知道创宇 KNOWNSEC.COM

创宇云图威胁检测系统
产品白皮书

2020-05-27

北京知道创宇信息技术股份有限公司

更好更安全的互联网

文档说明

本文的内容是 2020 年北京知道创宇公司统一文档模板。文中的资料、说明等相关内容归北京知道创宇信息技术股份有限公司（以下简称“知道创宇”）所有。本文中的任何部分未经知道创宇许可，不得转印、影印或复印。

本文中的全部及任何部分内容均受密级和扩散范围限制。

2020 年知道创宇公司统一文档模板

北京市朝阳区阜安西路望京 SOHO 中心 T3-A 座-15 层

客服热线（Customer Hotline）：400-060-9587；010-57076191

传真（Fax）：010-57076117

邮编（Post Code）：100102

Blog：http://blog.knownsec.com

Email：sec@knownsec.com

文档控制

文档名称	创宇云图威胁检测系统白皮书
保密级别	内部公开
拟制	
审核	
标准化	

版本控制

版本	提交日期	相关组织和人员	版本描述
V1.8	2020-05-27	朱琳	创建

目 录

1 前言 1
1.1 威胁发展趋势 1
1.2 传统安全面临的挑战 3
1.2.1 传统安全技术的不足 3
1.2.2 单点防御不足以抵挡新一代威胁 4
1.3 新一代威胁检测技术演进方向 5
2 产品简介 7
2.1 系统概述 7
2.2 系统架构 8
2.3 处理流程 8
2.4 功能特性 9
2.5 部署方案 10
3 主要功能介绍 12
3.1 网络流量分析（NTA） 12
3.2 下一代入侵检测（NG-IDS） 12
3.3 网络行为检测（UEBA） 12
3.4 病毒木马检测（AV） 13
3.5 沙箱（Sandbox）行为检测 13
3.6 威胁情报（TI）检测 14
3.7 人工智能（AI）检测 14
3.8 高级持续性威胁（APT）检测 14
3.9 攻击链（Kill-chain）关联分析 14
3.10 资产画像（Asset portrait） 15
3.11元数据（Metadata）采集分析 15
3.12 全流量抓包（pcap）取证 16
4 核心技术原理 17
4.1 文件基因图谱人工智能检测 17
4.2 流量基因图谱人工智能检测 18
4.3 加密流量人工智能检测分析 19
4.3.1 恶意加密流量人工智能检测 19
4.3.2 Tor 流量人工智能检测 20
4.3.3 VPN 流量人工智能检测 20
4.3.4 ShadowSocks 流量人工智能检测 21

4.3.5 移动应用加密流量人工智能检测……22
4.4 WEB 攻击人工智能检测……22
4.4.1 SQL 注入攻击人工智能检测……22
4.4.2 XSS 跨站攻击人工智能检测……23
4.4.3 WebShell 网页后门人工智能检测……23
4.5 隐蔽隧道人工智能检测……24
4.5.1 DNS 隐蔽隧道人工智能检测……24
4.5.2 ICMP 隐蔽隧道人工智能检测……24
4.5.3 HTTP 隐蔽隧道人工智能检测……25
4.5.4 HTTPS 隐蔽隧道人工智能检测……26
4.6 DGA 域名人工智能检测……26
5 典型应用场景……27
5.1 办公网高级威胁检测……27
5.2 生产网潜伏威胁检测……28
5.3 数据中心高级威胁检测……29
5.4 城域网统一威胁感知……30

1 前言

1.1 威胁发展趋势

国际著名 IT 市场研究机构 Gartner 公司曾在安全趋势报告中指出：你所知道的关于安全的一切都在变化。

- **常规路线逐渐失控**

可信能力取代被误导的概念“所有权=信任”

- **所有实体都必须考虑潜在的敌对方**

所有数据包、URL、设备、应用、用户都是可疑的

- **大量的资源组合使用**

环境成为作实时安全决策的关键

- **传统安全控制越来越无效**

反病毒、边界防火墙越来越无效

- **需要改变通过堆叠保护信息的方式**

超越网络和设备的最终边界

- **违规/高级威胁极难被检测**

你已经被感染，只是你没有意识到

正如 Gartner 报告所说，安全的一切都在变化，威胁环境也已随之而变。黑客攻击正从个人行为向组织化、国家化方向发展，他们目的性强，动机明显，往往具有明确的商业、经济利益或政治诉求，攻击手段从传统的随机病毒、木马感染、工具投递等方式演进为社会工程、零日漏洞以及高级逃逸技术（AET）等组合方式，经常发起有针对性的 APT 攻击，具有高级化、组合化、长期化等特点，我们称之为新一代威胁。

新一代威胁最明显的一个特点就是能够绕过传统的安全检测和防御体系。网络犯罪分子往往持有最新的零日漏洞、商业级的工具包以及社会工程技术，能够

发起针对性的高隐蔽攻击。这些攻击行动缓慢，且分布多个渠道、跨越几个阶段，分步、持续性完成，能够躲避传统的防御手段，高效利用已有漏洞的系统和敏感数据。因此在新一代威胁面前，传统基于特征/签名检测的统一威胁管理（UTM）、下一代防火墙（NGFW）、入侵检测/防御系统（IDS/IPS）、防病毒（AV）等安全产品并不能使组织得到充分保护。

当前全球 IT 的安全支出显示，几乎所有的费用都花在过时的、基于特征/签名的技术。基于特征/签名的技术只能检测已知威胁，而不是未知的目前正在使用的新一代威胁。针对威胁变种，传统的防御如防火墙、IPS、防病毒、反垃圾邮件和安全网关已经塌陷，给网络罪犯留下一个敞开的漏洞，这就是为什么尽管已经部署了多层传统防御措施，但还是有超过 95%的公司网络中存在高级恶意软件。

现今的攻击利用高级手段，如掺混多态性和个性化，对于基于签名的工具表现出是未知的，但却真的足以绕过垃圾邮件过滤器，甚至骗过有针对性的受害者。例如，网络钓鱼攻击利用社交网站制作精巧地个性化的电子邮件，发送不断变化的恶意网址绕过 URL 过滤器。

传统安全产品正日益成为策略的执行者，而不是网络的保卫者。例如，URL 过滤产品对于执行员工网络浏览的策略是有效的，但对于防范不断变化的网页木马攻击则稍显不足。同样，下一代防火墙（NGFW）只是增加了用户、应用等下一代策略选项，并加强了传统基于签名的保护。虽然 NGFW 可以加强传统 IPS 和 AV 保护，但这些基于签名的技术，在保卫网络方面并没有新的提高或创新，集成这些传统的防御措施并不能阻止新一代威胁。

“普遍认为是高级攻击正在绕过我们传统基于签名的安全控制，并持续存在我们的系统中长时间未被发现。这种威胁是真实的。你已经受到损害，你只是不知道这一点。”-- By　Gartner

1.2 传统安全面临的挑战

1.2.1 传统安全技术的不足

新一代威胁穿透一个网络窃取信息时，通常利用多种手段并经过多个阶段。攻击者结合使用 Web、电子邮件和基于文件的攻击方式进行攻击。当前的防火墙，IPS，防病毒和 Web 安全网关几乎没有能力阻止使用零日漏洞、一次性恶意软件以及 APT 高级攻击手段的攻击者。

这些混合的，多阶段的攻击之所以成功，是因为传统的安全技术依赖于静态的基于签名的或基于列表的模式匹配技术。许多零日和定向型威胁，通过在无辜的网页上或可下载的文件如 JPEG 图片和 PDF 文档里隐藏新型植入恶意软件来渗透系统。或者他们使用个性化的钓鱼邮件发送到精心挑选的受害者，带有貌似合理的消息和针对零日漏洞的恶意附件。或者他们在社交媒体网站上嵌入微博，包含恶意 URL。每次受害者访问网站或打开附件，恶意软件主体就会安装在受害者的计算机上。这种恶意软件的代码通常包含利用操作系统、插件、浏览器或应用程序的多个未知漏洞，以确保它在系统中获得一个立足点。

最终，该代码会回连网络犯罪分子以获得进一步的指令和一个新的主体，或传送登录凭证，财务数据和其他有价值的信息。罪犯也可以进一步探索或用新的目标扩大他的僵尸网络。

除了利用技术优势，网络犯罪分子也意识到，他们可以分而治之，因为传统的防御和 IT 部门是有组织的。传统的安全防御措施通常设置为把每个攻击方式作为单独的路径，每个阶段作为独立的事件来检查，而不是把这些阶段和方式作为精心策划的一系列网络事件来检测和分析。通过利用 IT 部门内部的技术和商业壁垒，一个水坑式网站感染看起来就像一个随机事件，归咎于一个终端用户访问可疑网站的拙劣决定。它不能追溯到原始的用来愚弄用户和启动一个多阶段的高级定向型攻击的鱼叉式钓鱼邮件。所以，经过多个阶段的网页和邮件攻击，网络罪犯可以获取数据而不被防护者发现，直到为时已晚。

1.2.2 单点防御不足以抵挡新一代威胁

- **防火墙**

防火墙基于策略规则检测及管控 http 和 Web 流量，下一代防火墙增加了基于用户和应用的策略规则，加强了传统保护技术如 IPS 和 AV，但并没有增加对流量内容或行为的动态检测。

- **IPS**

签名、包检查、DNS 解析和启发式分析不会检测出一个利用零日漏洞的异常攻击行为，特别是如果恶意代码被严重伪装或分段投送。

- **防病毒**

恶意软件及其利用的漏洞是未知的（零日），并且该网站有一个正常的声誉，传统的防病毒网关和 Web 过滤器将会让它通过。

- **反垃圾邮件**

伪造的钓鱼网站使用不断变化的域名和网址，所以黑名单滞后于钓鱼网站的变化。而关闭一个钓鱼网站所需的平均时间超过 26 小时。

- **WEB 过滤**

大部分出站过滤器阻止成人内容或浪费时间的娱乐网站，不到四分之一的企业限制社交网站。除此之外，动态 URL、被黑的合法网站以及短期活跃的地址使静态 URL 黑名单过时了。

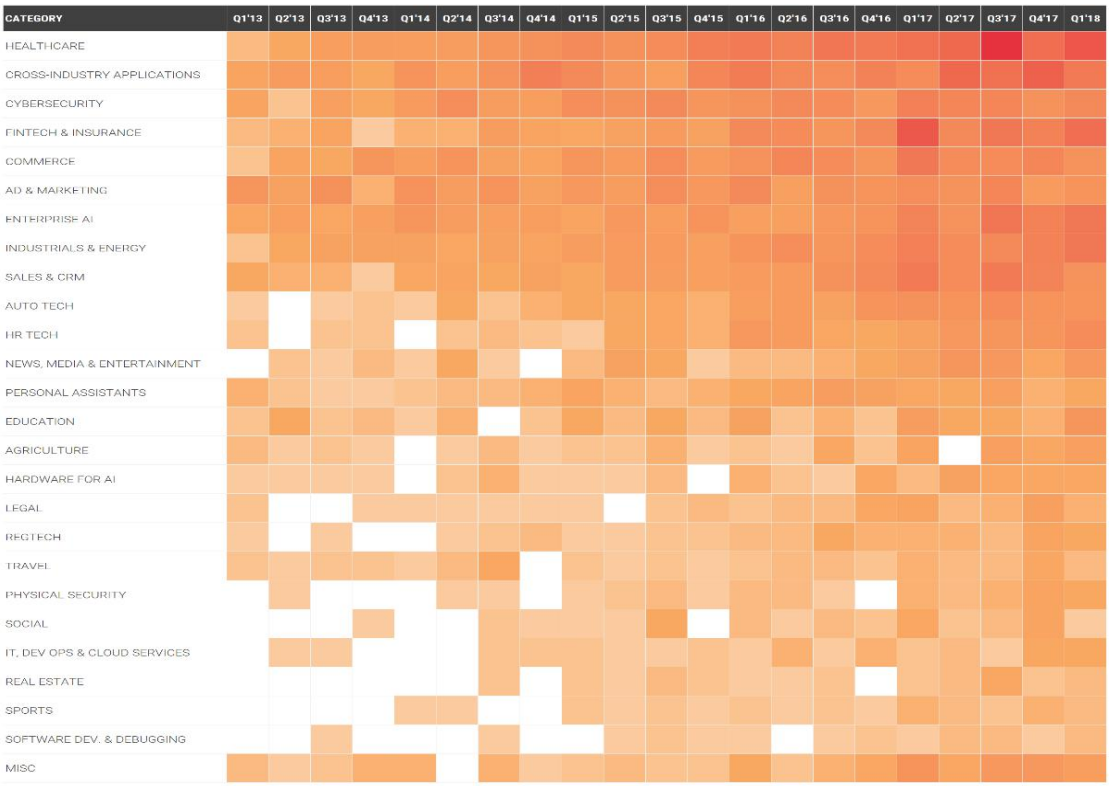
- **数据防泄露（DLP）**

DLP 工具主要是针对个人身份信息（PII），如身份证号码、社会保障号码、执照号码、或健康数据等。这些工具的好坏取决于他们的规则，但对于检测凭证或知识产权的外泄来说粒度较粗和规则繁琐。而外传通道的加密则使数据泄露内容不被看见，其静态的检测方法与新一代威胁的动态属性不相匹配。

1.3 新一代威胁检测技术演进方向

基于特征检测和行为检测的传统威胁检测手段已经越来越难以应对新型的安全攻击手法，难以识别安全攻击事件，且近年来随着人工智能技术的发展，攻击方在扫描、利用、破坏等攻击工具中对人工智能技术的应用，进一步加剧了对目标系统的破坏、缩短了攻击进程、隐藏了攻击特征，对新技术背景下的安全威胁检测手段提出了更大挑战。

自 1956 年达特茅斯会议 AI 的概念诞生至今，人工智能技术经历了起步探索、专家系统推广和深度学习三个阶段的长足发展。2006 年深度学习神经网络的提出以及 2013 年深度学习算法在语音和视觉识别上的重大突破，成为支撑深度学习商业推广的重要基石，人工智能步入新高潮。根据 CB Insights 的 AI Deals Tracker 所得到的统计结果，从 2013 年 Q1 到 2018 年 Q1，各行业在 AI 相关领域的股权交易达到了 4090 宗，共约 342 亿美元。其中在所有应用了 AI 技术的领域中，网络安全行业活跃度排名第四。



基于机器学习和深度学习的网络威胁检测技术能够识别变种威胁和未知威

胁，弥补了传统特征检测和行为检测仅能发现已知攻击的不足，但随着攻击方对人工智能技术的采用，人工智能之间的对抗正式拉开帷幕，意图躲避新型威胁检测技术的攻防对抗，对新一代威胁检测技术提出了更高要求。

集成学习和强化学习是现阶段实现安全威胁精准检测和对抗威胁检测躲避的有效技术手段。集成学习通过整合多个学习器，对安全攻击行为进行综合检测，通过多学习器之间的交叉验证、仲裁、投票等机制对意图欺骗威胁检测引擎的行为进行综合评判，提升检测结果准确率；强化学习通过持续的正向结果反馈活动，强化 AI 模型的检测模式，抵御来自攻击方的数据诱导，提高威胁检测模型的鲁棒性，保证新一代威胁检测技术的健壮性。

2 产品简介

2.1 系统概述

高级持续性威胁（APT）是指隐匿而持久的网络入侵过程，其通常是出于商业或政治动机，由某些人员精心策划，针对特定组织或国家，长时间内保持高隐蔽性，最后实施攻击。APT 通过零日威胁、特种木马变种、病毒变种等手段可以轻易绕过大部分传统安全设备， 基于特征检测的传统安全产品对 APT 的未知威胁攻击形同虚设。

创宇云图威胁检测系统将人工智能、大数据技术与安全技术相结合，实时分析网络流量，监控可疑威胁行为，内置多种检测技术，可对 APT 攻击链进行交叉检测和交叉验证。

创宇云图威胁检测系统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；通过基因图谱检测技术检测恶意代码变种； 还可以通过沙箱（Sandbox）行为检测技术发现未知威胁；对抽取的网络流量元数据，进行情报检测、异常检测、流量基因检测；最后将所有安全威胁进行关联分析，输出检测结果，对检测及防御 APT 攻击起到关键作用。

2.2 系统架构

图 1

创宇云图威胁检测系统系统架构如图 1 所示，创宇云图威胁检测系统监听口接收镜像/分光流量，通过 DPDK（Data Plane Development Kit，数据平面开发套件）对数据包进行快速处理以及硬件资源调度。通过筛选器过滤不必要的数据，将过滤后的数据进行二次处理，分别进行特征检测、元数据/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。之后通过中间件将元数据和事件进行泛化处理，将处理后的数据提交至 AI 检测引擎、异常行为检测引擎、文件检测引擎、威胁情报检测引擎、（Yara/JA3/SSL）检测引擎、关联引擎进行集中检测，最后将检测结果以日志/告警形式输出。

2.3 处理流程

创宇云图威胁检测系统系统业务处理流程如图 2 所示

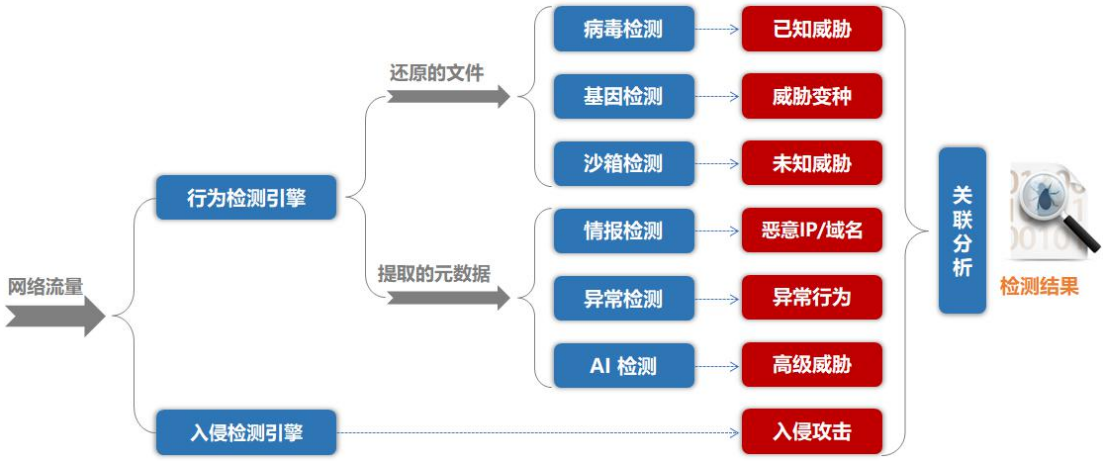


图 2

创宇云图威胁检测系统采集到的网络流量分别经由入侵检测引擎与行为检测引擎检测分析，入侵检测引擎能在内容、环境、应用层感知入侵。行为检测引擎对流量进行文件还原及元数据提取，还原出的文件通过内置的防病毒引擎对已知威胁进行静态检测；再通过基因检测技术对已知威胁的变种进行检测，并结合智能检测技术防止逃逸和躲避（AET），最后通过对恶意代码在沙箱中的主机行为和网络行为进行深入分析，对未知威胁进行检测。提取出的元数据则通过情报检测，检测恶意 IP/域名等；之后进行异常网络行为检测，如异常的内部和外部互联、C&C 通讯等，之后进行人工智能引擎检测，可对恶意加密流量、暗网流量、隐蔽隧道等进行检测。

2.4 功能特性

➢ 人工智能、大数据与安全技术的结合

创宇云图威胁检测系统采用了人工智能的机器学习/深度学习技术，基于大数据平台，用海量安全数据进行训练，从而具备检测未知威胁的能力，并有效减少安全运维人员的人工识别工作量。

➢ 高效的网络异常行为检测技术

创宇云图威胁检测系统可识别丰富的网络应用层协议，通过协议分析、网络异常行为模式匹配等检测技术快速鉴别出 C&C 通讯、DGA 恶意域名、DDoS 攻

击、SSH/FTP 暴力破解、SQL 注入、DNS/ARP 污染、漏洞扫描和漏洞攻击等网络恶意行为。

- **独特的基因图谱检测技术**

通过结合机器学习、深度学习、图像分析技术，将恶意代码映射为灰度图像，建立卷积神经元网络 CNN 深度学习模型，利用恶意代码家族灰度图像集合训练卷积神经元网络，并建立检测模型，利用检测模型对恶意代码及其变种进行家族检测。基于灰度图像映射的方法可以有效的避免反追踪、反逆向逻辑以及其他常用的代码混淆策略。并且该方法能够有效地检测使用特定封装工具打包（加壳）的恶意代码。

- **全面的已知、未知威胁检测**

通过内置的下一代入侵检测引擎，Multi-AV 防病毒引擎和威胁情报检测技术对已知威胁进行静态检测；通过基因检测技术对恶意代码的变种进行检测，通过对恶意代码在沙箱中的主机行为和网络行为进行深入分析，对未知威胁进行检测。

- **便捷的溯源取证能力**

创宇云图威胁检测系统支持解析并存储 HTTP、DNS、FTP、SMTP、POP3、IMAP、SMB 等几十种协议的元数据，具有完整的追溯取证能力。通过可视化操作，可快速定位攻击者，并定位出攻击者的 IP、MAC、攻击方式、攻击协议，以及攻击目标等详细信息。

- **强大的处理性能**

创宇云图威胁检测系统单台流量处理能力最高可达 10Gbps，文件处理能力最高可达 15 万文件/天，并可按需扩展处理能力。

2.5 部署方案

创宇云图威胁检测系统设备采用镜像或分光的方式旁路部署在需要被监测的网络位置，如图 3 所示：

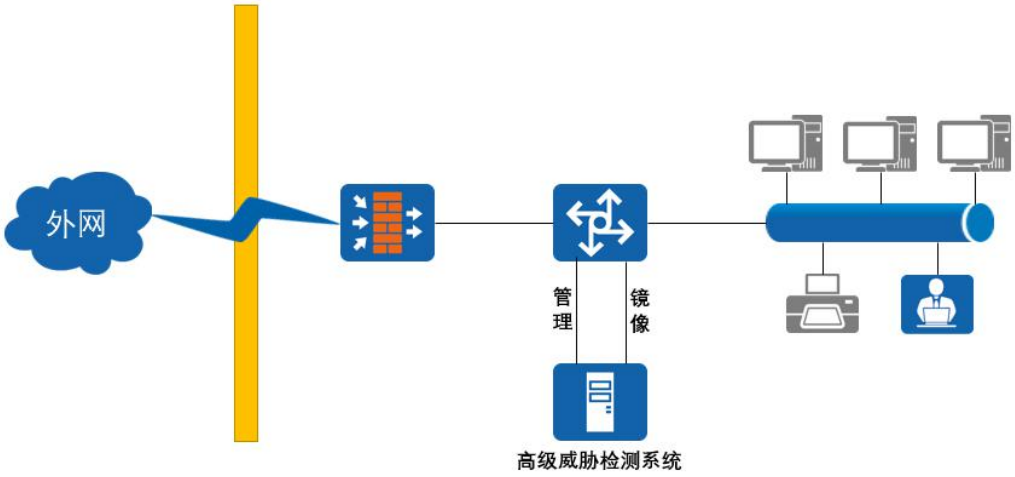


图 3

创宇云图威胁检测系统设备标准配置一个管理口，N 个监听口（N 由实际配置决定），其中管理口与交换机或电脑相连，用于设备控制、系统访问等；监听口与交换机镜像口相连，创宇云图威胁检测系统设备通过监听口接收交换机镜像流量，实现流量采集功能。

3 主要功能介绍

3.1 网络流量分析（NTA）

创宇云图威胁检测系统具备独立的流量采集还原能力，可将采集到的网络流量解析还原并以元数据/pcap 的形式存储，实现元数据/pcap 的高性能采集和预处理。通过系统内置的多个检测引擎进行交叉检测交叉验证，对流量中存在的网络威胁进行精确有效的定位。

3.2 下一代入侵检测（NG-IDS）

创宇云图威胁检测系统支持基于签名的网络入侵行为检测；支持应用感知，能够准确识别常见网络应用协议；支持内容感知，能够还原 HTTP、SMTP、POP3、FTP、IMAP、SMB 等协议中的文件。

创宇云图威胁检测系统的下一代入侵检测功能能有效弥补目前安全设备（防火墙、IDS 等）对攻击识别能力的不足，能够精确识别应用、内容和环境等各层面攻击，如 Web 应用攻击、恶意提权、漏洞攻击、网络扫描等，大大降低现有 IDS 产品的误报率，提升准确率。

3.3 网络行为检测（UEBA）

创宇云图威胁检测系统支持网络异常行为检测，支持 C&C 通讯和 DGA 域名检测，发现僵尸网络或被控主机；支持非法外联和数据外发检测，发现隐蔽通道和窃取数据行为；可以监测发现 DoS 和 DDoS 攻击、SQL 注入、跨站攻击等；支持传输层和应用层网络异常行为，自定义基线（模型）异常检测，例如异地登录行为、异常时间登录行为等；有本地和公网威胁情报关联等。

3.4 病毒木马检测（AV）

创宇云图威胁检测系统内置 4 个反病毒引擎，支持多反病毒引擎交叉检测，可以对已知威胁进行基于特征的静态检测和交叉验证，最终给出病毒木马家族检测结果。

3.5 沙箱（Sandbox）行为检测

创宇云图威胁检测系统支持基于沙箱行为的未知威胁检测，文件恶意行为模式库高于 700 个，处于行业领先水平。支持恶意文件的追溯取证和行为相似性聚类；支持各种主流的操作系统、浏览器、办公软件等虚拟运行环境。支持多种沙箱环境，包括 Windows 沙箱、Android 沙箱、Linux 沙箱、WEB 沙箱、Office 沙箱、PDF 沙箱等，并支持数十种文件类型检测，包括 PE 文件、Office 文件、PDF 文件、网页文件、压缩文件、APK 文件等。

图 4

如上图 4 所示，创宇云图威胁检测系统可基于沙箱技术对各种文件进行内容“引爆”，通过恶意行为模式匹配检测未知威胁，具有高检出率、低误报率、防变种、防逃逸等特点。

3.6 威胁情报（TI）检测

通过海量数据的采集、分析、验证获得威胁情报，内嵌于创宇云图威胁检测系统系统形成情报中心，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，进一步确认威胁来源的危害性，并支持 JA3、JA3S 和 SSL 恶意加密指纹检测。

对于高级威胁，可以优先利用情报引擎进行过滤，及时告警。

3.7 人工智能（AI）检测

创宇云图威胁检测系统内置多个人工智能（AI）检测模型，支持对文件基因、流量基因、加密流量、暗网流量、Shadowsocks 流量、VPN 流量、DNS 隐蔽隧道、ICMP 隐蔽隧道、HTTP 隐蔽隧道、HTTPS 隐蔽隧道、DGA 域名、Webshell 网页后门、SQL 注入攻击、XSS 跨站脚本攻击进行检测。

通过检测模型检测的方式可大幅度降低对特征规则数量的要求，具备更新频率低、数据量小、准确率高、误报率低、自动判断、人工干预少等优势。

3.8 高级持续性威胁（APT）检测

创宇云图威胁检测系统通过特征检测、行为检测、机器学习、深度学习、集成学习、强化学习的方式对安全数据进行有效的检测收敛降噪，并通过告警关联、情景关联的方式实现 APT 关联分析，进而迅速定位可能的 APT 攻击。

3.9 攻击链（Kill-chain）关联分析

通过网络入侵攻击检测、用户实体行为检测、流量人工智能检测、文件病毒

木马检测、文件基因图谱检测、文件沙箱行为检测、情报黑白名单检测、关联分析&威胁画像、元数据回溯分析取证等技术构建攻击链关联检测交叉验证体系，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检测全覆盖，如图 5 所示：

Kill Chain	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
网络入侵攻击检测	✓		✓		✓	✓	
用户实体行为检测	✓		✓		✓	✓	✓
流量人工智能检测		✓			✓		✓
文件病毒木马检测		✓		✓			
文件基因图谱检测		✓		✓			
文件沙箱行为检测		✓	✓	✓			
情报黑白名单检测	✓	✓		✓	✓		✓
关联分析&威胁画像	✓	✓	✓	✓	✓	✓	✓
元数据回溯分析取证	✓	✓	✓	✓	✓	✓	✓

图 5

3.10 资产画像（Asset portrait）

创宇云图威胁检测系统通过对流量的检测分析实现资产发现，对引擎产生的元数据进行处理，采集主机基本信息（IP、MAC 地址、制造商、软件信息以及设备类型等），并关联该主机对应的威胁告警日志，对资产状态、资产存在的风险进行精确评估，实现对资产威胁的精准画像。

3.11 元数据（Metadata）采集分析

创宇云图威胁检测系统支持对流量进行网络层、传输层、应用层元数据提取，可解析还原 DNS、FTP、HTTP、IMAP、POP3、SMB、SMTP、SNMP、ICMP、DCE-RPC、DHCP、DNP3、IRC、krb、Modbus、MySQL、NTLM、RADIUS、RDP、RFB、SIP、SOCKS、SSH、SSL、Syslog、Oracle、Telnet、TFTP、TCP、UDP 等协议并以元数据形式存储，用于威胁的溯源取证。

3.12 全流量抓包（pcap）取证

创宇云图威胁检测系统支持全流量抓包功能，支持抓包策略配置，并支持深度包解析、BPF 规则过滤功能，有效的抓取 pcap 流量包留存取证。

4 核心技术原理

4.1 文件基因图谱人工智能检测

如今病毒木马变种层出不穷，攻击者通过改变病毒木马的某一部分特征，实现对传统杀毒软件检测的绕过。

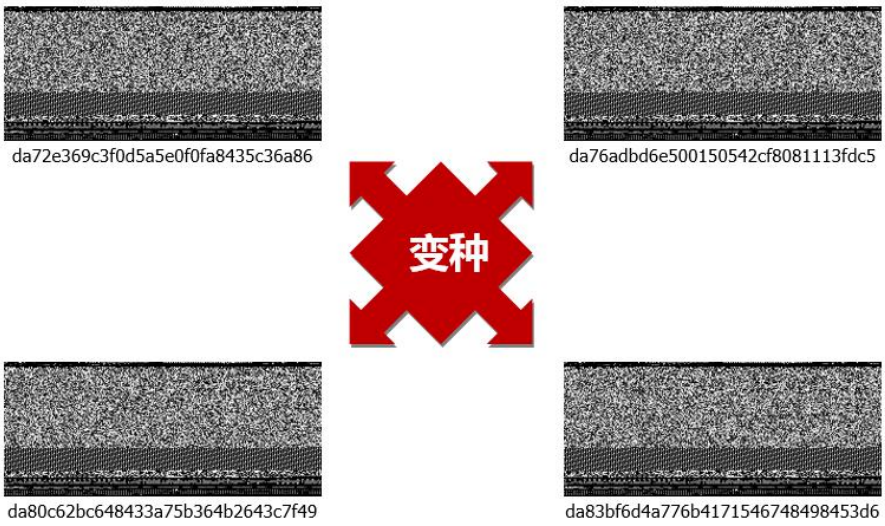


图 6

如图 6 所示，这些都是某个恶意软件的多个变种，但各自的 MD5 值都不一样，现有的基于特征的检测技术如果未曾更新到特征库，就无法识别。

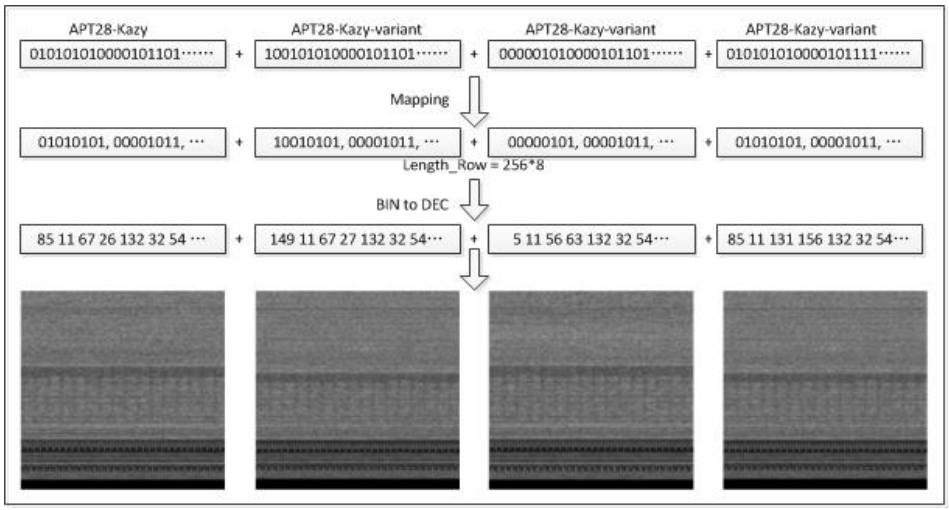


图 7

如图 7 所示，创宇云图威胁检测系统采用业界独特的基因检测技术，可以利用恶意代码在变种过程中的遗传学特征，即基因在遗传过程中的复制特性及部分基因突变特性，对恶意代码进行检测。通过基因比对，可以很轻易的识别出恶意代码变种，目前基因库恶意病毒基因高达数 10 亿样本，覆盖 5000 个以上家族，且在不断更新，检测的时间粒度在毫秒级别。

4.2 流量基因图谱人工智能检测

网络流量的规模和密度逐年增长，协议的类型和应用服务的类型更是多样化，更有恶意流量利用非标准协议进行数据的伪装或加密，以实现数据隐蔽传输。因此，如何准确识别网络流量的是网络安全中的重要问题。

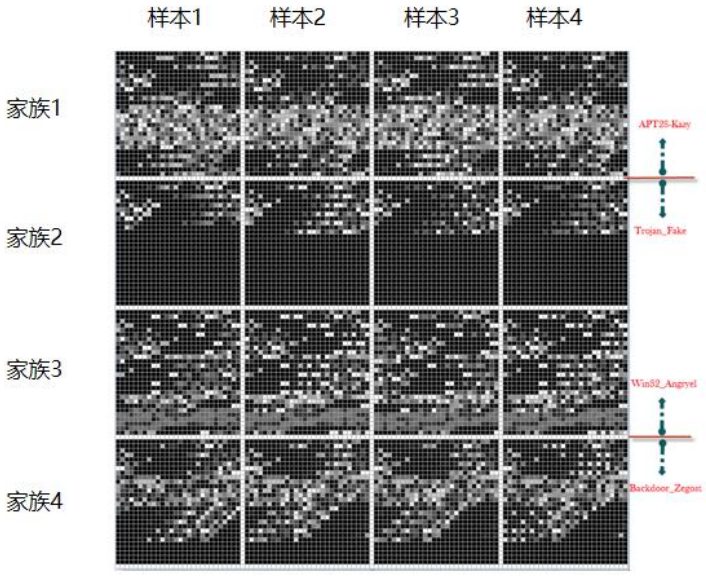


图 8

如图 8 所示，这些都是同一恶意代码家族的不同变种的外联通讯会话，不同会话的特征均存在差异，现有的基于特征的检测技术如果未曾更新到特征库，就无法识别。

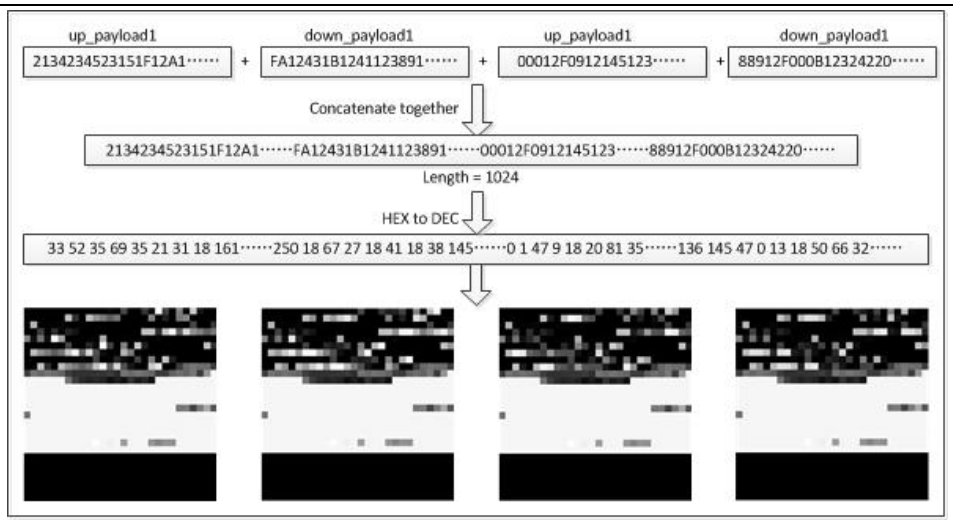


图 9

如图 9 所示，创宇云图威胁检测系统采用业界独特的基因检测技术，将流量会话映射成基因图谱，通过海量恶意样本家族产生的流量训练形成未知协议通讯检测模型，结合系统实时获取的网络会话基因特征，进行基因比对，实现精确的流量基因检测。

4.3 加密流量人工智能检测分析

4. 3. 1 恶意加密流量人工智能检测

创宇云图威胁检测系统支持恶意加密流量人工智能检测，通过提取恶意代码家族的加密网络会话基因特征（DNS 特征、TLS 元数据、HTTP 特征、包特征信息等）训练形成恶意代码加密通讯检测模型，如图 10 所示：

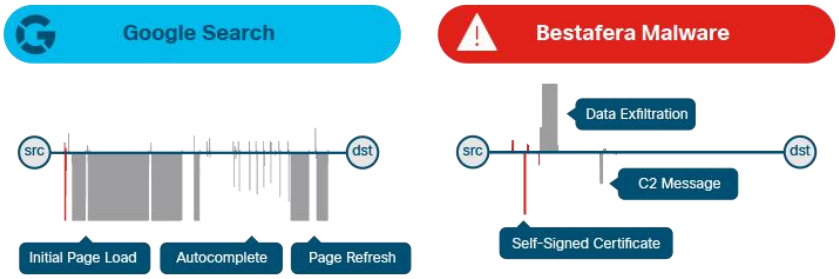


图 10

在现网中，创宇云图威胁检测系统系统获取实时网络会话元数据，构建特征

向量，使用检测模型对网络流量进行恶意代码加密通讯检测。

4.3.2 Tor 流量人工智能检测

创宇云图威胁检测系统支持 Tor（暗网）流量人工智能检测，采用构建 Tor 流量/非 Tor 流量捕获环境进行同类应用的数据传输（包括但不局限于浏览器、邮件、聊天工具、视频流、音频流、文件传输、P2P、VoIP 等），分别提取步态指纹特征数据集训练建立暗网检测模型，如图 11 所示：

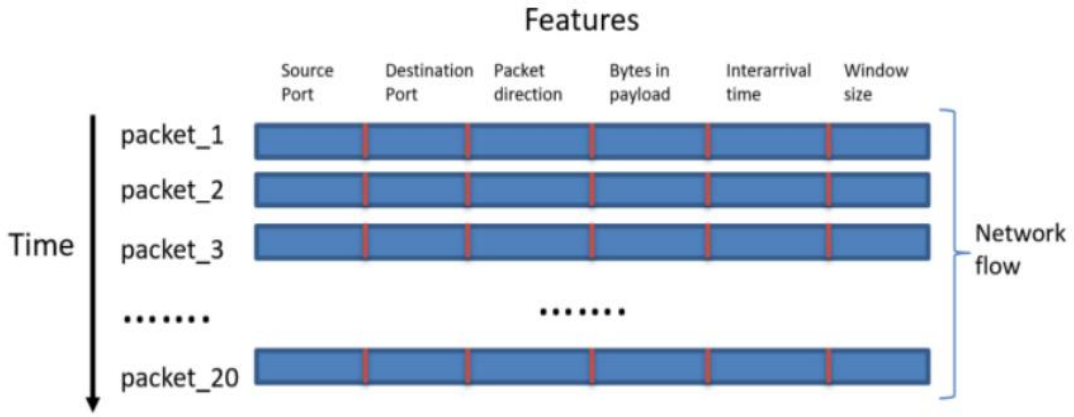


图 11

在现网中，创宇云图威胁检测系统系统获取实时网络会话元数据，构建实时步态指纹特征，使用暗网检测模型对网络流量进行暗网通讯检测。

4.3.3 VPN 流量人工智能检测

创宇云图威胁检测系统支持 VPN 流量人工智能检测，采用构建流量捕获环境进行同类应用的数据传输（包括但不局限于浏览器、邮件、聊天工具、视频流、音频流、文件传输、P2P、VoIP 等），分别提取步态指纹特征数据集训练建立 VPN 流量检测模型，VPN 流量检测模型框架如图 12 所示：

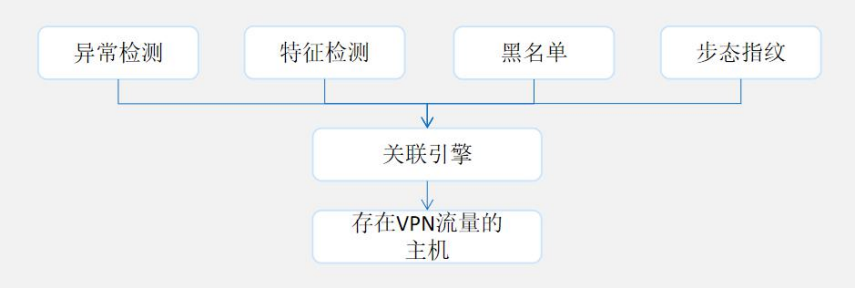


图 12

在现网中，创宇云图威胁检测系统获取实时步态指纹特征，使用 VPN 流量检测模型对网络流量进行 VPN 流量检测。

4.3.4 ShadowSocks 流量人工智能检测

创宇云图威胁检测系统支持 ShadowSocks 流量人工智能检测，构建流量捕获环境进行同类应用的数据传输（包括但不局限于浏览器、邮件、聊天工具、视频流、音频流、文件传输、P2P、VoIP 等），分别提取步态指纹特征数据集，通过 Shadowsocks 步态指纹检测结果生成 Shadowsocks 的服务端黑名单和客户端黑名单，经训练建立 ShadowSocks 流量检测模型，ShadowSocks 流量检测模型框架如图 13 所示：

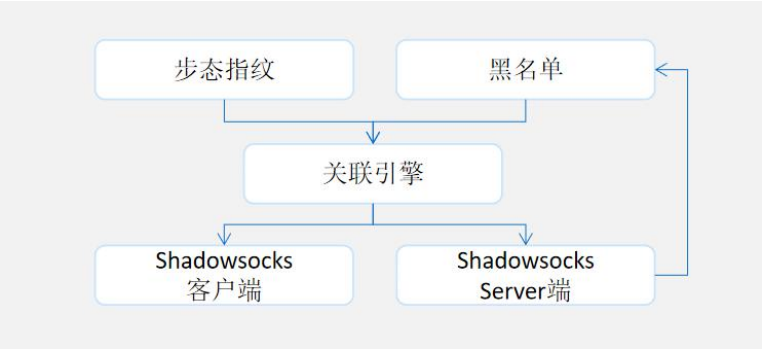


图 13

在现网中，创宇云图威胁检测系统获取实时步态指纹特征，使用 ShadowSocks 流量检测模型有效精准的定位存在 ShadowSocks 流量的主机。

4.3.5 移动应用加密流量人工智能检测

对手机 APP 应用程序流量检测整体检测架构如图 14 所示，分为静态指纹检测和动态 AI 检测。静态指纹检测主要依赖 SSL 通信中 Hello 数据包生成方式与相应的客户端关联，构建 JA3 和 JA3S 的指纹引擎。动态指纹检测分为通信特征 AI 模型和步态指纹 AI 模型。

分别刻画不同手机 APP 通信流量特征，通过 AI 大数据和机器学习集成模型算法来识别手机 APP 流量，三个模型输出的最终结果到达关联引擎，综合判定 APP 流量类型。

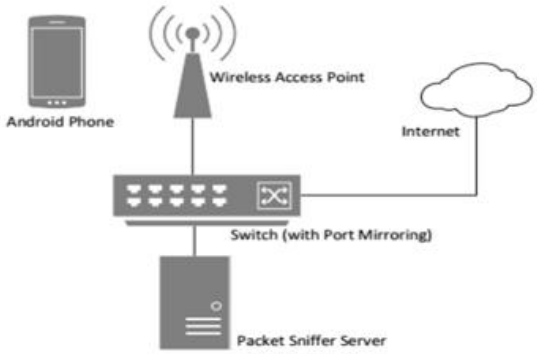


图 14

4.4 WEB 攻击人工智能检测

4.4.1 SQL 注入攻击人工智能检测

创宇云图威胁检测系统支持 SQL 注入攻击人工智能检测，利用机器学习、集成学习和强化学习技术构建 SQL 注入攻击检测模型。

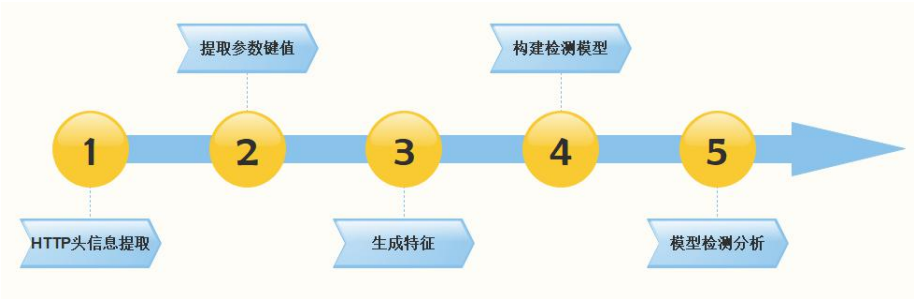


图 15

如图 15 所示，通过提取 Web 的 URI、POST 内容、User-Agent 等其他 HTTP 头部信息，递归解码后，提取参数键值内容，基于 SQL 关键字泛化后生成 word embedding 特征后进入模型检测，判断是否存在 SQL 注入。

4.4.2 XSS 跨站攻击人工智能检测

创宇云图威胁检测系统支持 XSS 跨站攻击人工智能检测，利用机器学习、集成学习和强化学习技术构建 XSS 检测模型。

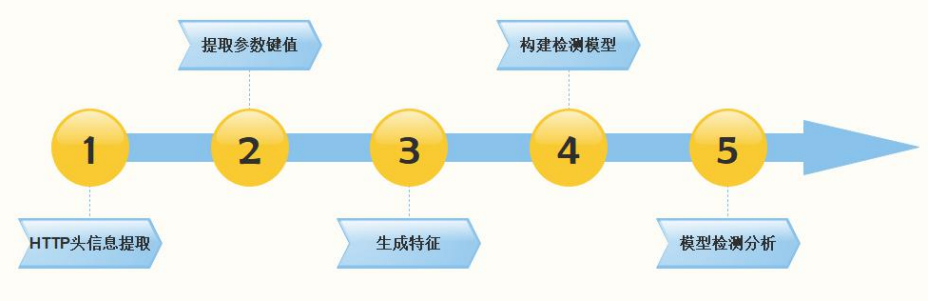


图 16

如图 16 所示，通过提取 Web 的 URI、POST 内容、User-Agent 等其他 HTTP 头部信息，递归解码后，提取参数键值内容，基于 JavaScript/HTML 等其他关键字泛化后生成 word embedding 特征后进入模型检测，判断是否存在 XSS。

4.4.3 WebShell 网页后门人工智能检测

创宇云图威胁检测系统支持 Webshell 网页后门人工智能检测，如图 17 所示，通过搭建 Webshell 运行环境，利用词袋与 TF-IDF 技术提取特征，同时利用 uri/request body/response body，URI 中的资源文件名称和动作建立静态 AI 检测模型；通过 php 动态脚本 opcode 提取 N-Gram 特征建立动态 AI 检测模型；通过异常特征统计、异常流量会话构建动态 AI 异常检测模型。

通过静态 AI 检测、动态 AI 检测、动态 AI 异常检测实现对 Webshell 网页后门攻击的精确定位。

图 17

4.5 隐蔽隧道人工智能检测

4.5.1 DNS 隐蔽隧道人工智能检测

DNS Tunneling，是隐蔽信道的一种，通过将其他协议或数据封装在 DNS 协议中传输建立通信。

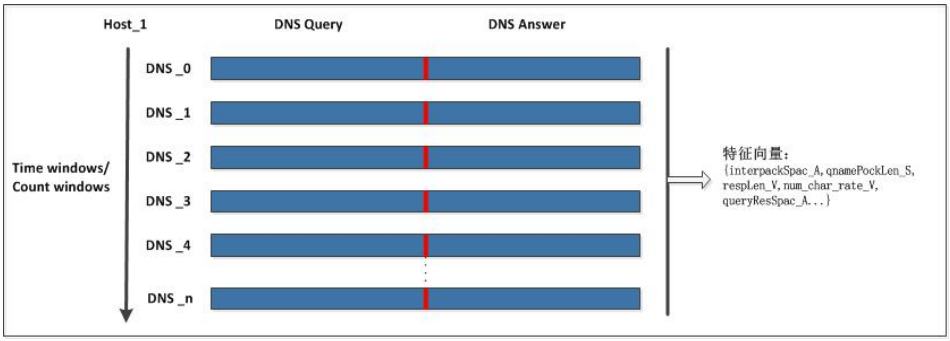


图 18

创宇云图威胁检测系统支持 DNS 隐蔽隧道人工智能检测，如图 18 所示，通过渗透环境搭建收集黑数据和白数据，生成用于分类 DNS 隧道和正常 DNS 数据的样本集合，利用基于窗口的 DNS 隐蔽隧道特征向量（DNS 隧道空间、回应包的长度、qname 中数字字符占比等），构建 DNS 隐蔽隧道检测模型。

在现网中使用 DNS 隐蔽隧道检测模型对网络流量进行 DNS 隐蔽隧道检测。

4.5.2 ICMP 隐蔽隧道人工智能检测

创宇云图威胁检测系统支持 ICMP 隐蔽隧道人工智能检测，通过搭建 ICMP 隧道流量捕获环境，使用 ICMP 隧道工具集合进行 ICMP 隧道数据传输，基于窗口的 ICMP 隐蔽隧道特征向量（pktlenMax、payload_n-gram-213、pktlenEnt 等）进行训练建立 ICMP 隐蔽隧道检测模型，如图 19 所示。

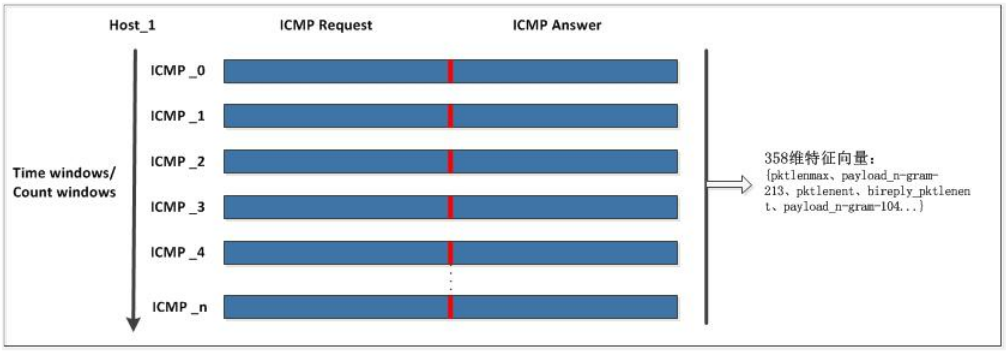


图 19

在现网中，创宇云图威胁检测系统获取 ICMP 隐蔽隧道特征向量，使用复合金字塔模型对网络流量进行 ICMP 隐蔽隧道通讯检测。

4.5.3 HTTP 隐蔽隧道人工智能检测

创宇云图威胁检测系统支持 HTTP 隐蔽隧道人工智能检测，如图 20 所示，通过提取原始流量 HTTP 流量特征，规则引擎用来打标和清洗过滤 HTTP 流量，经标注的正常流量和 HTTP 隧道流量分别经过自动化特征提取引擎，提取出重要特征，异常检测模型根据特征建立 HTTP 隐蔽隧道流量识别模型。

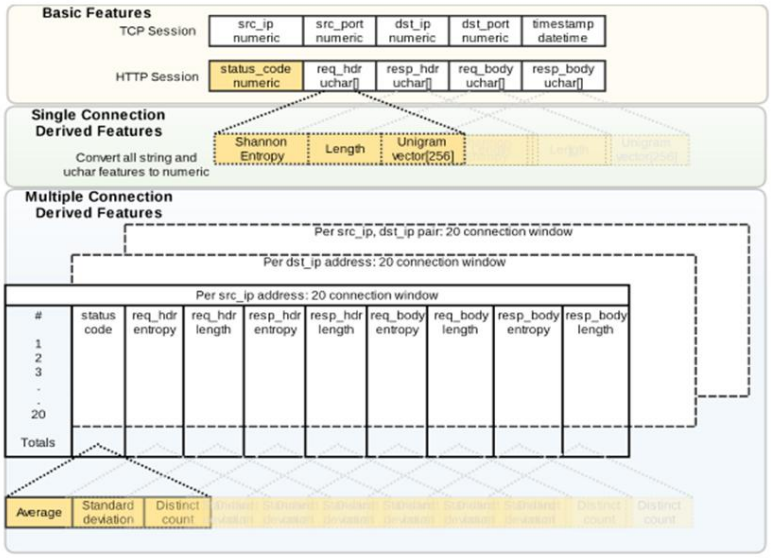


图 20

在现网中，创宇云图威胁检测系统获取 HTTP 隐蔽隧道特征，HTTP 隐蔽隧道检测模型对网络流量进行 HTTP 隐蔽隧道通讯检测。

4.5.4 HTTPS 隐蔽隧道人工智能检测

创宇云图威胁检测系统支持 HTTPS 隐蔽隧道人工智能检测，通过提取恶意代码家族的加密网络会话基因特征（TLS 元数据、HTTP 特征、会话负载等）训练形成 HTTPS 隐蔽隧道检测模型，如图 21 所示；

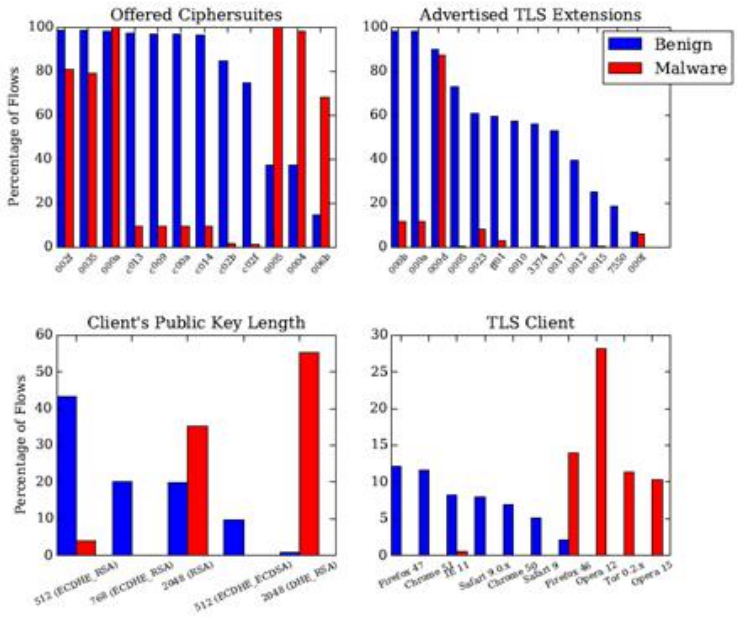


图 21

在现网中，创宇云图威胁检测系统系统获取实时网络会话元数据，构建特征向量，使用检测模型对网络流量进行 HTTPS 隐蔽隧道通讯检测。

4.6 DGA 域名人工智能检测

DGA (Domain Generation Algorithm，域名生成算法)的设计思想是，malware 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。

创宇云图威胁检测系统支持 DGA 域名人工智能检测，如图 22 所示，通过建立针对 DGA 生成域名的长短期记忆神经网络 LSTM 深度学习模型，用海量 DGA 生成域名和正常域名对深度学习模型进行训练，使深度学习模型具备识别

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，深度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。

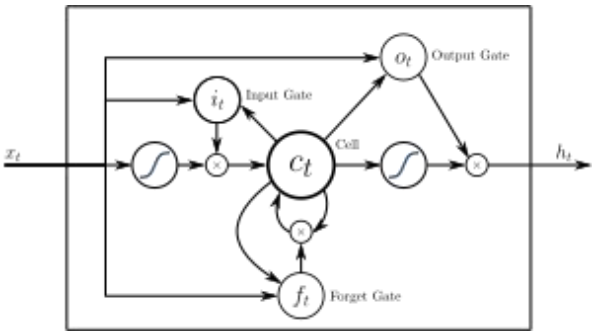


图 22

5 典型应用场景

5.1 办公网高级威胁检测

随着各行各业安全措施的逐步落实，直接针对目标系统的安全攻击越来越难以奏效，黑客等攻击组织逐步将攻击对象转移到安全意识薄弱的内部办公人员，以办公网为跳板，向内部系统发起攻击。办公网逐渐成为安全威胁的重灾区，钓鱼邮件、页面劫持、恶意 url 等诱骗手段防不胜防，稍不注意就会导致木马、病毒等恶意软件潜伏到办公网络中，给内部系统埋下安全隐患。

创宇云图威胁检测系统通过分光或镜像网络流量的方式，对 DMZ 区和办公网核心交换机的上联端口进行全流量监测，通过先进的人工智能检测技术捕获钓鱼邮件、恶意 url、页面劫持、恶意文件传播等行为，实时进行安全告警，弥补由于办公人员安全意识薄弱所导致的安全事故，发现潜在的安全威胁，常规部署图如图 23 所示：

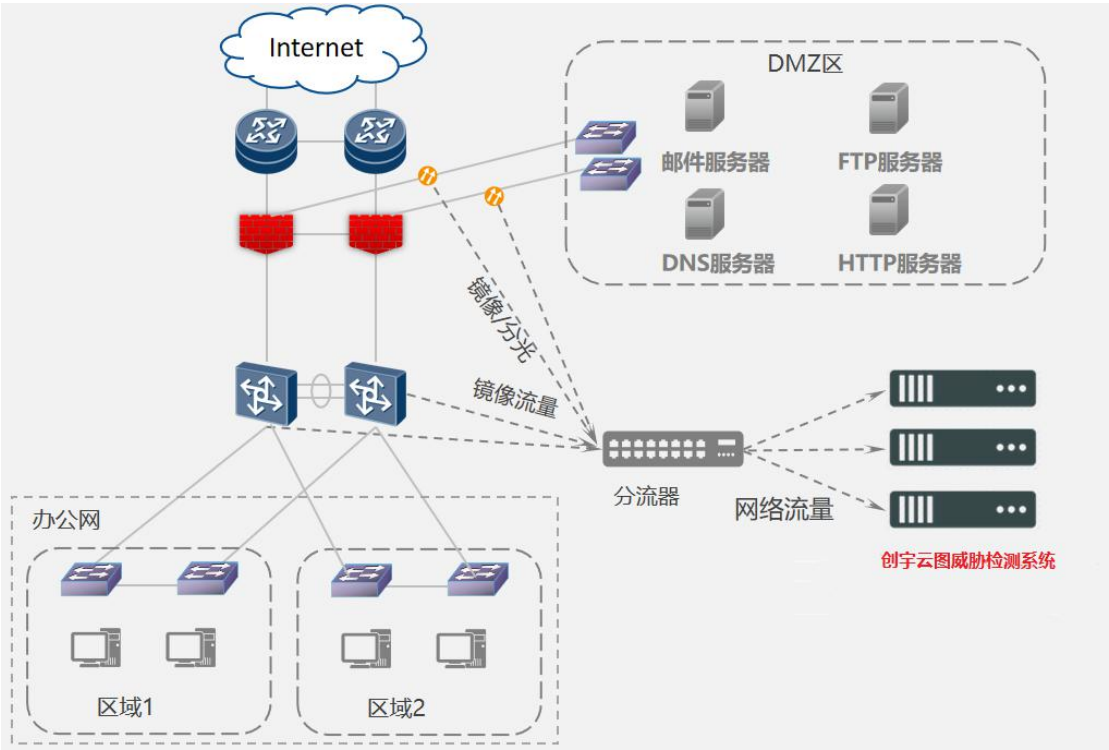


图 23

创宇云图威胁检测系统通过持续监测网络流量、分析安全威胁，能够帮助用户实时了解办公网的安全运行态势，发现潜在的恶意行为，找出易受攻击的办公电脑，发现已知威胁变种、未知威胁和恶意加密传输的流量，让办公网的安全隐患无处遁形。

5.2 生产网潜伏威胁检测

针对生产网进行持续攻击的震网病毒事件给处于隔离状态的生产网拉响了安全警报，隔离系统并不是无懈可击、百分百安全。

作为企业运营支撑的生产网伴随着业务的建立而长年、持续的运行，由于历史发展、业务迭代、合作伙伴更换、业务逻辑复杂等原因，生产网常常处于低安全防御水平，漏洞随处可见、薄弱环节数不胜数，且由于安全修复所造成的业务升级事故屡见不鲜，导致生产网对安全改造持谨慎态度。生产网系统自身的安全配置、安全管理以及恶意文件的传播控制成为生产网的首要安全需求。

创宇云图威胁检测系统通过镜像生产网内各业务分区的汇聚交换机上联端

口，对生产网东西向的网络流量进行实时分析，通过利用沙箱、多 AV 病毒检测、流量基因检测和文件基因检测等先进技术对恶意样本、恶意流量、行为异常等威胁进行重点识别，弥补生产网自身业务系统脆弱的不足，保护生产网安全，常规部署图如图 24 所示：

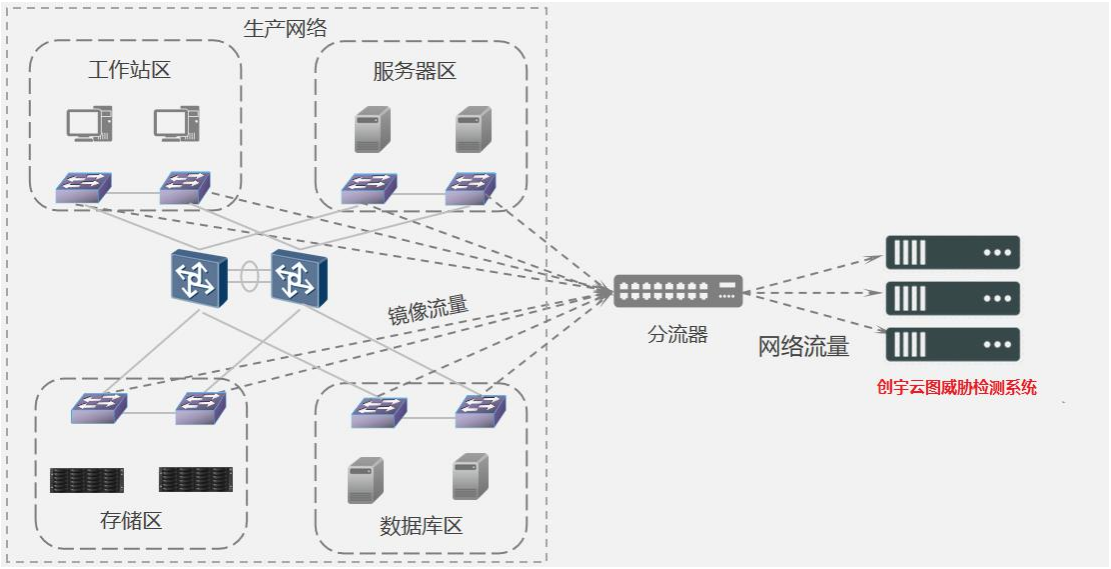


图 24

创宇云图威胁检测系统通过持续监测生产网，能够帮助用户实时了解生产网的安全运行态势，掌握生产系统的漏洞分布情况，发现高危漏洞主机，发现潜伏的恶意文件和恶意流量通讯行为，识别恶意文件的扩散。

5.3 数据中心高级威胁检测

回顾 2019 年的安全威胁态势，以信息泄露为例我们发现整体信息泄漏量较 2018 年相比有近 120%的涨幅(数据来源于情报供应商 Risk Based Security (RBS) 的 2019 年 Q3 季度报告)。在大数据分析的背景下，当今时代的信息泄露已经不仅仅是影响企业的声誉、品牌效应那么简单，通过数据的关联分析结果进行二次攻击，能够给企业造成直接破坏和经济损失，保护资产、保护信息泄露刻不容缓。

数据中心作为企业的核心数据存储区，通常保存企业所有的敏感数据和机密数据，一旦发生信息泄露、加密勒索等安全事故，损失无法估量。

创宇云图威胁检测系统通过镜像数据中心各业务分区的汇聚交换机上联端

口，对数据中心内部东西向业务流量进行安全监测，通过先进的隐蔽隧道检测技术、加密流量检测技术、JA3 和 SSL 指纹等检测技术重点识别可疑传输行为，告警信息泄露事件；通过流量基因检测、网络沙箱检测等技术识别加密勒索等行为，保护数据中心的安全，常规部署图如图 25 所示：

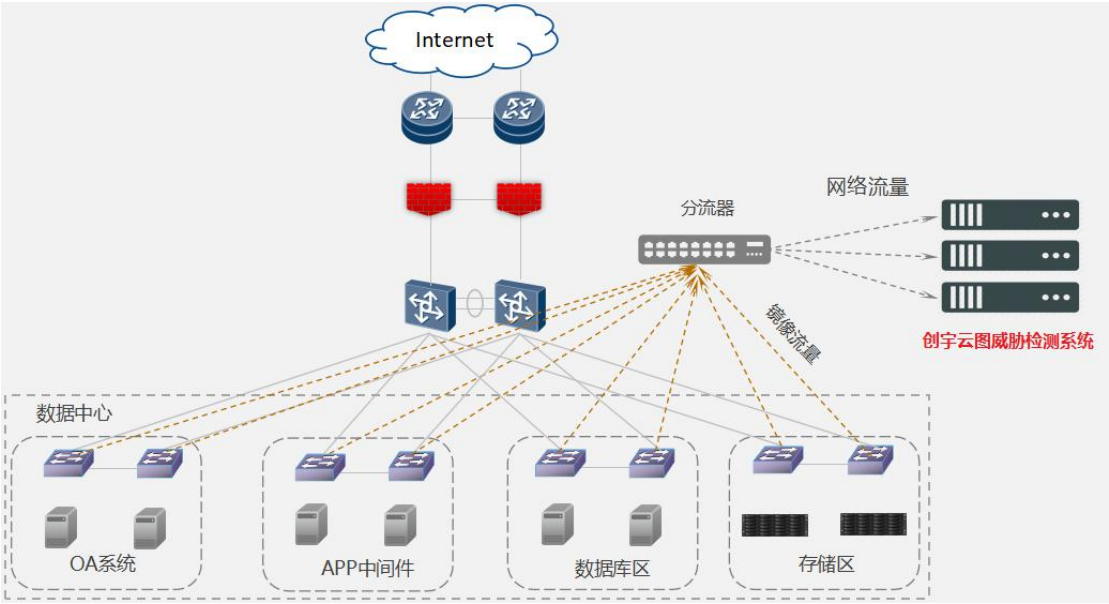


图 25

创宇云图威胁检测系统通过持续监测数据中心，能够帮助用户实时了解数据中心的安全运行态势，发现隧道传输、加密流量传输等可疑信息传输行为，找到潜在的 APT 攻击，识别加密勒索软件。

5.4 城域网统一威胁感知

回顾近些年的技术发展，4G、云计算、智能手机、移动 APP、大数据、5G 等新兴事物对广大民众生活产生了深远影响，大带宽、低延时、丰富内容的呈现等新时代的核心诉求对运营商提出了新挑战，促进运营商不断发展，运营商逐渐摆脱线路提供者的角色向更深、更广的增值服务转变。

作为承载驻地网用户角色的城域网，负责高质量的传输广大民众所喜爱的视频、语音、游戏、信息浏览等数据，任何环节质量的降低都将引起用户的不满，进而导致在网用户流失。据不完全统计，直接影响城域网服务质量的因素包括 DDOS 攻击、僵木蠕传播等安全威胁；且随着近些年运营商角色的转变，各业

务系统迁移至云平台并承受着不同租户间的威胁扩散，对云平台内部的安全威胁监测成为重中之重。

创宇云图威胁检测系统通过分光城域网数据中心、边缘机房的线路流量，对城域网进行分布式的安全监测，实时检测 DDOS 攻击、APT 攻击和僵木蠕传播等行为；在城域网安全管理中心部署一套 CIC 大数据安全分析系统，对分布式监测引擎的安全事件进行统一收集、合并和展示，通过大窗口的离线分析，精准告警安全威胁并在整个城域网的范围内发现相似的安全攻击、安全事件，形成整体联防，提高防护效率。

常规部署图如图 26 所示：

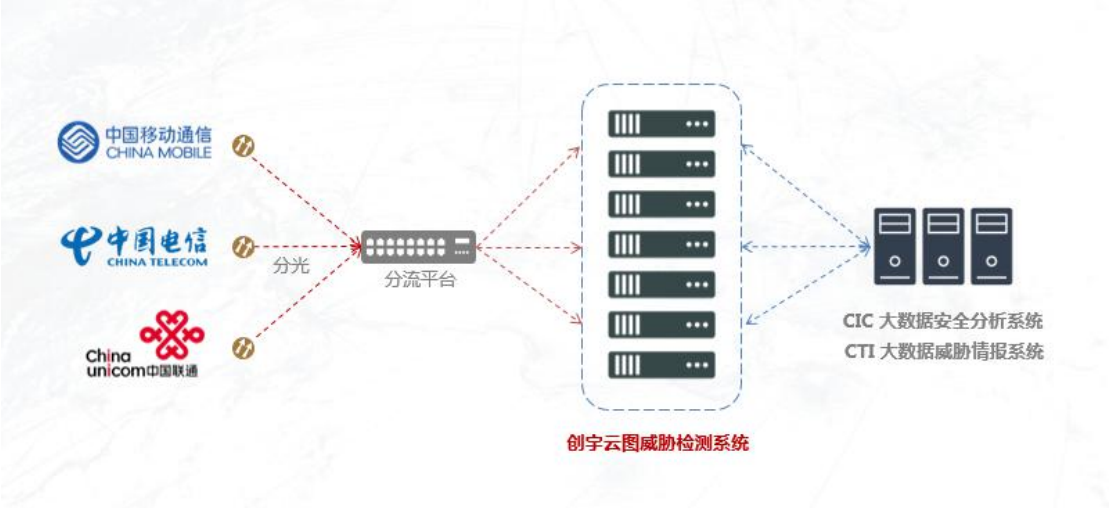


图 26

创宇云图威胁检测系统通过与 CIC 大数据安全分析中心级联，能够帮助用户实时了解城域网整体的安全运行态势，发现局部的 DDOS 攻击、APT 攻击和僵木蠕传播等事件，并能够指导全网进行进行联防、预防，大大提高安全防护效率。