

奇安信天眼威胁监测与分析系统 流量探针彩页

地址：北京市西城区西直门外南路26号院1号

邮编：100044

1 产品介绍

奇安信天眼威胁监测与分析系统（以下简称“天眼”）汇集流量传感器、文件威胁鉴定器、邮件告警、天堤防火墙、网神云锁等多种告警数据，基于奇安信自有的多维度海量互联网数据，进行自动化挖掘与云端关联分析，提前洞悉各种安全威胁，并向客户推送定制的专属威胁情报；同时结合部署在客户本地的软、硬件设备，奇安信天眼能够对未知威胁的恶意行为实现早期的快速发现，并可对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源；支持运用奇安信自研的 SOAR 编排技术，实现对确定的威胁进行多种类型的响应处置，真正实现监测预警、威胁检测、溯源分析和响应处置的天眼威胁监测与分析系统。

1.1 产品规格

TSS10000-S93G		
硬件规格	CPU	国产化处理器 1*8 核 CPU (2 颗物理 CPU)
	操作系统	国产化麒麟操作系统
	内存	32GB
	存储	4TB SATA
	网口	2×千兆电口 + 4×万兆光口 (含光模块)
	扩展	1 个扩展槽位, 可选配 4 千兆电口或 2 万兆光口网卡或 4 万兆光口网卡 (不含光模块)
	电源	冗余电源

	尺寸	2U 机箱
性能规格	吞吐量	3Gbps
	功能模块	网络入侵检测模块、恶意文件检测模块、web 应用检测模块；
TSS10000-S96G		
硬件规格	CPU	国产化处理器 2*24 核 CPU (2 颗物理 CPU)
	操作系统	国产化麒麟操作系统
	内存	64GB
	存储	40TB SATA
	网口	4×千兆电口 + 4×万兆光口 (含光模块)
	扩展	2 个扩展槽位, 可选配 4 千兆电口或 2 万兆光口网卡或 4 万兆光口网卡 (不含光模块)
	电源	冗余电源
	尺寸	2U 机箱
性能规格	吞吐量	10Gbps
	功能模块	网络入侵检测模块、恶意文件检测模块、web 应用检测模块；
TSS10000-S98G		
	CPU	国产化处理器 2*32 核 CPU (2 颗物理 CPU)

硬件规格	操作系统	国产化麒麟操作系统
	内存	128GB
	存储	40TB SATA
	网口	4×千兆电口 + 4×万兆光口 (含光模块)
	扩展	2个扩展槽位, 可选配4千兆电口或2万兆光口网卡或4万兆光口网卡 (不含光模块)
	电源	冗余电源
	尺寸	2U 机箱
性能规格	吞吐量	20Gbps
	功能模块	网络入侵检测模块、恶意文件检测模块、web 应用检测模块;

Figure 1-1

。

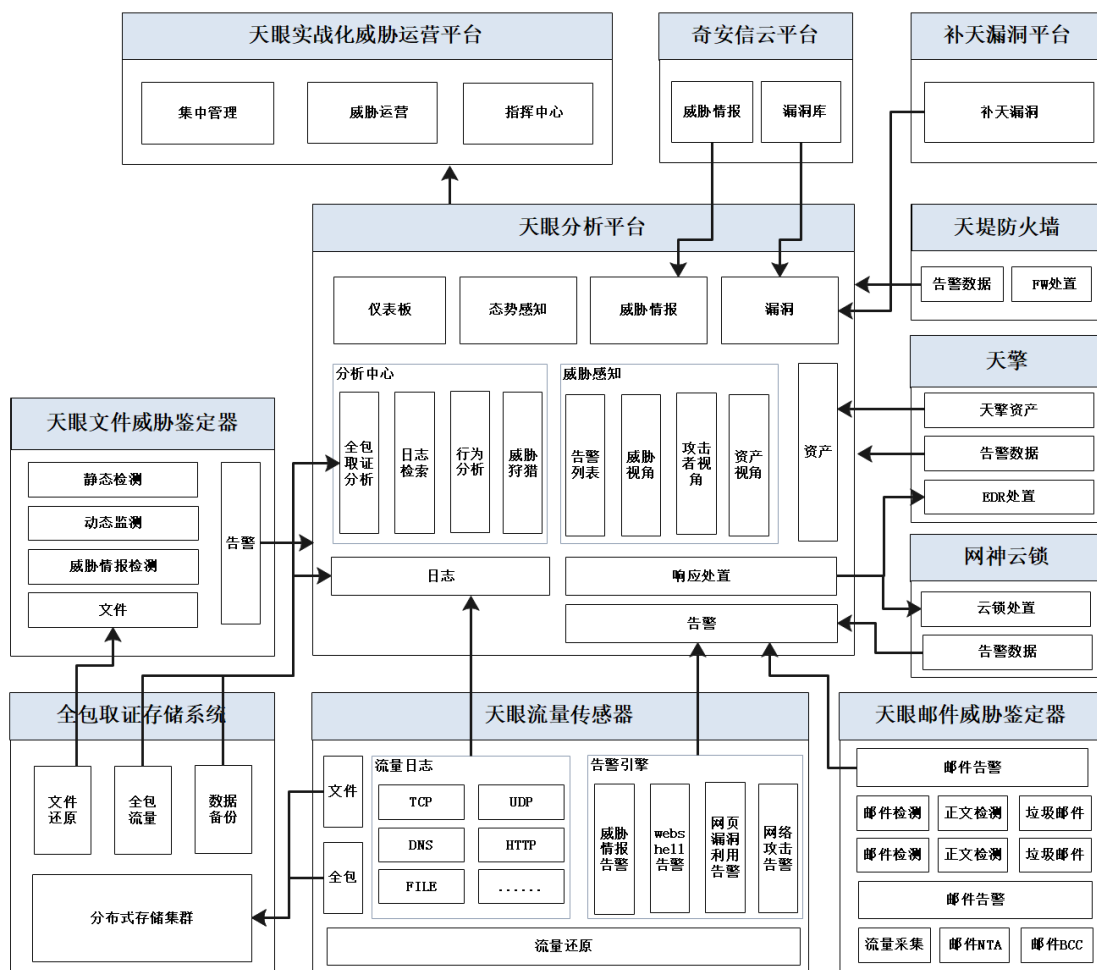


图-1 天眼架构图

天眼流量传感器提供流量采集和告警功能，借助全包存储系统，可以实现全流量存储，并在分析平台上实现全流量回溯分析能力。由流量中还原的文件和邮件数据，经天眼文件威胁鉴定器和天眼邮件威胁鉴定器处理，可进一步触发告警。全包存储系统的引入，使天眼具备对存储灵活扩容的能力。配合云平台、天堤防火墙、天擎 EDR、云锁等系统，天眼具备极强的联动响应能力。天眼分析平台对以上各系统的能力进行综合呈现，为用户提供多维度的威胁分析、呈现和联动响应服务。同时支持把告警上传给天眼实战化威胁运营平台，进行告警的处置、管控、调度。

2 产品核心功能

2.1 流量还原

天眼流量传感器对网络流量进行采集并还原，还原后的流量日志会加密传输给天眼分析平台，流量镜像中的 PE 和非 PE 文件还原后则加密传输给天眼文件威胁鉴定器进行检测。天眼传感器通过对网络流量进行解码还原出真实流量中出现文件传输行为进行发现和还原，并记录文件 MD5 发送至分析设备功能，如可执行文件（EXE、DLL、OCX、SYS、COM、apk 等等）、压缩格式文件（RAR、ZIP、GZ、7Z 等）、文档类型文件（word、excel、pdf、rtf、ppt 等），提取网络层、传输层和应用层的头部信息，甚至是重要负载信息，这些信息将通过加密通道传送到天眼分析平台进行统一处理。天眼传感器中应用的自主知识产权的协议分析模块，可以在 IPv4/IPv6 网络环境下，支持 HTTP（网页）、SMTP/POP3（邮件）以及常见数据库协议的识别或还原：国产化数据库、DB2、Oracle、MySQL 等协议；等主流协议的高性能分析。

2.2 高级威胁检测

天眼具备高级威胁检测能力。基于全球数百个威胁情报源和奇安信多个安全研究团队的 APT 事件发现、跟踪成果，运用威胁情报、文件虚拟执行、智能规则引擎、机器学习等技术，天眼系统可以检测和发现高级网络攻击和新型网络攻击，涵盖：APT 攻击、勒索软件、远控木马、僵尸网络、窃密木马、间谍软件、网络蠕虫、邮件钓鱼等高级攻击，并基于可视化技术，清晰的展示网络中的威胁。

天眼流量传感器内置的威胁检测引擎，除了高级威胁检测能力之外，还可检测多种网络协议中的攻击行为，常见的包括 TCP/UDP 会话记录、异常流量会话记录、web 访问记录、域名解析、SQL 访问记录、邮件行为、登录情况、文件传输、FTP 控制通道、SSL 加密协商、telnet 行为等行为描述；提供网页漏洞利用、webshe11 上传、网络攻击等多种维度的告警展示，可检测如僵木蠕毒、

溢出攻击、拒绝服务、间谍软件、端口扫描、网络钓鱼等多种网络攻击行为，也可检测如 SQL 注入、XSS、Webshell、代码执行、命令执行、文件包含等多种 Web 攻击行为，内置的 Webshell 沙箱和 Webshell 机器学习模块可以精准检测 PHP、ASP、JSP(X) 等后门并记录相关信息。

天眼传感器拥有威胁情报实时匹配能力，基于流量实时威胁情报匹配功能，设备具备主流的威胁情报，情报总量 50 万条；能发现恶意软件、APT 事件等威胁，产生的多种告警都会加密，并传输给天眼分析平台进行统一分析管理。

2.3 日志检索

天眼基于搜索引擎技术构建流量行为日志检索与存储，在本地数据的存储和检索方面，使用奇安信诺亚大数据平台做为平台基础，并配套了大量的检索和分析功能以对数据做到高效分析。

针对不同使用场景和不同技术水平的用户需求，日志检索模块分为快捷模式、高级模式、专家模式的检索功能，提供告警日志、网络日志、终端日志与第三方日志检索的功能。快捷模式快捷模式只需要填充胶囊字段的值，即可进行基于某一类告警数据的搜索；高级搜索兼容 lucene 语句进行搜索，在输入框内输入查询语句进行基于多种告警数据的搜索；专家模式专家模式为 SPL 命令语句搜索，用于专家用户对数据进行统计并支持各种可视化视图展示。支持敏感信息识别功能及检索功能，支持 HTTP 协议、数据库、文本文件等传输敏感内容提取。

2.4 响应处置

威胁处置能力在信息安全建设中具有重要作用，天眼系统为完善威胁分析后续的处置闭环，引入了响应处置能力，以模块化形式在天眼系统内置了一套自动化编排响应模型，通过标准的 API/openc2 接口与处置设备联动，安全管理

中心通过接口下发阻断策略，探针执行阻断动作并将阻断日志信息发送给安全管理中心；连接畅通的情况下支持自动/手动方式的响应指令下发。主要实现的功能是根据告警信息对相应（不同厂商不同功能）的设备构建完整的响应处置 workflow 进行联动与处置，实现安全设备间的协同防御。

根据不同使用场景，天眼系统响应处置模块提供不同级别的处置手段，主要包括以下场景：

加白名单：针对判定为误报的告警数据，天眼支持以添加白名单形式进行处理，后续产生的告警将不再通知给用户，降低误告警数量，提升事件处置的效率。

深度分析：基于 SOAR 的自动化处置编排能力，天眼响应处置模块结合各类告警和日志进行攻防场景的深度分析，提炼高价值告警和威胁溯源分析拓线，并将分析结果回注天眼系统生成新的告警。例如，我们基于远控木马的外连 CC 地址行为的威胁情报告警，通过 SOAR 的自动化编排能力来发现外连 CC 地址告警之后是否有持续的与 CC 地址的 TCP 通信行为来判断受害 IP 的受害程度，对于明确有后续通信行为的产生新的告警，这样即实现对告警的深度分析。

联动处置：通过接口与处置设备联动，支持自动/手动方式的响应指令下发，实现对威胁事件的处置动作。天眼内置的响应处置模块支持与多种设备联动：

➤ EDR 联动

在实际威胁运营过程中，天眼系统通过流量解析发现告警后，支持将告警与 EDR 设备进行联动，完成对某一些进程的封禁、关闭、隔离等操作。

➤ NDR 联动

在实际威胁运营过程中，天眼系统通过流量解析发现告警后，支持将告警与防火墙设备进行联动，完成对某一 IP 的封禁操作。

➤ SMAC 联动

在实际威胁运营过程中，天眼系统通过流量解析发现告警后，支持将告警与 SMAC 进行联动，完成对某一 IP 的封禁操作。

➤ 椒图联动

在实际威胁运营过程中，天眼系统支持接入椒图告警，同时天眼系统通过流量解析发现告警后，支持向椒图下发 IP，椒图可让服务器阻止本 IP 对服务器的响应、支持天眼向椒图下发弱口令排查指令，椒图排查所有服务器相关账号口令是否存在该弱口令并返回扫描结果。

➤ 传感器旁路阻断

在实际威胁运营过程中，天眼系统通过流量解析发现告警后，基于流量的旁路阻断技术与传感器进行联动，完成对特定 IP、域名的网络访问的阻断操作。

2.5 旁路解密

基于旁路非代理方式解密 HTTPS 流量（需提供私钥），解密后为 HTTP 流量再进行流量还原及威胁分析。

HTTPS 基于 SSL 协议加密，SSL 加密流量主要分为两类，具有前向安全性（DH 算法）和非具有前向安全性（RSA 算法），对于旁路流量，前者不可以解密，后者可以，也就是旁路可解密 RSA 算法，无法解密 DH 算法。

2.6 恶意代码检测

基于人工智能的杀毒引擎，依靠海量数据挖掘、引入机器智能学习算法，能够有效准确识别未知恶意软件，能够根据已知的正常软件和恶意软件的大量样本，通过数据挖掘找出两类软件最具有区分度的特征，建立机器学习模型，使用机器学习算法，得到恶意软件的识别模型。基于工具特征的 WEBSHELL 检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：中国菜

刀、小马上上传工具、小马生成器等。通过获得的模型对未知程序进行分析判断，即可获得软件的恶意概率，从而在可控的误报率之下尽可能多的发现恶意程序。

机器学习引擎的学习流程如下图所示：

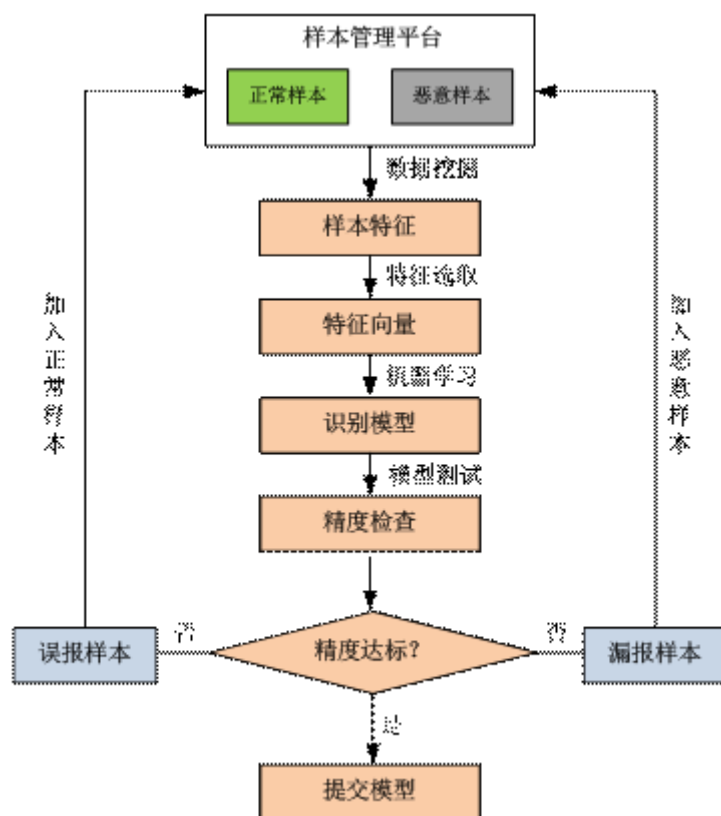


图 2 机器学习引擎流程示意图

样本管理平台负责管理训练样本，并且对可疑样本可进行人工分析，保证训练样本的纯度，并给下面的阶段提供数据。

通过对训练样本的数据挖掘，例如导入 API 函数、PE 头部信息、代码反汇编信息等等进行海量数据挖掘，找到海量 PE 文件特征。应用特征选取算法，选取最有效的特征，建立特征模型。

利用特征模型对训练样本数据进行数据特征化变换，生成对应的特征向量，利用成熟的机器学习算法（例如 SVM），对样本进行训练，得到恶意程序识别问题的识别模型。

对生成的模型进行测试，如果精度达到要求，则终止。否则对误判样本进行分析（在样本不确定的情况下，需要人工分析确认），调整样本的分类属性，再次迭代。

该引擎的运行环境如下图所示：

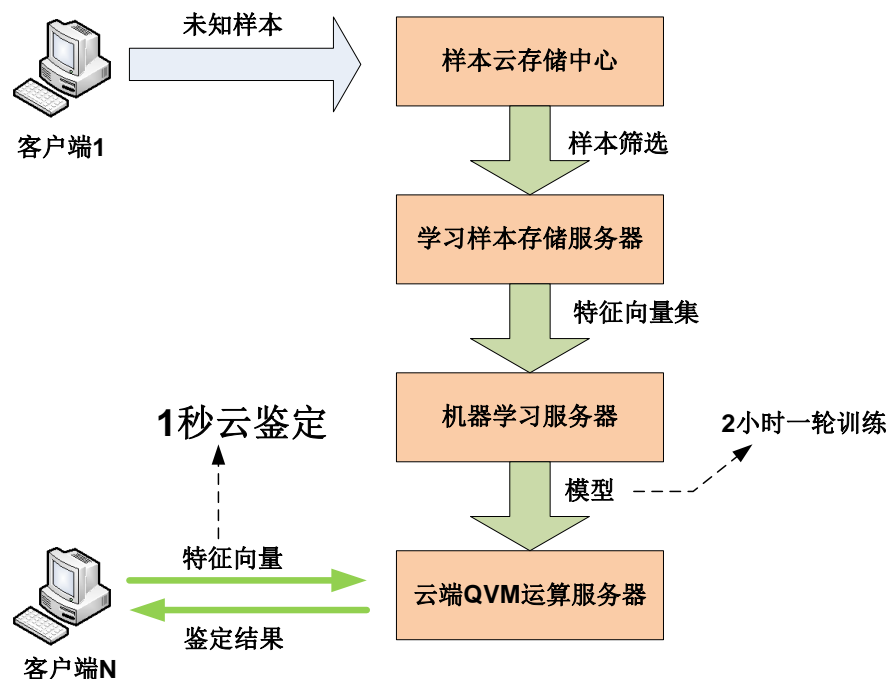


图 3 机器学习引擎运行环境示意图

由于安全领域用户对误报的敏感性和特殊性，导致长期以来机器学习算法在本领域一直作为不大，多数研究者尝试后，无法达到预期的精度而放弃。所以对本技术而言，首要处理的就是降低误报率。根据前期研究的结果，一个合适的机器学习算法的选择对误报控制是相当重要的，目前初选 SVM 作为基本学习算法，并设计了快速的参数选择，和快速训练方法。

机器学习算法在人工少量干预样本（添加、删除、修改黑白属性）指导的情况下，系统能够实现自我学习，自我进化。目前该引擎学习一轮的时间仅为2小时。

机器学习有效的解决了大部分未知恶意程序的发现问题。由于传统杀毒技术严重依赖于样本获得能力和病毒分析师的能力，基本只能处理已知问题，不能对可能发生的问题进行防范，具有严重的滞后性和局限性。本技术对海量样本进行挖掘，能够找到恶意软件的内在规律，能对未来相当长时期的恶意软件技术做出前瞻性预测，实现不更新即可识别大量新型恶意软件。

传统杀毒软件技术基本基于简单的特征或者规则进行查杀，很容易被病毒作者免杀。本算法单特征贡献相当微弱，所以简单免杀很难奏效。

机器学习使得对样本分析人员的要求相对较低，仅仅需要分析员能够区分文件是否恶意，而不需要人工分析恶意软件实现方法和识别方法，降低了人员参与门槛，大大节约了人力成本。

2.7 动态沙箱检测

天眼新一代动态沙箱引擎采用基于硬件模拟的虚拟化动态分析技术，沙箱检测功能，能够通过采用沙箱动态检测技术进行分析，可以手动导入样本文件进行动态检测各种加壳病毒及未知恶意代码。对 APT 攻击的核心环节“恶意代码植入”进行检测，这种利用对恶意代码的行为进行动态分析的方法，可以避免因为无法提前获得未知恶意代码特征而漏检的问题，亦即在无需提前预知恶意代码样本的情况下仍然可以对恶意代码样本进行有效的检测，因为未知恶意代码是 APT 攻击的核心步骤，因此对未知恶意代码样本的有效检测，可以有效解决 APT 攻击过程的检测问题。

新一代安全感知系统相对于最大特点在于：将会提供了非常丰富的沙箱环境，这种规模化的沙箱环境可以有效保障每种待检测的文件样本都有其适合打开、运行的沙箱环境，同时新一代安全感知系统的沙箱采用了高级优化技术，

可以有效降低样本文件在沙箱之中打开、运行过程中的内存资源消耗、CPU 资源消耗，与其他同类型产品相比，可以以最小的资源消耗、最快的速度得出准确的检测结果。

目前新一代安全感知系统需要模拟沙箱环境包括：PDF 沙箱、Word 沙箱、浏览器沙箱、邮件沙箱、图片沙箱等。同时，借助于新一代安全感知系统的多核平台，新一代安全感知系统中的各种规模化沙箱可以绑定在处理器的物理核心上进行快速运行，这种进程与处理器绑定的方式可以有效降低进程在处理器的不同处理核心上切换所带来的资源开销，降低并发检测线程之间的资源竞争，有效提高资源利用率。

2.8 场景化分析

天眼系统基于特定场景的安全威胁分析技术，根据多种威胁类型全面检测用户环境的异常行为，提炼了覆盖全面的行为分析场景，主要包括了 DNS 服务分析、非常规服务分析、邮件行为分析、WEB 服务器行为分析、登录行为分析、数据库行为分析以及访问行为分析等。

➤ DNS 服务分析

DNS 服务分析包括可疑 DNS 分析（DGA 域名检测以及 DNS Tunnel 隧道）、DNS 服务器发现、链路劫持和 DNS 重绑定检测等场景。DGA（域名生成算法）是一种利用随机字符来生成 C&C 域名，从而逃避域名黑名单检测的技术手段。DNS Tunnel 则是黑客可疑利用 DNS 信道来传输数据。链路层劫持是指第三方（可能是运营商、黑客）通过在用户至服务器之间，植入恶意设备或者控制网络设备的手段，侦听或篡改用户和服务器之间的数据，达到窃取用户重要数据（包括用户密码，用户身份数据等等）的目的。DNS 重绑定是指攻击者控制恶意 DNS 服务器来回复域的查询，可以通过滥用 DNS 来诱骗 Web 浏览器与他们不想要的服务器进行通信。

➤ 非常规服务分析

非常规服务分析主要完成常规行为分析之外的重要分析任务，包括可疑代理、远程工具和反弹 shell 等行为检测，让用户了解内部资产受到哪些代理工具、远程服务和反弹 shell 的威胁。

服务器转发客户系统的网络访问请求，并且可以过滤掉用户的指令，从而达到控制用户的目的，可疑代理分析为用户提供监测这一威胁的窗口。远程工具，用于主机远程控制，一般分客户端程序(Client)和服务器端程序(Server)两部分，控制端上的 Client 与被控端的 Server 建立连接，完成各种操作。反弹 shell，表现为控制端监听被控端的 TCP/UDP 端口，被控端发起请求到该端口，并将其命令行的输入输出转到控制端，实现客户端与服务端的角色翻转。这些非常规服务存在潜在威胁，其检测分析任务满足用户需求场景。

➤ 邮件行为分析

邮件行为分析场景针对邮件相关威胁所做的安全检测，主要包括检测邮件正文的敏感关键字分析和检测邮件附件的敏感后缀分析。

电子邮件拥有成本低、效率高等特性，已经成为企业通信最重要的形式之一，因此也成为网络攻击者最常攻击的对象，其中包含的恶意信息和恶意软件成为攻击的常见形式。检测恶意信息的方式是匹配敏感关键字，一封邮件存在一定数量的敏感关键字能反映其威胁情况。检测恶意软件的方式是提取邮件附件中的相关敏感后缀，一般是电脑能直接或间接运行的文件格式，过滤掉存在敏感后缀的文件可以在源头控制威胁。

➤ 登录行为分析

登录行为分析针对用户登录场景存在的威胁进行相关检测，防止用户账号被恶意控制和窃取密码，分别对应异常登录、特权账号登录，以及弱口令、明文密码泄露。

账号安全是安全控制的最重要一环，针对账号的恶意行为层出不穷，从登录类型和密码检测两个维度可以较全面地检测到登录行为相关异常信息。异常登录分析资产被外网登录和异常时间登录的情况，从源头保护资产。特权账号

登录是为了防止攻击者利用特权账号展开攻击，一般包括 administrator 和 root 等，特权账号登录信息的分析能预防潜在威胁。明文密码泄露是检测登录日志中可以被解析的密码，通常存在于 http、smtp 和 pop3 协议中。弱口令分析强度不够或重复次数较多的密码，弱口令的检测是在明文密码泄露的基础上进行的。支持自定义弱口令字典，支持 HTTP、HTTPS、Telnet、FTP、POP、SMTP、IMAP 等协议的自定义弱口令检测，采用弱口令字典和口令强度两种方式检测，弱口令字典支持导入、导出。

➤ Web 服务器行为分析

Web 服务器行为分析包含非常用请求方法、可疑爬虫和扫描和后门上传利用。非常用请求方法是指攻击者经常使用一些不常用的方法来获取服务器的敏感数据为后续的非合法活动做准备，我们需要检测非常用的请求来判断是否有信息泄露。可疑爬虫和扫描指攻击者通过网络非法扫描、爬虫等多种攻击来扫描随机生成的 url 和随机方法来获取服务器数据。后门上传利用是指攻击者通过现有漏洞向服务器上传非法文件以获取信息的行为。

➤ 数据库行为分析

数据库行为分析是指分析各个用户的语句来获悉用户行为。攻击者的恶意数据库行为包括篡改数据、删除重要数据和盗取数据信息。我们通过分析数据库行为日志，可以分析和获取攻击者的行为。篡改数据是指攻击者修改数据信息致使数据库无法正常使用。删除重要数据是指攻击者删除数据信息致使数据库无法正常使用。盗取数据信息是指攻击者非法获取数据。

➤ 访问行为分析

访问行为分析包含外部访问、横向访问、内部主机外联和风险端口访问四类。外部访问是指外部主机访问内部服务；横向访问是指内部主机访问内部服务；内部主机外联是指内部主机访问外部服务的信息；风险端口访问是指通过高危风险端口访问服务器。

行为分析每天要处理海量数据，因此需要采用分布式计算技术，行为分析利用奇安信诺亚大数据平台的分布式特性实现分布式，同时采用了奇安信自研分布式计算框架 Bear 提高程序执行效率。

2.9 报表报告

天眼系统报表报告模块主要包括快速报表、周期报表及报表模板三个能力，在新建报表任务时可新增过滤条件，在导出生成的报表文件时，增加文件导出类型以及增加新的报表模板。

快速报表、周期报表模块支持自定义配置新增快速或周期报表，支持配置报表格式（新增 HTML 格式的导出文件类型）、报表模板等信息，其中新建周期报表任务时，支持配置攻击维度、威胁级别、告警类型、资产分组、资产 IP、安全事件分析六类过滤条件，支持快速报表任务支持自定义时间过滤。

报表模板部分，提供多种报表模版（支持用户自定义模版），包括告警、受害资产、日志、威胁分析等，并新增天眼分析报告模板，用于展示失陷事件和尝试攻击事件的详情。

2.10 第三方日志接入

提供 API 接口识别功能；提供开放接口，实现对接联调，为支持第三方设备日志接入，天眼系统通过集成奇安信诺亚平台实现了数据采集、数据处理、数据存储及日志接入模块的管理和监控内容。

诺亚平台的数据采集、数据处理、数据存储构成第三方日志接入运行平台，完成数据接入并存储到系统，数据采集是整个环节的最前端，完成多种不同类型、不同协议数据的采集封包并发送到下一个环节；数据处理模块完成格式化、富化等操作，将不同来源的数据归一化到业务需要的格式；数据存储则完成数据最终的存储动作，控制数据的保存位置、形式，根据不同的业务需求，数据还可以分发一份到流处理，处理完的结构再进入存储。

集成了诺亚平台第三方日志接入模块的天眼系统，支持接入奇安信安全设备日志、第三方安全设备日志、网络设备日志、数据库日志、Windows 主机系统日志、Linux 主机系统日志、Web 服务器日志、虚拟化平台日志、其他日志；日志类型包括 SNMP Trap 日志、文本格式日志、数据库日志、WMI 日志、Netflow 日志、Syslog 日志等，并进行数据解析、入库、展示。

2.11 告警日志外发

为满足企业用户不同安全管理系统之间数据同步的场景，天眼系统提供告警联动能力，支持通过 SYSLOG、SNMP、邮件、KAFKA 等多种方式与其他安全管理系统进行数据对接。

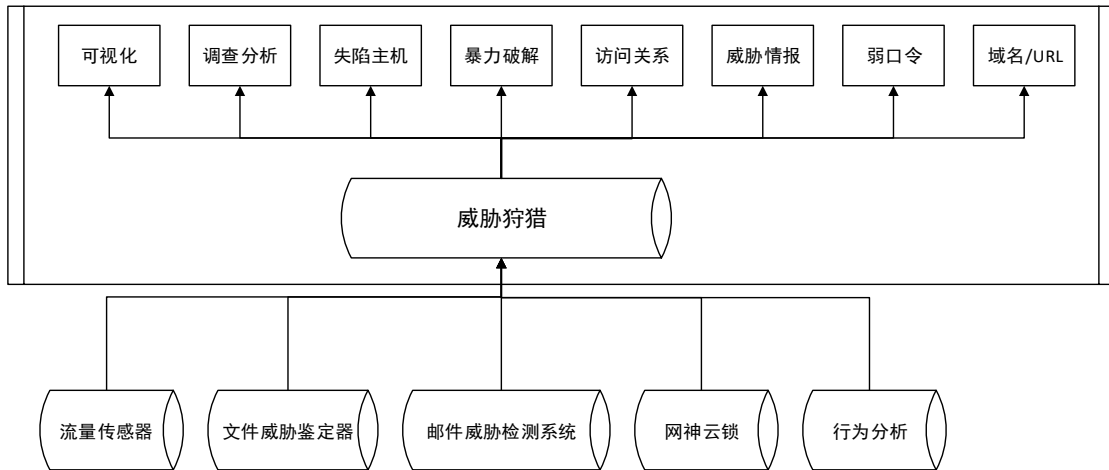
天眼系统每类告警外发功能均支持外发服务开关设置，可根据需要进行开启或关闭，以及对外发的告警数据进行灵活设置，包括系统日志、告警日志、原始告警日志、行为分析日志等。在 SYSLOG 方式外发配置支持 TCP 和 UDP 两种方式，并可灵活设置分隔符，并可配置多个 SYSLOG 接收服务器地址；SNMP 配置包含 SNMP 服务配置和 SNMP Trap 服务配置两个模块，用来对设备运行状态进行实时监测。管理员可通过 SNMP 客户端主动访问设备 MIB 库查询，也可通过配置 SNMP Trap 在客户端接收设备发出的 Trap 消息；邮件告警外发包括邮件服务信息配置、系统日志开关配置和告警日志开关配置三个模块可进行服务器使用协议、服务器地址、服务器端口、发件人、服务器认证开关、用户名、密码（邮箱服务器的密码）、SSL 等配置；KAFKA 对接外发告警支持设置 TOPIC、IP 及域名等信息，同时支持开启 kerberos 认证以保证数据的安全性验证。

2.12 威胁狩猎

传统的防护设备只能对攻击行为进行告警，无法向用户描述整个攻击过程。天眼系统依据多年积累的经验从攻击链的维度将攻击行为进行重新划分，对告警进行深度关联分析，以告警中的受害主机为线索还原整个攻击过程（侦察-入侵-命令控制-横向渗透-数据外泄-痕迹清理）。

天眼系统运用先进的可视化呈现技术，支持与用户在可视分析画布上对任意线索的自定义拓线及溯源分析，该过程通过用户与系统的灵活交互对已有数据进行拓线分析，从侦查、暴力破解、弱口令、主机外联、异地登录维度分析呈现安全风险行为，最终可以将威胁攻击的全过程推演并呈现在用户面前。同时，拓线分析过程支持结果快照导出，对于给定线索的溯源结果进行攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等维度的展示

威胁狩猎是将分析平台中告警，日志的信息进行汇总，进行多维度关联展示，可以有效的分析出数据之间的关联性，并获取相关的信息。



通过收集流量传感器，文件威胁鉴定器，邮件威胁检测系统，网神云锁数据，行为分析数据，对告警，资产，漏洞中的 IP，域名，文件 MD5，URI 等多种维度对数据进行分析

可视化图是通过图的方式展示告警和行为分析告警的数据，IP，域名，URI，邮箱和文件 md5 的关系。

