奇安信 威胁情报中心

奇安信 新一代网络安全领军者

2020 威胁情报手册

高级网络安全能力的标配

奇安信威胁情报中心
奇安信集团
2020-1-1

目 录

奇安信
新一代网络安全领军者

奇安信 威胁情报中心

奇安信威胁情报中心持续跟踪40个主要APT团伙

2013

摩诃草
别名：Patchwork、白象
内部序号：APT-C-09

摩诃草最早由 Norman 安全公司曝光，是一个来自于南亚地区的境外 APT 组织，主要针对中国、巴基斯坦等亚洲地区国家进行网络间谍活动，以窃取敏感信息为主。

Lazarus Group
别名：Hidden Cobra
内部序号：APT-C-26

Lazarus Group 最早的攻击活动可以追溯到 2009 年，包括针对韩国的 DarkSeoul、2014 年攻击 SONY 事件、2017 年的 WannaCry 事件。近几年来，该组织的活动主要针对全球金融、银行及加密货币交易相关的目标。

2014

APT29
APT29 最早攻击活动至少可以追溯到 2008 年。该组织被认为从 2015 年夏季就攻击了美国 DNC。

Molerats
别名：Gaza cybergang

Molerats 是一个出于政治动机的威胁组织，攻击目标主要是中东、欧洲和美国。

Kimsuky
Kimsuky 至少从 2013 年 9 月开始活跃。该组织针对韩国智囊团以及与朝核相关的目标开展攻击活动，曾被认为与 2014 年韩国水电与核电公司（Korea Hydro & Nuclear Power Co.）被攻击事件有关。

Sandworm
别名：BlackEnergy

Sandworm 是网络间谍组织，主要针对能源、工业控制系统、SCADA、政府和媒体相关的乌克兰实体开展攻击活动；该组织与 2015 年底的乌克兰能源部门袭击事件有关。

Energetic Bear
别名：Dragonfly

Energetic Bear 疑似网络间谍组织，其攻击对象最初主要针对国防和航空公司，但在 2013 年初，其攻击目标转移到能源、工控领域。

APT28
内部序号：APT-C-20

APT28 历史攻击活动非常频繁，主要开展网络间谍活动；该组织被认为和 2016 年美国 DNC 被攻击及干扰美国大选事件有关。

Turla
Turla 拥有非常复杂的 TTP，主要实施网络间谍活动，其前身可能和 Moonlight Maze 有关。

2015

El Machete
El Machete 疑似一个熟悉西班牙语并活跃在拉美地区的 APT 组织，其攻击目标主要针对拉美国家的政府实体。该组织使用 Python 编译的可执行文件并结合色情图片进行诱导攻击。

Darkhotel
内部序号：APT-C-06

Darkhotel 是卡巴披露的 APT 团伙，其早期针对高级酒店网络实施攻击活动，主要使用的攻击手法为鱼叉邮件攻击。

Inception Framework
别名：Cloud Atlas、RedOctober

Inception Framework 是一个持续多年的 APT 组织，最初攻击目标主要是俄罗斯和东欧地区，后续延伸至全球，主要针对金融、能源、外交等领域开展攻击活动。该组织擅长利用云服务和物联网隐藏其控制基础设施，并且同时拥有针对 PC 和移动终端的攻击工具。卡巴曾披露该组织与 RedOctober 行动有关。

CopyKittens
CopyKittens 是网络间谍组织，攻击活动主要针对以色列、沙特阿拉伯、土耳其、美国、约旦和德国等目标。

方程式
方程式是一个拥有全平台载荷攻击能力的攻击组织，掌握多个 0Day 漏洞。

毒云藤
内部序号：APT-C-01

毒云藤是奇安信威胁情报中心披露的 APT 组织，其最早攻击活动可追溯到 2007 年；该组织主要针对国内政府、军事、国防、科研等机构，使用鱼叉邮件攻击和水坑攻击等手段来实施 APT 攻击。

2016

黄金眼
别名：GOLDENEYE、证券幽灵

黄金眼是奇安信威胁情报中心披露的 APT 组织，主要针对国内证券相关行业实施攻击活动。

海莲花
别名：OceanLotus、APT32
内部序号：APT-C-00

海莲花是奇安信威胁情报中心披露的 APT 组织，其最早活动可追溯至 2012 年。该组织主要使用鱼叉攻击和水坑攻击等攻击手法和 Denis 木马、Cobalt Strike 等攻击工具，先后针对中国政府、海事机构和东南亚国家等开展攻击活动。

蔓灵花
别名：BITTER

蔓灵花曾针对中国、巴基斯坦政府等相关目标实施 APT 攻击。奇安信威胁情报中心后续发现该组织使用 InPage 漏洞，并与 Confucius 和摩诃草存在关联。

Group 123
别名：APT37、ScarCruft

Group 123 是网络间谍组织，至少从 2012 年开始活跃，曾针对韩国、中国等目标区域实施攻击活动。

索伦之眼
别名：Strider、ProjectSauron
内部序号：APT-C-16

索伦之眼是一个极为复杂的网络间谍平台，至少从 2011 年开始活跃，其攻击目标包括俄罗斯、中国、瑞典、比利时、伊朗和卢旺达等。

2017

人面狮
内部序号：APT-C-15

人面狮行动是奇安信威胁情报中心披露的 APT 攻击活动，它是活跃在中东地区的网络间谍活动，主要目标可能涉及到埃及和以色列等国家的不同组织，目的是窃取目标敏感数据信息。活跃时间主要集中在 2014 年 6 月到 2015 年 11 月期间，该组织主要利用社交网络进行水坑攻击。

美人鱼
内部序号：APT-C-07

美人鱼行动是主要针对欧盟国家政府机构开展的持续时间长达 6 年的网络间谍活动，已经证实对丹麦外交部实施过攻击活动，其攻击手法主要使用水坑攻击。

APT34
别名：OilRig

APT34 至少从 2014 年开始针对中东地区实施攻击，攻击目标包括金融、政府、能源、化工和电信等行业。该组织过去以 APT34 和 OilRig 两个不同的名称被分别进行追踪分析。

肚脑虫
别名：Donot
内部序号：APT-C-35

肚脑虫是奇安信威胁情报中心披露的 APT 组织，活跃在南亚地区，主要以巴基斯坦为攻击目标，攻击工具主要使用 yty 和 EHDevel 两套恶意软件框架；分析师研究发现该组织与 Hangover 和 Patchwork 存在联系。

MuddyWater
MuddyWater 最早被发现于 2017 年 2 月至 10 月期间，针对中东实施了网络间谍活动，其主要使用的 PowerShell 后门也被称为 POWERSTATS。

Longhorn
别名：Lamberts

Longhorn 疑似情报机构背景的攻击团伙，维基解密于 2017 年 3 月泄露的 Vault 7 项目资料曝光了其内部的网络武器项目。

2018

Charming Kitte
Charming Kitte 网络间谍组织，从 2014 年左右开始活跃，主要针对从事学术研究、人权和媒体的个人目标开展攻击活动；该组织在 TTP 上和 Magic Hound 组织存在大量重叠。

APT33
APT33 是 FireEye 披露的 APT 组织，攻击目标包括美国、沙特阿拉伯和韩国，主要针对航空和能源领域实施攻击活动。

双尾蝎
别名：Big Bang
内部序号：APT-C-23

双尾蝎是奇安信威胁情报中心披露的 APT 组织，其曾对巴勒斯坦教育机构、军事机构实施 APT 攻击，攻击范围主要为中东地区，攻击工具包括 Windows 和 Android 平台，主要采取鱼叉或水坑等攻击方式配合社会工程学手段进行渗透，向特定目标人群进行攻击。后续国外安全厂商也将 Big Bang 攻击行动与双尾蝎联系到一起。

BlackTech
BlackTech 疑似网络间谍组织，主要针对台湾、日本、香港实施 APT 活动，攻击目的疑似窃取目标公司的技术和证书，该组织常用的恶意工具也被称为 PLEAD。

Gamaredon Group
Gamaredon Group 至少从 2013 年起活跃，曾攻击过乌克兰政府相关人员。该团伙的攻击手法与工具不断演进：由过去严重依赖于 off-the-shelf 工具转变为自定义的恶意软件。OPERATION ARMAGEDDON 行动与该组织有关。

Gorgon
Gorgon 的历史攻击活动混合了网络犯罪活动和针对性的网络攻击活动，其针对性网络攻击活动与 C-Major 行动、ProjectM 存在联系。

黄金鼠
内部序号：APT-C-27

黄金鼠被安全厂商证实为某电子网军背景的 APT 组织，同时具备 Windows 和 Android 平台的恶意攻击能力。

蓝宝菇
内部序号：APT-C-12

蓝宝菇是奇安信威胁情报中心披露的 APT 组织，主要针对国内政府、军工、科研、金融等机构实施 APT 活动，攻击历史主要关注核工业和科研相关技术。

2019

军刀狮
别名：ZooPark
内部序号：APT-C-38

军刀狮是卡巴披露的一个针对中东目标实施 APT 攻击的组织，其主要通过 Telegram 和水坑攻击分发恶意软件，该组织也重点针对库尔德人目标实施攻击活动。

Sidewinder
别名：响尾蛇
内部序号：APT-C-17

SideWinder 疑似南亚的 APT 组织，曾针对巴基斯坦进行鱼叉式钓鱼邮件攻击。

DarkHydrus
DarkHydrus 曾针对中东的政府机构和教育机构，并且大量利用开源工具和自定义有效载荷进行攻击。

黄金雕
内部序号：APT-C-34

黄金雕的大部分攻击行动主要是针对哈萨克斯坦国境内的情报收集任务，其中也波及到了我国驻哈萨克斯坦境内的机构和人员，除了传统的后门程序，黄金雕（APT-C-34）组织还采购了 HackingTeam 和 NSO 的商业间谍软件。

盲眼鹰
内部序号：APT-C-36

盲眼鹰是奇安信威胁情报中心披露的疑似南美洲地区的 APT 组织，从 2018 年 4 月起，针对哥伦比亚政府机构和大型公司（金融、石油、制造等行业）等实施针对性攻击活动。

拍拍熊
内部序号：APT-C-37

拍拍熊是一个针对某武装组织进行持续攻击的 APT 组织，同时拥有针对 Windows 和 Android 的攻击平台。

奇安信首发的APT团伙
奇安信持续跟踪的主要APT团伙
针对中国境内有攻击行为的APT团伙

一、为什么我们要写《2020威胁情报手册》

1. 网络安全形势的三个转变

“APT是不胜不归”。群众生活、经济社会和国家安全对网络的依赖度越来越高，奇安信集团总裁齐向东总结，网络空间安全形势正发生三大转变。

◆ 第一个转变 网络攻击事件由小打小闹向国家大事转变

以前，网络安全事件多与个人用户相关，主要是为了获取不法利益，比如流氓软件、木马黑产、倒卖个人信息等。现在，网络攻击的目标升级到了企业、政府等机构和组织，开始影响物理世界，攻击者也有了很多政治上的诉求。

◆ 第二个转变 网络攻击技术从简单粗暴向复杂精细转变

以前，网络攻击者使用的技术相对简单，比如捆绑下载、劫持流量等。现在，攻击技术越来越复杂，攻击工具多为复杂攻击技术的结合。比如2017年的“永恒之蓝”勒索病毒，攻击者使用了多种攻击技术，包括1个微软漏洞。

◆ 第三个转变 网络攻击形式从通用型向APT攻击转变

以前，网络攻击主要是为了获利，没有固定目标，现在，网络攻击的特点是任务导向，不达目的誓不罢休，“不胜不归”。比如以前攻击者要赚100万广告费，只需要劫持1000万pv的流量，因为当时1个pv的流量能卖1毛钱，至于劫持谁并不重要。现在，攻击几乎都针对定向目标，并且长期潜伏。比如奇安信累计监测到针对中国目标的境内外APT组织，在被发现前都已完成了潜伏和秘密活动，最长的已潜伏14年。

2. 持续追踪的 40 个 APT 组织

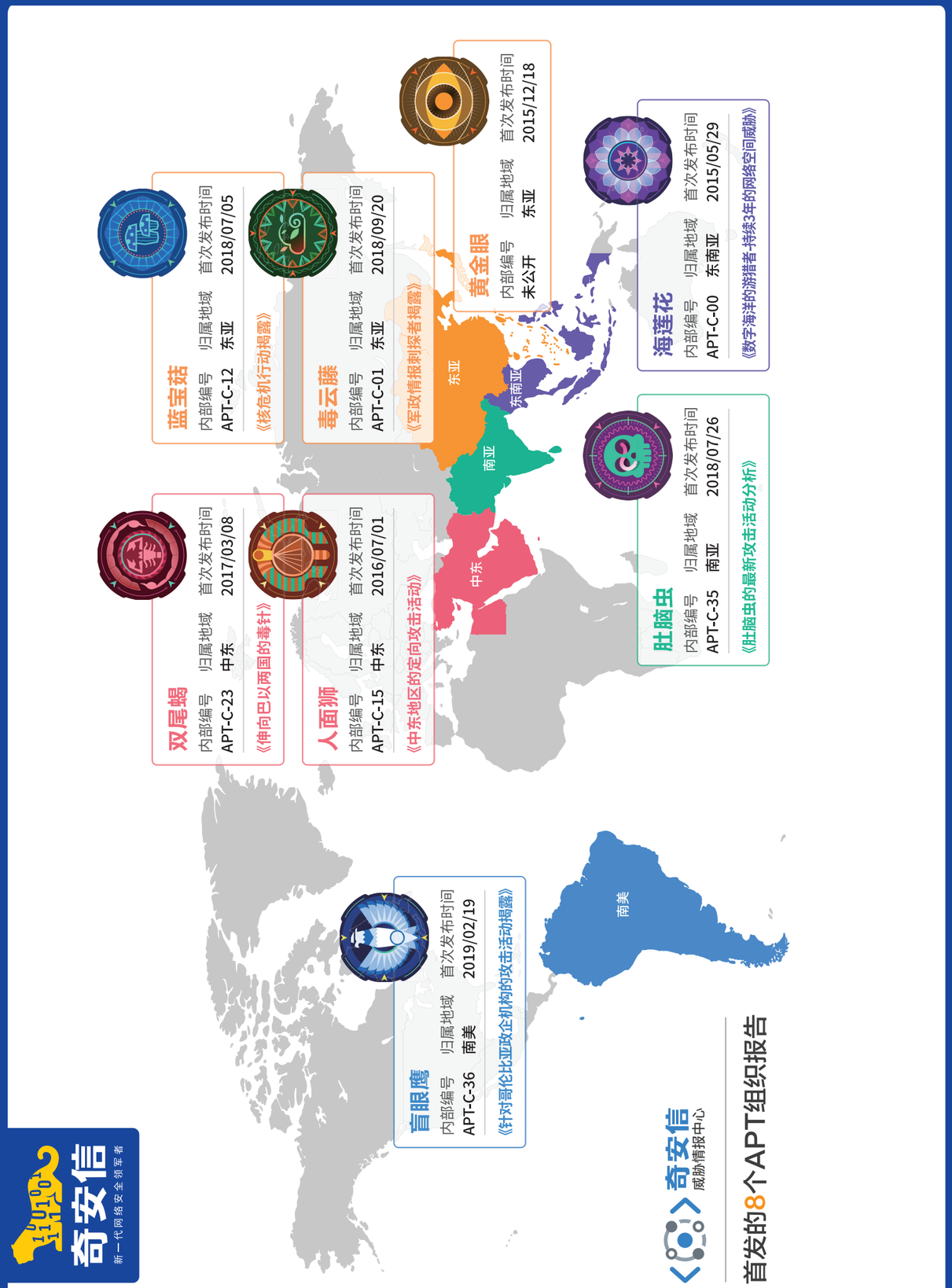
为了把握网络空间安全形势，奇安信威胁情报中心持续跟踪分析了超过40个主要APT组织，在此过程中首发的APT分析报告超过7篇，发布APT组织跟踪报告超过30篇，整体APT事件发现及分析能力在业界领先。2018以来，中心独立发现了两起0day漏洞在野利用的定向攻击事件，在第一时间通知了相关大型软件厂商并获致谢，展示出强大的高级攻击检测和分析能力。奇安信首发的8个APT组织报告包括：

截至2019年12月底，威胁情报中心依据积累数据，持续跟踪分析了境内外40多个主要的APT组织，最早可追溯到2007年，其中13个APT组织在近3个月依然活跃，其攻击目标涉及国家公共基础设施和各行业厂商供应链；另一方面，由于APT组织之间的“黑吃黑”，他们的网络武器库遭到泄露和扩散，具有国家背景的APT活动似乎由过去的隐蔽战线部分转向更加明显的网络战争对抗的趋势。

奇安信威胁情报中心长期致力于追踪分析高级持续性威胁（AdvancedPersistent Threat，APT），截至目前已经涵盖了超过170个相关组织或战役（Campaign）。为了更好地帮助政府、企业及安全社区对抗这类威胁，我们决定发布我们所掌握的所有失陷标记（Indicators of Compromise，IOC）中的样本HASH及相关分类信息（目前仅提供在VirusTotal上存在实体文件的样本Hash）。基于奇安信威胁情报中心对于威胁情报的层次分类，攻击者所使用的恶意代码文件是其最基础的数字武器，而APT攻击相关的恶意代码体现了相对高端而独特的技术水平，值得安全研究人员深入分析。更多详情可访问”APT_Digital_Weapon资料库”（https://github.com/RedDrip7/APT_Digital_Weapon）。

这些成果的背后，是威胁情报中心近百人的研究分析团队支撑，这些专业人员覆盖了威胁分析的各个环节，包括公开情报收集、数据处理、恶意代码分析、网络流量解析、线索挖掘拓展、追踪溯源等，团队将持续积累的基础情报数据、及时的安全预警通告和有效的威胁研判，汇总为失陷检测情报和威胁情报订阅服务，帮助企业及时发现、解决重大安全风险。

另外，奇安信每年还会发布两份全球高级持续性威胁（APT）活动报告，其中2019年中报告如下。按照惯例，奇安信将在2020年早些时间发布2019年度APT报告，请关注奇安信威胁情报中心公众号的信息。



3. 奇安信做出了三个判断

针对目前严峻的安全形势，奇安信集团总裁齐向东做出了三个判断。

第一个判断 没有攻不破的网络

做安全的总是有一种期望，希望网络永远都不被攻破，要万无一失，但事实是没有攻不破的网络，结果一失万无。“网络安全是相对的，不是绝对的”，任何有生产力的行业都不可能做到绝对安全，那就意味着生产力归零，所以真正应该做的是：相对安全中的绝对安全。

第二个判断 导向从合规到实战

政府和企业现在面临着不达目的誓不罢休的APT攻击，手段不断在变化。“网络安全是动态的，不是静态的”，合规无疑是静态的防护标准，需要向实战导向转变，公安部强调应对网络威胁应做到“三化”：实战化、体系化、常态化，实战摆在第一位。

第三个判断 金鸡独立到三足鼎立

传统的安全防护主要是边界思维，就像古代修长城，这种思维已经不适应现在的安全形势，过度重视边界带来的往往是过度忽视内部安全，安全防御技术应该由注重边界的“金鸡独立”，转向边界、终端和大数据的“三足鼎立”，终端和数据的重要性甚至超过边界。

二、实战化情报内生运行机制

1. 威胁情报是新一代网络安全的“血液”

奇安信总结多年实战经验，以“数据驱动安全”核心技术理念为基础，创新提出了“44333”新一代网络安全体系，即四个假设、四新战略、三位一体、三同步和三方制衡，实现了从技术理念到方法论、从安全产品技术到精细化服务的全面创新。

其中四新战略提到

◆ 以第三代网络安全技术为核心的新战具

过去我们把安全二元化地分为黑和白，第一代技术是“查黑”，把符合病毒库特征的“黑名单”干掉；第二代技术是“查白”，只允许“白名单”进入；第三代技术的核心是“查行为”，通过采集数据，利用大数据安全分析技术及时查出异常行为，做到“三不”：不依赖黑名单、不信任白名单、不放过可疑行为。

◆ 以“数据驱动安全”技术理念为核心的新战力

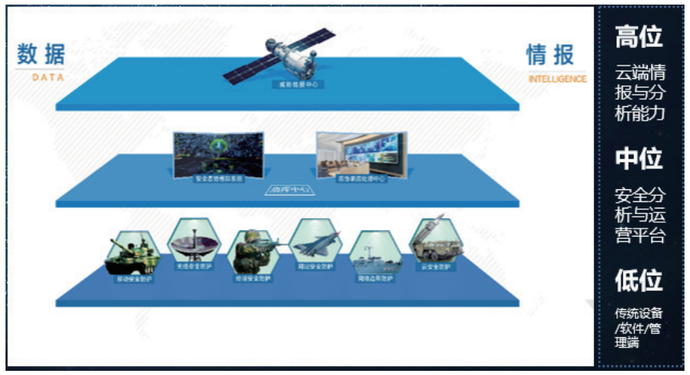
大数据时代，要充分利用大数据分析技术，利用大数据处理、数据挖掘、各类分析引擎与人工智能方法，把最新的深层次安全威胁分析锁定，进行告警处置、追踪溯源，做到“四得”：看得清用户、抓得住行为、报得准风险和响应得及时。

◆ 建立“人+机器”安全运营体系的新战法

新形势下的网络安全，本质是“三人”的对抗：人与人的对抗、人与机器的对抗、人工智能的对抗。人工智能时代，机器人可以替代一切，但不能替代网络安全工程师，因为网络安全是逆向思维、是不走寻常路，而人工智能是经验的决定。只有采用“人+机器”的方法，把人的知识驱动和机器的数据驱动结合起来，才能真正做到对看清谁来了，做了什么，拿走了什么，从而掌控全局。

而在**三位一体**中提到，网络攻防应建立高位、中位和低位安全能力联动的“三位一体”体系：低位能力相当于一线作战部，直接关系到安全事件的应急和响应；中位能力相当于指挥中心，以态势感知、告警、决策、指挥以及提供云端引擎为核心内容；高位能力相当于外脑，以云端威胁情报与分析能力为核心，对中位和低位提供支撑和决策。

2. 威胁情报是高级网络安全能力的标配



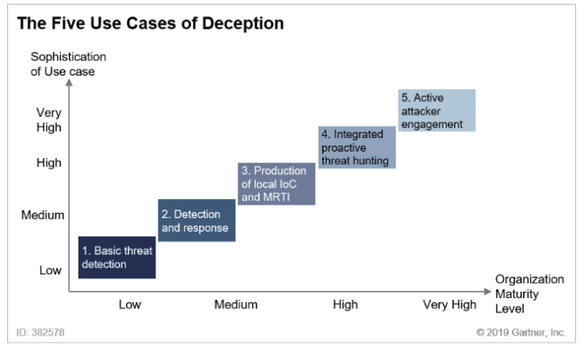
借鉴SANS的网络安全滑动标尺基础模型，安全能力建设分为五个阶段，第一个阶段是基础结构安全，第二个阶段是被动防御，第三个阶段是积极防御，第四个阶段是威胁情报，威胁情报包括了收集数据，将数据利用转化信息，并将信息生产、加工为评估结果，第五阶段是反制进攻。

前两个阶段是偏静态的综合防御能力；第三、四阶段是偏动态的综合防御能力，前面阶段是后面阶段的基础，后面阶段是前面阶段的叠加，不同阶段相互依赖，相互促进，是叠加演进的过程，而不是淘汰演进或者相互替代。

比如偏静态综合防御能力中的零信任是一个新的访问模型，它解决的是大量终端、应用和人群在访问集中数据时能否动态、能否可信的授权，不仅防御外部黑客攻击，也能防御内部威胁。零信任的实现需要结合业务流程，结合业务数据，还要叠加威胁情报、大数据分析等能力。

偏动态综合防御能力中的态势感知与安全运营平台，更多的是把安全能力和信息化进行结合，基于来自前两个阶段的安全数据采集，还要结合核心应用系统和业务系统的数据，进行综合研判进行分析，从而掌握态势、发现威胁，并作出处置和响应。

在这个方面，Gartner在威胁情报用例中也指出，当组织成熟度达到中高级，就应该将威胁情报用例由基础的情报消费推向更高级的本地化威胁情报生产，以期更精准的、更好的服务于组织业务发展，缓解组织面临着数字化转型的压力，并在现有及新业务模型下关注客户体验。



资料来源：Gartner（2019年3月）

3. 威胁情报需要情报内生并开放生态

在2019年8月21日举行的北京网络安全大会上，奇安信集团董事长齐向东在做主题演讲时表示，网络安全已经进化到了“内生安全”时代，即把安全能力构建在业务系统上，让业务系统能不断从内生长出安全能力，真正解决客户的业务安全问题。

“我们做安全的总是有一种期望，希望网络永远都不被攻破，一定万无一失，但事实是没有攻不破的网络，一失万无。”齐向东表示，所有挑战的核心都是对漏洞的利用，而漏洞无处不在、不可避免，传统的安全防护手段已经失效，网络变革推动安全技术进入第三代：内生安全。由此他提出了保护业务安全的三个构想：

◆ 一是具备“免疫功能”

建立一个自适应的安全系统。在他看来，网络被攻破，就像人体被病毒和细菌入侵。免疫系统的作用，就是调动身体的防御力量，消灭病菌。因此，安全体系也需要“免疫功能”，在即使网络被攻破的时候，也能保证业务安全。针对一般性网络攻击，能自我发现、自我修复、自我平衡；针对大型网络攻击，能自动预测、自动告警和应急响应；应对极端网络灾难时，能保证关键业务不中断。

◆ 二是做到“内外兼修”

拥有一个自主的安全系统。完全依靠外在力量，建立不了具有免疫功能的安全系统。无论外部检测技术有多高明，都无法感受内部细胞遇到的困难。比如，中医的“望闻问切”，问是关键环节；西医的化验和透视手段，目的也是探究内部细胞变化。同样的道理，安全系统也需要与业务系统深度融合，因为如果只有外部的力量、外部的安全数据，或者只有泛化的安全大脑，解决不了内部的安全问题。

◆ 三是能够“自我进化”

成为一个自成长的安全系统。 齐向东以免疫系统举例说，大人的免疫系统就比小孩强，锻炼身体、适应严酷环境、对抗疾病都会提高免疫力，网络安全体系在不断抵抗网络攻击的过程中，也会提高防护能力。因此，安全能力需要伴随业务变化日渐强壮，其核心是人的进步和成长，只有不断发现问题、解决问题，才能形成正循环。

就威胁情报本身来说，虽然种类有很多，但整体上分为两大类：

- **一是人读情报**

这类情报主要包括描述行业综合网络安全态势的战略情报和描述某次攻击或者某一类攻击战术的TTP情报，主要面向分析人员。

- **二是机读情报**

可机读情报更多的是为安全产品赋能，让它们可以检测发现更多的关键性威胁，同时为报警提供优先级、上下文等事件响应必要的内容，从而提高安全设备的检测和响应能力。奇安信威胁情报中心输出的机读情报中，最常见的就包含失陷检测IOC情报、文件信誉情报和IP情报。

这些情报在进行大范围应用的时候，需要考虑到几个方面：

- **情报本身可信任性**

威胁情报不是一条信息，而是综合很多信息经过分析加工得出来的结果，往往供应商本身的底层数据能力就决定了威胁情报的质量。奇安信在云端拥有样本库100亿+、安全日志18万亿+、DNS解析记录100亿+、补天漏洞平台漏洞33万+，在本地拥有企业全量数据的采集能力，结合机器学习和安全研究双引擎驱动，奇安信可以快速生产高质量的威胁情报。

- **情报能力集成**

IDC认为，将威胁情报数据提供给企业其他安全防护软硬件产品，如防火墙、入侵检测/防御系统、态势感知系统、安全信息与事件管理系统（SIEM）等，能够显著提升传统安全解决方案对于未知威胁的发现和防护能力。奇安信集团作为新一代网络安全领军者，基于“44333”新一代网络安全体系，将威胁情报能力集成到态势感知、应急响应、NGSOC、天眼、云安全、NGFW、EDR等产品及解决方案中去，形成了实战化统一威胁运营机制，即可统一指挥、检测、分析、处置，且服务可视、工作可视、过程可视可控、全程可监控，大大提升了用户对抗APT等高级威胁的能力。

- **威胁情报规范**

无论是在单一厂商的不同产品之间，还是在不同厂商的不同设备之间，这些设备要想展开协作，就需要读懂威胁情报，也就需要统一威胁情报的“语法”。奇安信一直不遗余力地推动威胁情报的规范，并且深度参与了由中国电子技术标准化研究院牵头制定的中国首个威胁情报标准。该标准已于2018年10月正式发布，填补了此前国内该领域的空白。

- **行业情报联盟**

奇安信正在各行业组织展开积极协作，在为行业客户构建本地化威胁情报能力中心的同时，与行业主管机构一起，积极推动行业内情报共享，共同缓解行业网络风险。

有了这些，威胁情报才能真正走出去，形成一个开放的生态。

三、威胁情报能力建设及应用场景

基于如上描述不难看出，在如今数字经济大潮中，企业需要进行数字化建设或者数字化转型，就需要以客户为中心，洞察客户需求及快速解决客户遇到的问题，持续交付满足客户期望的产品/服务的能力，进而提升客户满意度。企业为了实现这个目标，必然需要将以客户为中心的思想渗透到信息化及网络安全工作中，并进行一系列工作指标调整。Gartner预测到2023年，企业数字化转型过程中失败的第一大原因将是糟糕的客户体验。

如此同时，网络安全的发展是一个叠加演进的过程。如今威胁情报作为网络安全发展到高级阶段的标配，并不意味着抛弃传统安全的基础架构设备，相反，更需要回头看，将威胁情报能力融入基础架构中去，成为网络安全纵深防御架构中不可或缺的一个环节。

1. 威胁情报驱动：以情报为中心构建能力框架

威胁情报战略及内部投资

在企业内构建以威胁情报为中心的网络安全体系，主要考虑两大方面：

- **威胁情报能力建设阶段**

首先，需要将现有安全设备逐步过渡到支持消费机读威胁情报，建设自有威胁情报管理平台将商业化、定制、开源情报转化为可机读检测特征和处置措施提供给安全设备。

其次，内部分析人员利用态势感知等积极防御手段，将检测到的相关信息并进行分析以创建有关攻击者的情报。

- **以安全决策为导向的内部投资**

此外，分析人员从已被来自位于自身或其他网络中的攻击者攻陷的系统中收集数据，从而得出关于所面临威胁的情报，形成内生情报能力。并根据得到的威胁情报帮助决策者把握当前的安全态势，在安全决策上更加有理有据。包括了什么样的组织会进行攻击，攻击可能造成的危害有哪些，攻击者的战术能力和掌控的资源情况等。

制定威胁情报驱动的安全体系框架

成功的威胁情报计划之所以能够产生有效的建议和行动，来源于企业内部构建以威胁情报为中心的体系架构，该架构一方面对称并分解了业务关联指标，另一方面拓展了情报数据源。为了确保威胁情报能够真正服务于业务，必须（最好以自动化方式）处理已经汇总的数据，并将其放入企业特定的业务环境中去，然后必须关联分析上下文相关的信息，以便准确发现针对业务的攻击并制定相应措施。最重要的是，这些措施将通过威胁情报体系架

构形成统一的建议和行动，并在体系内形成有效共享，共同为企业决策者提供信息。

本手册尝试提出粗略的威胁情报框架体系，其中包含了不同的角色、应用场景及工具，我们将在后续章节中展开描述，同样也期待您在工作中进行不断修正及完善，进而形成有明确实施步骤的威胁情报战略地图。

威胁情报驱动的安全体系				
级别	**阶段**	**角色**	**职责**	**工具**
L6：	规划 **（业务价值关联）**	CIO	信息化建设及安全风险	规划方案及信息化战略
L5：		CISO	安全资源分配、风险管理和沟通	规划方案及TI战略
L4：	建设 **（关键能力建设）**	CSO	报告和沟通，情报赋能	态势感知平台及战略情报、SOAR
L3：		威胁分析师	高级分析及攻击溯源	TIP+样本自动分析+情报生产与消费
L2：	运行 **（实现安全运行）**	应急响应组长	事件响应和威胁发现	天眼+安服
L1：		运营分析师	实时监控、信息收集及事件升级	NGSoC+安运

三同步实践：如何选择威胁情报服务

企业在自建威胁情报能力的过程中，除了需要强化已有基础架构安全和静态的防御体系，兼顾“深度结合、全面覆盖”的防御体系，将网络安全防御能力与各种基础架构、技术栈等层级深度结合，使信息化系统具备内生的安全能力，同时还必须加强积极防御和情报等动态防御体系的建设，按照“三同步”的思路在规划设计中，将威胁情报体系的构建作为动态防御体系的重要组成部分。

三同步是将信息化建设与网络安全的防护与响应过程结合，达到工作任务事项级别的深度绑定，实现二者的同步规划、同步建设、同步运行。

◆ 同步规划

是内生安全的关键与起点，强调关口前移与预算保障。具体指在信息化系统的设计规划中，充分考虑网络安全，确保网络安全成为信息化系统的有机组成。

◆ 同步建设

是内生安全的落地和保障，强调在信息化建设的方方面面，充分考虑引入并融合安全能力，既要积极建设网络安全基础设施，又要开展信息系统内建安全机制的建设。

◆ 同步运行

是内生安全的生命和活力。指在信息化运维中将所有与网络安全相关的环节都与网络安全工作充分对接，实现安全运行，而不仅仅是扫描、检查、渗透等零散工作。

为了实现上述目标，企业选择合适的供应商是不可或缺的。供应商能力各不相同，一般而言，情报产品的质量威胁情报生命周期覆盖度、执行力度以及分析人员的能力密切相关，威胁及相关原始信息的收集、处理和分析是主要区别，其中重要的决策点包括：

- 内容是仅仅基于事件观测，还是来自深入的APT组织分析；
- 内容是仅是公开信息中获取，还是自身具备生产能力，以及具备客户侧的非公开信息；
- 其原始信息是仅从国外来源收集，还是也具备国内来源收集能力；
- 是仅仅具有一系列独立数据点，还是具备关联归属分析能力，并能够得出独立的结论；
- 是否有能力和资源，为关键信息基础设施的风险和威胁定制情报输出；
- 供应商是否有能力，构建适合您的组织使用威胁情报能力及情报输出。

2. 威胁情报能力：APT 分析只用 ATT&CK 不够

ATT&CK框架早在2014年就已提出，该框架有效解决了 TTP（战术、技术和过程，全称为Tactics, Techniques, and Procedures）中描述性过多、不易比对的问题。最近两年该框架的热度呈指数级增长，如今已经包含40项战术目的和519项达到战术目的的技术实现方式。简单来说，可以这样理解ATT&CK：

◆ 是对 TTP的一种标准化表达

包括战术目的、技术手段以及攻击过程中技术手段的选择。

◆ 该框架是偏实战化的

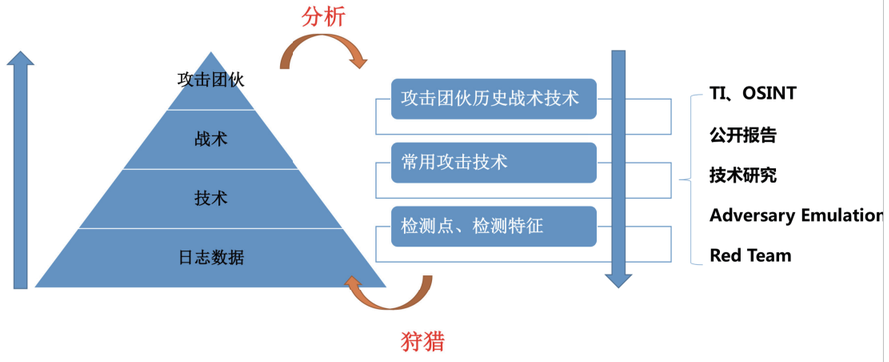
其研究基础是基于真实曝光的网络威胁活动，而且也有一些便于实际演练的项目。

◆ 该框架适用范围有限

因为其关注的威胁类型和研究基础所选取的来源范围，其更适用与面向具有网络边界的网络攻防场景，而和像云安全、业务安全、工控安全，甚至移动安全的威胁场景都存在一些不太适用或不太全面的情况。

ATT&CK具有指导意义并利于知识积累

与日常的威胁分析类似，对 ATT&CK 的运营和更新一方面依赖于对已知团伙的攻击 TTP 的分析和归纳，以及新的活动中使用的 TTP，另外基于一些红蓝对抗、安全研究中所发现和披露的常用攻击技术、攻击面、攻击向量同样可以补充到矩阵中，并且需要向下拆解映射到具体的检测点和检测特征中，从而可以应用于 Threat Hunting（威胁狩猎）过程。



目前大多数APT报告主要是分析投放载荷和恶意攻击工具，因为这些更容易被采集和捕获。如果需要结合ATT&CK全面还原整个攻击活动的过程，除了需要对其攻击载荷进行更细致的分析外，还需去分析一些日志数据等信息，以此来补齐所缺失的观察部分。这方面可以通过如下四个维度进行分析：

- **技术分析**

即对攻击的样本，使用的漏洞利用工具等进行分析，一方面分析其具体使用哪些技术手段，用来做什么，另一方面是提取指纹特征。

- **战术分析**

需要判断当前的攻击阶段，是初始立足阶段，还是横向移动过程。

- **意图分析**

攻击的意图可以是短期也可以是中长期。如短期意图可以是一阶段载荷和初步的信息收集，中长期可能是要拿下一个内网核心节点，目标数据库或是制定的战略目标。

- **归属分析**

是对攻击来源的可信程度进行判断，归属判定的依据可以是一个具体的 IP、终端设备，也可以是一个网络 ID。

相对于ATT&CK来说，我们需要更多思考攻击者是如何在实战中实现的，可能会采用什么样的方式去绕过已有的防御，并完善现有的检测点和检测策略。虽然该框架非常具有指导意义并能够提供知识基础，但在真实场景下仍需进行拆解，并通过运营来完善缺失的攻击面和攻击向量。

ATT&CK对APT关联归属分析用处不大

经过多年的APT分析，奇安信威胁情报中心认为利用ATT&CK进行APT攻击的关联分析，是不靠谱的。具体原因如下：

- **ATT&CK矩阵记录事实的能力受限**

从APT分析的角度看，光看到环节本身是远远不够的，目击到一系列环节本身并不足以导向足够的区分度，甚至都不是关联归属的核心点所在。

- **关联分析的核心在于细节**

ATT&CK所枚举的技术手段应该理解为Key，除非手法本身已经有高度的独特性，不然绝大多数用于关联的特征存在于Key对应的Value或“参数”中，而不是手法本身。

- **现实APT关联基于强特征**

这包括非常特定的目标，只被某特定团伙使用的数字武器，已有明确归属的网络资源，需要特定资源操控能力的手法等等，在这方面钻石模型是比ATT&CK有用得多的工具。

- **元数据为王**

APT分析的核心是看见的能力，获取信息量的能力，随着摩尔定律主导下的计算存储成本的指数级降低，以及支持大数据处理技术的完善，APT分析进入元数据为王的时代，这些元数据甚至包括特定IP的访问记录、特定IP与社交账号的关系、人员所使用的IP、人员使用的社交账号、人员的邮件记录、人员的社交信息收发、人员的搜索记录等等，基于这些数据做分析，只需要简单的图关联就够了。

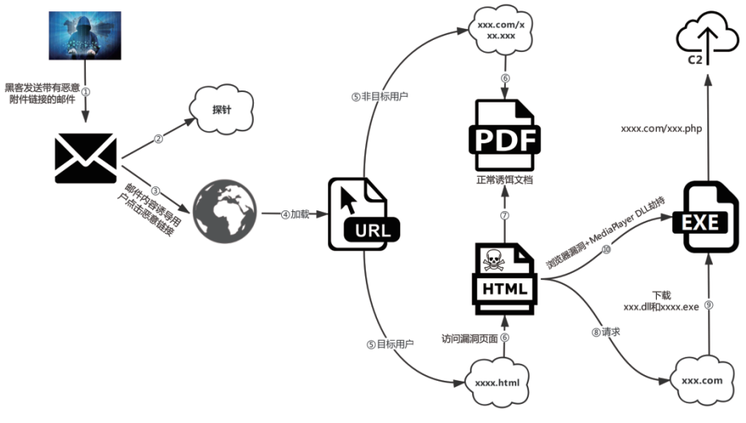
APT分析实践：斩断东北亚APT组织“虎木槿”的魔爪

奇安信威胁情报中心在全球范围内率先监测到多例组合使用多个浏览器高危漏洞的定向攻击，并基于威胁情报和流量分析，实现了在野实时检测真实APT攻击，对国内重点客户的网络攻击防护起到了不可替代的作用。

在此次检测中发现，APT攻击目标包括多个国内核心教育科研政府机构和个人，只要受攻击目标使用特定浏览器近期的版本打开网页就可能中招，被黑客植入后门木马甚至完全控制电脑。分析显示，该攻击利用了多个较老版本的Chrome浏览器内核的漏洞，国内外使用了这些较老版本渲染核心且没有对应漏洞缓解措施的浏览器用户成为本次APT攻击的目标。

中心确认本波次攻击活动背后的团伙为东北亚来源，并将该APT团伙命名为“虎木槿”。“幻影”行动意指虚幻而不真实的影像，取意于攻击者在浏览器漏洞利用过程中通过播放一个不存在的Windows Media Video影音文件来启动Media Player插件，从而劫持执行下载的恶意DLL以达到执行木马获取控制的目的，体现了攻击者变幻莫测的攻击技巧和高超的技术能力。

出于对提升安全业界对于攻击过程的了解以发现并归属同类攻击活动的考虑，我们仅将总结的该APT组织攻击流程披露如下图所示：



近期的攻击监控显示，境外APT攻击者越来越多地使用影响面大的已知网络武器，针对国内一些使用低版本组件的产品进行攻击，这也证明APT攻击无所不入的攻击特点。本次所发现的攻击邮件内容设计上体现了高度的定向性和对于目标的深入了解，当一个好用的数字武器再结合高端的社会工程学的诱饵，那么最终必将产生高强度的渗透能力。

3. 威胁情报驱动：态势感知绝不是简单的“地图炮”

准确地说，“态势感知”这个词并不起源于网络安全领域，它来源于战场，美国空军在上世纪80年代把它系统地提出来，却因为网络安全火遍全球。随着数字经济的全球竞争加剧，网络安全已经上升到国家安全的层面。习近平“419”讲话中提到，要“全天候、全方位感知网络安全态势”，“态势感知”骤然变成了热词。

奇安信集团董事长齐向东举过这样一个例子，四万名攻击者与四万名防御者同时针对一万个关键基础设施展开攻防。通常而言，攻击者只需要攻破其中一个系统就齐活了，但防御一方因事先难以知道攻击者的动向，必须同时防御这一万个基础设施，那么平均到一个基础设施的防御人员就只有四个。攻击一旦开始，攻防力量对比很可能是四万对四，结果可想而知。

更糟糕的是，在实战攻防中，情况还要更加复杂，可能还有大量的资产不知道在哪里，可能还有大量不知道的漏洞、不知道的攻击手法。在充满大量X因素的安全态势下，想要做好安全防御的难度可想而知。

态势感知是数据驱动安全的极致体现

到现在，几乎所有的国内安全厂商都推出了各自的态势感知产品或者解决方案。Gartner在2011年对态势感知做出了定义，态势感知是对威胁情报及资产漏洞信息的集成和分析，形成一幅对业务系统安全状态的准实时视图。包括四方面的能力：

- **资产状态信息的收集**

包括资产的配置状态、漏洞状态、连接情况和关键度。

- **威胁行为信息的收集**

包括外部威胁行为、用户行为、对手的信息，以及目标参数的风险级别。

- **分析**

支持风险估计、响应优先级划分、调查与即时查询。

- **汇报**

包括长期存储，以及预置和即席报表生成。

从这个定义来看，态势感知的核心就是大数据。如果将这个范围从企业扩大到各行各业，再上升到国家层面的话，那毫无疑问，态势感知就成为数据驱动安全的极致体现。奇安信态势感知系统基于奇安信安全大数据与核心技术，能够有效地持续监测互联网乃至城域网DDoS攻击、漏洞、网站安全状况、僵尸木马蠕虫以及高级威胁，从而掌握网络安全隐患和实时了解攻击态势，协助有关监管部门预警通报监测到的网络威胁活动，并为追踪溯源提供线索。

威胁情报是构建积极防御的核心技术

在态势感知的检测、预警、响应、处置的闭环过程中，威胁情报成为其构建积极防御能力的核心技术之一，其作用主要体现在以下两个方面。

基于机读威胁情报，控制事态发展

及时发现失陷主机是防范重大损失实际发生的关键，IOC情报依赖DNS日志或者上网行为日志就可以进行检测分析，并且提供攻击类型、团伙、攻击方式、危害以及处置建议等上下文信息，结合企业内部数据、辅助安全人员完成对威胁的检测、分析、研判和处置。

奇安信威胁情报中心将威胁情报下发到系统中后，与检测到的特定事件或者异常行为进行关联分析和数据挖掘，结合规则关联引擎+人工智能引擎+虚拟执行检测引擎的多引擎检测架构，从而快速对事件定性，并且锁定失陷主机、远控木马或者其他潜在的威胁。

通过TTP情报，强化攻击者画像

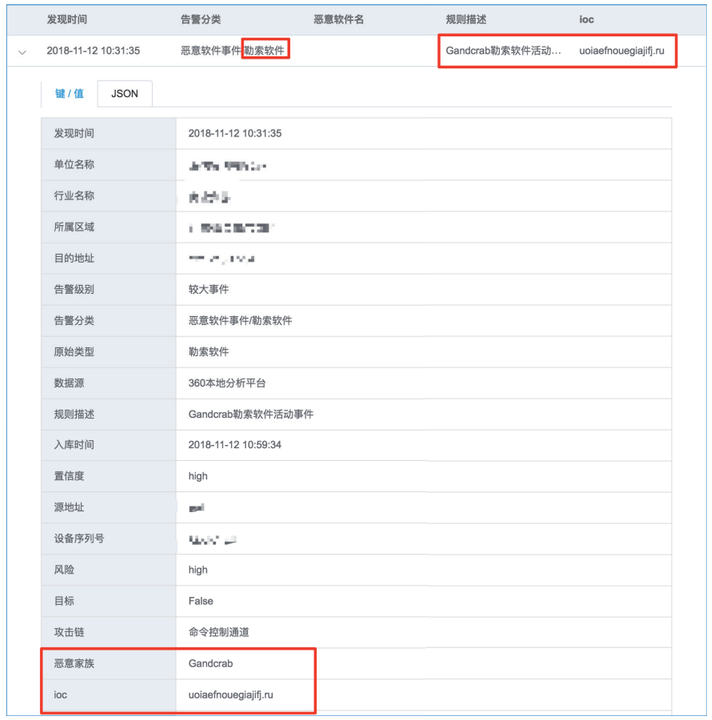
TTP情报（战术、技术、攻击过程）是提供给安全分析师及安全运营者使用的情报，关注于恶意软件、漏洞、攻击事件，着重分析其目的、危害、机制、影响范围以及检测防范机

制。分析师可以快速了解攻击者的技战术特点，增强对威胁的研判和狩猎能力。

网安客户实践：在城域网监测中捕获勒索软件

在威胁情报的帮助下，态势感知系统可以提供僵木蠕毒活动感知、DDoS攻击感知、网站安全感知、高级威胁态势感知等全天候、全方位的态势感知能力。

某网安部门在部署奇安信态势感知系统后，结合奇安信威胁情报中心实时下发的定制化威胁情报，与城域网流量数据进行匹配，通过规则关联引擎+人工智能引擎+虚拟执行检测引擎的多引擎检测架构，成功捕获了Gandcrab勒索软件，如下图：



具体而言，奇安信态势感知系统具备以下显著优势：

◆ 严格坚持业务导向

做到底数摸得清、告警报的准、重点抓得到、监管推的动、成效看得见、警力受得了、指挥臂使指、配侦效果好、情报促协同、源头看得见，并以此为基础为不同用户量身定制态势感知系统功能。

◆ 纯正的大数据基因

奇安信态势感知系统采用了Sec-LDM驱动的数据治理融合技术、业务导向的大数据分析建模技术、可视化直观呈现技术+智能解读技术。

◆ 伙伴式的大型项目实施能力

奇安信利用强大的实施运营团队为不同用户组建专门实施保障团队，并针对该解决方案的项目专业分工明确，在项目实施阶段最大程度保证项目进度及质量。

◆ 以攻防为核心的动态防御能力

奇安信态势感知系统可通过攻防态势板块，对攻击方、受害方以及网络空间战场态势进行全方位、多维度分析研判及预测，对攻击者身份、能力、活动规律动态画像，并可对攻击战场实时还原，场景重现。

◆ 内嵌智能、开放的态势大脑引擎

奇安信态势感知系统设计理念从IT思维转变为DT思维，以大数据为驱动，建设低门槛、可视化的分析建模工具，打造众创建模，汇聚众智的安全生态平台。

◆ 强大的追踪溯源与情报输出能力

奇安信态势感知系统具备虚实映射能力，可最大化发挥数据价值，同时利用人工智能引擎AlphaD推荐的侦查方向和侦查手段，能够能够洞察敌情，输出案件线索，为侦查打击提供情报支持。

4. 威胁情报驱动：提升安全运行效能要用 NGSOC

在一个复杂的企业网络环境内，SIEM或者SOC平台的应用非常普遍。Gartner预测，到2022年，50%的SOC将集成事件响应、威胁情报和威胁捕获功能，而在2015年这个比例不到10%，SOC的成长异常迅猛！

企业之所以愿意花重金部署SOC，是需要看清楚自己的网络资产、安全设备和各类数据，然而，传统SOC的使用情况却与预想有一些偏差：

◆ 误告警总是难以应对

作为一个指挥中心，SOC对误报率有着相当高的要求。当大量的日志数据、行为数据被引入的时候，其规则引擎会产生大量的噪声，这会白白消耗甲方安全团队的精力，导致真正的威胁被忽略掉，甚至，有时候传统SOC会因为无法处理如此多的数据而瘫痪。

◆ 未知威胁总是难以发现

之所以持续的检测和响应非常重要，就是存在太多的未知因素。当攻击者利用零日漏洞和新鲜的攻击手法，规则引擎就难以发现和识别。

◆ 攻击总是难以研判

安全人员通过传统SOC的告警发现失陷主机或者远控木马后，往往试图找到攻击行为背后的攻击者，了解攻击者的攻击企图、常用工具、技术和攻击手法等，以评估来自攻击者的安全风险，并采取有针对性的防范措施。但在缺少威胁上下文相关数据的条件下，这一点也很难做到，自动化响应处置更无从谈起。

高质量情报是实现自动化处置的关键

2016年，在Gartner发布的十大信息安全技术里提到了情报驱动的安全运营中心，他们认为情报驱动的SOC超越了传统的预防工具和以事件为基础的监测，强调情报关联和自动化的响应处置，并总结了其五大特征，包括在战略和战术上运营威胁情报；通过高级分析将安全智能落地；极尽所能地实现自动化；捕猎和调查（侦查与猎取）；部署自适应安全架构。

同年9月，奇安信集团发布了NGSOC，利用大数据、威胁情报突破传统SOC面临的瓶颈。引入关联性强、上下文体系完整的威胁情报后，企业将从关注单一威胁告警变为更加关注威胁目标、攻击手法、路径等技术指标、决策依据等全方位数据，从而通过威胁情报驱动来进行高级威胁的发现，验证疑似攻击，辅助安全协同并辅助决策。具体而言，威胁情报在NGSOC中的应用包括以下两个部分：

◆ 检测

奇安信威胁情报中心将情报自动下发到NGSOC中进行警报，并将来自NGSOC的特定事件，协同威胁情报信息来进行关联分析和数据挖掘，从而检测出威胁并在网络中进行定位，安全人员可以锁定失陷主机、远控木马或者其他恶意文件的所在位置。

◆ 研判

当安全人员通过SOC告警发现威胁后，可以利用本地全量的网络和主机行为日志，并且结合威胁情报进行深入的调查，利用搜索、统计、可视化关联等方法和技术，找出与攻击者相关联的更多蛛丝马迹，从而拼凑出攻击者完整的行为链条，做出有针对性的防御措施。

当然，实现这两点的一个重要前提是需要保证高质量的情报，否则噪声等问题依然会出现，也就是需要底层强大的数据能力作为支撑。除了云端海量的数据外，奇安信NGSOC最重要的特点之一就是本地全量数据的采集和分析，并从中分析得出失陷主机、文件信誉、IP等威胁情报。

同时，为了解决传统SOC面临海量数据时的性能瓶颈，NGSOC采用了可灵活水平扩展的分布式架构，数据采集使用分布式采集探针，可根据采集数据量和网络拓扑的需要来灵活增加探针的数量，数据存储和分析系统亦可根据需保存的数据量和计算资源需求，通过增加节点的方式进行灵活水平扩展。

这也就是说，NGSOC在结合威胁情报以后，可以有效地降低设备噪声，提高未知威胁的发现能力并且实现自动化的应急处置。

央企客户实践：在2千台主机的内网中阻断勒索攻击

在服务企业客户的过程中，某大型央企希望针对总部2000台终端主机做全方位的安全监控和预警。奇安信集团需要部署一定数量的流量传感器和探针，分别用于采集企业内外网流量交换情况和各终端日志情况。

安全人员在处理NGSOC日常告警时发现，客户内网某IP存在违规访问恶意域名的现象。通过与威胁情报上下文信息比对发现，该样本属于一种特定的勒索木马，从而快速判定了攻击意图。安全人员通过调查分析功能找到了所有受害终端，并且能够对该终端做持续的检测和响应。

从这个案例中可以看到，情报驱动的SOC为警报和事件添加了情景和关联丰富的上下文，能够帮助企业更加快速、精准、全面地掌握风险所在，对企业日常的安全检测和响应有着非常大的作用。

5. 威胁情报驱动：应急响应处置起来要快准狠

综合业界观点来看，网络安全应急响应服务是在第一时间采取紧急措施，恢复业务到正常服务状态，调查、分析研判安全事件发生的原因，提供数字证据，它可以分为五个阶段：

◆ 事前准备阶段

制定应急响应计划，分析并明确应急需求，保证在突发紧急状况时，应急工作可以有条不紊的展开。

◆ 检测分析阶段

安全分析人员介入现场之后，明确检测范围及对象，对异常行为、告警等进行检测与分析，检测完成后输出检测结果。

◆ 抑制与清除阶段

分析人员会根据检测结果入手，阻止威胁在内部的扩散，控制感染范围，并将威胁清除，把损失降到最低。

◆ 灾难恢复阶段

在将所有威胁清除后，安全人员将会协助用户做好系统的安全加固，保证系统的重新正常运行。

◆ 复用阶段

所有参与人员应该对整个入侵和应急响应过程进行全面的复盘，并用于完善应急响应和安全防御策略。

在过去，企业应对网络安全事件应急响应就像“救火队”，由于缺乏事态发展的评估依

据，大多只是“就事论事”，着力与攻击事件本身的响应和事后补救，往往造成同类攻击的反复中招，

应急响应往往面临了这些问题：

- **评估影响面**

如何高效地发现攻击和入侵活动，并对事件性质及事态发展做出准确判断。

- **阻断同类入侵**

对攻击者进行画像，以阻止来自相同对手或类似攻击手法的入侵。

- **查找失陷主机**

在全网搜索同类文件和行为特征，找到全部失陷主机，并且做出针对性的应急处置。

- **对内投资参考**

理解目前安全威胁的全貌以实现明智有效的对内安全投资。

融合威胁情报的应急响应

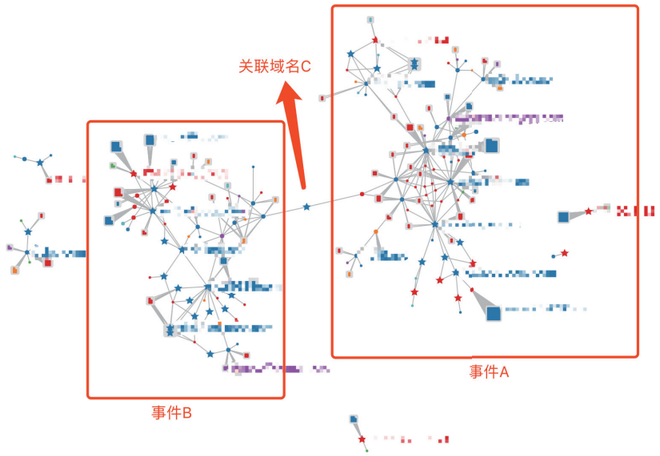
有鉴于此，奇安信安全服务团队将威胁情报能力引入到了应急响应的过程中去。奇安信威胁情报中心总结了应急响应的几个阶段，威胁情报（包括战术情报、作战情报和战略情报）起到的作用，如下表：

	作战情报	战术情报	战略情报
准备阶段	引入威胁情报数据并用于SIEM/SOC平台，增加异常告警相关的上下文信息和准确性。	明确应对的威胁类型，主要攻击团伙，使用的攻击战术技术特点，常用的恶意代码和工具； 针对上述信息分析内部的攻击面和对应的响应策略。	全面了解企业面临的威胁类型及其可能造成的影响； 了解行业内同类企业面临的威胁类型及已经造成的影响； 决策用于应对相关威胁的安全投入。
检测与分析阶段	针对告警提供更丰富的上下文信息，并能聚合其他相关的异常信息，提高安全人员识别的效率。	基于威胁情报，明确威胁攻击的类型，来源，针对的目标，攻击的意图。	
隔离、清除与恢复阶段	根据相关的IOC集合针对企业内部资产能够加快评估影响面和损失。	基于攻击者的攻击战术技术特点的威胁情报信息，能够帮助安全人员判断当前攻击者已实施的攻击阶段和下一步的攻击行动，针对性进行响应决策。	
事后复盘阶段	发现新的IOC信息作为威胁情报补充到内部威胁情报平台，并用于后续的安全运营工作。	帮助完善对整个事件过程的回溯和还原； 更新对攻击者的认知，以更好的应对未来同类的攻击； 结合威胁情报的共享也能够帮助相关行业相关企业应对同类威胁。	

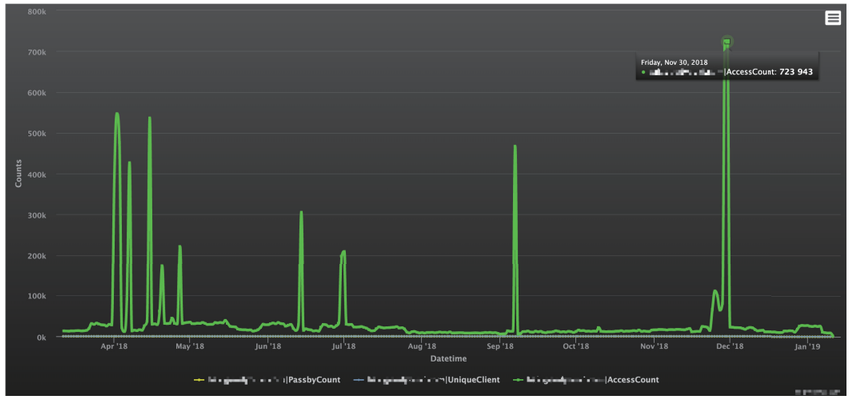
互联网客户实践：从单一事件发现行业性攻击

某网站发现被挂黑链，安服分析人员快速提取了后门样本，并发现样本的行为特征与威胁情报库中的样本极度相似，体现为样本实现的功能基本一致，关键代码实现一致，CC域名信息均为追加到文件尾部，且配置信息加密方式一致。

通过现有威胁情报数据对两起事件中涉及的IP地址、CC域名进行分析，从历史DNS解析记录、历史Whois信息等层面进行关联。最终发现A事件中的CC域名存在一个历史解析记录指向IP x.x.x.x，B事件中的CC域名通过Whois信息关联出域名C，而域名C也存在历史解析记录指向IP x.x.x.x，至此确定两起事件背后存在一定关联，并最终牵涉出大量黑链域名及境外的回联IP、CC域名。



进一步对这些境外IP、CC域名进行分析，发现DNS查询量巨大，受影响网站众多，并且受影响网站均为同一行业。



由此可确认，这是针对某行业的特殊攻击，安服应急不仅解决单一客户问题，借助奇安信威胁情报，可更早发现针对行业的范围攻击，提早准备应对方案，防患未然。

6. 威胁情报驱动：未知威胁用“天眼”才能有效处置

有人说，从前的网络空间里，黑白之间泾渭分明，肉眼可见，我们只需要告诉机器什么是黑，什么是白；但现在的网络空间里，黑白之间盘根错节、星罗棋布，甚至形成了大片的灰色地带。网络威胁就躲在其中，蠢蠢欲动。

洞悉“未知”威胁的眼睛

企业在威胁方面面临太多的未知数，涉及目的动机、攻击者画像、威胁趋势、攻击面、防御战略等，这些维度产生了海量和压倒性的信息，对企业构建本地化安全能力产生了巨大挑战，企业管理者往往只选择他们已经了解的内容。在这种情况下，只是将希望寄托于数据统计，往往让业界已知的威胁，在企业侧变成了未知；而另一方面，APT组织攻击手法多变且技术手段不断创新，关键信息基础设施及相关科研院所面临较高的风险。

奇安信天眼新一代威胁感知系统可对本地流量进行全量还原、存储与深度分析，同时结合威胁情报、规则引擎、场景化分析、机器学习和沙箱检测，从多个维度来发现高级威胁事件，并且以攻击链的视角重现整个攻击过程，从而为客户提供围绕高级威胁的检测、溯源和响应的完整解决方案。看清那些原来看不到的未知威胁并收效处置，这正是奇安信威胁情报+天眼的特点。

有了威胁情报就能有效处置

对于一个机构而言，想要在入侵早期就把威胁抓住，必须借助威胁情报的支撑。

奇安信威胁情报中心可以将所有与攻击相关的信息，如攻击团体，恶意域名，受害者IP，恶意文件MD5等相关信息汇总，按照标准格式封装成威胁情报并通过加密通道统一下发到天眼系统内。鉴于威胁情报有着特别强的行业属性，奇安信天眼可以为客户提供定制化的专属威胁情报服务。

威胁情报做为天眼整个方案的核心内容承担了连接互联网信息和企业本地信息的重要作用，为APT事件在企业侧的最终定位提供了数据线索和定位依据。在这样一个过程中，威胁情报能够起到两个非常重要的作用：

◆ 快速定位

天眼可以将来自奇安信威胁情报中心的威胁情报，与检测到的特定事件或者异常行为进行关联分析和数据挖掘，并且规则关联引擎+人工智能引擎+虚拟执行检测引擎的多引擎检测架构，从而快速对事件定性，并且锁定失陷主机、远控木马或者其他潜在的威胁；

◆ 精准溯源

当天眼发现威胁后，安全人员可以利用本地全量的网络和主机行为日志，并且结合威胁情报进行深入的调查，并且利用搜索、统计、可视化关联等方法和技术，为企业客户呈现一次攻击的完整过程，覆盖攻击的源头、手段、目标、范围等相关信息。

举个简单的例子。假设一家店里的摄像头发现一个人在顾客当中东张西望、鬼鬼祟祟，同时你通过新闻得知，穿这种衣服的可能是某盗窃团伙中的一员，并且专挑年轻女性下手。这时候，你就可以偷偷安排保安针对年轻女性进行特别保护，一旦发现小偷下手就可以当场抓获。

摄像头（天眼）发现异常，结合新闻（威胁情报）上下文信息，这家店挽回了一笔可能发生的损失。

另外，威胁情报在天眼系统中还有一项非常重要的作用。大家都知道，传统的防护体系在多台设备间进行联动往往需要通过特别开发的接口对一种或几种特殊类别的告警或信息进行分发和通知，这种设计往往会制约多种不同设备或系统之间的信息传递。

同时由于对消息接口缺乏一个系统化、规范化的描述，很难对复杂的攻击行为进行准确定义。天眼的一大创新点在于用威胁情报的形式对各种攻击中常出现的特点和背景信息进行记录和传输，而威胁情报将通过统一的规范化格式将攻击中出现的多种攻击特征进行标准化，可满足未来扩展攻击特征以及后续扩展联动设备的需要。

商业银行客户实践：有效改善APT攻击检测及呈现

在天眼服务过的各行各业中，金融行业由于其高价值的特性，往往成为网络攻击的重点目标。伴随着互联网业务的发展，银行等传统金融机构同样在大力发展电商、网银、在线理财等互联网金融业务。与此同时，其受攻击面也大大增加。

例如，国内某商业银行已经通过部署专业的防火墙、IPS、防病毒软件、终端安全软件等安全防护手段，能够针对主流威胁实现防护。然而基于特征检测的传统安全防御手段只能识别已知威胁，却难以防范以APT为代表的高级威胁，并且难以解决防御设备的误报和联动防御的问题。

在部署奇安信天眼后，可以采集企业网络流量、终端日志等全量数据，并结合定制化的威胁情报上下文，对特定事件进行关联分析，有效帮助该银行解决了高级威胁检测和误报率高的问题。同时，奇安信天眼通过网络流量取证可以还原威胁在本地的历史行为，可清晰的给安全管理人员呈现APT攻击的完整流程。

从2013年推出至今，奇安信天眼在公检法、金融、政府部委、运营商、石油石化、电力、教育、医疗等行业都具有成功案例，累计成功帮助客户发现和处置超过百起APT攻击事件，包括海莲花、摩诃草、蔓灵花、黄金鼠等等。

7. 威胁情报驱动：“云”安全，更加适配更加智慧

云计算的快速发展与应用落地，推动了业务孤立的烟囱模式向融合化模式转变，企业的IT规模越来越庞大，环境也越来越复杂，也因此带来了更多的安全风险。

如何让安全解决方案适应复杂多变的虚拟化和云计算环境，为网络安全提出了全新的需求，让云上客户甚至是安全厂商都为之头疼。

云计算环境对网络安全的新要求

- 数字化转型过程中用户的业务需求不断变化，防护手段不能一成不变，安全策略需要能自动适应其变化，根据存在的威胁和漏洞建立起针对性的安全防线，实现灵活可靠的防护机制，支撑业务应用所需；
- 在规模庞大的云计算环境中，任意虚拟主机被入侵或感染，入侵者都可以以该宿主机为跳板做横向移动，因此整个业务都存在着被破坏的可能，及时识别被入侵或感染的虚拟主机是降低数字资产风险的关键；
- 如果物理机还能够依靠人工进行安全运维的话，那么巨大的虚拟机集群已经无法完全依靠人力来完成，安全运维团队在面对复杂的云环境需要投入大量的时间及人力成本，并且很难做到及时准确的响应。为了将入侵范围和损失控制到最小，当虚拟主机被入侵或感染成僵尸主机的情况时，及时、准确的自动化响应处置非常重要。

自适应的虚拟化防护体系

2016年，在Gartner发布的十大信息安全技术里提到了情报驱动的安全运营中心，他们认为威胁情报驱动的安全检测超越了传统的预防工具和以事件为基础的监测，强调情报关联和自动化的响应处置。基于威胁情报的失陷主机检测可以弥补传统的病毒库扫描的不足。

奇安信虚拟化安全管理系统为云计算安全基础架构（包括服务器、虚拟化、容器）提供统一的安全防护能力。产品是遵循Gartner CWPP（云负载保护平台）的完整方案，不仅具备传统的安全防御功能，在基于威胁情报技术上，也为用户提供安全风险从发现–响应–处置的完整自动防御解决方案。

在威胁检测方面，奇安信虚拟化安全管理系统具备对全网虚拟机流量进行检测的能力，包括数据中心的南北向流量，以及虚拟机之间的东西向流量。结合奇安信威胁情报中心实时下发的威胁情报进行比对，检测其中的恶意流量，及时发现潜在的失陷主机。

针对新型的APT攻击和病毒变种，传统的病毒库检测方式难以查出与发现。奇安信虚拟化安全管理系统通过威胁情报对恶意连接及访问行为分析，建立新的测检模式，也提升了对未知威胁的防护能力。

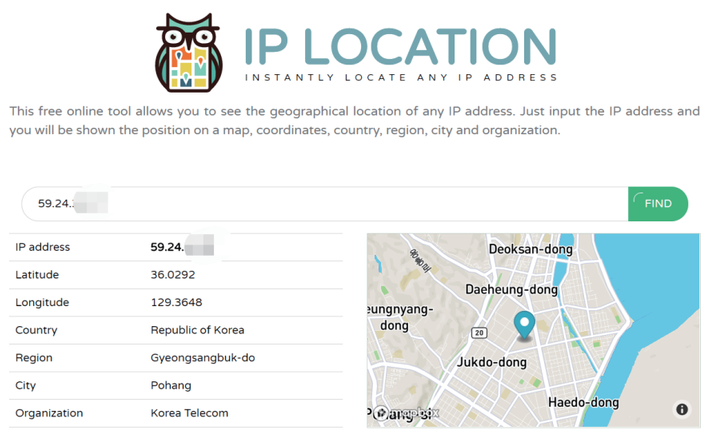
在自动响应与处置能力上，当奇安信虚拟化安全管理系统发现失陷主机告警后，可与防火墙功能进行联动，自动隔离失陷主机，防止恶意软件和攻击在数据中心蔓延。同时，利用威胁情报的上下文信息，进一步找出与攻击者相关联的更多蛛丝马迹，从而梳理出攻击者完整的行为链条，做出针对性的防御措施。

随着威胁情报技术在不断更新，奇安信虚拟化安全管理系统会不断提升对入侵行为的有效检测和自动响应能力，实现以智能、集成和联动的方式应对各类攻击，为云计算环境提供立体化防护。

互联网公司实践：在500+主机的云中拦截境外攻击

江苏某大型互联网公司部署了奇安信虚拟化安全管理系统有一年多时间了，覆盖500多台重要业务主机。某日，其负责服务器运维人员在值班期间查看到系统提示的安全告警，显示安全控制中心内网主机处于失陷状态。

经运维人员排查，发现这台服务器因为远程排障需要临时开启了远程桌面服务，且在使用完后未及时关闭，从而导致被可疑站点所利用入侵其系统和内网。

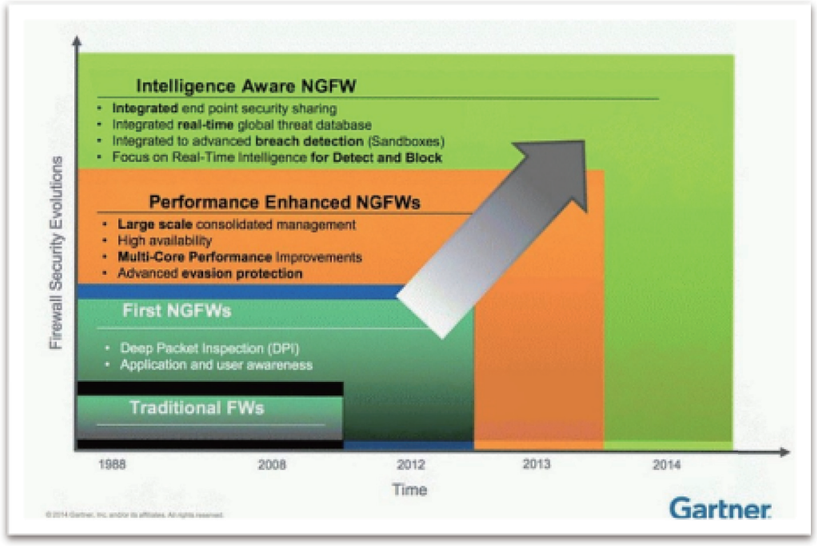


可疑IP归属地查询

奇安信虚拟化安全管理系统监测到该主机短时间内曾多次与某外部可疑IP（经分析该IP来自于韩国）进行通信，产生75条流量访问日志，并且发现网内受到mimikatz的大规模扫描（该软件是一款能够从Windows中获取内存，并且获取明文密码和NTLM哈希值的渗透工具）。

通过威胁情报对比分析后得知，此IP多次被威胁情报源标注为高风险、恶意站点、勒索等标签，且近期活动频繁，因此判定此主机已失陷的可能性极高，通过联动防火墙策略，将其访问阻断并发出告警。因此次安全风险被及时发现和迅速处理，未对业务网产生影响，避免了安全事件恶化的危机。

8. 威胁情报驱动：“边界”安全，NGFW 第四代



最早提出NGFW定义的Gartner认为，防火墙产品的演进经历了几个阶段，第一阶段：称之为“传统防火墙”阶段，第二阶段“第一代NGFW”阶段，第三阶段：“性能增强的NGFW”阶段。第四阶段：当解决了性能和环境适应性问题后，当下NGFW要解决的是什么？ Gartner认为“下一代防火墙是深度包检测防火墙，它超越了端口/协议检查和阻塞，增加了应用层检查、入侵预防，并从防火墙外引入了情报”。除此之外，Gartner还提出了防火墙要具备终端安全协同、具备全球威胁信誉库等新一代安全技术的协同能力。

由上述路标演进可以看出，尽管在安全域边界部署防火墙设备已在某种程度上被视作“基础防护”手段，但在高级威胁大行其道的今天，客户更加关注的是其安全有效性。

事前：大幅提升预防效果

防火墙上的威胁情报绝不是传统特征库那么简单，相比于传统AV、IPS特征库1~2周更新一次，防火墙云端威胁情报库可以做到实时更新，而本地的威胁情报也能达到分钟级的准实时更新。当某个原本未知的样本或域名在云端威胁情报被标记为恶意之后，在数分钟内推送给防火墙作出自动响应，达到更好的预防效果。而防火墙通过内置精准、热度威胁情报信息，可以对目前流行、突发事件进行精准防御，同时也能支持隔离内网的离线升级补充传统防御手段的不足。

事中：阻断恶意访问行为

高级威胁通常会伪装正常的网站或恶意网站传播僵尸木马、蠕虫病毒。威胁情报通过自有安全团队挖掘和交换全球威胁情报，通常能获得比传统签名库实时性、准确性更高的恶意网站和非法IP名单，防火墙通过网络流量分析就能知道所有的网络访问行为，当防火墙发现精确度非常高的情报匹配则触发的阻断动作，阻断每一次的恶意访问行为，而用户的正常上网是不会受影响的。而即使匹配到情报精确度不高，那么防火墙上也会记录“日志”，让安全团队通过日志分析快速定位问题，回溯问题。

事后：定位失陷主机并一键处置

众所周知，没有绝对的安全，被动防御也往往是不可靠的，总有被绕过的防御，最大的风险就是不知道风险，中招后不知道。而下一代防火墙通常只能通过IPS签名库和AV库里面文件MD5值匹配方式发现正在发生的常见攻击行为，而防火墙和威胁情报联动后，通过网络行为碰撞威胁情报发现异常，发现已经“失陷”的主机，通常这种主机被植入木马、 僵尸等恶意程序，并受到恶意软件远程控制，成为攻击者进行数据窃取、 横向侧移、传播蠕虫以及发起 DDoS 攻击的工具，其危害度较高且具备高级威胁特征。当这些在受控情况下产生恶意行为的失陷主机，通常会主动反连外部的域名或IP，如果这些外联的对象是在威胁情报中心里定义为恶意网站、恶意IP或是黑客组织活动域名等，通过对比威胁情报网站上的数据进一步确认事件的准确性，最后通过防火墙一键处置能力，阻断失陷主机与外部控制端的通讯，一定程度上避免失陷主机被“傀儡”。

二甲医院实践：一键阻断挖矿僵尸网络攻击

近两年，勒索病毒肆虐医疗行业，因其直接关系百姓民生，引发了巨大社会关注。湖南某地市一家二甲医院在测试新一代防火墙产品时，在短时间内就发现了大量的挖矿僵尸活动，并且蔓延趋势明显，而帮助技术人员发现这些情况的，正是奇安信威胁情报。

当时情报显示，大型挖矿MsraMiner 僵尸网络，以及大型DDoS Avzhan 僵尸网络活动频繁，主机一旦中招，可能不会立刻发作，网络管理员很难察觉异常，但是这些失陷主机通常会连接到僵尸网络的C＆C告知自己存活的状态，可随时接受控制者的命令发起攻击行为，因此具有非常大的安全隐患，而这一情报已经通过威胁情报中心下发至奇安信新一代防火墙NGFW。

在实际测试中，NGFW发现该医院1台主机向 5 个 MsraMiner Botnet 相关的 C&C 域名发起请求，共计 186 次，访问次数较多，尝试与 C&C 域名 swt.njaavfxcgk3.club 对应国外IP 进行通信，产生 69 条流量访问日志；通过奇安信威胁情报中心进一步对比，发现该主机的两方面重要特征：

- 该类域名被多个威胁情报源标记为MsraMiner 僵尸网络，具有远控、 恶意站点等恶意标

签，主要利用 NSA 武器库感染主机，通过SMB 445端口传播，并显示近一次监测到该域名参与恶意行为的时间为 2018 年 10 月，说明该事件目前处于活跃传播阶段；

- 根据奇安信威胁情报显示，域名swt.njaavfxcgk3.club、rer.njaavfxcgk3.club、tar.kziu0tpofwf.club 等多个域名均被标记为 MsraMiner Botnet，通过对该类域名的解析，C2主机地址被返回传递至发起访问的主机。因此，尝试解析该域名的主机极有可能已被植入了对应的恶意软件，并向僵尸网络控制中心注册，请求进一步的指令。

综合以上分析，鉴于该失陷主机向僵尸网络相关域名发送解析地址请求的异常行为，且检测到该主机尝试对解析后的国外IP 进行通信行为，因此判定该主机已失陷的确认度为“高”。

最后，通过智慧防火墙上的“一键处置”阻断该失陷主机的网络行为避免了威胁的进一步扩散。

虽然高级的威胁可能攻破防火墙，但是每多一项安全措施和防火墙联动，黑客成功的概率就越小，进攻的成本就越大，有了威胁情报的防火墙不仅能对正在攻击的行为进行阻断，更能对已经被攻陷的主机或者通过其他途径被感染的主机进行实时监测，及时发现失陷主机实现闭环处置才是目前边界防御安全有效性的最佳实践。

防火墙遇上威胁情报，可以简单高效地发现很多传统安全产品无法发现的威胁，甚至是已经渗透到内部勒索病毒、挖矿蠕虫等高级威胁，在安全有效性、防御实时性等方面给边界安全带来切实、明显的提升。

9. 威胁情报驱动：“终端”安全，守好 EDR

现阶段，企业的端点资产越来越多，其中脆弱的端点很容易成为黑客突破企业防线的关键。随着近年针对特定地域、特定行业发起的高级威胁事件持续曝光，APT攻击开始被大家所熟知。

传统的杀毒防护解决方案主要基于历史已知威胁的对抗经验，依靠已知样本来识别恶意文件、URL等相关信息，主要针对样本静态代码特征进行对比分析，同时依靠特征库的更新来发现较新的恶意威胁。当高级威胁通过增加混淆、沙盒对抗、0day漏洞利用等技术后，攻击者可以轻松绕过现有的防护体系进行进一步入侵。

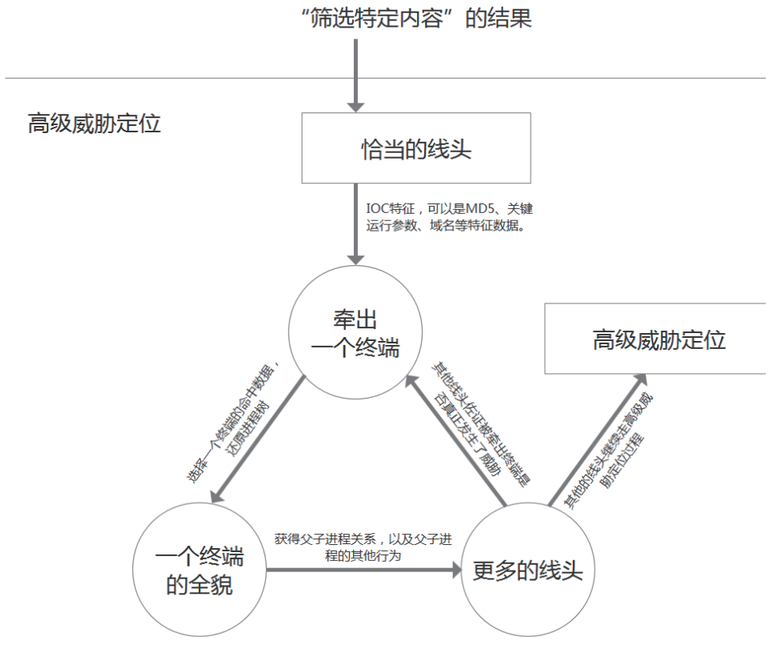
由于国内大型的政企客户多是隔离网环境，数据相对封闭，安全厂商很难针对企业内部数据进行高级威胁分析，并做出快速的威胁检测与响应。

因此，采取主动防御的方式保护端点安全越来越有必要，这种方法应该兼备实时监控、检测、高级威胁分析及响应等多种功能。在2014年，Gartner就将端点检测与响应技术（EDR）放在了十大网络安全技术之中，并将其列入五种检测高级威胁的技术之一。

值得注意的是，在2016年和2017年，EDR同样入选了榜单。Gartner预测，到2020年，80%的大型企业，25%的中型企业和10%的小型企业将投资EDR能力。

早在2016年，奇安信企业安集团就推出了EDR产品——奇安信终端检测响应系统（以下简称奇安信 EDR），以弥补传统EPP产品的不足。

奇安信 EDR围绕着检测能力与响应能力而设计，并与奇安信威胁情报中心进行联动，将威胁安全情报落地到奇安信 EDR产品中，帮助客户解决安全对抗经验不断更新的问题，同时基于终端的背景数据、恶意软件的行为以及整体的高级威胁的生命周期角度进行全面的检测和响应,进行快速、自动化的阻止、补救、取证，为终端提供真正有效的防护。



通常，一次高级威胁定位是从恰当的线头开始的，线头包括文件MD5、运行命令参数、IP、域名等。而线头的来源既可以是企业内部运行规则，也可以是奇安信威胁情报中心推送的威胁情报。

奇安信 EDR通过数据采集引擎，持续采集终端各类动态行为数据与静态属性信息,并上报到奇安信硬件大数据分析平台，结合威胁情报进行自动化分析判断，进而精确定位到沦陷终端。通过奇安信 EDR的进程树还原功能，对沦陷终端进行追本溯源，包括攻击步骤和影响范围，还原攻击者的整个入侵过程。

与此同时，对未知威胁的捕猎也是EDR产品的一个重要功能方向。基于所有终端采集数据，奇安信 EDR提供了丰富的数据聚合与筛选语法，帮助分析人员快速获取到终端的异常行为数据，再结合上下文数据以及奇安信威胁情报推送的IOC信息，最终实现对威胁的确定。

政府事业单位实践：斩断Wannacry内网渗透之手

国内某重要政府事业已经根据国家等级保护条例要求，部署了防火墙、IPS、终端管理控制软件、杀毒软件等。所有办公终端都部署在隔离网环境，不允许接入互联网。

在部署奇安信 EDR后，意外发现某一台终端出现大量异常外网IP与域名请求，通过与奇安信威胁情报结合分析，发现该终端发起的DNS解析记录和IP访问行为，都指向了WannaCry的C2站点，同时还有大量内网445端口探测行为。通过分析确定该终端已沦陷，被攻击者作为跳板进行内网渗透。

通过终端资产确认，发现这台终端属于一个运维人员。该运维人员为了工作方便，开通了远程访问端口，但恰恰就是这个暴露的端口被黑客暴力破解入侵进入，通过黑客工具把终端的防护软件卸载，再将病毒样本投递到内网。通过奇安信 EDR确定了整个威胁的受影响面后，客户对受影响的终端都进行了处置，并加强了网络安全管理。

四、迈向情报内生的安全能力体系化建设

我们从介绍本手册开始，介绍了网络安全形式的三个转变、40个APT组织的近况以及奇安信做出的三个判断，这也是我们撰写本手册的初衷，即全球数字经济建设竞争形势以及APT组织日益明显的网络战争对抗趋势，已经开始倒逼关键信息基础设施相关行业及大型企业，推动其网络安全工作从合规走向实战。在随后的两个章节中，我们介绍了实战化情报内生运行机制，描述了威胁情报能力框架以及9大应用场景，帮助企业从情报消费的初级阶段迈向情报内生的安全能力体系化建设阶段，以便帮助企业更好的应对数字化转型带来的压力和挑战。

为了便于您快速理解本手册中的主要观点，我们对内容进行提炼如下：

本书中给您的关键提示

威胁情报是高级安全能力的标配

在基础架构安全和被动防御，威胁情报消费主要应用于威胁检测及响应，当组织成熟度达到中高级，建设动态的积极防御体系应将威胁情报用例由基础的情报消费推向更高级的本地化威胁情报生产，以期更精准的、更好的服务于组织业务发展，缓解组织面临的数字化转型压力。

威胁情报不只是用来消费的

威胁情报的生命周期从采集、处理、分析、共享、反馈到再生产，构成消费与生产的闭环能力才能实现威胁情报价值最大化。企业应当以情报为中心构建能力框架，实施本地情报生产，以便准确发现针对业务的攻击，进而在业务、信息化及安全等多部门间形成统一的建议和行动，并在行业内形成有效共享。

选威胁情报要看三同步

三同步是将信息化建设与网络安全的防护与响应过程结合，达到工作任务事项级别的深度绑定，实现二者的同步规划、同步建设、同步运行。以此为标准考察供应商是否有能力和资源，构建适合企业使用的威胁情报能力、积极防御体系及情报输出。

只用ATT&CK是不靠谱的

该框架在APT攻击事件复盘、产品覆盖度比对、知识积累等方面具有指导意义且实操性强，可以应用于威胁狩猎过程；但在实际的关联性及归属分析中，需要更多思考攻击者实战细节，完善现有的检测点和检测策略，以强特征、元数据强化APT分析。

威胁情报至少有9大应用

奇安信威胁情报中心已经形成实战化情报内生运营机制，并在9大应用场景中成熟应用，这些场景包括本地化情报能力构建、APT组织追踪分析、监管侧态势感知、企业高效安全运行、精准应急响应处置、未知威胁发现及防护、智慧云安全防护、边界安全防护、终端EDR。

五、附录

1. 奇安信威胁情报中心

奇安信威胁情报中心是奇安信集团旗下的威胁情报专业机构。奇安信威胁情报中心基于长期积累的核心安全技术，依托亚太地区顶级的安全人才团队，结合强大的数据分析能力，实现全网威胁情报的实时、深入、全面地整合分析，为企业和机构提供安全管理与网络防护的威胁情报预警及分析能力。

奇安信威胁情报中心对外服务平台 https://ti.qianxin.com

该服务平台以海量多维度网络空间安全数据为基础，为安全分析人员及各类企业客户提供基础数据的查询、攻击线索拓展、事件背景研判、攻击组织解析、研究报告下载等多种维度的威胁情报数据与威胁情报服务。

Alpha威胁分析平台

奇安信 ALPHA威胁分析平台，是奇安信集团面向企业安全分析师和事件响应分析人员提供的一站式云端SaaS服务的威胁分析工具平台，该平台具备全网监测覆盖的威胁情报和海量互联网基础数据，在数据覆盖度、信息种类、数据的时间/空间跨度都具备较大优势。

用户价值：

提升威胁检测能力：ALPHA集成了网络威胁全方位检测能力，包括IP信誉情报、失陷检测情报、文件信誉情报、文件动静态行为分析数据、IOCTag情报、网络基础设施情报数据等。

平台模块和用途：

威胁研判分析

直接判定报警真实性、了解攻击团伙/软件的意图和能力，进而快速筛选出真实、重要的报警。

威胁关联分析

针对无法直接判定的分析对象，提供基于内置安全模型进行的自动化、可视化分析，自动过滤噪点数据。进行一键自动化分析域名、IP、注册信息和样本间的关联信息，同时还可以生成攻击者画像信息。

文件深度分析

用来了解恶意软件的详细的静态、动态行为，并提取IOC形成自己的威胁情报。已支持Windows、Android、 Linux平台下的样本自动化分析。

分析任务管理

将一次攻击事件所涉及到的域名、IP、样本等信息进行整合并统一管理。后续还可以依照标准威胁情报格式STIX，进行威胁情报分享。

产品特色及优势：

情报积累

数亿样本的云沙箱运行数据，上百亿的文件信誉相关情报，每天新增百万级以上，全球超过40亿IP的网络基础信息及超过10亿的恶意Tag标签历史信息。

数据支撑

海量pDNS数据（包括解析的终端规模等）和Whois历史数据。

追踪监控

跟踪全球近千个攻击团伙/恶意家族的档案信息，全球APT团伙（40个）/恶意家族使用的远控服务器信息。

更准确的IOC判定

全面升级IOCTag数据与开源情报数据，完善白名单库，提供更准确的情报判定。

更丰富的情报上下文

专业安全分析师倾情打造，提供更完善的情报基础数据信息与细粒度更高的情报上下文，帮助对安全事件的分析与溯源。

更灵活的情报交流

提供平台内多系统互通的情报交流“自留地”，不仅有“我觉得”，也支持“你觉得”，还可以悄悄告诉我“你想要的”。

更便捷的平台访问：支持移动设备访问，减轻前场支持负重。集团内部已开放APP访问，对外也已支持手机浏览器上的查询，后期还会上架小程序哦。

交互能力：针对安全分析师工作提供有效支撑，使攻击定性、事件溯源从过去的纯手工转变为半自动化，大大缩短了事件响应所需的时间提高了工作效率。

威胁雷达

奇安信威胁雷达产品是奇安信集团利用大数据技术和行业内领先的威胁情报监测技术，面向政府和监管行业打造的一套包含技术威胁分析和城市全境大网监测的等保SaaS安全服务产品。

产品特色和优势

- 云端SaaS轻量级交付；
- 技侦人员案件技术分析辅助利器；
- IP、域名、样本哈希自动化判定平台；
- 病毒木马样本自动化分析可视平台；
- 大数据威胁建模一键自动化威胁可视化分析视图；
- 案件Case统一管理支持Stix格式情报导出；
- 全球视野的安全报告推送；
- 不需要部署探针即可纵观全城威胁态势。

产品模块和用途

技术侦查模块

威胁研判分析模块

提供域名、IP、文件hash更多详细的威胁和网络上下文信息，可以帮助判定事件真实性、了解攻击团伙/软件的意图和性质，并获得更多案件背景信息。

威胁高级可视化模块

针对无法直接判定的分析对象，可一键自动化分析域名、IP、样本哈希，自动化下钻分析，可以用于案件的拓线分析。

◆ 样本深度分析模块

用于了解恶意软件的详细的静态、动态行为，并了解其进一步的危害。

◆ 分析任务管理模块

可以将一次案件涉及到的域名、IP、样本等信息进行整合并统一管理，同时支持STIX格式情报导出。

等保通报管理模块

◆ 失陷主机监控模块

基于大网数据监测城市全境被APT团伙、各种僵木蠕等威胁控制的失陷主机，可以掌握区域内被不同攻击团伙或恶意软件控制的受害者主机IP，为重保资产监测防护提供有效的情报和案件线索。

◆ 安全通告模块

推送奇安信和全球其他安全厂商的事件预警、恶意软件、漏洞报告、APT攻击报告，用于安全事件的预防或紧急处置。

威胁情报系统

奇安信网神威胁情报系统（简称QAXTIP），是一款面向企业安全大数据平台提供威胁情报数据和分析工具的安全产品，协助用户从海量告警中发现关键威胁并支撑响应处理。QAXTIP具备领先的威胁情报能力以及开放的产品架构，可以与大多数厂商的SIEM/SOC（包括奇安信NGSOC、QRadar、Splunk等）或态势感知等大数据安全分析产品整合，发挥作用。

客户价值：

- 基于情报即时、精准发现关键现实威胁。包括APT（高级定向攻击）、窃密木马、勒索软件、网络蠕虫、僵尸主机等；
- 对报警数据进行研判、筛除误报并确定事件优先级。从海量报警中筛选出真正需要响应处理的部分，并提供响应需要的更多上下文信息；
- 提供预警和应急支撑能力，指导运营团队及时了解、处理可能发生、正在发生的重大威胁，并提供更多线索和处置建议；
- 情报运营能力，为运营团队建立自己的威胁情报能力提供平台支撑。

产品优势：

◆ 价值高

国内领先的APT追踪发现能力，全新发现并命名多个APT团伙。其平台蕴含的威胁情报价值领先于其它厂商并有持续的输出，实现特有的发现能力。

◆ 检测准

精度99.9%以上，多次用户现网测试证明，检测精度高于竞争厂商，为安全运营团队节省大量精力。

◆ 规模大

QAX TIP作为本地化平台，具备6千万级的失陷检测库，超过十亿级IP信誉库，超过十亿级的文件信誉库，数据量与查询输出性能远超其它厂商。

文件深度分析系统

奇安信文件深度分析系统，是奇安信威胁情报中心根据多年APT样本分析经验总结出品云沙箱产品，该产品适合安全分析师和事件响应分析人员进行恶意样本威胁鉴定。该系统结合自有威胁鉴定引擎和多种业界知名AV引擎检测、高对抗沙箱环境行为分析、威胁情报关联、自动化文件tag等技术，提供更精准的检测结果、更具体的威胁类别以及更直观的分析结果，可以满足多个场景下对恶意软件的检测、研判、分析需求。

典型场景

- 企业/安全厂商的产品或工具通过API集成，获取深度恶意文件检测能力；
- 安全分析师/事件响应分析人员对已有样本文件进行自动化专家级判别；
- 让事件响应人员了解恶意文件的详细运行机制，以便快速处置；
- 特定行业的内部私有云沙箱机群（本地化部署）；
- 威胁分析人员通过关联分析，发现特定攻击团伙的新样本（本地化部署）；
- 作为威胁情报分析工具，支撑本地化的情报分析以形成行业威胁情报。

产品特点：

- 支持Windows、Android、Linux沙箱样本威胁鉴定；
- 多种动静态检测技术综合评分，检测结果更精准；
- 自动化提取文件关键特征形成tag，文件特点一目了然；

- 基于威胁情报的关联，获取攻击团伙、恶意家族信息；
- 样本进程可视化行为分析图，直观呈现进程、网络访问、释放文件、异常行为的关系，恶意软件运行过程一目了然。

样本同源分析系统

奇安信样本同源分析系统是奇安信威胁情报中心在长期APT样本分析中总结和实现的一套基于恶意代码基因图谱分析获取样本相同家族样本的分析平台。

该系统主要解决了如下几大问题：

- 恶意代码数量呈爆发式增长，但真正新型恶意代码不多，大部分为已有代码的变种；
- 恶意代码通过变形、加壳、多态等手段混淆已有特征，企图逃避安全软件的分析检测；
- 如何快速发现海量数据中的威胁：APT攻击、木马、勒索、各类病毒家族。

我们怎么做的？

- 基于样本“基因”深度拆解（支持PE和非PE文件动静态特征）及抽象化“基因”特征；
- 引入符合抽象后的样本“基因”特征的分类聚类算法；
- 收集已知的APT团伙样本、恶意家族样本，进行分类聚类数据训练及预处理；
- 未知样本通过同源流程自动分类聚类。

样本同源效果：

- 未知样本自动判定属于哪一个APT组织或者哪一个病毒样本家族，并给出置信度（准确的可能性）；
- 大量样本（数十万）的自动聚类，可以得到未知样本属于哪一个聚类后的样本集（找出所有相似样本）；
- 根据样本的特定“基因”特征“搜索”样本库中具有相同特征的所有样本。

产品优势：

在奇安信红雨滴实战APT样本分析中，样本同源分析系统经过了大量的样本同源效果验证。

- 海量恶意样本模型的训练；
- 样本深度文件解析引擎进行启发式检测和信息提取；
- 样本文件基因提取；
- 云端高对抗沙箱机器；
- 专家干预的机器学习和模型训练；
- 通过机器学习和模型训练识别样本家族和攻击团伙；
- 识别的新型攻击和家族信息进入到模型库中；
- 样本同源的可视化展示。

高级威胁分析服务

奇安信威胁情报中心红雨滴团队提供的高级威胁分析服务，主要面向网络安全主管部门和职能部门、政府机构和行业客户与高校科研机构，为其提供决策和参考。目前战略情报服务内容主要包括：威胁情报通告服务、APT深度分析服务、APT定向分析服务、APT持续跟踪分析服务、威胁线索拓展服务。

服务价值

多线索关联分析

帮助客户通过恶意网络行为的扩展线索发现出更多信息，如攻击者所用的网络资源、攻击者信息、受害人信息等线索。

提供针对性防御

提供定期安全情报资讯，客户可优先关注与其自身紧密相关的攻击产生的预警和通知，并及时据此做针对性的预防。

支撑战略性决策

APT深度分析报告、重大事件分析报告等能够支撑机构高层人员做战略性决策，帮助其理解组织威胁的整体情况，以及对抗这些威胁所需要的防御建议。

高威胁防御对抗

网络攻击事件由小打小闹向国家大事转变，网络攻击技术从简单粗暴向复杂精细转变，网络攻击形式从通用型向APT攻击转变。本服务帮助客户了解攻击对手、识别哪些威胁是最有可能影响所处行业/环境的APT威胁。

独家优势

奇安信旗下的红雨滴团队专注于APT攻击类高级威胁的研究，是国内首个发布并命名“海莲花”（APT-C-00，Ocean Lotus）APT攻击团伙的安全研究团队。红雨滴团队的全球领先的安全大数据能力和专业分析师丰富经验，使高级威胁分析服务具有以下独家优势：

• 丰富的威胁情报来源

奇安信威胁情报中心当前已经建立的多维度、多来源的数据基础，能从多个来源采集多维度数据和威胁信息，为进一步数据清洗、融合和关联分析打下坚实基础。

• 高质量的威胁情报数据

奇安信威胁情报中心通过对多源化情报数据进行清洗、整合、分析并对冲突数据进行研判，利用大数据分析技术和机器学习技术提取威胁情报中的有效信息，并给出前瞻性的预测和决断依据，保障了输出的威胁情报准确性和时效性。

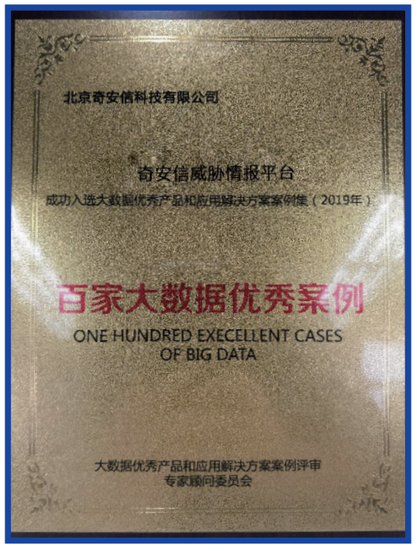
• 超强的APT分析发现能力

威胁情报中心依托奇安信在全球领先的安全大数据能力以及攻防研究团队专业领先的高级威胁事件跟踪、发现能力，持续跟踪分析的主要APT团伙超过40个，首发并命名的APT组织超过7个，持续发布APT组织的跟踪报告超过30篇。

2. 权威机构的认可

工信部：2019年大数据优秀案例

威胁情报分析平台，在多次同类产品测评中获得第一的成绩，并成功入选全国大数据优秀产品和应用解决方案案例集，被工信部授予“大数据优秀案例”。



2019年《大数据优秀产品和应用解决方案案例集》

信通院：2019年网络治理能力评估证书

威胁情报分析系统在数据中心联盟“网络治理能力规范”中，符合数据中心联盟技术文件《网络治理能力评估规范：第1 部分 威胁情报服务系统》，通过了威胁情报服务系统评估测试。

2019年《网络治理能力评估》证书

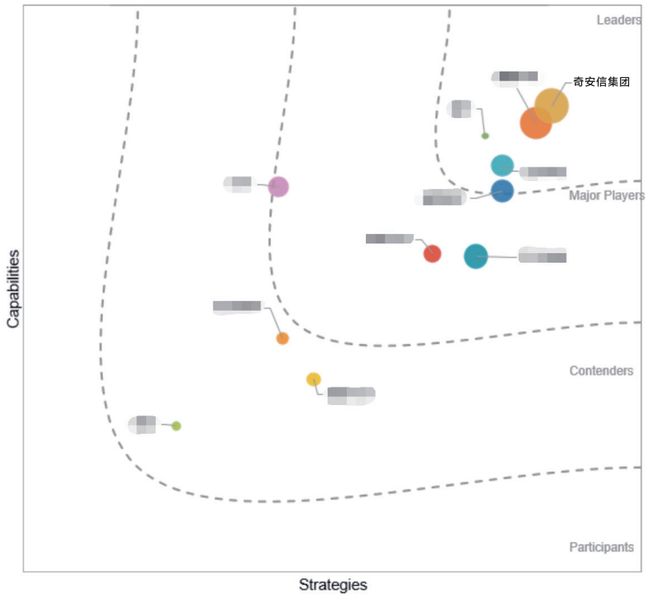
RSA：2019年RSA大会威胁情报最佳产品–CDM

2019 年，RSA大会上，奇安信集团威胁情报斩获全球知名网络安全杂志CDM（Cyber Defense Magazine即《网络防御杂志》）的Best Product（最佳产品）奖项。

《Best Product Intelligence for 2019》

IDC报告：奇安信是中国威胁情报市场的“领军者”

11月30日，国际权威咨询公司IDC发布了2018中国威胁情报安全服务市场研究报告。报告显示，奇安信凭借独特且丰富的数据、专业的高级威胁事件跟踪/发现能力、成熟的内部运营流程等优势，在产品和服务成熟度、行业影响力和持续投入能力等三个维度上均名列所有入围厂商前茅，成为中国威胁情报市场的“领军者”。



数据来源：IDC，2018

"威胁情报"在 2015 年进入中国市场后，短短几年的时间，在中国发展十分迅速，市场需求不断增加。IDC认为，尽管中国威胁情报市场还处于初期发展阶段，但广大技术买家，尤其是政府、金融、能源、互联网、电信等重点需求行业，对于威胁情报安全服务在企业整体安全策略中起到的积极作用给出了很高的评价，为威胁情报市场的持续快速发展奠定了良好的市场基础。

截至目前，奇安信已经发布了Alpha威胁分析平台、威胁情报系统TIP、监管行业威胁情报平台（威胁雷达）、高级威胁情报分析服务、云端SaaS API等多个威胁情报产品，全面覆盖了国内威胁情报服务的四种主流模式（威胁情报数据应用程序编程接口、威胁情报平台、威胁情报软件即服务、安全产品赋能），奇安信天眼、NGSOC、态势感知、奇安信智慧防火墙、EDR、云安全、虚拟化安全等核心安全产品和服务均集成了威胁情报能力，并且能够为不同客户提供定制化的行业解决方案，交付成功率居业内领先地位。

未来，奇安信威胁情报中心还将以联盟的方式向第三方输出威胁情报能力，提升业界整体的安全防护水平。

IDC认为，奇安信在威胁情报安全服务领域拥有独特且丰富的数据优势。基于国内庞大的安全终端软件装机基础，能够提供海量终端样本库、主动防御数据、文件信誉情报、各类安全产品（如网站安全、防火墙、态势感知、高级威胁发现等）的攻击发现日志，通过整合关联实现威胁来源的判定和画像，提供信息有用且维度全面的 IP 信誉，实现各种流行性及高级定向攻击的发现、评估与跟踪。同时作为批量生产机读情报的基础数据，能够实现本地化流行攻击 IOC 覆盖。

以海量历史Passive DNS和Whois数据等威胁情报源数据为依托，可实现高效的威胁发现、关联及溯源。另外，奇安信重点安全服务团队覆盖国内大量政府和大型企事业单位的重点安全服务团队，日常工作中执行大量的应急响应服务，能够提供众多独有的威胁线索，以此形成多个对高级威胁组织挖掘分析并揭露的成功案例。

奇安信具有专业的高级威胁事件跟踪/发现能力，曾率先发现多个高级持续性威胁（APT）攻击团伙并对其命名。威胁情报研究分析团队持续跟踪超过40个 APT 团伙的境内攻击行为，持续输出已知或未知组织的最新活动分析。奇安信 拥有近百人的威胁情报研究分析团队，在威胁分析的各环节，包括公开情报收集、数据处理、恶意代码分析、网络流量解析、线索挖掘拓展，都有专才覆盖，为威胁情报安全服务产品研发和能力提升提供了强大的基础数据、威胁研判支撑。

奇安信拥有成熟的内部运营流程，早在 2015 年就在安全产品中集成威胁情报进行检测/防御，相关的数据处理基础设施及信息挖掘关联分析继承了互联网公司的成熟技术体系，经过多年不断完善，情报运营体系趋于成熟，情报的检出率、误报率、上下文关联分析、情报及时性等方面的控制已经比较成熟。

安全牛：威胁情报矩阵头名

国内知名安全媒体安全牛发布了《中国网络安全细分领域矩阵图(Matrix 2018.11)》。其中，奇安信集团在威胁情报领域领跑国内市场。

本矩阵图(TIM)中的“威胁情报”是指：由第三方专业机构提供的网络安全威胁数据，可进行传输交换、关联分析、挖掘应用，以反映组织存在的网络威胁和安全影响。包括但不限于设备日志、报警或描述威胁事件等情报消息。

矩阵图分为三个矩阵区，领先者、竞争者与潜力者。每个厂商所处的区域主要与三大系列指标有关，影响力、规模和技术创新力。影响力主要是指品牌知名度、行业口碑、市场地位等；规模主要是指营业收入、人员数量、利润等；技术创新力主要是指研发投入、产品化能力、技术定位等。三个指标之间互有影响，并非完全独立，如技术创新力就会给影响力带来重要支撑，规模也会给技术创新力和影响力带来辅助作用。

安全牛认为，当前大型安全硬件厂商，提供威胁情报的方式主要以搭配安全产品服务及订阅服务为主，约占威胁情报采购市场的60%。随着态势感知市场的扩大，“API数据接口”的采购模式也呈快速上涨趋势，约占市场威胁情报采购市场的30%。SaaS模式大多以免费/开放形式为主，市场采购率较低约占市场威胁情报采购市场的5%到10%。

奇安信威胁情报的主要优势在于：

◆ 第一、自身百亿级别的PE样本收集能力

全量数据的收集能力和快速的数据处理能力使得奇安信在威胁情报的生产环节就快人一步，最大程度保证了威胁情报的实效性。

◆ 第二、产品化能力非常强

截至目前，奇安信已经发布了Alpha威胁分析平台、威胁情报系统TIP、监管行业威胁情报平台——威胁雷达、高级威胁情报分析服务、云端SaaS API等多个威胁情报产品，并且能够为不同客户提供定制化的行业解决方案，交付成功率居业内领先地位。

◆ 第三、体系化协同作战

目前，奇安信智慧防火墙、EDR、NGSOC、态势感知、云安全、虚拟化安全等核心安全产品和服务均集成了威胁情报能力，机读情报可以快速下发到各个安全设备中，形成威胁情报驱动的联动防御体系。

◆ 第四、领先的APT发现能力

基于威胁情报，奇安信还有着独步国内的APT组织发现与追踪能力。据统计，奇安信累计监测到超过40个境内外APT组织，是中国发布APT报告最多的厂商，包括海莲花、蓝宝菇、毒云藤等都是奇安信首先发现并命名的APT组织。


奇安信
威胁情报中心
奇安信
新 一 代 网 络 安 全 领 军 者