控制，避免影响扩大，实现安全事件快速闭环。设备可提供确定性安全事件的运维入口，提供大屏展示、汇总分析、自定义报表等日常运维手段。通过标准 RestfulAPI 接口与终端引擎、与网络边界防护网关设备进行联动实现处置动作；也可与全流存储设备 NFT 联

动，进行未知威胁攻击链还原和溯源反制；通过北向标准的 Syslog、Kafka 接口向上一级系统上报安全事件。

5. 威胁举证关联，识别准确攻击

TAR-AIO 网络流检测引擎基于报文的头或载荷特征，匹配到攻击特征后产生安全告警事件上报攻击日志。从两方面进行增强，一是关联响应报文检测，通过确认响应报文内容，进而确定攻击是否成功，这样实现了攻击的双向检测；另一个是增加流量行为特征检测功能，基于源和目的之间的报文交互行为特征进行安全检测，既可以检测确定的攻击，又能够对加密传输的攻击进行检测。

TAR-AIO 网络流检测引擎产生的安全事件在很多业务场景中，与业务存在冲突而产生误报。引入威胁情报关联分析，通过离线情报或在线的 API 接口，安全事件的关键属性 IP、URL 域名或文件 HASH 与威胁情报进行比对确认，给出明确的安全检测结果，这样可以去掉大量的误报。

6. 建立多源数据关联模型，发现更深层次威胁

网络安全检测方法采用特征检测、恶意代码检测、隐蔽信道检测、威胁情报检测等多种检测技术结合，通过时间戳、IP 关系和文件 HASH 等因素，发现 APT 高级威胁。针对 APT 攻击组织进行画像，网络威胁深度分析中心提炼整理攻击样本、手法，通过 API 接口与威胁情报进行关联，直接获取关联的的 APT 高级威胁攻击组织。网络威胁深度分析中心接收从终端引擎、网络检测引擎发过来的安全事件。在分析中心上定义二次统计分析模型，用来发现新的安全威胁。包括网络资产主动外连、DGA 域名发现、HTTP 代理发现、DNS Tunnel 发现等安全事件。

三. 产品架构

3.1 分层设计

天阗威胁分析一体机体系架构如下图所示，主要包括 TAR-AIO 网络流检测引擎、TAR-AIO 文件检测引擎和 TAR-AIO 威胁分析系统。

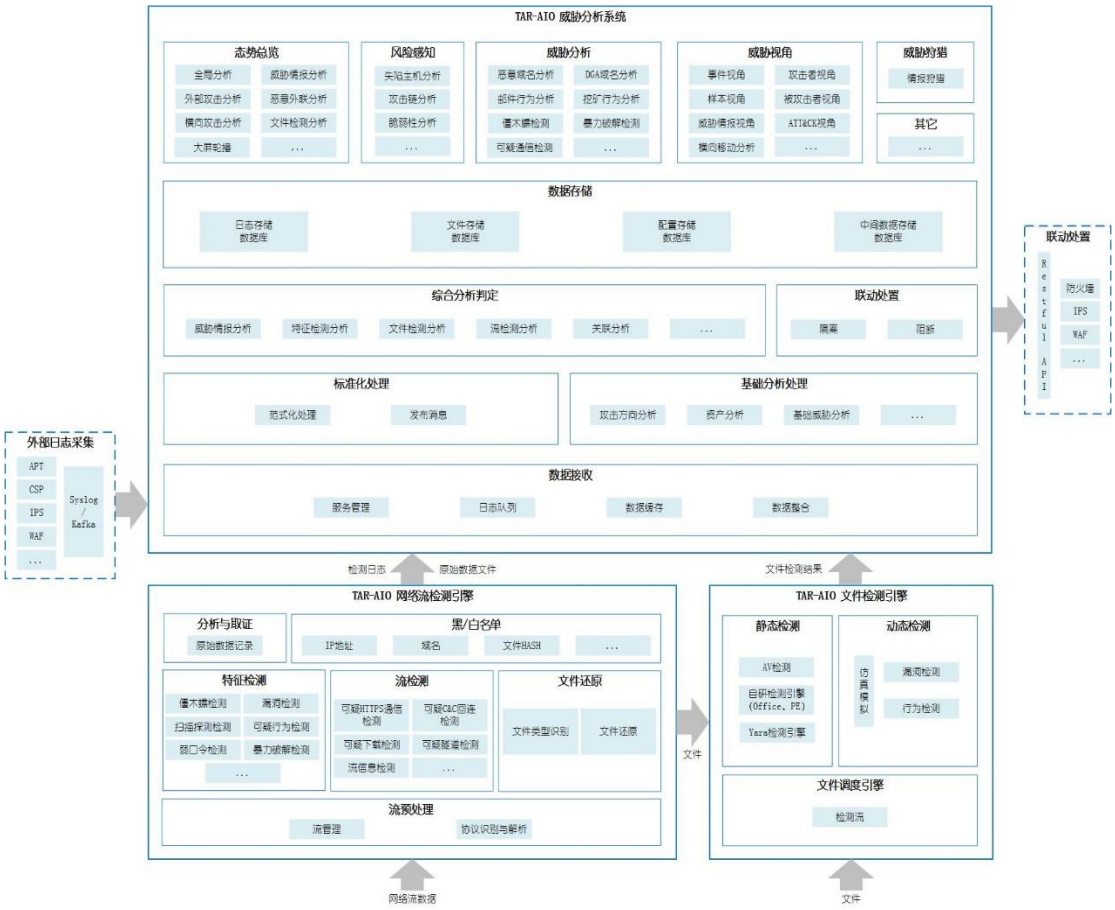


图 8_天阗威胁分析一体机体系架构

3.1.1 TAR-AIO 网络流检测引擎

TAR-AIO 网络流检测引擎是一个实时网络报文分析引擎，采用旁路流量镜像的方式，根据预定义的规则进行实时检测。

在 TAR-AIO 网络流检测引擎中设计了一套适合网络报文检测系统的规则描述语言，采用开放化的检测规则模型，且设计成了具有良好扩展性的实时网络报

文分析模块。

1. 流检测

1) 流量全字段检测

TAR-AIO 网络流检测引擎，基于会话进行网络报文全字段提取检测，支持多分析场景的流检测：可结合威胁情报，对可疑 C&C 回连、恶意域名请求等进行检测；结合机器学习算法对可疑 HTTPS 通信、DGA 域名进行检测；通过对相应字段信息提取判断，对可疑下载、可疑隧道进行检测等。

2) 协议解析

TAR-AIO 可识别主流的 HTTP、FTP、POP3、SMTP、SSH、MySQL、Oracle、IMAP、Webmail 等网络协议，从而确保识别并还原网络传输文件；同时支持解析识别 RPC、SMB 等协议，适配横向移动场景；设备支持工控协议检测，支持检测的协议包括：MODBUS、S7COMM、BACNET、DNP3、ENIP、IEC104、GOOSE、MMS 等。

TAR-AIO 支持对协议元数据进行提取检测，支持提取元数据的协议类型包括但不限于：TCP、HTTP、DNS、ICMP、SMTP、POP3、FTP、SMB、IP、TLS、UDP、PPTP、L2TP、MySQL、Telnet、ARP、WebMail、MSSQL、Oracle、IPSecVPN、IMAP、IPV6、RADIUS。

3) 可靠性

数据可靠性传输保证是实时网络报文分析引擎最为重要的方面，也是 TCP 协议区别于其它协议的最重要特性。所谓提供数据可靠性传输不仅仅指将数据成功的由本地主机传送到远端主机，数据可靠性传输包括如下内容：

- 能够处理数据传输过程中被破坏问题；
- 能够处理重复数据接收问题；
- 能够发现数据丢失以及对此进行有效解决；

- 能够处理接收端数据乱序到达问题；

使用用户态协议栈省去了用户态与内核态的通讯过程，这样会明显地提高发包和发流的处理性能。TAR-AIO 网络流检测引擎自主设计的用户态协议栈高效且易于扩展。

2. 特征检测

TAR-AIO 基于流量全字段检测技术，采用双向特征判定，通过返回信息直接检测攻击是否成功；支持对恶意软件利用、可疑行为、攻击利用、攻击探测、挖矿事件、APT 攻击事件等常见攻击类型进行检测。

在特征关键字匹配方面，采用了一套全新的匹配方法，设计了一套全新的编译器，将规则文件编译成可执行的二进制机器代码，就像 GCC 编译器一样，由 CPU 直接运行，所有的匹配比较操作均在程序代码段中实现，则避免出现 CPU 内存寻址等操作，避免 CPU Cache missing，降低了 CPU 的开销，从而提高了系统的整体处理性能。

3. 原始数据记录

无论基于报文特征的检测，还是流量轮廓的检测，支持对目标流量进行留存，并对留存目标流量进行分析取证。

从检测技术实现来看，检测通常针对部分报文特征或轮廓，但留存的目标流量应当基于三个时间段：

1）当前预警，当前受检测的报文，命中规则后，产生预警，此段目标流量需要留存。

2）预警后，对相应源或目的 IP 地址的后续一段时间的目标流量进行采集留存。

3）预警前，源或目的 IP 地址的相关会话流量进行留存。

在报文检测系统中，对当前预警和预警后的目标流量留存，实现难度不大。

但是对预警前的目标流量留存，具有相当大的难度。而预警前的样本留存，对跟踪攻击起源、了解攻击手法等具有非常大的意义。且尤其对流量轮廓的检测，目标流量留存基本是唯一的取证方法。

4. 文件还原

样本文件还原是报文深度检测的延续，对 TAR-AIO 文件检测引擎进行源数据支撑，发现藏匿于网络流量之中以文件的形式（例如脚本，宏代码等）的恶意攻击代码。

TAR-AIO 网络流检测引擎除还原样本文件外，还会上报攻击摘要信息，同时也可附带上报样本流量，以助于上层分析。

另外一方面，随着攻击手法的复杂，以及压缩、加密等技术的使用，恶意文件已经很难通过特征进行描述定义，此时我们可能需要使用“流量轮廓”的方法来描述，最简单的例子，网络中出现一次大字节的 HTTP POST 上传行为，为可疑违规行为，可以进行样本文件还原，以供 TAR-AIO 文件检测引擎进行深度的分析。

3.1.2 TAR-AIO 文件检测引擎

TAR-AIO 文件检测引擎针对恶意代码等未知威胁具有细粒度检测效果，可实现包括对：未知恶意代码检查、嵌套式攻击检测、木马蠕虫病毒识别、隐秘通道检测等多类型未知漏洞（0-day）利用行为的检测。采用国内领先的双重检测方法（静态检测和动态检测），多种核心检测技术手段：二进制检查、堆喷检测、ROP 利用检测、敏感 API 检测、堆栈检测、Shell code 检查、沙箱检查等，可以检测出 APT 攻击的核心步骤。内置沙箱具备 100 种以上文件格式检测能力，对压缩文件解压深度至少支持 10 层解压，支持对反沙箱恶意样本检测。同时，通过 TAR-AIO 威胁分析系统进行威胁分析，有效发现 APT 攻击。

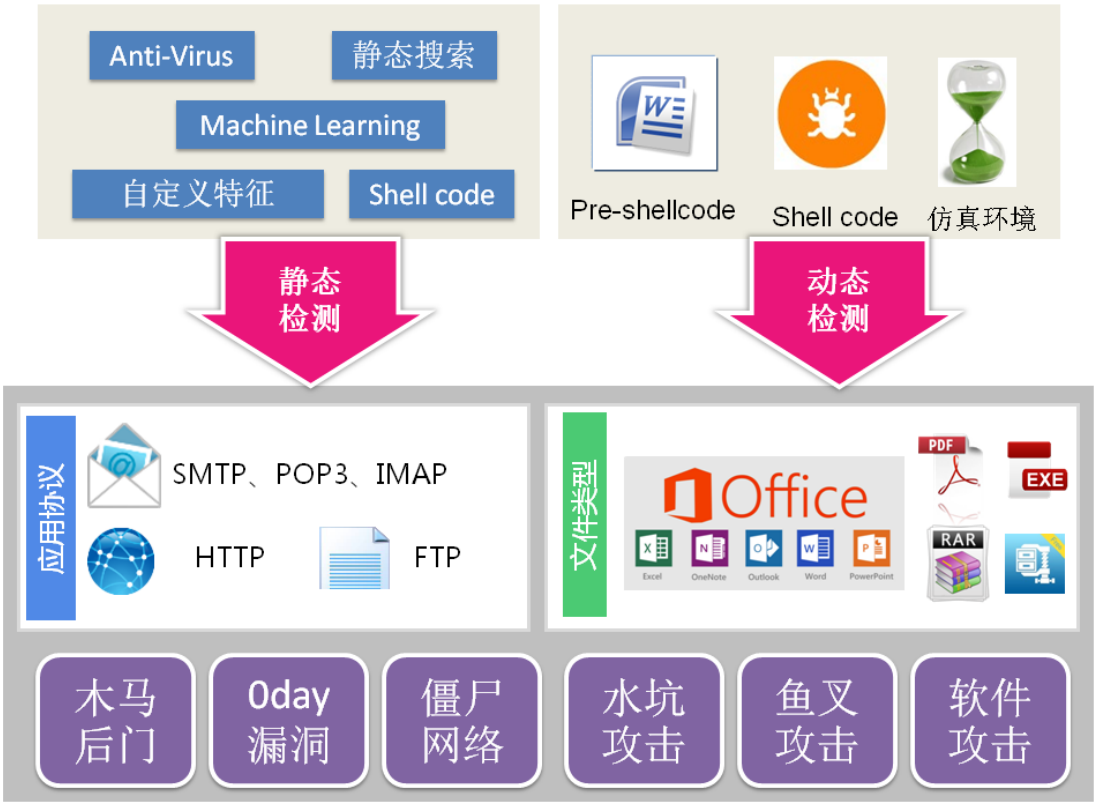


图 9_TAR-AIO 文件检测引擎

3.1.3 TAR-AIO 威胁分析系统

TAR-AIO 威胁分析系统按照 ATT&CK（可看作 Kill Chain 的扩展。“杀伤链”的概念源自军事领域，它是一个描述攻击环节的六阶段模型，洛克希德·马丁公司开发的“网络杀伤链”模型描述了网络攻击从最早的阶段——侦察到最终的阶段——数据提取）的理念进行构建，结合启明星辰在网络信息安全领域二十多年的技术和产品积累，构建一套终端检测、网络流检测，安全威胁分析到联动处置的闭环软件系统，主要的构建思路参考图示：

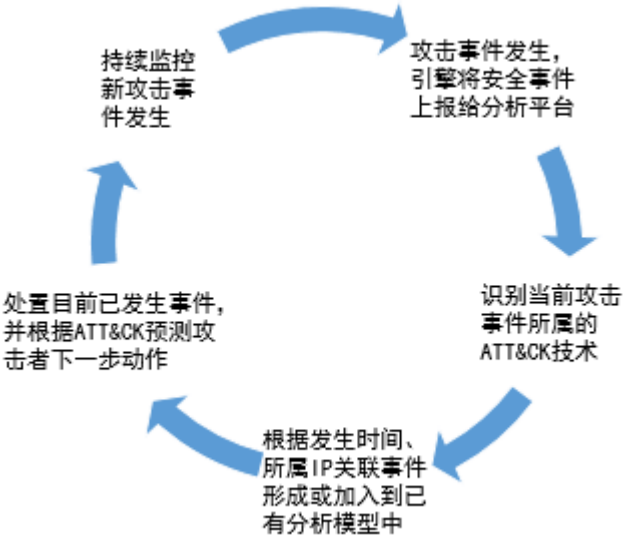


图 10_TAR-AIO 闭环构建思路

网络安全事件检测和处置是一个持续的过程，新的攻击事件发生要及时的检测出来，上报到 TAR-AIO 威胁分析系统，TAR-AIO 威胁分析系统通过综合分析，结合威胁情报，识别攻击事件的 ATT&CK 技术和相关信息，根据发生的时间因素、事件的源目的 IP 因素、攻击手段等形成相关的攻击阶段信息，可以根据提前预制的脚本，或管理员参与，对事件进行完整的处理。

天阗威胁分析一体机通过 TAR-AIO 威胁分析系统与 TAR-AIO 网络流检测引擎和 TAR-AIO 文件检测引擎相结合，配合本司网络边界防护产品和终端检测产品形成相应闭环，如图所示：

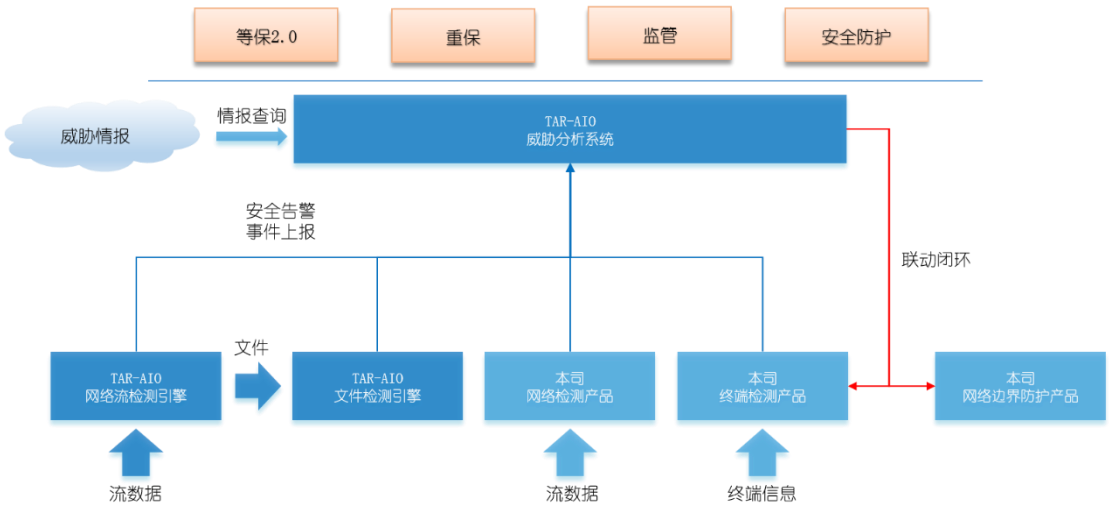


图 11_TAR-AIO 事件完整处理闭环流程

3.2 ELK 大数据架构

网络检测产品、网络边界防护产品、终端检测产品产生的安全告警事件都是以日志形式出现的，单个点的安全告警日志量很大，汇总到统一的分析处理系统会更加庞大。天阗威胁分析一体机采用的 ELK 技术架构在机器数据分析和日志处理领域的第一选择，能够支撑 PB 级数据的存储和搜索。ELK 支持集群部署方式，扩展性和可靠性有很好的保障。

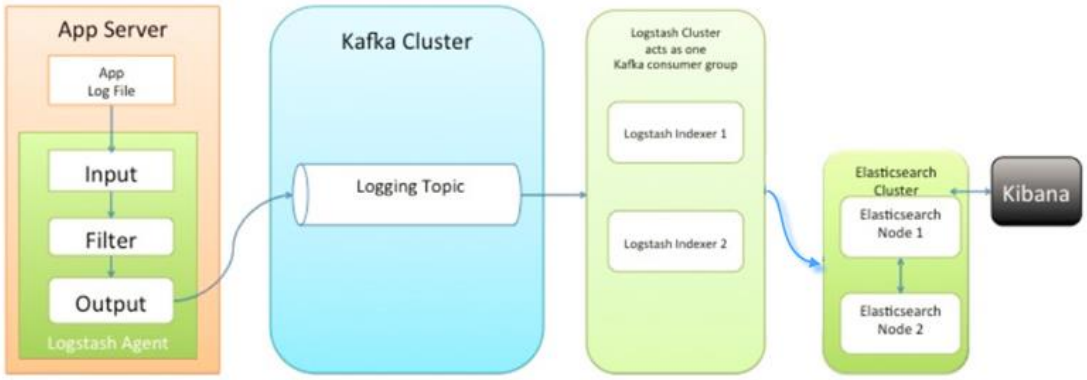


图 12_ELK 架构

1. 大数据集群存储层

主要是网络威胁深度分析中心用来处理存储数据，ElasticSearch 大数据集群主要用来存储告警日志，实现海量存储；同时使用 ES 结构引擎（大数据分析通用引擎）为基础元数据、分析数据、分析结果提供了快速检索能力。

2. 大数据消息队列系统

Kafka 是一种高吞吐量的分布式发布订阅消息系统，它可以处理消费者在网站中的所有动作流数据，有如下特性：

- 通过 O(1)的磁盘数据结构提供消息的持久化，这种结构对于即使数以 TB 的消息存储也能够保持长时间的稳定性能。
- 高吞吐量 ：即使是非常普通的硬件 Kafka 也可以支持每秒数百万的消息。
- 支持通过 Kafka 服务器和消费机集群来分区消息。

- 支持 Hadoop 并行数据加载。

Kafka 主要用途是数据集成，或者说是流数据集成，以 Pub/Sub 形式的消息总线形式提供。但是，Kafka 不仅仅是一套传统的消息总线，本质上 Kafka 是分布式的流数据平台，可提供 Pub/Sub 方式的海量消息处理；以高容错的方式存储海量数据流；保证数据流的顺序。

四. 关键技术应用

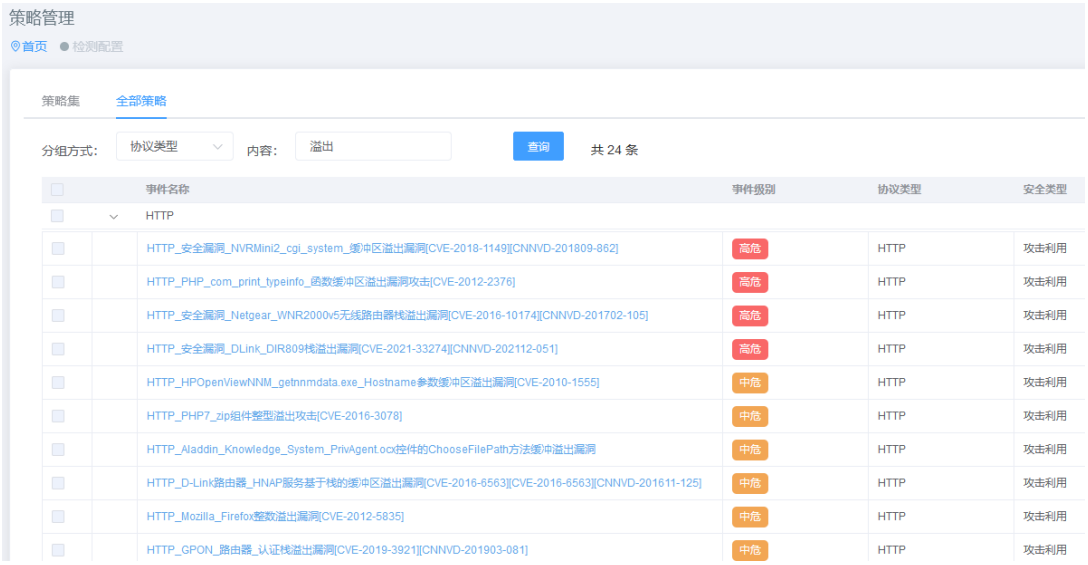
4.1 支持双向特征匹配特征检测

天阗威胁分析一体机在特征检测方面，凭借着多年基于特征的威胁检测领域的技术积累，在原有丰富、全面的特征检测规则库的基础上，利用双向特征匹配能力，对规则库进一步优化，增加攻击有效性判定，确保事件准确性，产品有效性检测能力显著提升。在保持原有对病毒、木马、蠕虫、僵尸网络、缓冲区溢出攻击、拒绝服务攻击、扫描探测、欺骗劫持、SQL 注入、XSS 攻击、网站挂马、隐蔽信道、AET 逃逸、C&C 行为等各种威胁的全面有效检测外，针对僵木蠕类攻击、Web 攻击等热点攻击手段的攻击特征进行进一步优化，确保产品的有效检测能力。

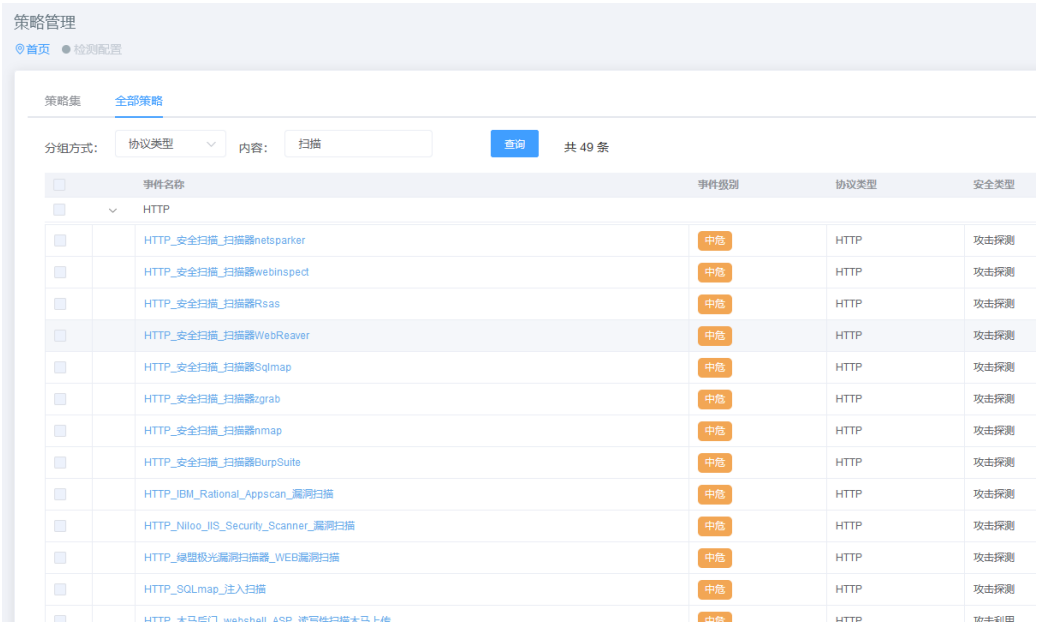
TAR-AIO 支持自定义规则进行特征检测，自定义规则支持工控协议，支持自定义检测规则的协议类型包括：TCP、UDP、ICMP、HTTP、SMTP、IMAP、POP3、MySQL、MSSQL、Oracle、MODBUS 等。自定义维度、可自定义的影响设备、可自定义攻击阶段（ATT&CK）均可多维度扩展选择匹配，可从容应对各种应急事件与场景。

- 漏洞检测

天阗威胁分析一体机支持多种类型的漏洞检测，具有丰富、全面、精准的特征规则库，规则库中包含多种漏洞攻击类型，例如：缓缓冲区溢出、拒绝服务和恶意扫描。

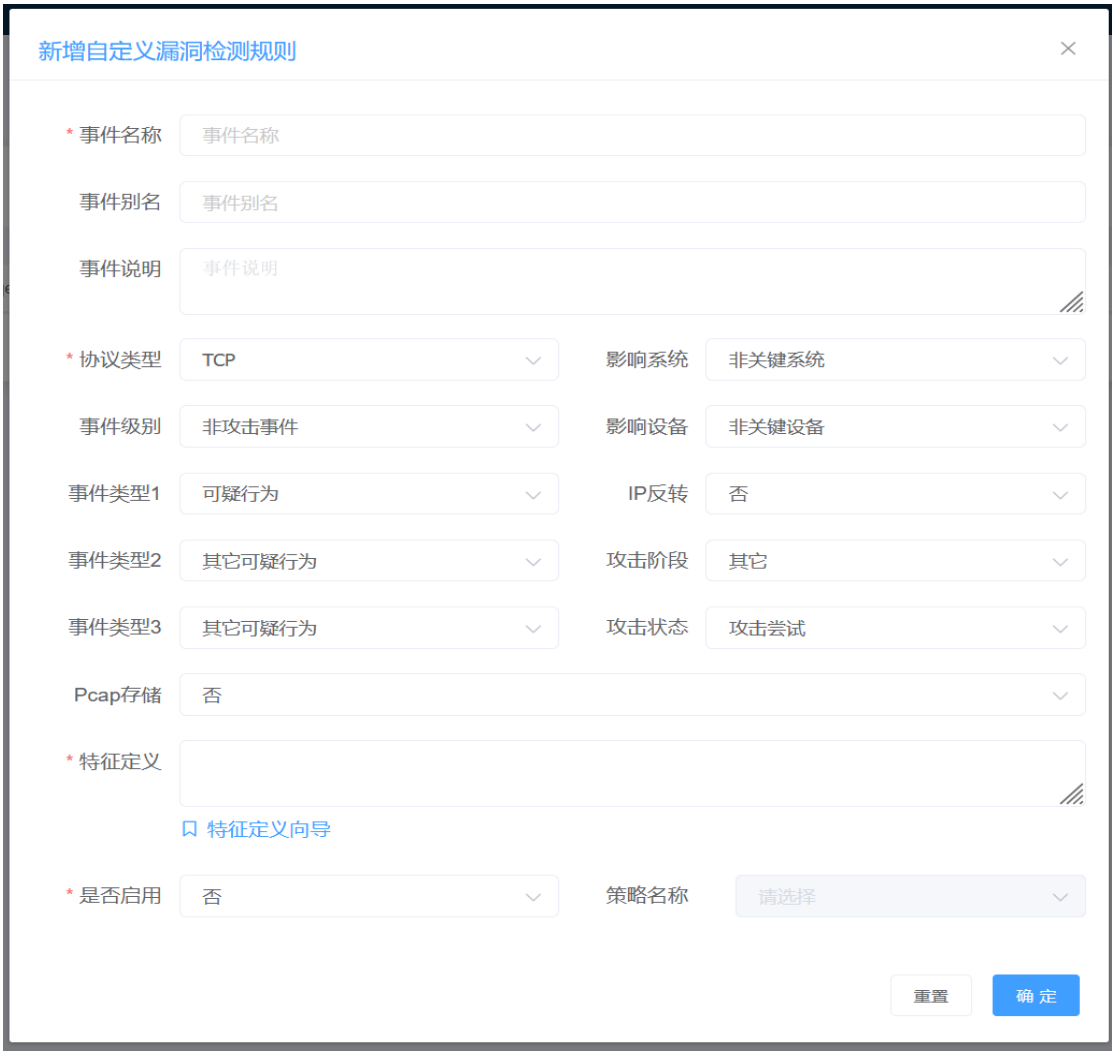

策略管理
首页
检测配置
策略集
全部策略
分组方式:
协议类型
内容:
溢出
查询
共 24 条
事件名称
事件级别
协议类型
安全类型
HTTP
HTTP_安全漏洞_NVRMini2_cgi_system_缓冲区溢出漏洞[CVE-2018-1149][CNNVD-201809-862]
高危
HTTP
攻击利用
HTTP_PHP_com_print_typeinfo_函数缓冲区溢出漏洞攻击[CVE-2012-2376]
高危
HTTP
攻击利用
HTTP_安全漏洞_Netgear_WNR2000v5无线路由器栈溢出漏洞[CVE-2016-10174][CNNVD-201702-105]
高危
HTTP
攻击利用
HTTP_安全漏洞_DLink_DIR809栈溢出漏洞[CVE-2021-33274][CNNVD-202112-051]
高危
HTTP
攻击利用
HTTP_HPOpenViewNNM_getnnmdata.exe_Hostname参数缓冲区溢出漏洞[CVE-2010-1555]
中危
HTTP
攻击利用
HTTP_PHP7_zip组件整型溢出攻击[CVE-2016-3078]
中危
HTTP
攻击利用
HTTP_Aladdin_Knowledge_System_PrivAgent.ocx控件的ChooseFilePath方法缓冲溢出漏洞
中危
HTTP
攻击利用
HTTP_D-Link路由器_HNAP服务基于栈的缓冲区溢出漏洞[CVE-2016-6563][CVE-2016-6563][CNNVD-201611-125]
中危
HTTP
攻击利用
HTTP_Mozilla_Firefox整数溢出漏洞[CVE-2012-5835]
中危
HTTP
攻击利用
HTTP_GPON_路由器_认证栈溢出漏洞[CVE-2019-3921][CNNVD-201903-081]
中危
HTTP
攻击利用


策略管理
首页
检测配置
策略集
全部策略
分组方式:
协议类型
内容:
拒绝服务
查询
共 10 条
事件名称
事件级别
协议类型
安全类型
HTTP
HTTP_Windows_win32k.sys代码错误远程任意代码执行或拒绝服务漏洞[MS12-008][CVE-2011-5046]
高危
HTTP
攻击利用
HTTP_拒绝服务_slowhttptest_攻击
高危
HTTP
攻击利用
HTTP_Oracle_Data_Integrator_拒绝服务漏洞[CVE-2014-2417]
中危
HTTP
攻击利用
HTTP_Firefox_v54.0.1拒绝服务漏洞
低危
HTTP
攻击利用
ICMP
TCP
UDP


策略管理
首页
检测配置
策略集
全部策略
分组方式:
协议类型
内容:
扫描
查询
共 49 条
事件名称
事件级别
协议类型
安全类型
HTTP
HTTP_安全扫描_扫描器netsparker
中危
HTTP
攻击探测
HTTP_安全扫描_扫描器webinspect
中危
HTTP
攻击探测
HTTP_安全扫描_扫描器Rsas
中危
HTTP
攻击探测
HTTP_安全扫描_扫描器WebReaver
中危
HTTP
攻击探测
HTTP_安全扫描_扫描器Sqlmap
中危
HTTP
攻击探测
HTTP_安全扫描_扫描器zgrab
中危
HTTP
攻击探测
HTTP_安全扫描_扫描器nmap
中危
HTTP
攻击探测
HTTP_安全扫描_扫描器BurpSuite
中危
HTTP
攻击探测
HTTP_IBM_Rational_Appscan_漏洞扫描
中危
HTTP
攻击探测
HTTP_Nilloo_IIS_Security_Scanner_漏洞扫描
中危
HTTP
攻击探测
HTTP_绿盟极光漏洞扫描器_WEB漏洞扫描
中危
HTTP
攻击探测
HTTP_SQLmap_注入扫描
中危
HTTP
攻击探测

设备同时支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMTP 等多种协议的漏洞检测。

设备通过自定义漏洞，可使用文本匹配或正则匹配定义漏洞特征，从而进一步丰富自定义规则库，对网络中攻击行为持续检测。



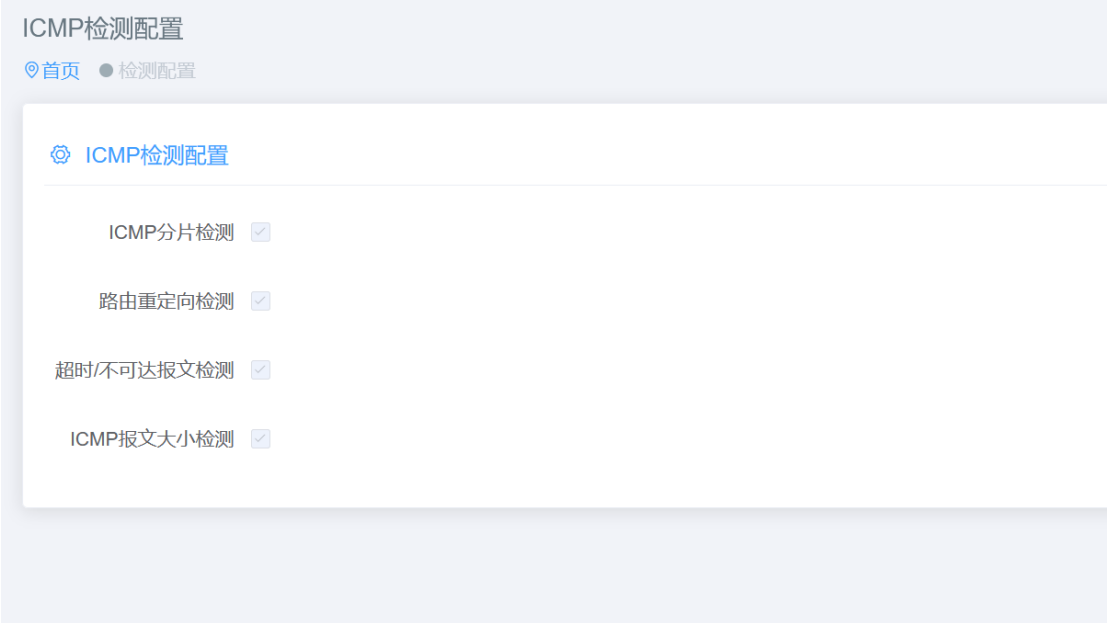
- 网络层攻击检测

针对网络层的攻击也是目前互联网上常见的几种主要的攻击方式，通性都是通过制造大量的无用数据包，对目标服务器或者主机发动攻击，使得目标对外拒绝服务，可以理解为 DDOS 或者是类 DDOS 攻击。天阗威胁分析一体机支持 Flood 攻击检测，包括 SYN Flood、ICMP Flood、UDP Flood 和 IP Flood。可对恶意扫描进行检测，包括 Tracert 检测、IP 地址扫描、端口扫描。对网络通信中的异常包攻击进行检测，包括 Ping of Death、Teardrop、IP 选项、TCP 异常、Smurf、Fraggle、Land、Winnuke、DNS 异常和 IP 分片。

当攻击行为发生时需要设备对其进行有效处置，从而避免攻击行为的进一步扩散，天阗威胁分析一体机通过基于 IP 地址的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断。

设备满足多种方式的威胁处置，可通过基于 URL 的旁路阻断，并能将 URL 请求进行重定向。

天阗威胁分析一体机支持 ICMP 管控检测，包括 ICMP 分片检测、路由重定向报文检测、不可达报文检测、超时报文检测和 ICMP 报文大小限制。



4.2 动静态相结合的未知威胁检测

天阗威胁分析一体机采用国内领先的双重检测方法（静态检测和动态检测），多种核心检测技术手段：二进制检查、堆喷检测、ROP 利用检测、敏感 API 检测、堆栈检测、Shellcode 检查、沙箱检查等，可以检测出 APT 攻击的核心步骤。可实现包括对：未知恶意代码检查、嵌套式攻击检测、木马蠕虫病毒识别、隐秘通道检测、恶意文件、间谍软件等多类型未知漏洞（0-day）利用行为的检测。同时，通过 TAR-AIO 威胁分析系统进行威胁分析，有效发现 APT 攻击。

1. 文件调度

TAR-AIO 文件检测引擎设计了一套全新的高效智能虚拟机调度引擎，该引擎能根据当前的系统资源占用和自动启动或关闭相应的虚拟环境，保证样本的实时检测性。另外当样本数量突发时虚拟机调度引擎亦能智能调节虚拟机任务的分发。文件检测引擎内置 windows 系列、Linux、安卓、中标麒麟等 6 种主流类型、共近 50 个虚拟系统，可并发至少 20 个 OS 同时运行。

图 13_智能虚拟机调度引擎

2. 静态检测

静态检测引擎方面，主要充分利用公司原有的在软件功能与安全事件检测能力的技术积累，进行有效的扩充，以保障该检测的高效与准确，大体包含如下几部分：

- 已知恶意木马病毒检测：集成国内外流行的病毒检测引擎，对提交的文件进行检测，如发现为已知木马病毒，则汇报已知木马病毒攻击事件。
- 已知漏洞攻击样本检测：使用已知漏洞攻击样本签名技术检测常见已知的基于漏洞攻击样本，对提交的数据文件和 URL 对应的 HTML 内容进行检测，如发现为已知漏洞攻击，则汇报已知漏洞攻击事件。
- 恶意代码行为特征检测：通过对各种恶意代码的行为进行研究，提取出相应的网络及系统行为特征，具体来说，就是把恶意代码通常的网络连接、注册表操作、文件操作以及进程操作等行为特征提取出来做为一个恶意代码行为特征库。该检测不再依赖于具体的已知漏洞和病毒木马样本，而是分析文件中是否包含具有威胁的行为特征来进行检测，该算法可以检测针对数据文件应用的未知漏洞（0 day 漏洞）的攻击而无须知道漏洞信息。
- 静态仿真检测技术（SSE）：通过模拟真实 CPU 环境对文件中可能存在的可疑代码进虚拟执行，使用一定的算法，当发现可疑的 shell code 时便可判定为恶意文件。例如：微软的文档(RTF,DOC)的 shell code 代

码一般直接存在于文件中，因此可以先对其进行格式解析，对各段数据进行解密。然后将合适的数据送入到模拟执行函数尝试进行执行，看其是否为可执行代码。如果为可执行代码则判定该文档存在问题。对于不易直接检测出 shell code 的 PDF，SWF 等文件，我们也会使用相应的算法提取出可疑的 shell code 特征，并送入对应的静态模拟器中进行代码识别，以识别出其是否为真正的二进制代码。

- 策略匹配检测技术：使用一定的策略算法，发现文件中异常的情况。例如：在文档文件中，通过一定的算法，检测是否内嵌有 PE 文件，如有 PE 文件，则可判定为恶意文件。

- 自定义 YARA(一个知名的恶意软件识别和分类工具)规则：支持自定义 YARA 规则，对检测算法进行扩充。

值得一提的是，项目实施单位研发的静态恶意代码检测技术，通过恶意代码行为特征检测、静态仿真检测技术（SSE）以及策略匹配检测技术同样能够识别未知漏洞。

3. 动态检测

恶意代码的动态检测，主要用于发现 0 day 攻击，并对恶意代码进行行为分析，自动提取样本与检测规则，并进一步完善静态检测引擎。在虚拟环境下执行可疑样本，分析其行为，对应用软件以及系统的影响，来判定是否有漏洞触发。若明确触发了漏洞，则提取相应的恶意样本，并根据行为分析自动生成静态检测规则。本部分涉及到的关键技术有：

- 虚拟环境调度技术：通过指纹识别，确定可疑样本涉及的虚拟环境，并行调度，提高检测的准确度与性能。

- 虚拟环境下的动态检测技术：采用调试方式启动应用程序，能够发现程序执行过程中的所有异常，并基于此发现攻击行为的发生。

- 动态检测规则：判定真实 0 day 攻击产生的依据，包括但不限于以下几

种：

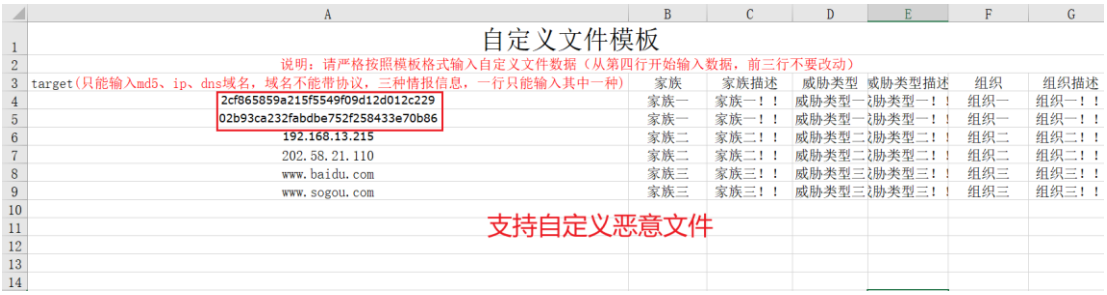
- 数据代码的执行
- 可疑文件的创建
- 系统资源的异常占用
- 应用进程的崩溃
- 外部资源的异常访问
- 下载外部文件

动态虚拟检测技术，是在真实的虚拟机环境中，启动对应的文件应用打开可疑的样本，并分析其产生的行为。这里的行为主要有两个方面：一是漏洞利用行为，包括但不限于程序崩溃，可疑的堆喷行为，非代码执行区试图执行代码的行为，运行时内存中是否有可疑 shell code 特征等等。二是检测文档文件执行过程中是否有异常行为，包括但不限于是否有生成或下载新的可疑文件，是否启动异常进程，是否注册系统服务或启动项，是否有外连行为等等。以上述行为来判定是否有漏洞触发。

4. 恶意文件检测

什么是恶意文件？恶意文件指带有程序设计者出于攻击意图所编写的一段程序文件，一旦运行该文件就会被感染，从而达到传播的目的。天阗威胁分析一体机通过全面、强劲的恶意文件检测和发现能力，对 HTTP、FTP、SMTP、POP3、IMAP、SMB、TFTP、NFS 协议进行恶意文件还原检测。有效发现网络内传输的恶意文件，快速定位功攻击者及被攻击者，从而降低风险的持续扩散。

天阗威胁分析一体机可以自定义恶意文件，通过 MD5 码来定义恶意文件特征。丰富恶意文件的名单列表，从而对网络内环境持续监测，发现恶意文件传播的行为。



5. 间谍软件检测

什么是间谍软件？间谍软件可能是计算中最好命名的一种软件了。它偷偷溜进你的电脑，并在你不知情的情况下窥探你的私人信息，就像一个真实的间谍一样。如何有效发现间谍软件？天阗威胁分析一体机支持多种类型的间谍软件检查，包括：木马后门、病毒蠕虫、僵尸网络、自定义签名。同时设备支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMTP 等多种协议的间谍软件检测。

设备可以通过自定义间谍软件，允许通过文本匹配或正则匹配定义间谍软件特征。通过灵活方式对间谍软件进行定义，从而对网络流量中持续监视间谍软件的通信情况。


新增自定义间谍软件规则
* 事件名称
事件名称
事件别名
事件别名
事件说明
事件说明
* 协议类型
TCP
影响系统
非关键系统
事件级别
非攻击事件
影响设备
非关键设备
事件类型1
可疑行为
IP反转
否
事件类型2
其它可疑行为
攻击阶段
其它
事件类型3
其它可疑行为
攻击状态
攻击尝试
Pcap存储
否
* 特征定义
特征定义向导
* 是否启用
否
策略名称
请选择
重置
确 定

4.3 攻击链还原自动化扩线分析

目前市面上的相关产品，基本无法全面的从海量告警中发现有效供给和有价值的线索；均不具备完整攻击链还原能力；未充分、有效利用专业分析模型进行分析，ATT&CK 分析框架应用普遍被作为产品宣传卖点，但未达到应有应用效果，只是噱头。

- TAR-AIO 并非只是利用规则告警，结合威胁情报产生线索；也不是以 UEBA 概念进行包装，进行单点前后串联分析。
- TAR-AIO 并非只是利用规则告警，单点对应 ATT&CK 技战术，结合威胁情报产生线索；也不是以知识图谱的展现形式，进行单点技战术分析，突出 APT 组织威胁情报能力。
- TAR-AIO 并非只是以威胁情报为主，结合规则告警，对应 Kill Chain；也不是以 Kill Chain 作为攻击链还原模型，对应有限攻击属性。

图 14_ TAR-AIO 攻击链还原分析流程

天阗威胁分析一体机，利用当前确定性线索为中心，以事件名称、事件标签、攻击者、被攻击者、攻击结果等作为基础信息原点，向前、向后进行检索，利用历史流量数据发现确定性线索关联可疑行为线索，从而对整个攻击链进行扩线分析,并与 ATT&CK 模型映射生成攻击行为画像，形成支持自定义的 web 可视化拓扑。还可联动全流量分析取证系统（NFT）对未知威胁进行威胁狩猎，进而无遗漏、更完整的还原所有攻击链。

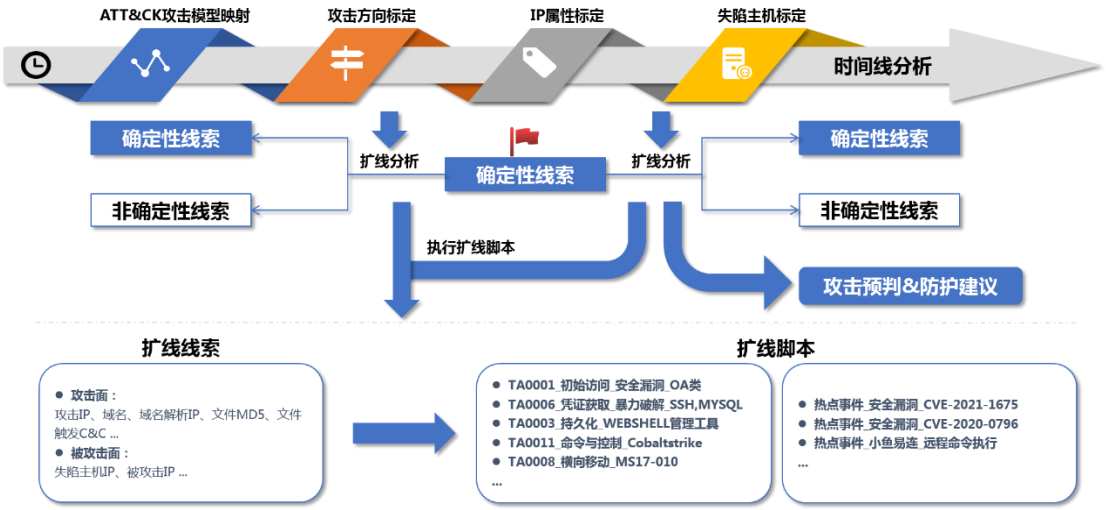


图 15_自动化扩线分析原理

4.4 基于算法模型的检测能力

1. DGA 域名检测

基于 APT 组织恶意域名算法，自动生成 DGA 域名列表，检测网络中试图绕过黑名单检测机制的行为。通过机器学习模型分析域名解析流量，读取 dns 解析日志里面的 host 字段，取出域名（例如： www.google.com, google.com 为域名），通过机器学习模型判断该域名安全性。呈现内容包括源 ip、请求域名、请求次数、准确率、最近访问时间等。检测流程如下：

- 预处理：提取域名中的主域名名称部分。
- 特征提取：提取出元音所占比例、数字和字母转换所占比例、主域名熵、N-gram 等特征。
- 多模型打分：根据每个模型得到的总分进行 DGA 域名分类。

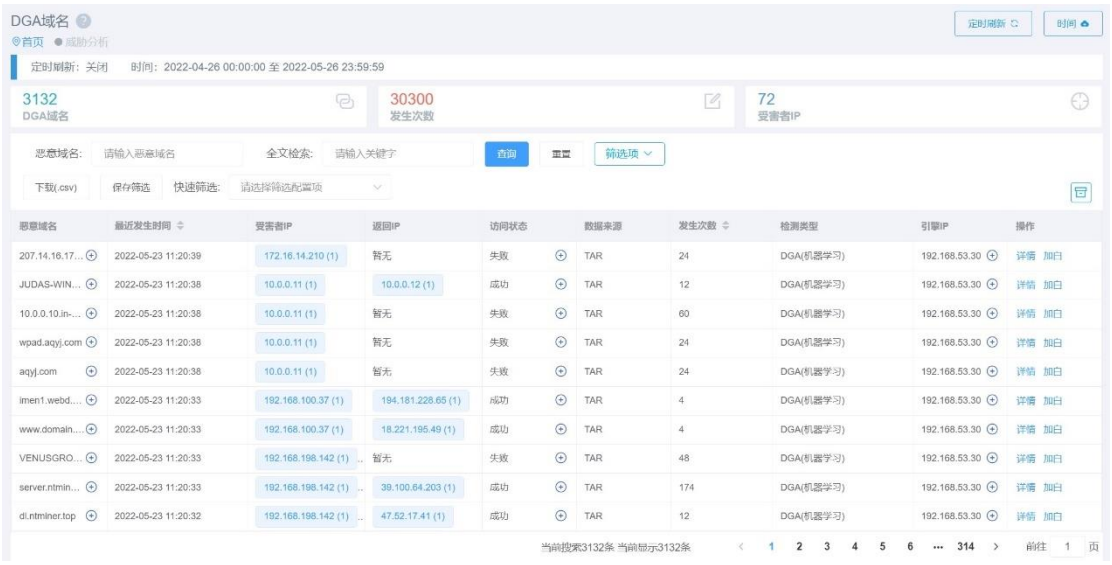


图 16_ DGA 域名检测

2. 精准失陷主机检测

失陷主机，指因遭受 APT 攻击、僵木蠕毒等风险而被攻击者控制的主机。天阗威胁分析一体机结合智能分析技术、威胁情报关联等，发现内部已经失陷的主机。结合攻击链，发现主机在每个攻击阶段发生的所有事件。结合事件情况为主机评定状态。检测流程如下：

- 情报匹配：高价值域名情报匹配。
- 域名请求行为分析：请求次数大小，周期性规律，响应情况。

- 后续流量行为分析：上下行流量关系，周期性规律，是否包含敏感文件，是否长连接等。

图 17_失陷主机分析

3. 智能分析模型

天阗威胁分析一体机通过智能分析模型检测方式，对网络中的请求访问、通信行为、非正常访问、恶意攻击等进行智能分析，通过模型分析有效识别网络中的攻击行为，从而对恶意行为及时处置，避免攻击行为的进一步扩散。

- 网络攻击检测模型

支持通过对原始流程采集结，经过多元异构数据融合，进行网络攻击样本特征训练，分析出高精准网络攻击行为。

- WEB 访问检测模型

支持通过对 web 访问流量匹配多种 web 异常访问特征来检测 web 访问类告警，检测特征包括但不限于 weblogicWar、Struts2、敏感文件泄露、代码执行、跨站脚本攻击 XSS、SSRF 攻击、任意文件下载等。

- TCP 流量检测模型

支持通过对 TCP 流量匹配 9 种 TCP 异常特征检测出网络告警，检测特征包括但不限于利用 redis 写 webshell，Weblogic 反序列化、Linux 反向 shell、Windows 反向 shell、Http 代理、Socks 代理、Teamview、Irc(互联网中继聊天)、恶意邮件发送者等。

4.5 结合威胁狩猎的主动防御

威胁狩猎是指采用人工分析和机器辅助的方法，针对网络、终端等的日志或告警数据进行主动搜索、关联和分析，从而检测出以往被动检测无法察觉的威胁。威胁狩猎一般分为四个过程：

- 首先，安全专家需要结合资产信息、威胁情报对网络中可能存在的高风险点进行预判；
- 其次，利用已收集的数据，使用可视化、数据统计分析等方法对数据集进行挖掘与分析，查找已知或未知的攻击线索；
- 之后，结合威胁模型对已发现攻击者的攻击工具和攻击技术进一步挖掘，发现攻击者的 TTP；
- 最后尝试对上述威胁发现过程进行标准化或自动化。

图 18_威胁狩猎情报应用

TAR-AIO 从以下几点，可完整匹配威胁狩猎流程，挖掘更多未知威胁：

1. 威胁情报云查（详见 4.6）

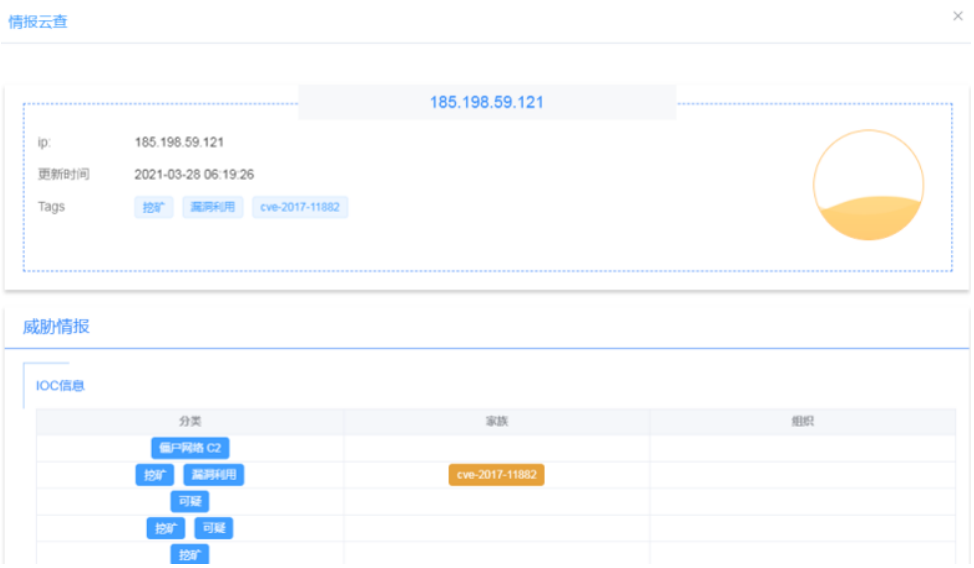


图 19_情报云查

2. 可视化数据分析挖掘（详见 5.3）

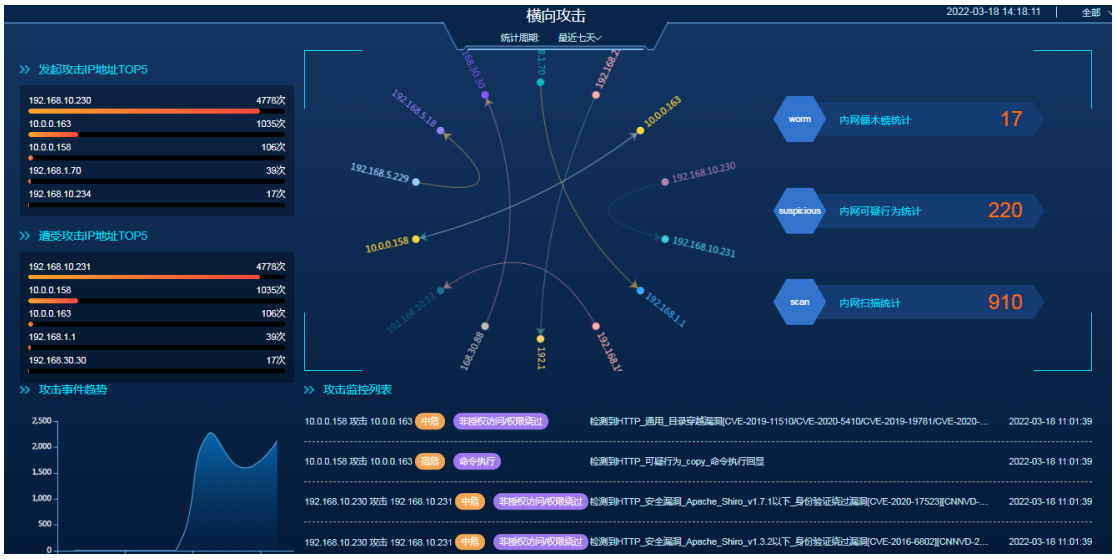


图 20_威胁感知分析大屏

3. 情报狩猎

历史数据匹配时通过自定义报表中的 ip、dns 域名、MD5 值系统历史数据中的 ip、dns 域名、MD5 进行对比。匹配到对应的值以后展示相对应的自定义情报信息，对可疑威胁进一步挖掘。

图 21_情报狩猎

4. 攻击链分析（详见 4.3）

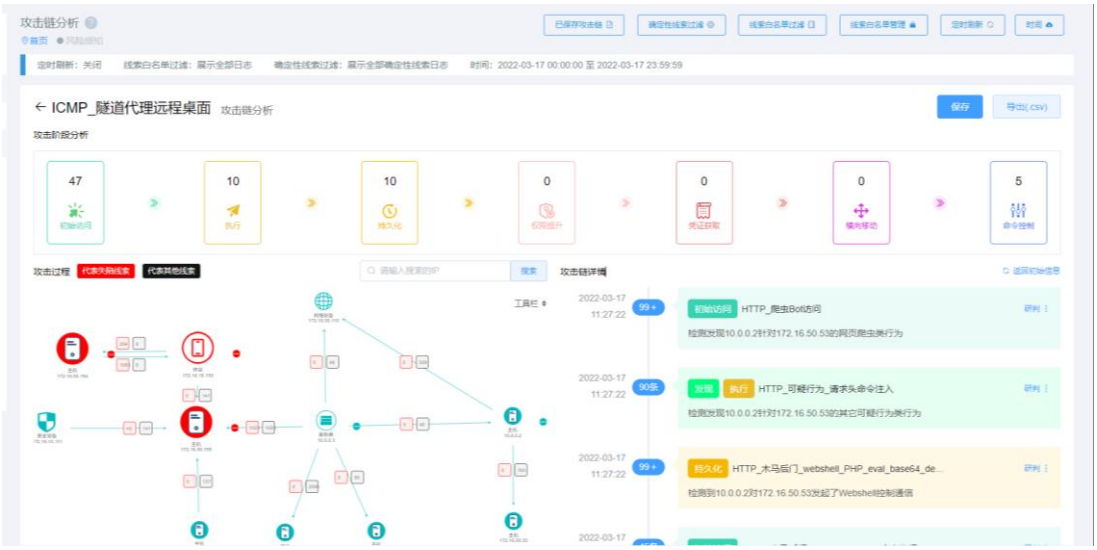


图 22_攻击链还原分析

4.6 VenusEye 情报云查辅助降低甄别难度

天阗威胁分析一体机内置可机读的 VenusEye 威胁情报，结合本地智能分析引擎，对本地网络中采集的流量元数据进行实时分析比对，发现已知威胁及可疑连接行为，增加智能分析技术的准确性和检出率。如通过行为分析发现的隐蔽隧道通信行为（如 DNS 隧道）仅为可疑行为，但若其连接的地址信息与威胁情报的僵木蠕毒情报相关联，通过分析模型可检测为远控行为。

同时，下发的威胁情报结合本地流量数据，可形成本地化的威胁情报，安全专家可利用威胁情报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，准确地进行威胁追踪和攻击溯源。VenusEye 威胁情报保持 Day 级更新频率，设备可实时自动升级下发，保证时效性。

图 23_VenusEye 威胁情报中心

启明星辰 VenusEye 威胁情报，已经积累了过亿级的 IOC 情报数量，涵盖基础信息、攻击威胁、可疑行为、恶意站点、恶意软件、攻击组织、失陷主机等情报类型。与全量信息采集进行有效配合，对所有采集信息进行威胁碰撞，实时检测终端每一个运行过程的安全性。

启明星辰多年网络安全研究经验积累的集中体现，参与了多项国家级、行业级的威胁情报标准制定。启明星辰 VenusEye 威胁情报中心拥有庞大的数据基础，数据采集方式以自动化数据采集为主，同时辅以威胁情报专家的人工分析。威胁情报的主要来源包括自有的样本分析系统的循环挖掘、第三方商业情报交换、开源情报（开源沙箱、技术论坛、开源样本网站、安全从业人员社交媒体、开源情报网站等）、用户和产品上报等，总体的威胁情报来源数量已达到 200 多个。通过大量的样本分析和跟踪研究，一方面提取各种攻击行为事件；另一方面总结和提炼出各种攻击组织的来源、目标、工具、手段等攻击组织相关特性。

4.7 数据采集及配置管理

天阗威胁分析一体机支持解析、生成及外发 TCP 流量日志、UDP 流量日志、Web 访问日志、域名解析日志、FTP/SMB/TFTP 协议的文件传输日志。设备通过解析、生成、外发多种日志类型及多种字段有助于对网络流量进行详细的分析，便于分析人员按需查看字段信息，辅助分析人员对日志事件的研判。

设备通过灵活的策略配置对接入设备的流量进行安全分析，对策略配置的调整便于客户更能贴合实际业务情况进行监测。

- **日志字段支持情况**

1、TCP 流量日志字段：

传感器序列号、UDP 数据流开始的时间、UDP 数据流结束的时间、源 ip、源端口、目的 ip、目的端口、源 mac、目的 mac、协议、上行字节数、下行字节数、上行包数、下行包数字段等；

2、UDP 流量日志字段：

传感器序列号、UDP 数据流开始的时间、UDP 数据流结束的时间、源 ip、源端口、目的 ip、目的端口、源 mac、目的 mac、协议、上行字节数、下行字节数、上行包数、下行包数字段；

3、Web 访问日志字段：

传感器序列号、日志生成时间、源 ip、源端口、目的 ip、目的端口、HTTP 请求方法、HTTP 包头的 URI 字段、uri_md5 值、host 字段、host_md5 值、origin 字段、cookie 字段、ser-Agent 字段、referer 字段、链接来源、原始数据、http 状态码、Content 类型等；

4、域名解析日志字段：

时间、源 ip、源端口、目的 ip、目的端口、DNS 访问类型、Host、Host 字段_MD5 值、地址资源、MX 记录、响应结果状态、域名规范名称等；

5、FTP/SMB/TFTP 协议的文件传输日志字段：

传感器序列号、协议、日志生成时间、客户端 IP、客户端应用端口、服务端 IP、服务　端应用口、传输模式、文件名字、文件 md5、文件类型等。

- 策略配置情况

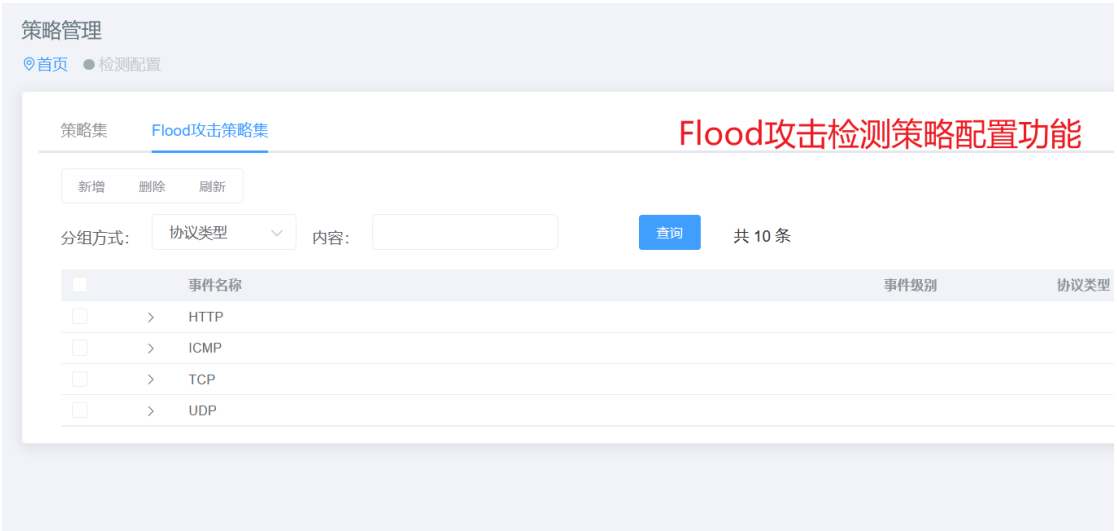
天阗威胁分析一体机设备基于源地址、目的地址、服务、流量采样比、时间进行选择数据采集对象，针对采集对象进行网络流量数据采集和威胁检测数据采集，网络流量数据采集自定义流量载荷的格式和流量上下行载的长度。

设备基于 SSL 协议的 HTTPS 流量进行解密、威胁检测，通过添加源地址、目

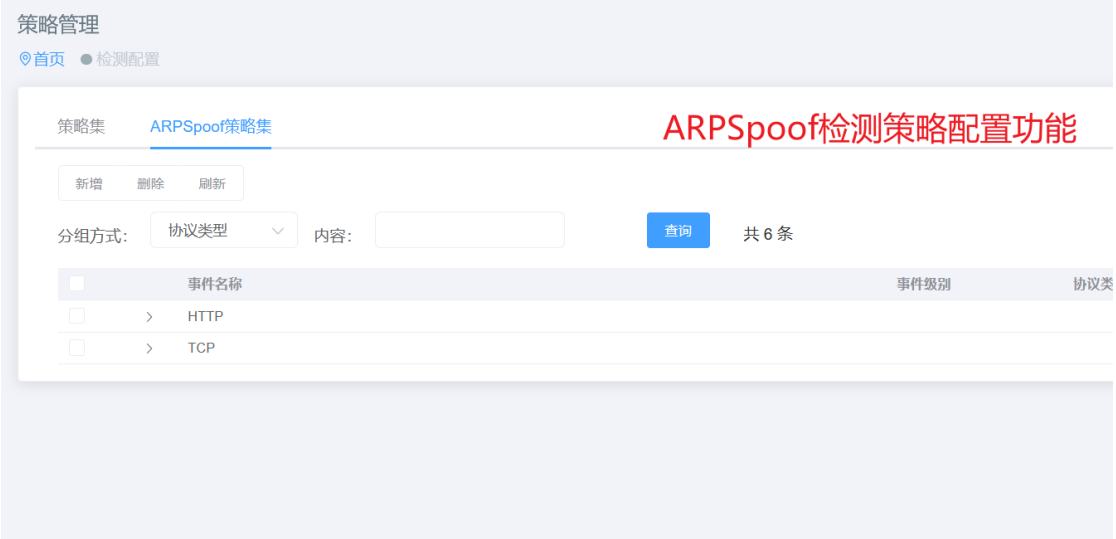
的地址的解密策略。通过添加 SSL 入站检查配置文件。SSL 入站检查配置文件中指定 SSL 解密证书。

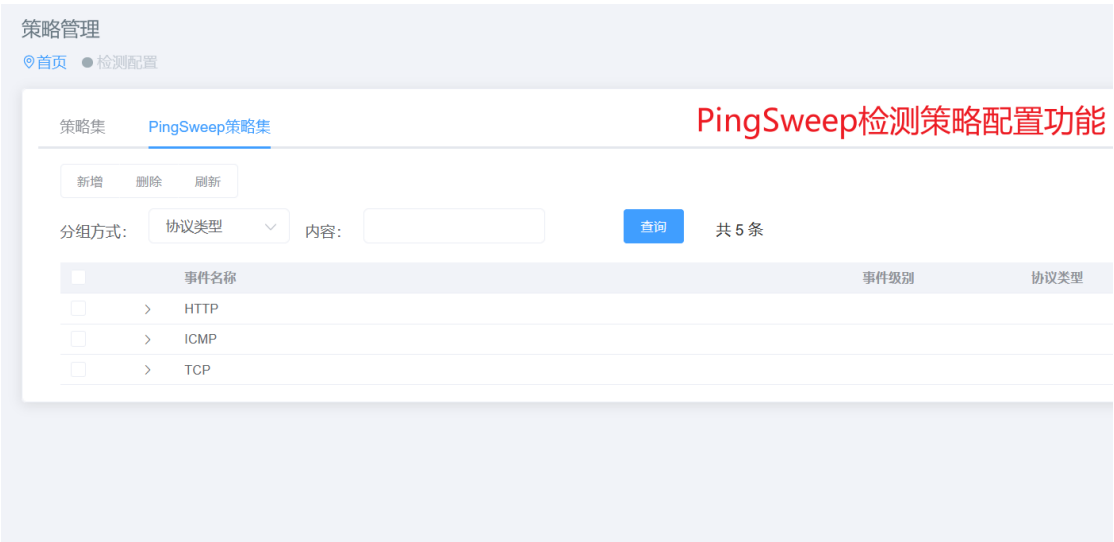
天阗威胁分析一体机设备可以对 WEB 端攻击提供监测，例如针对恶意扫描、Flood 攻击、IP 碎片攻击、ARPSpoof、PingSweep 等检测进行策略配置。


策略管理
首页
检测配置
策略集
恶意扫描策略集
恶意扫描检测策略配置功能
新增
删除
刷新
分组方式:
协议类型
内容:
查询
共 51 条
事件名称
事件级别
协议
HTTP
TCP
TCPSTREAM
UDP


策略管理
首页
检测配置
策略集
Flood攻击策略集
Flood攻击检测策略配置功能
新增
删除
刷新
分组方式:
协议类型
内容:
查询
共 10 条
事件名称
事件级别
协议类型
HTTP
ICMP
TCP
UDP


策略管理
首页
检测配置
策略集
IP碎片攻击策略集
IP碎片攻击检测策略配置功能
新增
删除
刷新
分组方式:
协议类型
内容:
查询
共 1 条
事件名称
事件级别
协议
IP





设备通过旁路 IPv4 和 IPv6 的 IP 阻断、URL 重定向、DNS 重定向方式对攻击行为进行处置，可与监管平台对接联动。

五. 功能价值呈现

5.1 基于完整流的取证与研判分析

为了应对网络安全事件处置过程中的分析研判诉求，本着适度采集记录的原则，天阗威胁分析一体机采用攻击事件完整流量存储能力。用户可通过上报事件进行分析研判，不仅具备原始流量文件下载的能力，还能够对原始流量进行解析，支持研判分析可视化呈现、流跟踪以及 wireshark 解码，帮助客户收集尽可能多的信息或证据。

图 24_分析研判

图 25_取证溯源

5.2 全面实时的监测与威胁分析

要做到全网威胁分析，必须需要具备多维度的监测、分析体系。天阗威胁分析一体机从威胁视角、风险感知、威胁分析进行三大维度的安全实时监测能力构建，来达成全面的检测体系。这三大维度均有其对应的最终目标，包括：

- 威胁视角：基于 ATT&CK 攻击模型的思路，提供各阶段攻击展示，包括威胁情报视角、攻击者视角、被攻击者视角、事件视角、样本视角、横向移动分析等。
- 风险感知：以业务资产为核心，寻找暴露面，包括失陷主机分析、攻击链分析、脆弱性分析等。
- 威胁分析：从分析场景的角度展开，进行专题分析，包括 DNS 服务分析、邮件行为分析、挖矿行为分析、暴力破解检测、扫描探测检测、DDOS 检测、Web 攻击检测、僵木蠕检测等。

5.2.1 威胁视角

1. ATT&CK 视角

通过我司安全专家在业内多年的经验积累，结合 ATT&CK 知识体系构建了一套更细粒度、更易共享的知识模型和框架。在这套体系中，结合当前常用攻击手段及热点事件，总结并整理出一系列的专题性的价值分析模型，并在天阗威胁分析一体机中进行应用，利用产品自身的威胁检测能力提供基础事件，通过有效的威胁分析，将分析结果进行可视化呈现，形成一系列价值分析场景。

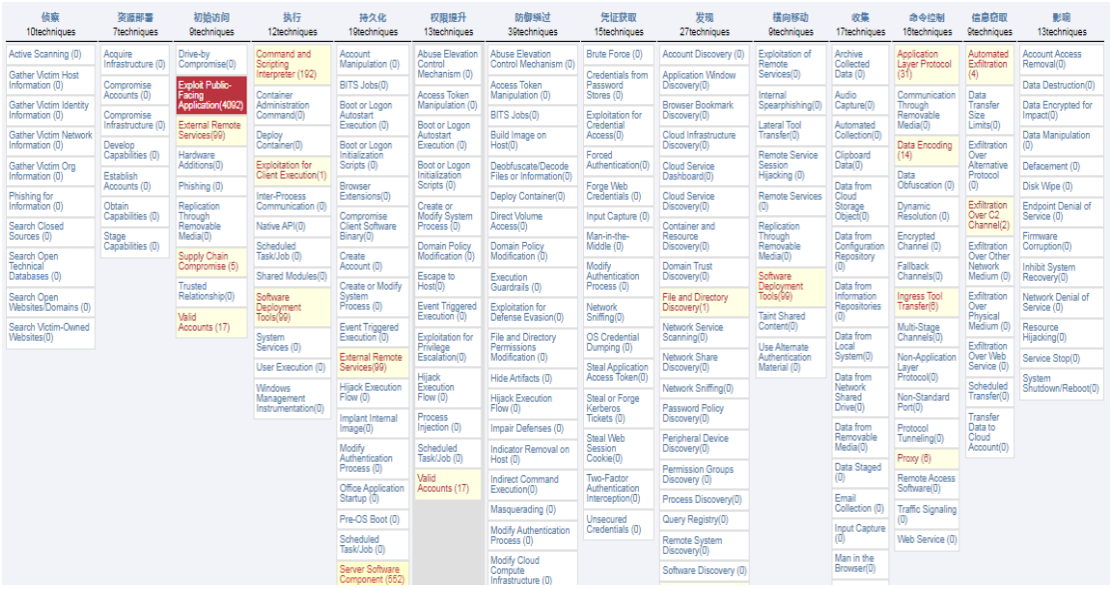


图 26_ATT&CK 视角

2. 事件视角、样本视角等

天阗威胁分析一体机通过攻击者视角、被攻击者视角、样本视角、事件视角等多维线索聚合，深度挖掘可疑关联，提供攻击者、被攻击者双向的威胁分析起点，在攻击面与被攻击面之间寻找深度隐藏的线索关联。

图 27_特征事件视角

3. 横向移动分析视角

横向移动分析视角，基于对东西向流量的抓取，结合规则检测、基线分析，挖掘内网主机之间存在的异常威胁行为，定位异常的内鬼主机，识别内网主机对其他内网主机发起攻击的情况，如漏洞利用攻击、向 SMB 服务器传毒等。可发现可疑的跳板源或内鬼。

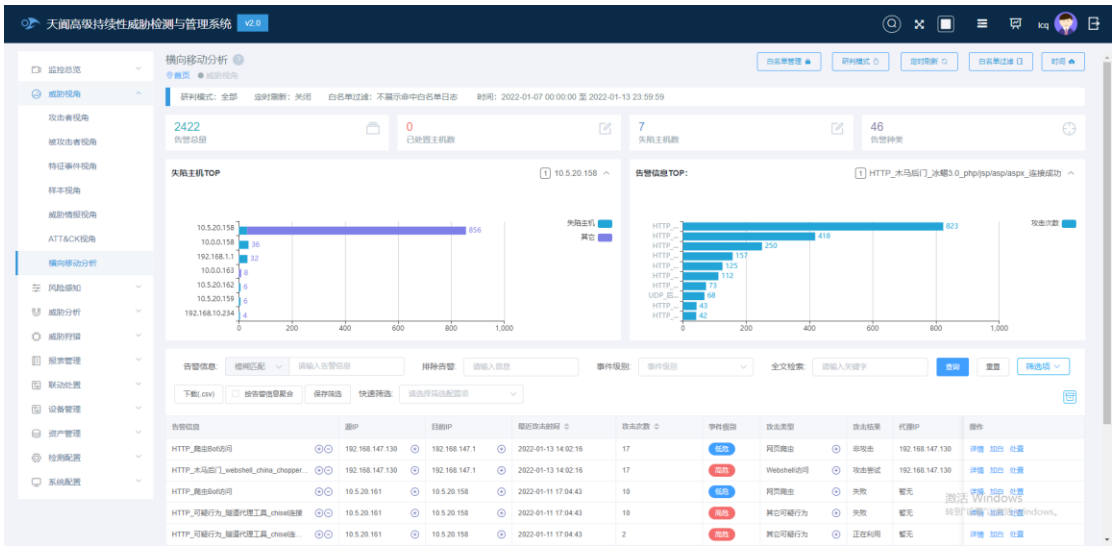


图 28_横向移动分析视角

5.2.2 风险感知

资产是全网安全最重要的防护点，尤其是承载业务的服务器资产。所有的威

胁都必须利用服务器的某个脆弱性才能造成伤害，因此，服务器脆弱性的识别和加固便显得十分重要，能够有效预防威胁的发生。

1. 漏洞感知

基于探针组件的被动流量信息和漏洞指纹特征，识别疑似存在具体漏洞的主机/URL、疑似漏洞的举证信息及修复建议，为安服人员快速定位。

2. 脆弱口令

可针对 HTTP、FTP、SMTP 等登陆协议。弱密码指密码强度低，如简单的数字组合、与帐号相同、密码长度过短等。弱密码很容易被黑客破译利用，从而使用合法的帐号密码进行登录控制，隐蔽性较强。

图 29_脆弱口令

3. 高危端口

识别服务器资产开放的风险端口及端口被使用情况（如标准端口跑非标准协议），同时结合启明星辰十几年的应用识别积累能力，识别因暴露风险应用访问方式（如 RDP、SSH、数据库）被非法连入的情况，即使非标准端口亦能识别具体应用。

失陷主机分析详见 4.4，攻击链分析详见 4.3。

5.2.3 威胁分析

1. DNS 行为分析

- DNS 隧道：从专题场景角度分析，可以发现网络中试图通过 DNS 协议进行网络通信的行为，可检测隐匿木马后门的通信流量。
- DGA 域名：基于 APT 组织恶意域名算法，自动生成 DGA 域名列表，检测网络中试图绕过黑名单检测机制的行为。
- 恶意域名：基于 VenusEye 提供的威胁情报，对流量中的域名进行匹配，可快速检测出 APT 组织、僵木蠕家族。

图 30_DNS 隧道分析

2. 邮件行为分析

该场景可对邮件进行发件人检测、恶意链接检测、附件检测、垃圾邮件检测等专题分析。

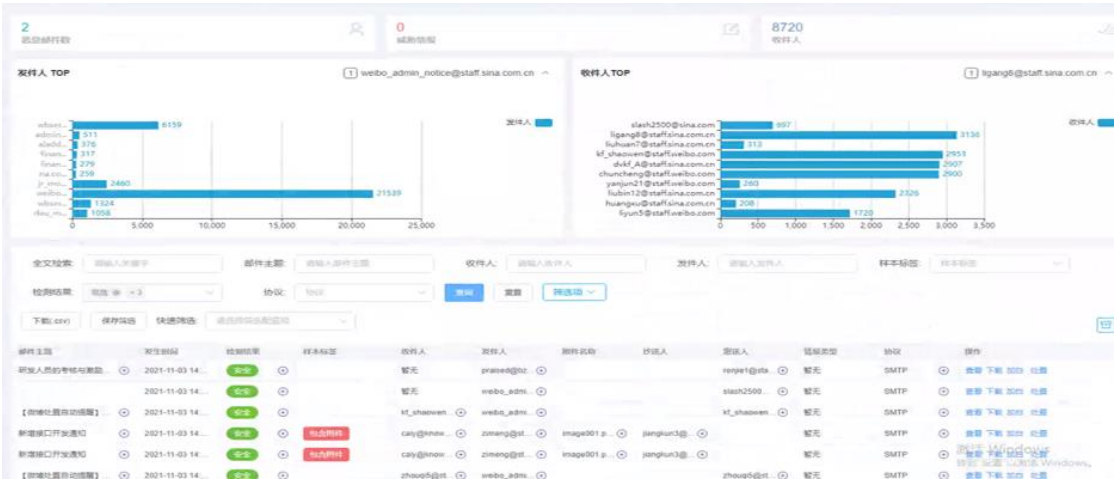


图 31_邮件行为分析

3. 挖矿行为分析

针对挖矿场景行为进行分析，统计展示维度包括币种统计、阶段分析、矿机统计、趋势分析等。

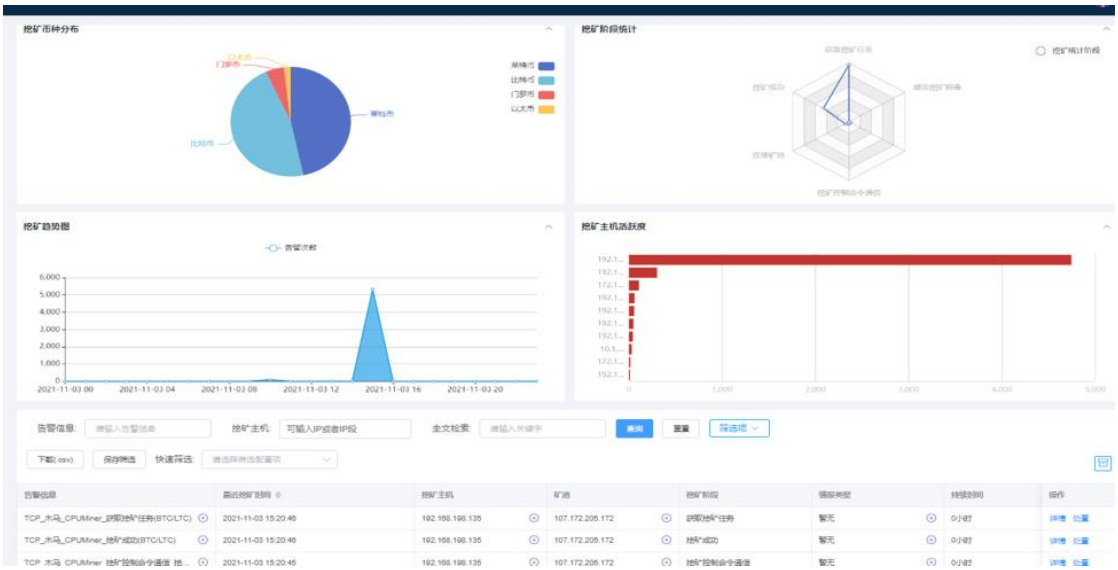


图 32_挖矿行为分析

4. 其他威胁分析

包括暴力破解检测、扫描探测检测、DDOS 检测、Web 攻击检测、僵木蠕检测、可疑行为检测。其中可疑行为检测，用于识别区别于具体攻击类型的可疑行为。包括异常的敏感文件下载、机器扫描行为、异常流量行为、异常文件上传等，发现潜在的泄密或窃取行为。

图 33_可疑行为

5.3 多维度可视化安全预警

基于宏观视角，展示整体安全情况，能清楚的了解当前网络安全状况、评级分数、爆发的重大事件等，并能评估防御不足还是内部威胁，决策哪里需要加固。

主要用于领导层面掌握全网态势：

- **全局视野呈现全网态势**
- **辅助安全建设决策**

宏观视角主要以大屏展示为主，以 1 个主大屏 + 7 个辅助大屏+1 个轮播大屏组合呈现整体安全现状和细分安全情况。

1. 全局分析大屏

主屏基于安全域视角，展示全网各个区域的整体安全实况及综合评级。该大屏主要展示重要风险，不是简单统计，而是从高价值事件通报视角、资产可视、ATT&CK 攻击阶段分析、区域横向威胁、外部威胁、恶意外联等多个角度呈现重要问题，让预警更有价值。

多个区域模块实现下钻能力，可通过点击各具体内容一步步下钻到具体详情，最终到日志数据及问题指派，以此形成可分析、可指派的安全监测指挥中心。

图 34_全局分析大屏

2. 辅助大屏+轮播大屏

目前共有 7 个辅助大屏+1 个轮播大屏，围绕主大屏进行多个视角的详细展示，并支持下钻挖掘分析。包括外部攻击、威胁情报、横向攻击、恶意外联、文件检测等。

图 35_多维度大屏展示

5.4 可感知的威胁告警

为便于运维体验和安全专家分析，天阗威胁分析一体机设计可感知的安全告

警，让威胁具有易识性、易理解。

1. 标签化

通过打标签形式，将每个安全事件告警以其分类、样本标签、家族名称、ATT&CK 等以短名称的颜色标签进行表示，每个标签均提供详细说明。

图 36_样本视角标签化告警

2. 描述性评级

如下所示，为更易理解所发生的安全事件的重要性和紧迫性，天阗威胁分析一体机对每个事件均提供“事件级别”、“攻击结果”、“攻击阶段”、“响应码”、“攻击方向”等描述性评级。

事件级别	响应码	攻击类型	攻击结果	攻击方向	攻击阶段
高危	201	其它可疑行为	攻击成功	内网->内网	初...

图 37_描述性评级

3. 关联分析

结合天阗威胁分析一体机探针组件的细粒度采集能力和系统智能分析能力，能覆盖整个攻击链的所有攻击流程，检测攻击者的每个阶段发起的所有安全事件和造成的影响。

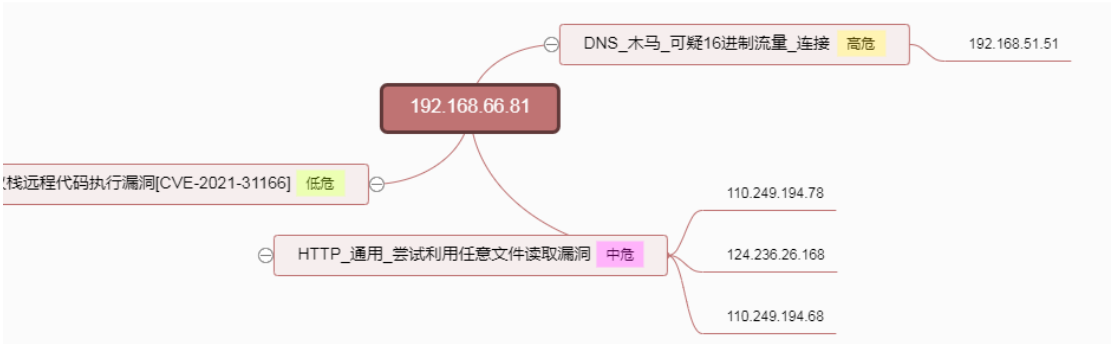


图 38_关联分析

5.5 加密流量检测

目前在应对加密流量检测方面，APT 检测产品目前主要采用解密检测或不解密检测的方式，两种方式各有利弊。如果在 SSL/TLS 应用上解密流量，首先会打破原有加密机制，使合法数据传输的安全性降低，其次在证书替代和网络应用支持上可能存在覆盖不全的情况（提供导入单独的解密证书，只能针对该证书对应的加密流量进行解码，从而导致遗漏其余非对应加密流量）。另外，大流量的卸载非常耗费计算资源，对产品整体的性能影响较大，但解密的好处是可以还原数据原始内容，这有利于检测分析工作。不解密检测采用“加密前特征检测”+“加密后机器学习对比检测”两者结合的方式，这种方式的检测结果准确与否依赖于样本规模和训练周期。如果没有一定积累，可能会存在较多误报/漏报等情况。

天阗威胁分析一体机，面对加密流量，采用“解密”+“不解密”检测相结合的方式。导入 SSL 证书对特定加密流量（对应需重点保护的设备地址）进行解密，然后正常解析检测，发现攻击威胁；无证书场景，采用 JA3 指纹检测，进行“不解密”检测，覆盖非特定加密流量盲点，识别恶意攻击。

图 39_JA3 检测配置

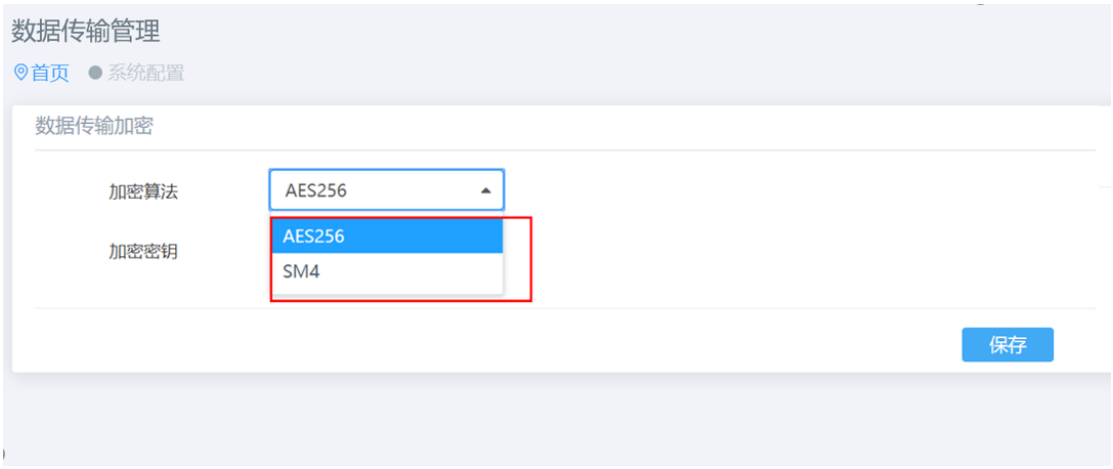
由于 Tor 服务器总是以完全相同的方式来响应 Tor 客户端，所以，这一特征能够为确认相关流量来自于 Tor 提供更高的置信度。在反复观察后，发现服务器始终以完全相同的方式来响应恶意软件客户端，应该说是分毫不差。因此，即使流量被加密，并且，即使不知道服务器的 IP 地址或域名，因为它们会不断变化，我们仍然可以通过指纹来识别客户端和服务器之间的 TLS 协商，以提高恶意通信识别结果的置信度。简单来说，JA3 就是一种在线识别 TLS 客户端指纹的方法。

5.6 易运营的运维处理

5.6.1 运维管理

天阗威胁分析一体机全面支持 IPv6,支持配置接口 IPv4 地址或 IPv6 地址；支持对 IPv6 协议流量检测，支持对 IPv4 路由监控和对 IPv6 路由监控。

支持 AES256、SM4 数据传输加密，确保数据传输的安全性。



5.6.2 自动化联动应急处置

当安全事件发生时，为避免势态升级或影响到重要业务，需要对事件进行快速应急处置。

1. 联动防御

天阗威胁分析一体机是旁路部署方式，并不具备防御能力。因此，我们设计了协同响应的安全联动防御能力，让 TAR-AIO 通过联动具备防御能力或网络隔离能力的设备以实现主动防御的能力。

天阗威胁分析一体机通过标准 Restful API 接口，支持与我司网络边界防护网关设备、终端产品等进行联动实现处置动作。天阗威胁分析一体机利用自身的威胁检测与威胁分析能力，发现攻击行为，通过联动响应策略，对发现的攻击源或被保护的目标主机进行相应的处置动作，实现自动或手动的联动处置，实现安全事件快速闭环。

图 40_联动阻断

2. 联动取证溯源

TAR-AIO 可与全流量分析取证系统（NFT）联动，对未知威胁进行追踪溯源。NFT 主动采集全流量日志与威胁事件，实现东西向、南北向流量全面检测与包存储。

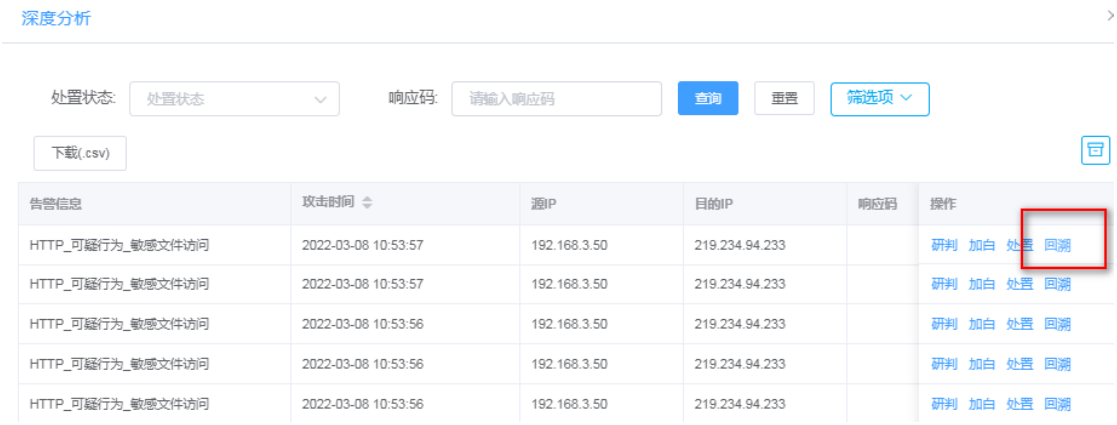


图 41_联动 NFT 溯源

3. 联动深度关联

TAR-AIO 可与我司天镜漏洞扫描设备进行深度关联，在特征事件视角，直接下发漏扫任务，对告警源目 IP 设备进行漏洞扫描，并一键查看下载报告。

图 42_漏扫报告

5.6.3 多维度报表

为应对不同分析场景，天阗威胁分析一体机内置多维度报表，报表提供不同维度、不同类型、多场景与视角的数据统计与分析的可视化呈现，实现直观、易懂的结果呈现效果。

图 43_安全报表

5.6.4 多元日志集中管理

为了能够有效支撑威胁分析的有效性，天阗威胁分析一体机提供了强大的威胁检测能力，可以提供多元、有效的数据。同时，为了进一步放大我司其它检测产品的检测效果，天阗威胁分析一体机还支持我司检测本部其它检测产品安全事件的采集与分析。面对海量实时数据采集、分析、存储的要求，天阗威胁分析一

体机提供一套整体解决方案，无论是攻击事件、流数据，还是文件、数据包，都能够结合分析场景，进行相应处理，保证高效的实时采集、分析与存储。

图 44_第三方日志接入配置

5.6.5 APT 设备集中管控

天阗威胁分析一体机不仅支持多元日志的集中管控，不仅能够对我司 APT 产品进行单点登录，还能够针对我司 APT 产品进行集中管控，实现统一状态监控、整体配置下发、模块升级等管控动作，有效提高运维效率。

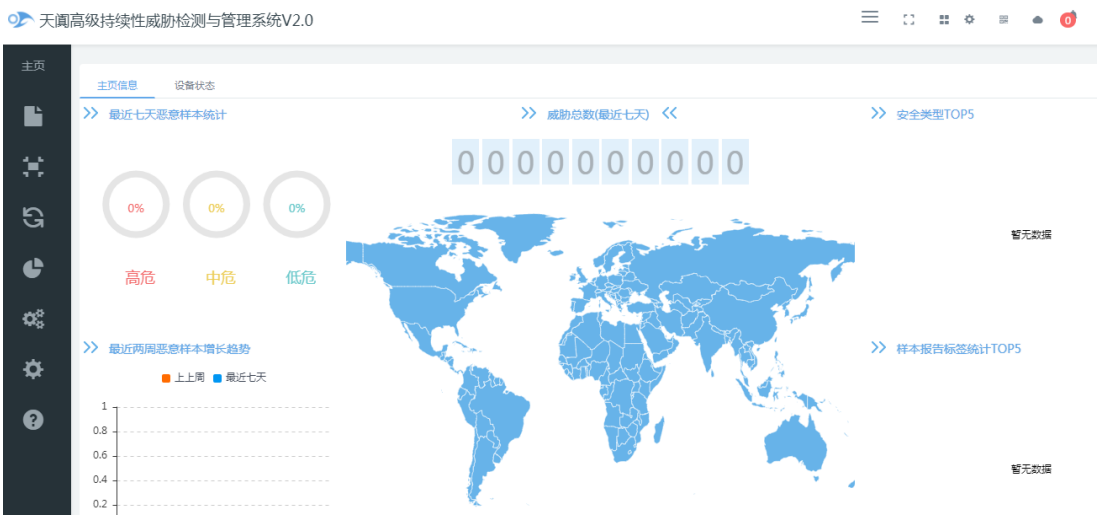


图 45_天阗高级持续性威胁检测与管理系统（APT）

图 46_APT 特征检测配置下发

六. 部署与解决方案

天阗威胁分析一体机支持旁路部署模式，在实现网络流量检测功能的同时，完全不需要改变用户的网络环境，避免设备对用户网络造成中断的风险。在旁路部署模式下，天阗威胁分析一体机可采用单机部署模式；也可利用产品对分支节点的集中管控能力进行整体解决方案部署；更可以与我司检测本部其他产品联动配合，适配 HVV 等立体防护部署模式。

6.1 一体化威胁感知场景——单机部署模式

2016 年 4 月 19 日，习总书记在与网络安全业界人士座谈会上明确指出：“加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，

增强网络安全防御能力和威慑能力。”全天候全方位感知网络安全态势，知己知彼，才能百战不殆，**没有意识到风险是最大的风险**。网络安全具有很强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是“谁进来了不知道、是敌是友不知道、干了什么不知道”，长期“潜伏”在里面，一旦有事就发作了。

单机部署的天阗威胁分析一体机，具备对局部网络空间安全的持续监控能力，能够及时发现各种攻击威胁与异常；具备威胁调查分析及可视化能力，可以对威胁相关的影响范围、攻击路径、目的、手段进行快速判别，从而支撑有效的安全决策和响应；能够建立安全预警机制，来完善风险控制、应急响应和整体安全防护的水平。

通过天阗威胁分析一体机的旁路部署模式，可支持对互联网区、DMZ 区、办公区、服务器区多区域的综合或针对性的威胁检测、分析与响应。

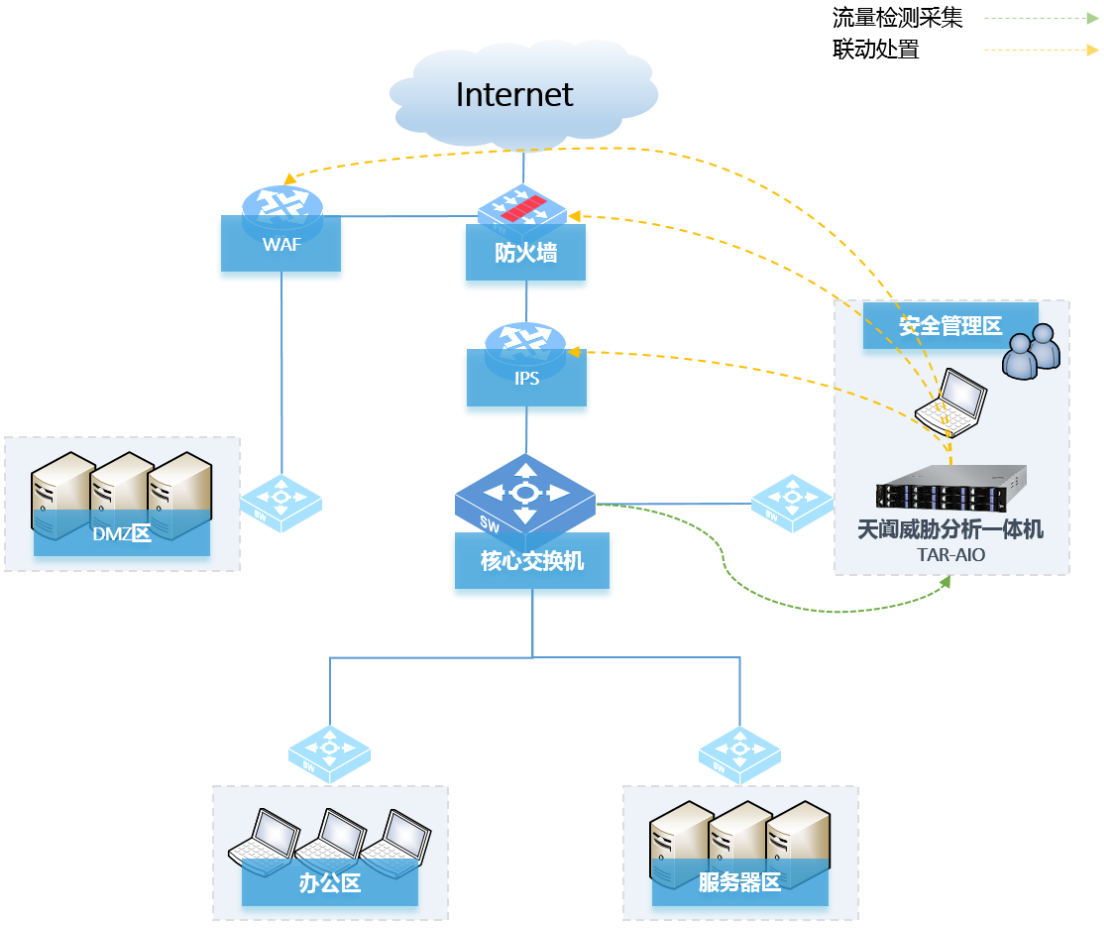


图 47_单机模式部署

将天阗威胁分析一体机旁路部署在互联网区，通过数据镜像抓取互联网出口流量并进行检测，发现对内网各单元发起的异常行为和攻击，分析失陷主机，进行攻击溯源，并能够自动与防火墙等边界产品进行联动阻断。

也可根据实际场景将天阗威胁分析一体机旁路部署在 DMZ 区、办公区、服务区等区域，对各区域流量进行针对性检测，发现异常或攻击。

天阗威胁分析一体机通过旁路方式部署在网络中，此种部署接入方式不会对客户网络结构造成影响。接入镜像流量不限于互联网出口、业务网出口流量等。设备通过被动指纹识别、浏览器识别技术，根据资产识别的条件进行流量分析及应用检测，识别出网络中资产信息。平台可以通过节点设备管理功能对节点设备策略配置、升级维护进行便捷管理。

6.2 全网威胁感知场景——整体解决方案部署模式

在整体解决方案部署模式下，可通过天阗威胁分析一体机的旁路部署模式，进行综合或针对性的威胁检测、分析与响应。同时利用天阗威胁分析一体机的集中管控能力，在总节点集中管控各分支机构的 APT 设备，进行对分支机构的统一日志采集、威胁分析与集中管控，形成以天阗威胁分析一体机为核心的整体解决方案。

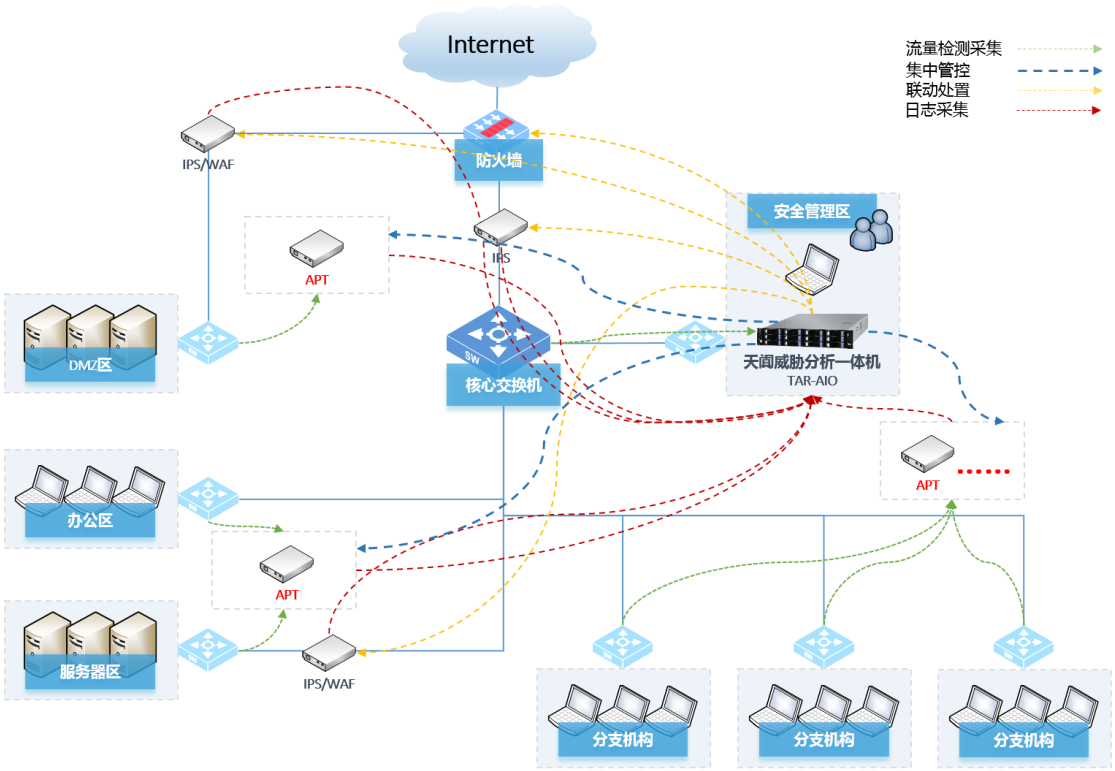


图 48_整体解决方案分布式部署模式

1. 部署方式说明

- 集中管控：分布式部署——分支机构部署若干 APT 设备，总节点部署 TAR-AIO，集中管控子节点 APT，由 TAR-AIO 统一下发策略、配置与升级，统一监控设备状态，收集各分支 APT 日志进行统一分析管理。
- 流量检测：利用旁路部署的检测模式对目标流量进行有效检测，结合天阗威胁分析一体机的威胁分析能力进行有效分析与可视化呈现。
- 日志采集：天阗威胁分析一体机支持我司 APT、EDR 等产品的日志采集与威胁分析。可对不同产品的不同日志类型进行集中管理与关联分析，提供快速、多维的日志检索能力，并对分析结果进行直观的可视化呈现。
- 联动响应：依托于天阗威胁分析一体机的威胁分析能力，发现有效攻击行为，并通过与我司 IPS、WAF、防火墙等设备进行联动响应，对攻击源头进行联动阻断。

2. 方案价值体现

- TAR-AIO 对应多个分支 APT 设备的集中管控分布式部署模式，作为单机部署模式的升级版，能够全面感知全网安全威胁、洞悉网络及应用运行健康状态，通过全流量分析技术实现完整的网络攻击溯源取证，帮助安全人员采取针对性响应处置措施。

- 大型机构或企业层面，此整体解决方案可从体系内部建立威胁感知，应用于内部系统的安全运营，发现重要威胁，解决问题，把安全能力落地；同时通过威胁感知对多分支或二级单位进行外部监管，以提升整体的安全状态的掌握，同时与监管机构进行事件应急处置及威胁情报的合作。

- 从国家层面、省市大地域层面，此解决方案可对国计民生相关的关键信息基础设施的安全态势进行整体且持续的监测与关注，让威胁无处躲藏。

6.3 一站式立体防护体系——HVV 综合部署模式

该方案为一站式立体防护体系，同时也具备协同联动特性。

以天阗威胁分析一体机（TAR-AIO）为中心，通过与天清汉马 T 系列防火墙（T 墙）、天清 Web 应用安全网关（WAF）、全流量分析取证系统（NFT）、天阗欺骗防御系统（CDS 蜜罐）配合，5 款 HVV 检测防护产品互相协同联动，实现产品互相衔接，形成闭环防护体系，最终形成完整的 HVV 组合套餐。

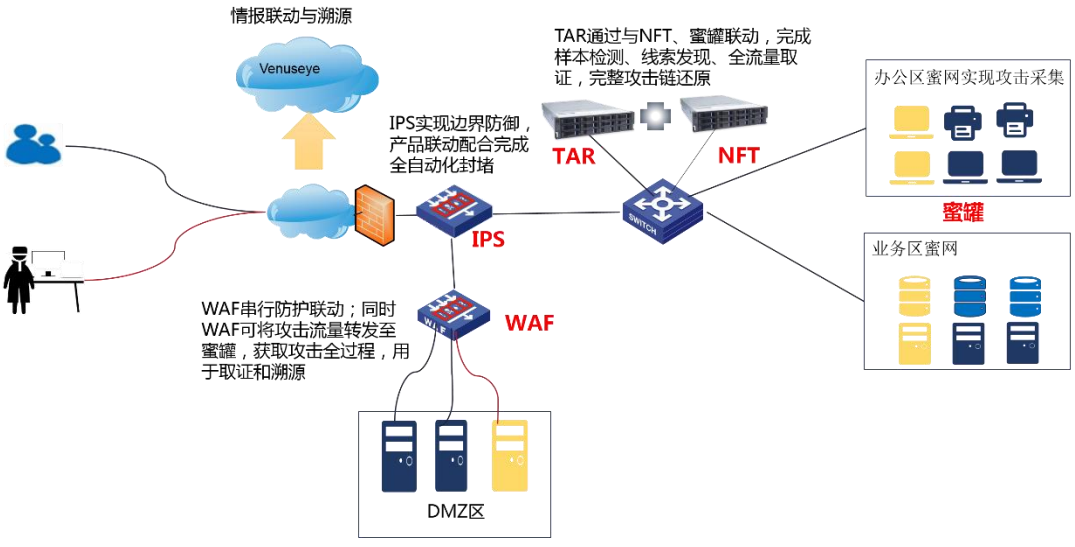


图 49_HVV 综合部署模式

该一站式立体防护体系，实现安全防护由被动防护向**“主动防护+被动防护”双向立体防护模式**转变。5 款 HVV 检测防护产品组成的综合方案，实现了**边界防护、数据采集、攻击检测、威胁分析、溯源处置、攻击反制**，全流程防护实现避免丢分，争取得高分的目标。

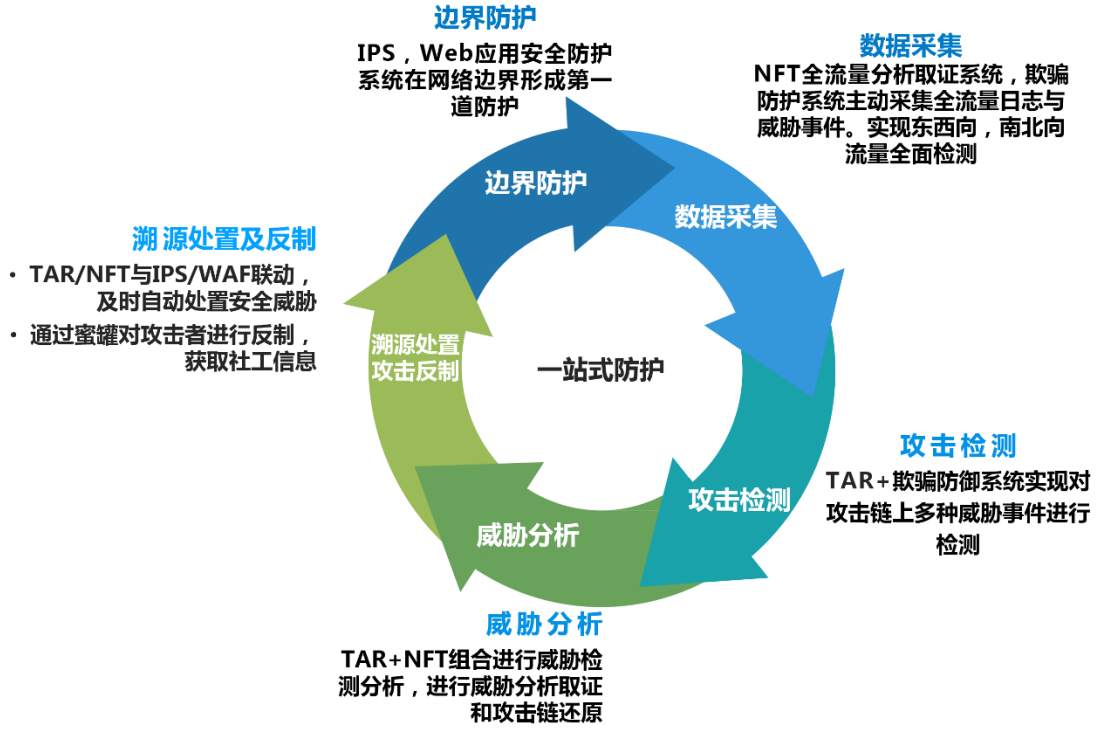


图 50_双向立体防护模式

6.4 扩展与组件

以下组件为启明星辰自有安全体系的设备，用于作为天阗威胁分析一体机的扩展组件，在提供有针对性的安全数据输入的同时，可配合部署、或联动进行安全防护、检测。

组件名称	组件描述
天阗高级持续性威胁检测与	• APT 利用沙箱技术检测基于文件的 0day 漏洞、nday 漏洞及未知威胁的攻击、检测针对客户网络的特定工具攻击

管理系统（APT）	的检测。利用特征检测技术检测已知攻击。已知检测+未知检测=全面提升客户的检测能力。 • TAR-AIO 可对子节点 APT 设备进行集中管控与分析。
全流量分析取证系统（NFT）	• 全流量分析取证系统是一款集全流量原始数据包存储、全量数据检索、应用元数据解析、攻击回溯取证和数据安全分析等功能于一体，面向网络安全运维人员和安全分析人员的网络安全产品。 • TAR-AIO 可与 NFT 联动对未知威胁进行溯源取证。
天阗超融合检测探针（CS Plus）	• CSP 采用特征检测技术、异常行为检测技术、威胁情报技术、黑白名单技术、基线技术、静态 APT 技术等多种相结合的方法，通过对网络流量的深度包解析和流解析，实现了网络各种威胁的全面有效检测，同时也可以通过配置策略方式，让探针记录所关注的流量，便于后期可以根据相关的事件日志，对当时的攻击进行回溯分析，追踪取证。
天阗欺骗防御系统（CDS）	• 天阗欺骗防御系统是启明星辰自主研发的网络安全产品，基于公司在攻防方向的积累和研究成果，产品采用欺骗防御思想，通过业务仿真构建蜜网，诱惑攻击行为进入蜜网，实现攻击捕获，延缓攻击者对实际业务网络的攻击，全程记录攻击轨迹和行为，实现攻击行为的快速取证溯源，保护真实网络资产，同时以技术手段实现对攻击者的追踪。欺骗防御系统打破了现有攻防不对称的局面，结合其他安全系统共同构成安全防御体系。 • CDS 可配合 TAR-AIO 对多种威胁进行攻击检测采集、主动防御反制。

天清 Web 应用安全网关（WAF）	• 天清 Web 应用安全网关，是启明星辰公司自行研制开发的新一代 Web 安全防护与应用交付类应用安全产品，主要针对 Web 服务器进行 HTTP/HTTPS 流量分析，防护以 Web 应用程序漏洞为目标的攻击，并 针对 Web 应用访问各方面进行优化，以提高 Web 或网络协议应用的可 用性、性能和安全性，确保 Web 业务应用快速、安全、可靠地交付。 • TAR-AIO 可联动 WAF 对应用层威胁进行阻断处置。
天清汉马 T 系列防火墙（T 墙）	• 天清汉马 T 系列防火墙，作为下一代防火墙一般部署在互联网或数据中心的出口，具备七元组访问与会话控制，应用行为控制等 ACL 功能，基于第三代多核并行化架构，提供业界最佳性能表现。 • 与 TAR-AIO 联动后，实现对攻击源的联动阻断和异常访问的 ACL 策略控制，让天阗威胁分析一体机具备基础防御能力。同时，由 TAR-AIO 具备未知威胁检测能力，可联动形成对未知威胁的有效防御和脆弱性入口点的针对性策略控制，应对出口安全的攻击绕过问题。
天清入侵防御系统（NGIPS）	• 天清入侵防御系统（Intrusion Prevention System）是启明星辰自行研制开发的入侵防御类网络安全产品，融入了启明星辰公司在入侵攻击识别方面的积累和研究成果，使其在精确阻断方面达到国际领先水平，可以对网络蠕虫、间谍软件、木马软件、溢出攻击、数据库攻击、高级威胁攻击、暴力破解等多种深层攻击行为进行主动阻断，弥补了其它安全产品深层防御效果的不足。 • TAR-AIO 可联动 IPS 对七层以下威胁进行全面阻断处置。
天镜脆弱性扫	• 天镜脆弱性扫描与管理系统 v6070（以下简称“天镜”）

描与管理系统	是启明星辰自主研发的基于网络的漏洞扫描、分析、评估与管理系统。天镜综合多种国际最新的漏洞扫描与检测技术，能够快速发现网络资产，准确识别资产属性，全面扫描安全漏洞，清晰定性安全风险，给出修复建议和预防措施，并对风险控制策略进行有效审核，从而帮助客户在弱点全面评估的基础上实现安全自主掌控。 • TAR-AIO 可与天镜漏扫深度关联，本地化方式对事件告警所有源目 IP 资产进行扫描来发现脆弱性风险。

6.5 设备规格形态

天阗威胁分析一体机具备丰富的产品型号，可覆盖各种类型的网络吞吐和应用场景，主要型号和相关说明如下（定制型号除外）：

型号	简介	样图
TAR-AIO-3	2U 机架式设备，板载 4 个 GE 口，支持 7 个扩展槽位，可扩展模块类型 2*SFP+、4*GE、2*GE、4*SFP、2*SFP，带一个 MGT 管理口,新建连接 10w/s，吞吐 3G，http 并发连接数 200W。	
TAR-AIO-5	2U 机架式设备，板载 4 个 GE 口，支持 7 个扩展槽位，可扩展模块类型 2*SFP+、4*GE、2*GE、4*SFP、2*SFP，带一个 MGT 管理口,新建连接 15w/s，吞吐 6G，http 并发连接数	

	400W。	
TAR-AIO-7	2U 机架式设备，板载 4 个 GE 口，支持 7 个扩展槽位，可扩展模块类型 2*SFP+、4*GE、2*GE、4*SFP、2*SFP，带一个 MGT 管理口,新建连接 18w/s，吞吐 8G.http 并发连接数 450W。	
TAR-AIO-9	2U 机架式设备，板载 4 个 GE 口，支持 4 个扩展槽位，可扩展模块类型 2*SFP+、4*GE、2*GE、4*SFP、2*SFP，带一个 MGT 管理口,新建连接 18w/s, 吞吐 15G，http 并发 500W	
TAR-AIO-20s	2U 机架式设备，6 个 GE 口，支持 4 个扩展槽位，可扩展模块类型 2*SFP+、4*GE、2*GE、4*SFP、2*SFP，带一个 MGT 管理口，设备网络吞吐 20Gbps，并发数 600W，新建连接数 20W	

七. 结论

“十四五”规划开启了中国经济发展的新阶段，随着数字经济加速发展，数据已经成为重要的生产要素，随之而来的数据安全，逐渐被人们所熟知。

目前，我们将数据安全划分为三个阶段——1.0、2.0 以及 3.0，三个阶段之间的关系并不是抛弃与更迭的，而是包容与涵盖，每个阶段也分别代表了不同的含义。早期以零散的文件，数据库安全为主，我们把他划分为第一阶段，即面向数据对象的安全；第二阶段是随着大数据的兴起，由此而产生的“数据汇聚”的安全；第三阶段是随着数据流动属性、经济属性的增加和产生，而带来的新挑战，即“数据流通的安全”。

2021 年 6 月《中华人民共和国数据安全法》正式颁布，标志着我国数据安全进入有法可依、依法建设的新阶段，也揭开了数据安全 3.0 的新篇章——数据流通安全。去年启明星辰集团发布**数据绿洲**，致力于解决在“数字中国”和 3.0 阶段数据流通安全中的网络安全问题，在数据安全赛道再次领跑。

由于数据本身具有流动性、多样性、可复制性等不同于传统生产要素的特性，数据安全风险在数字经济时代被不断放大，因此，对数据安全治理的要求也越来越高。**天阗威胁分析一体机**正是数据安全治理中的重要一环与不二选择，凭借自身的检测优势，利用支持双向匹配的特征检测、支持多分析场景的流检测和基于沙箱检测技术的文件检测，可进行：

- 一体化威胁监测，针对 APT 攻击持续有效监测
- 提供多元日志提供集中管理与分析能力
- 针对威胁分析结果的可视化呈现
- 安全事件快速闭环，针对威胁的联动响应处置

天阗威胁分析一体机，是以攻防研究为核心，配合场景分析、资产构建、自动响应、协同防御能力，构建下一代一体化高级威胁检测与响应体系，意在为客户提供一套集检测、分析、可视、闭环响应为一体的本地网络安全分析中心，让安全可感知、易运营。

TAR-AIO 站在启明星辰数字绿洲之上，乘着数据安全的洪流，必将在数据 3.0 大势中乘风破浪！