金融行业

RSA2020专报

3 月报
2020 年

安全月报

RSA观察 | 参会之路 | 闪亮RSA | 创新沙盒

绿盟科技金融事业部出品

RSA观察

RSA 2020：绿盟科技赵粮对国际网络安全市场的三个观察

参会之路

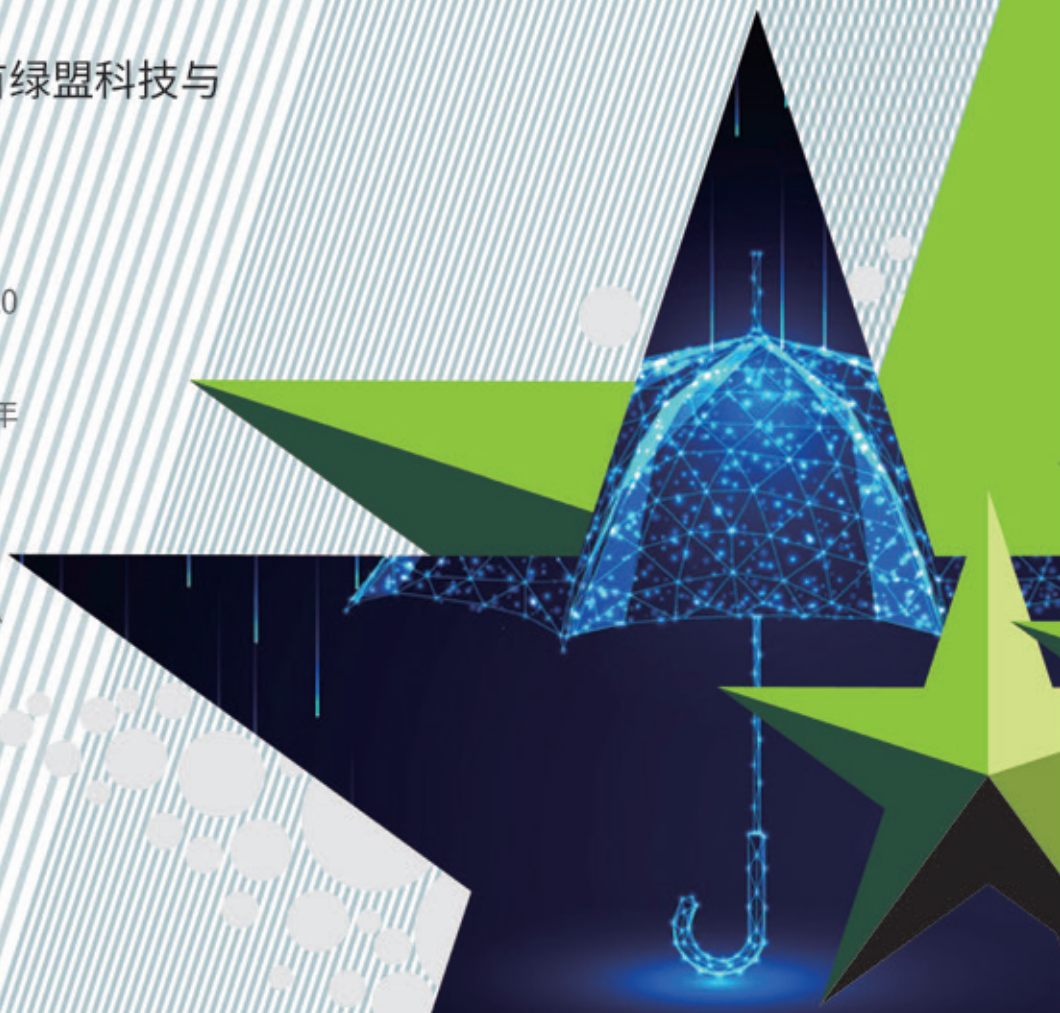
二十分之十三 | 再回首绿盟科技与RSA的安全发展之路

现场直击 | 绿盟科技RSA 2020展区亮点全揭秘

为什么绿盟科技要连续十三年参展RSA大会？

绿盟新一代WAF，究竟有什么不一样？

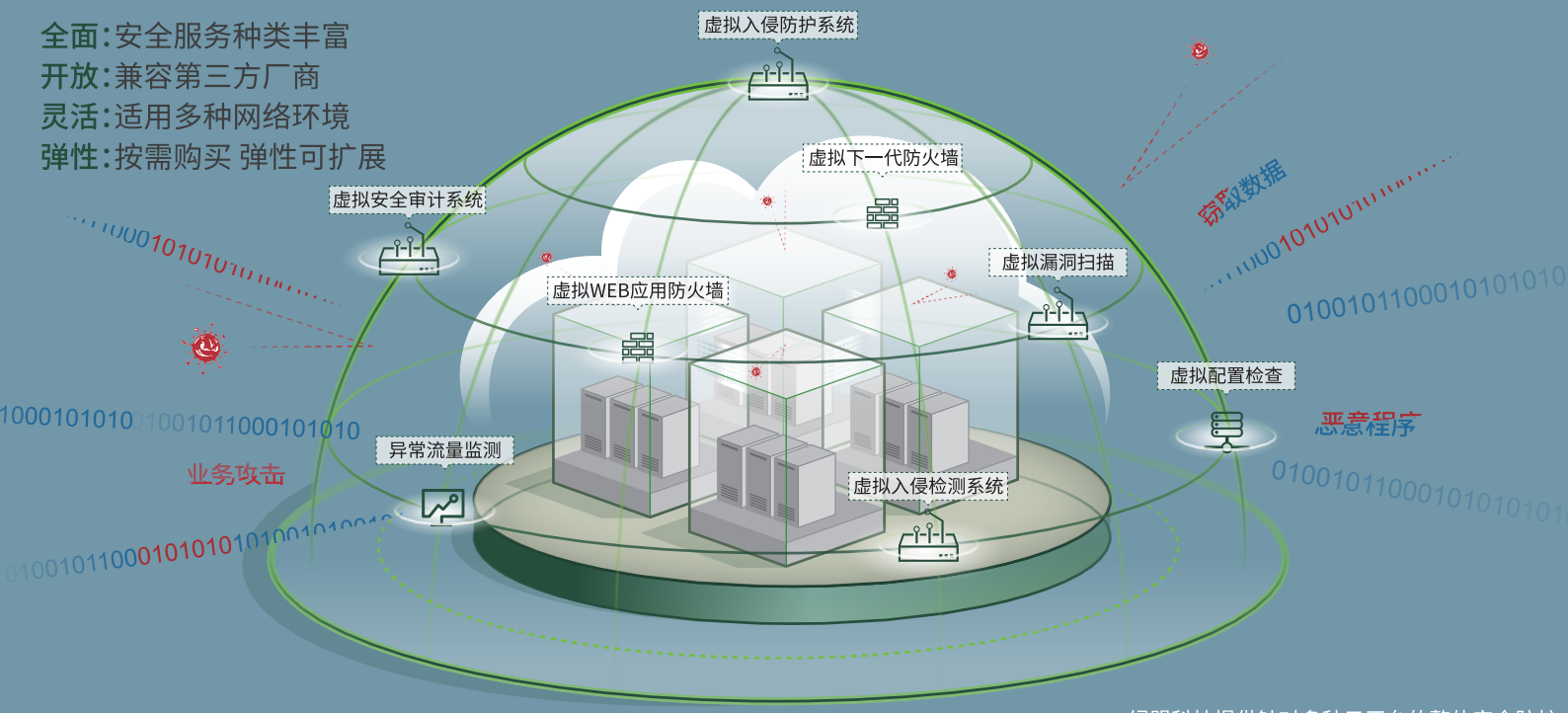
绿盟威胁情报交出这样一份“成绩单”



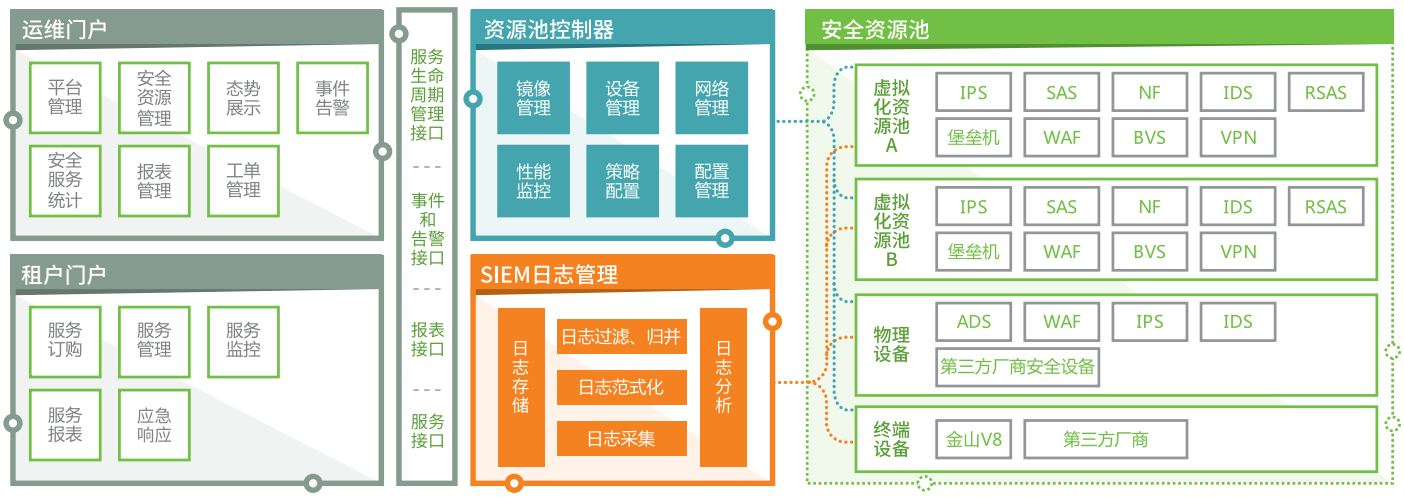
NSFOCUS

绿盟科技
云计算安全解决方案

全面:安全服务种类丰富
开放:兼容第三方厂商
灵活:适用多种网络环境
弹性:按需购买 弹性可扩展



绿盟科技提供针对多种云平台的整体安全防护



THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为运营商、政府、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技

本 | 期 | 看 | 点

安全月报

2020年第3期

绿盟科技金融事业部

目录 CONTENTS

RSA观察

参会之路

闪亮 RSA

创新沙盒

安全月报在线阅读

绿盟科技官方微信

NSFOCUS

RSA 观察

RSA 2020：绿盟科技赵粮对国际网络安全市场的三个观察

孟祥聃

北京时间25日凌晨开始，RSA 2020正式开幕。绿盟科技作为为数不多中国参展商之一，也带着近些年在国际安全市场广受好评的数款自家产品和方案，悉数赴会。

既然这届 RSA 大会的主题是“Human Element”，绿盟君从“人”的角度，对话绿盟科技首席技术官及国际业务首席运营官赵粮博士，透过 RSA 大会聊聊他个人参会这几天，最为突出的感受和观察。

观察1：回归安全本源——如何用“新技术”解决“老问题”

可以说，如同世界经济宏观上分为发达国家和发展中国家一样，一个国家的网络安全整体水平和这个国家的人均 GDP 有着令人惊讶的正相关性。以恶意IP占比、网络安全相关投入占比等指标来看，目前发达国家要明显优于发展中国家，这基本已是业界共识，并且有明确的数据支持。而 5G 在人口、设备众多的发展

中国家快速且广泛的应用，也势必为这些安全防护水平没那么高的国家，带来了更多更激烈、强度更高的网络安全威胁。

但是，这些威胁一定是全新的威胁么？在网络安全整体水平较高的发达国家，“老问题”就已经解决了么？我们看到的事实是，并没有。在发达或者相对发达国家里，我们看到中小企业的网络安全能力也不令人满意。勒索、网络攻击、数据泄露等已经被公开的事件层出不穷。即使在发达国家的大型企业，无论是团队的专业性、相关投入、所采用安全产品的技术能力、安全架构和防护实践等角度来看，也已经是一家企业能够做到的“极致”的情况下，在刚过去的2019年，却依然出现了一系列数据泄露、隐私侵犯等重大安全事件。

所以，我们第一个观察或者说体会是，网络安全的本源，最原始和本质目的，是如何用“新技术”解决“老问题”。

“新技术”不多说，安全行业最热衷讨论的话题之一就是新的安全技术，以及可以用于安全防护的新技术。“老问题”有那些？围绕着人（human），身份、钓鱼、社工、隐私、甚至补丁，都是。今年 RSAC 的主题也是此意。超过99%甚至更多的安全事件都有由这些“老问题”引起的。人作为网络安全诸多因素间的一个重要交集，在参与到安全实践的过程中，会有疏漏，会产生缺陷，进而成为问题，甚至引发事件。

看今年 RSAC 的创新沙盒入围和获胜名单，也颇有此意。

先说比赛结果。北京时间2月25日上午结束的创新沙盒，专注隐私保护的 SECURITI.ai 获得了最后的胜利。中国安全行业的专家，有的表示赞同（当然大部分是做相关方向的），有的则表示不能理解（比如这届创新沙盒评委更关注商业市场而不是创新）。其实无论是 SECURITI.ai，还是在赛前关注度颇高，主做安全意识的 Elevate Security，都处理的是和人相关的已知威胁，但应用了新的技术。

以 SECURITI.ai 举例，作为成立于2018年，入围决赛10强，拥有最高融资额（8000万美元）背景的公司，它聚焦的是如何利用人工智能（AI）技术来实现个人敏感信息的发现，自动化数据主体权、文档责任，来帮助企业满足隐私方面的合规需求。人工智能和机器学习在网络安全的应用，也是今年 RSAC 议题的重要方向之一。基于面向人的知识图谱的构建，SECURITI.ai 可以为后续的分析提供模型支持，并通过 bot 实现智能化的交互。方案角度，为了解决个人隐私数据分布广泛且多涉及共享、难以统一管理的痛点，SECURITI.ai 也提供了运营平台 PrivacyOps，从消费者数据权利请求，到企业赋予用户数据的控制权利的响应流程，以及后续的合规性审查报告，全部实现自动化处理。这些都是其技术层面的突出亮点，而不能认为其仅仅是依赖隐私合规在全球的巨大潜在市场而“豪夺”了此次冠军。

这个结果也符合用新技术解决老问题的大势。

观察2：创新多，但也要关注如何把安全做“轻”，做“简单”

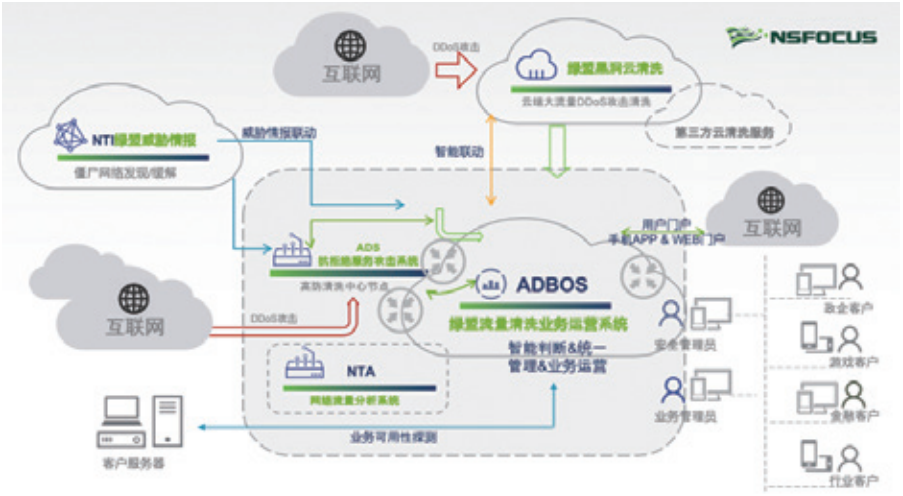
“轻”，指的是要配合不同国家的云战略，企业上云、应用云的步伐，安全能力要能更容易嵌入各种系统中，甚至做到内生。而“简单”，除了顾名思义，产品（能力）交付、部署更简易，运维和响应自动化程度更高外，还要从客户角度，强调能更容易感知到安全的有效性。

特别是后面这点，绿盟科技这次 RSAC 参展的产品之一，也是我们在2019年海外市场重要的新品——ADBOS（流量清洗业务运营系统），就有很好的体现。

抗 D 一直是绿盟科技的强项。ADBOS 的不同之处在于，它虽然是基于抗 D 设计，却是集管理、运维和运营一体的综合平台。除了通过流量检测基础引擎对传统流量实时清洗时的误报率问题进行了重点优化外，我们还特别加入了“业务可用性监测（即多点拨测）”模块，用于帮助用户实时监测和判断网络链路质量。这样客户就能更简单、直观的理解和观测安全防护的效果是怎样的，更快的从多维度了解自身的业务状况，也能和供应商承诺的 SLA（服务水平协议）更直接的对应上。

当然，抗 D 不是有了云清洗就不要本地方案。“云、地、人、机”四维一体的抗 D 体系，就是要从云清洗、本地清洗、安服专家/安全运营中心、以及机器可识别的威胁情报/策略配置四个大的角度，进行配合作战。将完整的流量监测、

清洗和拨测系统充分云化以增加安全的弹性，结合移动办公的趋势提升运维的灵活性等等，这些都是将安全做“轻”、做“简单”的具体体现。



此外，结合安全托管服务，围绕抗 D 这一核心目的，完全的将安全能力服务化、可订阅化，无论是对应供应商、合作伙伴还是客户，都可以更客观和直接。特别在抗 D 这个领域，我觉得这才是安全产品和运营的终极方向。

当然，除了抗 D 外，反钓鱼、反勒索、托管检测与响应等都有不错的机会。贯彻这种“做轻，做简单”的实践，可以让这整个生态的参与方都更加关注安全效果，而不是安全手段和过程。也就是说，从一个安全产品设计之初，就要将安全效果的闭环、客户侧的呈现、以及如何观测等问题考虑清楚，让产品价值在客户侧可以得到更充分的体现。

长期来看，这甚至可能帮助整个网络安全行业改变“劣币驱逐良币”的顽疾，让更有价值的产品和服务脱颖而出，而不是被那些只是“忽悠”见长的产品占领（好的安全产品和服务）应得的市场。

观察3：中美安全企业互相取长补短，不断完善生态

将观察的时间窗口稍微放宽些，聚焦世界范围内为数不多的一线安全供应商，我们不难发现，在“打法”上，中美双方的一些企业正在互相学习、取长补短。

中国安全供应商的能力在快速崛起，生态也在不断发展壮大，这是事实。但

不可否认，单论 RSAC 这场世界范围的安全盛会，绝大部分参展商仍然是美国企业。据部分媒体统计，今年 RSAC 参展的美国企业占比在70%以上。所以中美之间的比较和追逐，不会因为其它国家参与度的提高而被轻易稀释。

但目前还有不少国人，对美国网络安全企业发展的战略战术的认知，仍停留在5-10年前，即他们只专注于企业的核心“大”产品上，如 Palo Alto Networks 的下一代防火墙，F5 Networks 的负载均衡。近些年，这种状态其实已经有所变化。无论是通过自研还是收购，这些美国的头部安全公司，都在快速扩张产品线，在销售上采用“一站式”打法，通过牢固的客户关系，来增加每单位企业用户所能带来的收入。

一站式、全线厂商、同质化竞争，这些之前被用来形容中国安全市场的词汇，现在美国的网络安全市场也一样适用。

无疑，大量全线安全厂商的出现，会因为或多或少的商业竞争关系，让厂商间的合作受到更多限制。对于一些小而美的初创公司，因为全线厂商半垄断的销售模式，（这种现象）对其发展也是有不利影响的。但美国市场的自我修正能力很强，后续是否会延续这个趋势，还有待观察。

再看中国。

中国的本土安全生态，目前学习、追逐的发力点我感觉更多是在资本运作方面对美国的借鉴。从投资，到后续不同轮次的融资以及收购，美国整体的资本运作机制是相对完善的。国内之前确实做的没有那么理想，多数情况下只有上市这条出路。但时至今日，中国国内对于安全初创企业的扶持以及资本运作（比如创业退出、投资回报等）的理解已经更加完善，头部厂商对初创公司的收购案例也变多了，创业环境也更好。

总体来看，双方都在取长补短，完善自身的产业生态。这是一个可以看到的重要观察。当然，5-10年的时间窗还是太短，后续还需要持续跟进。产业层面的趋势如果判断足够准确，对企业自身发展战略的制定也会产生莫大的帮助。

NSFOCUS

参会之路

二十分之十三 | 再回首绿盟科技与 RSA 的安全发展之路

一年一度的RSA会议将于2020年2月24日--28日在旧金山再次起航，在San Francisco Moscone Center South Expo 1735展区，绿盟科技将展示以绿盟智能混合抗DDoS解决方案为主的多款安全研究成果，及《2019年DDoS攻击态势报告——国际版》《2019年网络安全观察--国际版》两部年度报告，与全球安全行业专家一起开拓国际视野，聚焦热点，分享智慧。

绿盟智能混合抗DDoS解决方案是由绿盟抗拒绝服务系统ADS与绿盟Cloud DPS防护服务相配合，形成的本地+云端的混合清洗方案，旨在解决客户出口带宽拥塞防护的安全难点问题。绿盟智能混合抗DDoS解决方案整合了云清洗和本地设备的能力，实现了智能切换流量路线云地联动的整体方案。并且可以根据流量大小和实际攻击情况自动切换，在流量超出本地处理能力时，促使ADS发出呼救信号，将流量牵引到绿盟全球云清洗平台，对付大流量攻击，让云地两端协同作战，真正实现了云地人机的方案结合。

十三载探索与感悟

回顾历年RSA大会主题，自2009年以来RSA每隔3年就会有一个方向上的转变。2009--2011年，加密安全占据主旋律；2012--2014年，业界的发展撬动集体智慧的共享；2015--2017年，安全威胁形势迫使我们做出改变，联合抵御才能及时把握机会。2018--2020年，技术的进步及安全形势让我们认清立即行动才会让网络环境变得更好，而其中关键正是取决于人的因素。

Security Made Smart and Simple

今年，绿盟科技以“Security Made Smart and Simple”为主题，将携绿盟智能混合抗DDoS解决方案、绿盟流量清洗运营系统、绿盟WEB应用安全解决方案、绿盟威胁情报系统等产品及解决方案，以及《2019年DDoS攻击态势报告--国际版》《2019年网络安全观察--国际版》两部年度报告亮相RSA2020展会，与国际业界专家共同关注世界网络安全发展趋势，同时分享对于中国网络安全产业发展的独道见解。更将全面展示绿盟国际云清洗中心，以及绿盟科技自主研发独立运营的云清洗解决方案，更多精彩，敬请期待！

智慧点燃传承之火 · RSA会议的29年

众所周知，RSA会议创始于1991年，发展至今已成功举办了28届，从开始为密码学家收集和分享互联网安全领域最新动态的小型加密会议，发展至全球瞩目的行业盛会，RSA会议无疑是网络安全领域从业人员一年一度趋势探索的良机，互相展示的平台，也是知识共享的纽带。今年的大

会主题是：Human Elements，人的因素。

这不禁让人想起，2014年上映的德国电影《Who Am I - Kein System ist sicher》（我是谁：没有绝对安全的系统）中，主人公的一句话：人类才是最大的安全漏洞。

当我们感叹着“云大物移”、5G等信息技术不断改变着人类生活方式的同时，更应该回归根本，关注这一切的本质是人类文明发展驱动下的科技进步。同样，什么才是防御网络攻击最有效的武器？人类的知识、智慧和创造力才是力挽狂澜的法宝。

我们探索未知，也内观根源与本质。

远渡重洋花开彼岸·绿盟科技与RSA的13年

2008年绿盟科技第一次来到大洋彼岸专程参与RSA会议，白驹过隙，2020年是绿盟科技成立20周年，同时也是伴随着RSA一路成长的第十三个年头。远渡重洋十三载，休戚相关万千情，十三年来绿盟科技持续参与RSA会议，携研究成果及行业观点与国际同仁智慧碰撞，共享新知。西海岸的风再次发出了知识与智慧的邀请，今年绿盟科技再次亮相旧金山，与您共赴这场安全盛会。

参会之路


Holistic Hybrid Security
云安全：Cloud-in-a-box
威胁情报：NTI
DDoS 防御：ADS 及 CloudDPS
Web 应用安全：WAF 及 WVSS
智慧安全 2.0
让安全变得智能而简单
Security Made Smart and Simple
紧跟发展趋势，在云安全服务、物联网安全、工控安全等方面持续发力。
TAM 绿盟全流量威胁分析解决方案
NCSS 绿盟新一代云计算安全解决方案
2015-2017 年
RSA 主题
Change 2015
Connect to Protect 2016
Power of Opportunity 2017
大数据
APT
物联网
云安全
勒索软件
行业安全
NSFOCUS
CHANGE→CONNECT→OPPORTUNITY
智慧安全2.0
智能 · 敏捷 · 可运营


APT 检测和防护
威胁情报
云计算安全
安全大数据分析
人 Expert
机 Device
地 Local/Campus
协同防御，围绕各种安全产品的连接、用户与提供商的连接、安全方案的联动协同防御及安全生态协同的新形势。
2012-2014 年
伟大密码胜于利剑
古腾堡的印刷机
分享 · 学习 · 保护
——利用集体智慧
WEB 安全
APT 攻击
NSFOCUS TAC
WEB 安全解决方案
绿盟威胁解决系统
绿盟解决方案及新产品
在行业安全市场取得了长足发展，厚积薄发
2009-2011 年
RSA 主题
埃德加 · 爱伦坡 2009
罗塞塔石碑虎符(中国) 2010
Alice & Bob 的奇幻冒险 2011
加密
APT
安全
云安全
云计算
NSFOCUS


COMMUNICATION→ENABLE→A PLAN
方案
NSS Labs
产品
展示未来的战略架构
探讨安全发展趋势
分享中国安全产业发展的见解
2008 年
RSA 主题
艾伦 · 麦库森 · 图灵
NSFOCUS
2009 年至今
RSAC 热点研讨会
计算机专委会主办
绿盟科技承办
IDC
Analyze the Future
国际权威分析机构关注绿盟科技的发展
NSFOCUS
关注绿盟科技官方微信公众号
了解 RSA 的实时资讯

现场直击 | 绿盟科技 RSA 2020 展区亮点全揭秘

美国时间2月24日至2月28日，RSA 2020在旧金山 Moscone 中心正式启幕。今年大会以“Human Elements”（即人的因素）为主题，聚焦与“人”相关的元素对网络安全产生的影响。

2020年是 RSA 大会的第29届，也是绿盟科技连续参展的第十三年。今年，绿盟科技以“Security Made Smart and Simple”为主题，携数款绿盟科技国际市场拳头产品及方案，以及两份重量级年度报告亮相RSA 2020展会。绿盟科技凭借在安全产品研发及技术革新方面的多年积淀，持续在国际网络安全市场发出属于中国网络安全企业的声音。

国际市场拳头产品现场一览

在参与此次展会展示的绿盟智能混合抗DDoS解决方案、绿盟流量清洗运营系统、绿盟WEB应用安全解决方案、绿盟威胁情报系统等解决方案的背后，其实是五款国际市场拳头产品历年来的不断迭代升级，他们分别是：绿盟抗DDoS产品、绿盟流量清洗业务运营系统ADBOS、绿盟绿盟国际云清洗中心Cloud DPS、绿盟科技新一代WAF、绿盟科技威胁情报。

下面就跟随绿盟君一起来了解他们吧~

1、绿盟抗DDoS产品

绿盟抗DDoS产品自2002年发布上市以来不断突破、更新，保持产品先进性与市场活力。防护能力贴合业务场景及技术演进方向，推出了威胁情报IP溯源、僵尸主机快速过滤、APP业务自动化定向防护、云地自动清洗互联等功能。在性能上，目前支持单体最大240G防护，后续还将推出更高性能的平台，用于大型防护节点建设。产品形态同时具备硬件和虚拟化两种可选，为与云计算、SDN等前沿方案的融合提供实现基础。此外，产品在方案可扩展性上不断延伸，将单一产品的DDoS检测与清洗能力与平台相结合，孵化出攻击溯源、DDoS运营增值、流量分析等多种方案。产品在满足DDoS防护的同时，通过提供网络优化建议和转变生产力创造实际业务价值，实现资源利用率最大化。深入业务、强化技术，确保了绿盟抗DDoS产品与时俱进的市场定位。

2、绿盟国际云清洗中心Cloud DPS

绿盟国际云清洗中心Cloud DPS（Cloud DDoS Protection Service）旨在为客户提供云端DDoS防护服务，根据攻击量和持续时间灵活调整部署，在全球8个主要数据中心节点，同时可以吸收超过7TB的全球攻击流量。绿盟Cloud DPS不但可以直接在云端直接对DDoS攻击进行防护，而且还解决了客户带宽不足、安全人员缺失、需要投资基础设施建设等一系列问题。不论通过电脑Web还是手机App都可以一键清洗一键查看，帮助客户做到运筹帷幄之中，决胜千里之外。

在2020年，绿盟抗D整合了云清洗和本地设备的能力，实现了智能切换流量路线的云地联动整体方案。云清洗处理超大流量攻击，本地设备处理复

杂应用层攻击，并且流量线路可根据攻击情况自动切换，仅有在流量超出本地处理能力时，ADS才会发出云呼救信号，将流量牵引至云绿盟国际云清洗中心进行清洗，应对大流量攻击这是国内首次实现全自动云地清洗切换。

3、绿盟流量清洗业务运营系统ADBOS

随着传统网络市场和互联网的竞争加剧新，网络服务提供商的“疆土”正在不断收缩，云端服务正在成为网络服务提供商业务转型的主战场。绿盟流量清洗业务运营系统ADBOS是一款基于抗DDoS产品设计的管理、运维及运营的综合平台。通过智能管理、多点拨测，流量调度等方式，使多节点的清洗和检测设备可以进行统一管理及资源调用。迅速准确地对各类DDoS攻击流量进行过滤。给客户提供调度、管理、增值运营等功能，在确保业务可用性的同时给客户带来收益。ADBOS良好的兼容性使得第三方厂家的抗DDoS设备也可以在平台上进行统一调度，统一管理，统一查看。客户可利用手机APP，随时随地了解业务&网络&攻击情况，打通了安全和业务的最后一公里，降低运维复杂度，高效利用时间。

4、绿盟科技新一代WAF

绿盟科技新一代WAF可保护客户Web业务和API安全。通过基于机器学习的智能检测引擎和海量威胁情报赋能，让WAF的检测能力进一步提升，并保护客户免受未知风险。同时新一代WAF具备资产自学习、细粒度策略配置以及策略自优化的专家系统，使得扩容和运维更加轻松。我们不仅是优质产品制造者，也是优秀解决方案提供商，本次也带来了新一代Web安全防护解决方案：大流量背景下的WAF集群方案、对网络“零”影响的插件化部署方案，并可联合专业抗DDos设备，保障Web业务高可用性，结合MSS for WAF远程代维服务，提供完整的WAAP解决方案。

5、绿盟科技威胁情报

绿盟科技威胁情报依托绿盟科技专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力；绿盟科技强大的安全研究团队持续输出大量独特自研情报，综合其它商业情报和开源情报，使得绿盟科技

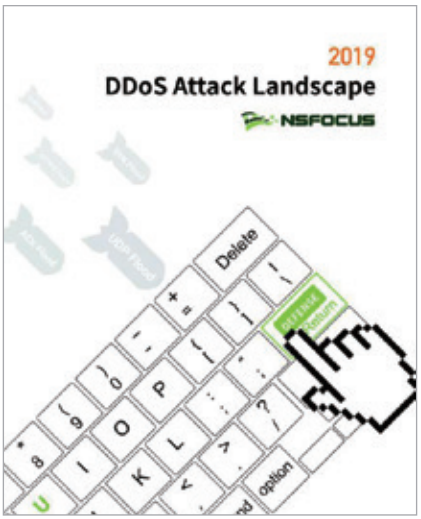
威胁情报具有极大的丰富度和覆盖度；绿盟威胁情报致力于帮助客户增强现有结构安全、被动防御、积极防御体系的防御能力，着力提升威胁预警、安全加固、入侵检测、应急响应等安全过程的准确性、及时性和有效性，帮助用户更好地了解和应对各类网络威胁。

重磅推出两部国际版年度安全报告

此外，展会上绿盟科技还将推出两部重量级年度安全报告：《2019DDoS攻击态势报告--国际版》和《2019 网络安全观察--国际版》。

1、2019年DDoS攻击态势报告

在网络安全事件频发，破坏威力越来越大的当下，如何及早洞察DDoS趋势，了解其攻击手法并做出有效应对，成为人们的焦点。绿盟科技《2019年DDoS攻击态势报告--国际版》即针对当前高发的DDoS攻击态势进行了总结与盘点。

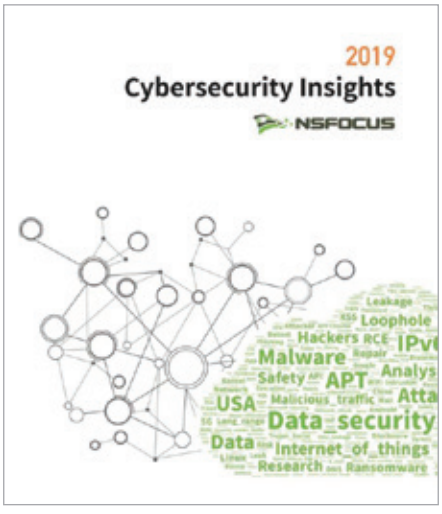


下载链接：

https://nsfocusglobal.com/2019-ddos-attack-landscape-report/

2、2019网络安全观察

绿盟科技《2019网络安全观察--国际版》报告从网络安全战略布局、网络威慑理念的国家级APT明暗争锋、网络空间内容治理、关键信息基础设施保护和个人信息保护等方面进行阐述，覆盖网络空间安全的治理重点、分析已经形成的全产业链布局。



下载链接：

https://nsfocusglobal.com/2019-cybersecurity-insights-report/

为什么绿盟科技要连续十三年参展 RSA 大会？

孟祥聃

650余家企业或机构参展，超过700位演讲者、500场议题分享……这就是2020年的 RSAC。

由 RSA 主办，拥有近30年历史的 RSA 大会（RSAC），作为全球规模最大的网络安全行业会议，一直着眼于推动全球网络安全界的共享、创新与进步。来自全球的领先安全公司或者安全部门高级专家都将齐聚 RSAC，对当下的安全趋势、挑战、解决方案和创新点进行探讨。这使得 RSAC 正逐渐成为一个网络安全从业者分享、学习的圣地，更是安全企业实现快速成长的秀场。

得益于绿盟科技北美分公司的高效协同，绿盟科技本次参展活动并未受到太多疫情的影响。无论是传统活动创新沙盒，还是各种圆桌会议还是业界大咖的主题分享，亦或是展区热火朝天的交流摸底，此次前方不仅收获颇丰，更是借助 RSAC 这样一个平台以及国内外多种传播渠道，向全球发出了拥有近20年积累，属于绿盟科技自己的观点与声音。

今年是绿盟科技连续参展 RSAC 的第十三年。作为一家总部在中国北京，企业规模逾3千人的安全企业，远在美国旧金山的盛会，确实离我们大部

分人有些距离。今年的 RSAC 虽然已经收尾，但相信不少人近期都会心生这样一个疑问：

我们为什么要大投入的参加这样一个远在美国的安全会议？而且还是连续十三年？参展 RSAC 对中国安全企业而言，核心价值在哪里？

有幸，绿盟君采访到了多位现绿盟科技的高管。本篇文章就以不署名的方式，将他们对绿盟科技参展 RSAC 意义的理解整理如下。

从中国安全企业视角谈参展 RSAC 的三大价值

可以说，每年都有大量优秀的安全厂商、业界专家和客户会来到 RSAC，在大会期间分享他们创新的技术方案、优秀的安全体系建设和运营实践，以及前沿的风险治理思路。绿盟科技作为中国的网络安全产品和服务提供商，毫无疑问可以借助RSAC这个舞台，向全球客户针对性的展示我们最具竞争力的产品和方案。

这是一种输出的价值和收获。但除此之外，对参展企业而言还有输入的价值。

从安全企业产品和技术发展的角度，参加 RSAC 对企业战略的指导和验证是有重大价值，而且几乎是其它任何行业会议都无法替代的。这个输入的价值可以概括为三点。

1. 指导企业国际化战略

要阐述这点，就要先简单介绍下此次绿盟科技在 Moscone 中心南厅的展位的设计思路。

我们此次在 RSAC 的现场，主要展示了抗 DDoS 和 Web 安全两方面的产品、方案，以及与之适配的服务——威胁情报和安全研究（2019年 DDoS 攻击态势和网络安全观察两份国际版年度报告）。其中，抗 DDoS 囊括了绿盟科技在这个领域近20年的积累，一套完整度极高的产品和方案。Web 安全则是以绿盟科技在国内有极高市场占有率的 WAF 为代表。

但是，在国内也可以称得上是“全线厂商”的绿盟科技，为什么只选择了这两个技术领域在 RSAC做展示？

主要有四方面考虑：一是这两类产品交付更简单。特别是放到国际视野下，高效的产品交付能力尤为重要。二是相较于漏扫、IDPS 等产品，抗 DDoS 和 WAF 作为互联网基础设施安全层面的防护产品，能够较好地避开一些在采购不同国籍安全供应商时所考虑的一些不成文的敏感区域，也就意味着更容易被国外客户所接受。三是绿盟科技抗 DDoS 产品和囊括多项安全服务的整体方案，能面向客户种类的多样性极强，这也是全球客户非常看重的一个点。四是做出这样的选择，也是基于绿盟科技国际业务运营和参展 RSAC 多年来的经验积累。

所以，对于参展的中国安全企业而言，参展 RSAC 第一个重大输入价值，就是可以指导这家安全公司，产品和方案在国际化时应有的走向，应集中发力的点。

在 RSAC 现场，有更多和潜在的国际客户甚至是国际友商间交流的机会，可以在现场收集到更多真实需求和改进建议，可以看到不同区域性客户在场景上的差异，这份正反馈，可以帮助我们更积极的去修正（国际化的战略），进而持续提升产品和服务在国际市场的竞争力。

2. 商业模式转变的验证

商业模式的转变意味着创新。创新是伴随风险的，所以坚持这份创新需要信心。而信心需要前瞻的视野，以及实践的验证。

可以说，包括绿盟科技自身在内，国内许多安全企业，都在谋求这样一种变革，那就是从之前的产品交付为主，到运营服务交付为主的转变。对企业而言，无论是内部资源的整合，还是客户已有采购思维习惯的渗透和改变，这都是非常大的挑战。

近两年绿盟科技在强调的安全有效性的实战，就是这样一种变革的体现。

以抗 DDoS 这个领域为例，绿盟科技从最开始做的本地流量过滤，到之后覆盖全球的云端的近源清洗，再到去年加入了多点拨测模块帮助用户更好的监测网络链路质量 ADBOS，再到和安全托管服务结合，在云端将抗 DDoS 能力完全服务化、可订阅化，这是绿盟科技对从安全产品到安全运营服务这样一种转变或者进化途径的理解，也是我们当前的前进方向。

反勒索、托管检测与响应等也是类似。一个安全产品和服务如果在设计之初就能更加关注效果而不是手段和过程，把安全效果的闭环、客户测的呈现等问题考虑清楚，产品和服务的价值才能在客户测得到更充分的体现。做到这些，好的产品和服务才有可能在商业性上也脱颖而出。

在 RSAC，基于大量甲方对自身实践的分享，让我们对如何将这种注重安全有效性、从产品交付转变到服务交付的理念，更好的契合甲方自身的信息安全管理实践，有了更深度的思考。同时，了解那些有类似想法，甚至已经成功转型的厂商的心得，对于还在途中的我们，也是一种莫大的鼓舞，和极为有效的经验参考。

所以，参展 RSAC，对增强我们坚持进行这样一个模式转变的信心，验证目前转变的方式方向是否合理，都大有裨益。

3. 对创新的借鉴与学习

创新是企业进步的源动力，对网络安全这样一个重技术、重产品化、重方案的行业而言，更是如此。但创新不等于从零开始。对国外技术应用和方案思路中创新性的学习和理解，是国内安全企业成长的必经之路。这是所有国内安全厂商不用回避，也无法回避，必需勇于承认的事实。

国家网络安全的整体水平可以说和人均 GDP 有着令人惊讶的正相关性。经济上越发达的国家，企业和信息化平均程度越高的国家，安全技术的创新和发展普遍也会越快，他们的网络安全整体水平也会越高。这基本已经是业界共识。

安全的本源是如何用新技术解决老问题。“新技术”，可以是新的安全技术，可以是原有安全技术的一种新的应用。要解决的“老问题”，一定是之前没有解决好的问题，所以要寻求新的“锤子”或者新的思路。闭门造车肯定是不可取的，在坚持自研的基础上，国内安全厂商还需要广泛的去交流、分享，进而借鉴、学习，甚至是投资、收购。

5天时间，650余家参展机构（今年受到疫情影响还比往年少了一些），500场议题分享，2020年的RSAC 又是一场学习的盛宴，RSAC 能够吸引全球安全企业参与的独特魅力也正在于此。全球的领先厂商在这样一场会议中，集中展示、分享他们最新的技术应用成果。在这样一个氛围下，安全企业如何更好的对这些创新点进行借鉴学习，使其能够将全球业界最前沿的成果、趋势和自家对产品和服务进行打磨，更契合的融为一体，这是至关重要的。而且如果能够做好这点，无疑对企业加快应用新技术的速度，以及提升安全产品效能都有极大益处。

此外，RSAC 延续多年、更聚焦创业的特色活动——创新沙盒，无论是对于追求“小而美”的安全初创，

还是已有大体量但寻求更多更具有商业前景创新方向的头部厂商，都具备很高的分析和参考价值。

如果把安全行业的创新划分为两个维度：攻防技术的创新与行业的创新，那么从今年入选创新沙盒决赛10强公司的产品，我们可以看到，今年攻防的创新点聚焦在模糊测试、响应以及人工智能落地；而行业的创新则集中在敏捷开发、数据安全等热点领域。同时，我们还可以看到，自动化已经成为了众多安全公司的产品兼具的特点，甚至贯穿安全活动始终。究其原因，是因为安全运营正面临更规模化、复杂化的挑战。通过自动化提升整体的安全防护效率，目前来看是一种较为行之有效的方式。

当然，无论是攻防技术创新还是行业创新，其最终目标还是解决用户面临的安全问题。今年 SECURITI.ai之所以能够夺冠，其根本原因也在于此。有着近二十年积累的绿盟科技，也始终秉承着以客户需求、合法合规为指引，不断更新客户化的行业安全解决方案，并通过安全产品和安全运营服务实现落地。

当今，国内网络安全行业的创新一直在前行，中国的网络安全整体水平也正稳步提升。所以， 对中国安全企业而言，对 RSAC 上所谈及的创新性更多还是要抱着了解、学习的态度，而不应是模仿和搬运；真正落地自家产品和服务，落地国内的客户和场景，还需厂商结合自身的积累和客观国情，为客户提供安全、合规、友好的产品和服务，才是我们的立足之本和发展之路。

NSFOCUS

闪亮 RSA

绿盟新一代 WAF，究竟有什么不一样?

2020年的RSA大会将于当地时间2月24日至28日在美国旧金山举行。时至今日，大会已成功召开了28届，最早一届可追溯到1991年，可谓是网络安全圈的年度盛会。上一届大会的主题为“Better”，意为伴随安全技术不断创新与发展，使世界变得更加美好。今年大会主题则为“HUMAN ELEMENT”，将安全的注意力转移到人类自身。无论在开发、管理还是决策环节，人都起着至关重要的作用，安全问题也伴随其中。

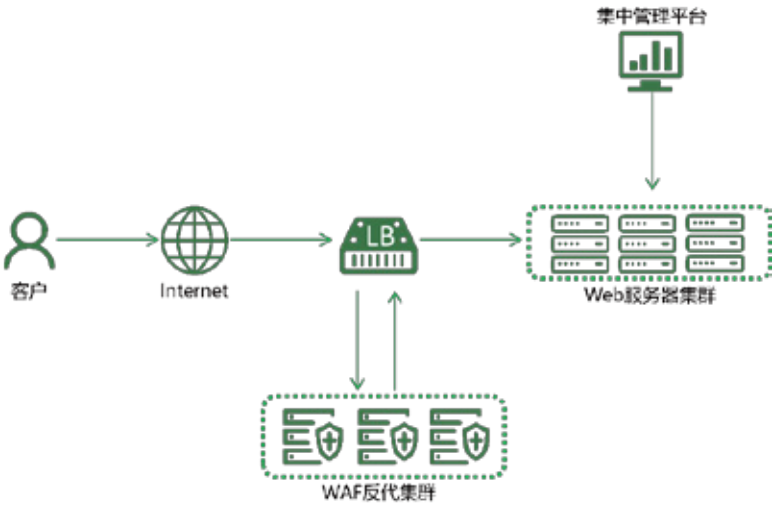
应用安全仍是本次大会的焦点。绿盟科技在Web安全领域深耕多年，并在IDC发布的《IDC MarketScape: 中国Web应用安全市场2019年厂商评估》报告中，被评为中国Web 应用安全市场战略性第一。在今年的展会上，绿盟科技将带来新一代WAF（以下简称WAF），它到底有哪些新特性？让绿盟君带大家先睹为快吧。

专攻术业 · 专利级机器学习检测引擎

WAF引入基于机器学习算法（专利：CN105187408A）的智能检测引擎，在成熟的细粒度规则防护体系基础上，可进一步提升WAF检测精度，降低误报率和漏报率。

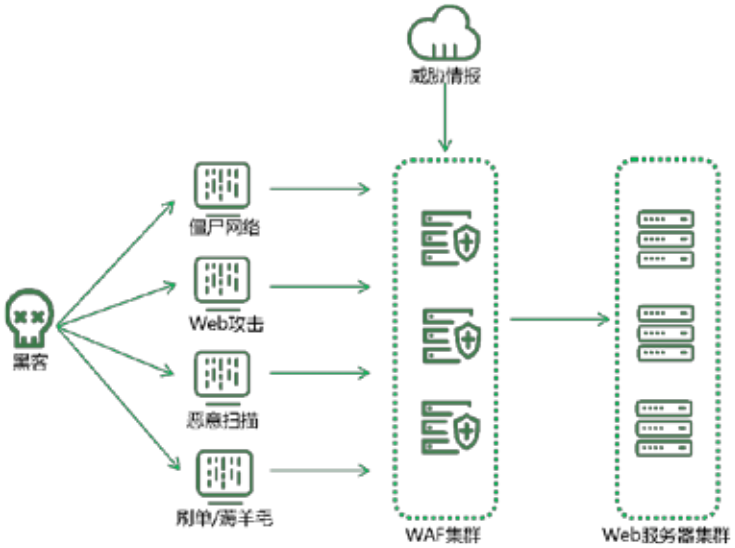
多管齐下 · 集群部署解决方案

WAF支持集群部署，通过与客户现有负载均衡设备进行无缝对接，当新业务上线及旧业务扩容时无需断网（可随时割接），并满足在报障应急时快速切走流量，对业务无影响，满足高可用性、高可靠性要求。并可通过集中管理平台实现对批量WAF接入、策略集中下发、状态集中监控等。



耳聪目明 · 海量威胁情报赋能

WAF可与具有42亿全球IP资产的绿盟威胁情报中心对接，从而实时获取丰富的高危信誉IP，在WAF上自动生成防护策略。通过启用IP信誉功能，可有效防止撞库、羊毛党（刷单、刷积分）的问题，同时有效减少疑似攻击行为的告警噪音，达到提升告警精度的效果。



防患于未然 · API安全防护

越来越多的产品选择开放API接口，以更加开放的心态去扩展生态，提升自身的影响与商业价值。便利的同时，也给黑客带来了新的机会，不得不说API防护未来会是一个新的挑战。着眼于未来，绿盟科技WAF目前已具备API安全防护能力，可保障客户XML、JSON、REST等安全使用。

本次大会另一个值得关注的主题仍是DevSecOps，针对开源代码的安全、开发生命周期和框架的安全也提出了新的需求。在“人为因素”的影响下，如何能保证业务开发的全生命周期安全，确保可以快速上线呢？绿盟科技同时带来了基于Web安全层面的闭环解决方案。

在2019年，绿盟科技推出了代码审计系统（简称：SDA），该系统可集成到软件生命周期（SLC）的toolchain中，并且可以和WAF进行联动，实现从源头保

障用户Web业务安全。

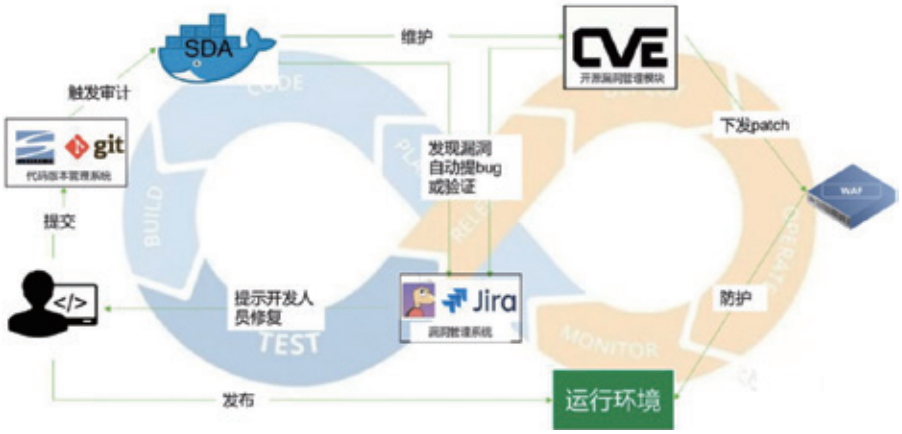
◆ 客户收益：

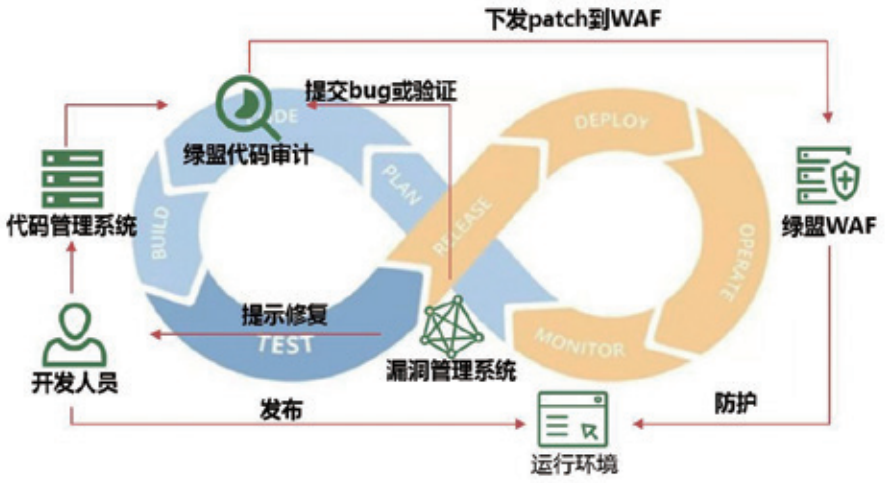
客户可通过SDA识别开发项目中的开源组件漏洞与基础信息（编程语言、数据库）等，并做到随时可查

WAF通过项目基础信息调整防护策略，SDA给WAF下发patch自动防护线上的开源代码漏洞

当有新的开源0DAY漏洞爆出时，SDA可查询到受影响的项目，并通过WAF进行防护

客户可使用SDA对新业务上线前进行扫描，可识别出因代码缺陷而导致的漏洞，并将其结果同步到WAF，可满足新业务快速上线需求

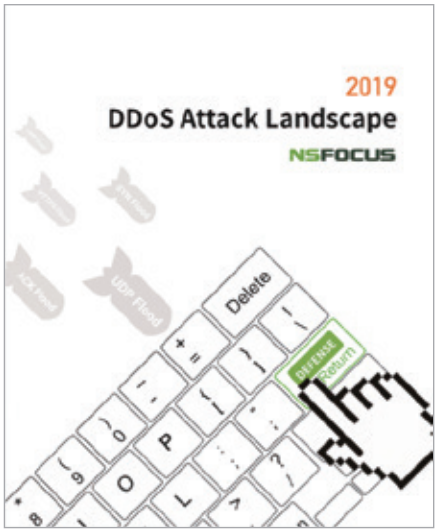




绿盟威胁情报交出这样一份“成绩单”

威胁情报已连续多年在RSA上受到业界关注，今年也不例外，威胁情报依旧是RSA2020十大网络安全热词之一。根据RSA2020趋势报告，安全人员同样关注分享情报的价值。许多议题在谈到人是安全要素时，特别指出了威胁情报和共享的力量，也提到自动化本身的弱点和存在的挑战，同时认识到要应对机器学习存在弱点和挑战，需要不断提高安全团队的技能。威胁情报依赖于信任，尽管人工智能具有提供信息的潜力，但人与自动化之间还是需要保持良好的平衡。

长期以来，绿盟科技威胁情报团队聚焦安全态势和热点，全面观测网络空间安全局势，进行安全预测与布局。2020年，绿盟科技威胁情报团队携两部重量级年度安全报告——《2019 DDoS Attack Landscape》和《2019 Cybersecurity Insights》再次亮相RSA峰会。



绿盟威胁情报中心（NSFOCUS Threat Intelligence center, NTI）依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察

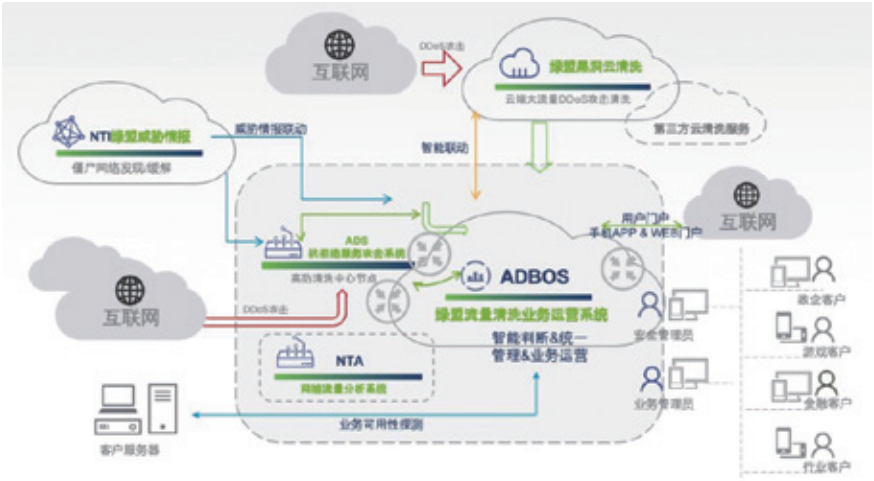
和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

客户价值

借助绿盟威胁情报中心的威胁情报能力支撑，客户可以洞悉互联网资产暴露分布情况及安全现状，获知情报来对安全威胁进行准确预警，了解最新的热点事件动态，使用情报对接能力使安全设备及平台能积极主动的防御攻击，结合安全情报数据的深度分析，全面掌握安全威胁态势并准确地进行威胁追踪和攻击溯源。

2019年，绿盟威胁情报中心监控的攻击源数量1412万，总攻击次数11486万次，其中7%的惯犯承担了78%的攻击事件。对于这一少部分高危IP，通过威胁情报为安全设备/安全平台赋能，我们能够直接阻断他们的网络活动，这可以大量减少企业日常安全运营的负担。对这些网络惯犯的针对性跟踪、分析、画像和对抗，已经成为了绿盟威胁情报（NTI）的重要能力之一。这也是一种威胁情报的重要实际应用方向。

今年绿盟科技在RSAC参展的产品ADBOS（流量清洗业务运营系统），就是威胁情报为安全产品赋能最好的例子之一。ADBOS借助绿盟威胁情报收集的海量IP信誉情报源在收到攻击前研判威胁、预置防御策略、主动规避威胁；事中，结合威胁情报和持续监控，可以实时感知威胁发展态势，以便及时调整防御策略、快速响应；事后，通过ADBOS收到的攻击数据，绿盟科技威胁情报中心亦可以支撑对攻击行为和攻击者进行全面的追溯、取证和反制。丰富、独特、准确的绿盟威胁情报极大地增强产品的检测及防护能力，显著降低威胁发现和威胁处置时间。有效和及时的情报应用，使威胁情报数据发挥出更大的价值，帮助客户建造更加坚实的安全壁垒。



产品荣誉：

- (2017年2月) 获RSA 2017“Hot product”

  IDG旗下国际权威媒体Network World网站收录了RSA 2017 中展示的48款热点产品。绿盟威胁情报中心（NTI）凭借自身优势成为48款热点产品中，唯一入选的“中国造”。
- (2018年8月) 荣获CNCERT“2018年网络安全创新产品(技术)”称号

  国家互联网应急中心（简称CNCERT）重点考察参选产品（技术）的实用性、创新性以及先进性，在来自56家单位提交的83份申报材料中，绿盟威胁情报表现优异，脱颖而出，斩获“2018年网络安全创新产品（技术）”称号。
- (2018年12月) 被IDC列入领导者象限

  IDC发布《中国威胁情报安全服务（TISS）市场，2018年厂商评估》报告，绿盟科技凭借自身实力，在威胁情报领域的销量、能力、战略三方面均名列前茅，被列入领导者象限。
- (2019年5月) NTI云沙箱(POMA)成为VirusTotal官方合作产品

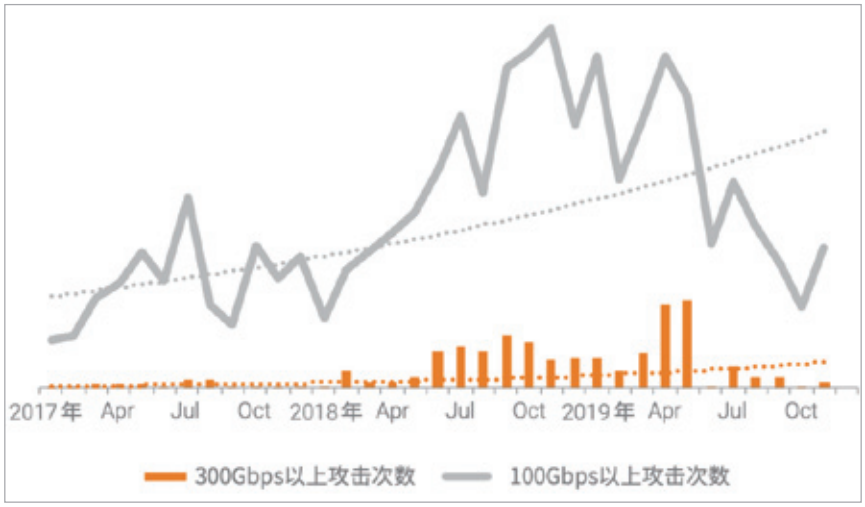
  2019年5月7日，VirusTotal发表正式声明，绿盟科技云沙箱（POMA）成为VirusTotal的官方合作产品，旨在可疑文件分析领域强强联合，为客户提供更好的服务。截止目前，VirusTotal的沙箱合作伙伴，全球仅有七家。
- (2019年5月) 绿盟威胁情报平台荣获2019数博会领先科技成果

  2019数博会面向全球征集了大数据领先科技成果，经过相关领域权威专家的严格评选，绿盟威胁情报平台最终斩获2019领先科技成果“优秀项目”。

绿盟抗 DDoS 方案更新四个重要内容

2月24日-28日，网络安全行业盛会RSA Conference在旧金山拉开帷幕。绿盟抗DDoS方案作为RSA的“常客”，不断提升技术的先进性和方案的扩展性，在Frost & Sullivan发布《DDoS市场分析报告》中，连续五年排名中国区抗DDoS产品市场第一。大会现场，绿盟抗DDoS方案结合业务和攻击发展趋势发布了产品最新动态。

在绿盟科技发布的《2019 DDoS攻击态势报告》中表明，2019全年监控到的DDoS攻击事件超过16.74万次，比2018年增长了30.2%，其中300G以上的大规模DDoS攻击约3000次，最高峰值达到885G，比2018年多了200多次。可见，DDoS攻击的热度并没有消退，并且在流量规模和数量分布上不断突破，持续危害业务安全。



在大流量DDoS攻击事件频发的当下，中小企业难以独自抵御，需要依靠云清洗服务来应对大流量DDoS的倾轧，而如何将本地防护与云清洗进行资源联动，实现自动高效的清洗是DDoS防护不得不解决的难题。另外，大型客户寻求业务转型，纷纷打造DDoS增值服务，产生了批量运营和服务交付的场景需求。云计算、SDN等新技术领域在业务发展的同时也对DDoS防护提出了要求。

在本次RSA展会上，绿盟抗DDoS产品主要发布了云地自动互联、虚拟化产品发布、可视化快速运营以及APP精细防护四大内容更新。

一、云地自动互联，实现“最潮”高端操作

云地混合防护是全球DDoS防护的热点话题之一。虽然云清洗近年来蓬勃发展，本地防护也早已屡见不鲜，但是将两者进行动态结合，实现自动化快速联动依然是个行业难题。一方面云清洗服务提供商大多不具备本地防护可交付的产品，另一方面传统产品提供商面对打造云清洗节点的巨大投入望而却步，而通过使用第三方产品或服务与自身方案融合，难以实现自动化及快速收敛。诸多障碍限制了云地自动互联方案的落地。

绿盟抗DDoS最新解决方案实现了云地自动互联的清洗能力。地端使用ADS等产品进行攻击防护，并支持在界面配置云清洗的启用阈值。当本地流量超过该阈值后，自动引流上云进行防护，当流量低于下云的阈值时再自动切换回本地。联动切换通过调整预配的引流策略的优先级来实现，大幅减少收敛时间，实现了自动化和高效性的结合。云端清洗资源包含自建节点与合作节点，可以覆盖全球的业务防护需求。

二、虚拟化产品发布，让安全更“轻盈”

绿盟科技经典的抗DDoS解决方案主要包含检测系统NTA、防护系统ADS和管理系统ADS M，继NTA和ADS M率先完成虚拟化之后，ADS发布了其虚拟化的产品形态。虚拟化ADS在防护功能上与硬件型号保持一致，但其产品形态丰富了方案的灵活性。与传统方案对比，产品更加轻量化，帮助小型客户快速部署；在新型方案趋势下，为与云计算等场景的融合提供了可行的基础。

三、可视化快速运营，让威胁一目了然

从近年的数据来看，DDoS增值服务迅猛发展，清洗节点不断扩容，客户数量倍数增长。在此情况下，服务提供者面临着多用户管理、业务统一监控、服务交付等挑战，简化运维和批量运营成为业务开展的关键。绿盟科技在前两年已经推出了DDoS增值运营平台，实现多用户场景下的订单管理、计费统计、清洗资源调度以及自助Portal等功能。而在新的方案中，绿盟科技还增强了攻击事件清洗监控的能力。在全面展示各业务安全状态的同时，支持对某一客户或某一业务遭受的DDoS攻击情况进行详细挖掘，将防护流程和策略可视化，帮助运维人员验证策略生效情况、快速判断策略合理性、掌握清洗力度。通过将防护过程透明化，简化运维消耗，快速响应防护，提高服务交付标准。

四、APP业务防护，灵活精准持续护航

精确的DDoS防护是产品核心价值的体现。攻击者通过恶意下载APP薅客户羊毛、通过PC和APP发起混合DDoS攻击，造成攻击防护难度加大。由于APP和PC的开发框架不同，而两者经常共享同一服务主机，就会出现防护策略无法灵活调整的困境。绿盟最新版本抗DDoS产品可通过自动化区分访问源，为APP和PC的访问提供差异化防护算法，策略灵活性强，防护精准度高，确保了业务的连续性。

闪亮 RSA，绿盟 Cloud DPS 打开云端 DDoS 防护正确方式

美国时间2月24日--28日，一年一度的RSA会议于旧金山举行，绿盟科技作为拥有二十年经验的安全服务厂商再度参展。

大会现场，绿盟科技重点介绍了绿盟国际云清洗中心Cloud DPS（DDoS Protection Service），获得了与会人士的广泛关注。

绿盟国际云清洗中心Cloud DPS（DDoS Protection Service，以下简称绿盟 Cloud DPS）致力于为用户提供云端DDoS防护服务，攻克关键技术问题，整合云清洗和本地设备的能力，实现全自动的云地清洗切换，这是国内产品首次实现全自动云地清洗切换。

一键防护，全球海量攻击

绿盟Cloud DPS旨在最大程度上的为用户提供云端DDoS防护服务，根据攻击量和持续时间灵活调整部署，在全球8个主要数据中心节点，同时可以吸收超过7TB的全球攻击流量。绿盟Cloud DPS不但可以直接在云端直接防护DDoS攻击，而且还解决了用户带宽不足、安全人员缺失、基础设施建设投资需要等一系列问题。让用户不论通过电脑Web还是手机App都可以一键清洗、一键查看，防护无忧。

云地协同，轻松应对大流量攻击

绿盟Cloud DPS清洗主要服务于超大流量的云端清洗，不仅为小型企业用户解决大流量攻击的问题，同时也为一些在本地拥有抗DDoS设备的企业提供服务，作为本地清洗的备援服务，是应对大流量攻击的关键手段。帮助用户突破本地清洗方案的局限，以最小的经济投入应对大流量DDoS攻击。绿盟

Cloud DPS清洗服务和本地ADS组成立体的抗DDoS防御体系，形成了绿盟智能混合抗DDoS解决方案，该方案通过云端和本地的混合清洗方式帮助用户有效缓解当前的DDoS攻击。

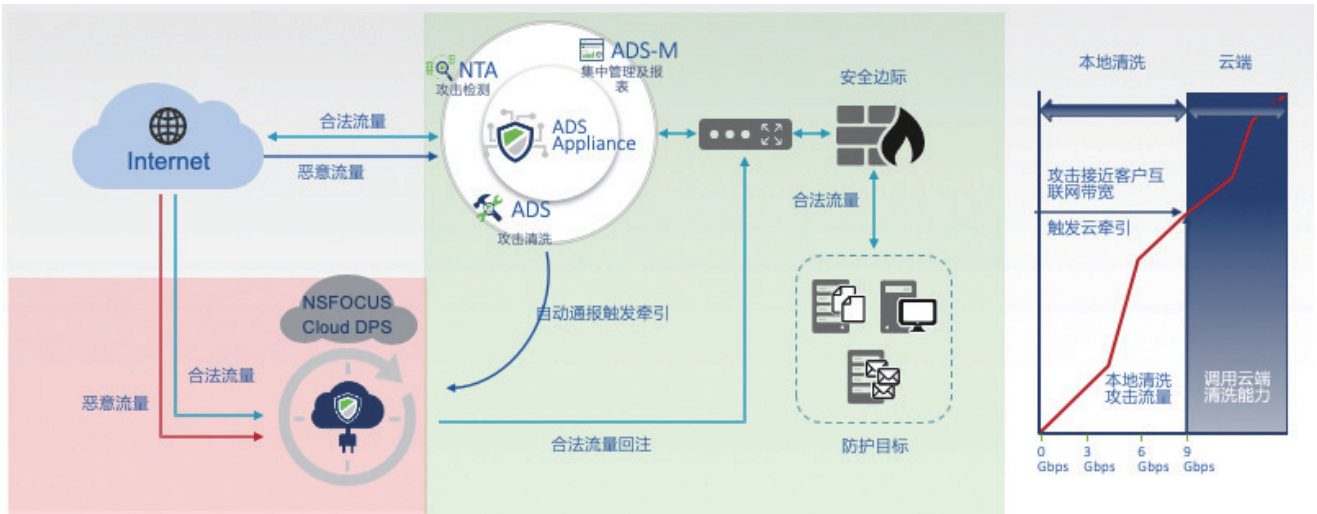
双层“精洗”，让DDoS攻击“无功而返”

根据绿盟科技20年的安全服务经验，DDoS攻击大多以应用层攻击为主，占所遇攻击数量的80%以上，本地清洗设备ADS可有效应对中小规模流量攻击，同时可以辅以提供MSS服务（安全托管服务），让用户无需操心安全运维工作。

绿盟 Cloud DPS突破本地清洗的带宽局限，可以抵御流量超过T级的大流量DDoS攻击，用户再也不用担心本地出口被攻击恶意堵死而束手无策。绿盟科技在国际市场根据用户分布，部署了多个不同的高防中心，随后又根据用户网络流量的变化和转移将高防中心的链路打通，最终形成了现在可以进行多地联动，近源清洗的防护体系。可以有效应对大流量和应用层混合攻击，让用户无论遭遇何种DDoS攻击都可以高枕无忧。用户遇到小流量复杂应用层攻击或脉冲攻击时，直接通过本地ADS进行清洗。遇到大流量攻击时，联动绿盟Cloud DPS清洗服务，生效速度快，通过云清洗服务的粗粒度过滤，清洗掉绝大部分攻击流量，剩下的“漏网之鱼”通过ADS的细粒度防御算法进行过滤。再复杂的组合型DDoS攻击都将无功而返。

近源清洗，全行业覆盖

通过Anycast技术，绿盟科技在全球实现近源清洗DDoS攻击流量，提供优质网络链路，时延低。不分攻击类型全面防护，提供4-7层DDoS攻击全面清洗。移植绿盟科技多年抗DDoS防护技术，高效清洗网络层攻击，并有专利防护算法保障业务连接性，同时提供多种应用层专利防护算法，可有效的处理各种复杂的混合攻击。保障游戏不掉线，业务时延低。针对政府，游戏、金融、医疗，能源、互联网、电商、通信、中小企业，每个行业进行细分，提供多种独立解决方案，保障不同客户的不同业务。与此同时，绿盟科技基于丰富的安全服务、产品研发以及技术探索经验，建立了一支反应速度快，技术能力好，应变能力强的安全运营团队。可以在短时间内给帮助用户解决



DDoS攻击问题，全天候监控保证用户业务可用性。

三零三真，体验抗D实力派

绿盟国际云清洗中心Cloud DPS具有以下优势：

1、零部署，交付简单，在线实施。需要清洗时享受一键清洗服务，事后在线随时查看清洗报表，对攻击及其清洗情况了如指掌。

2、零运维，绿盟SOC团队提供7*24小时运营运维服务，随时随地监控业务流量。

3、零等待，遇到大流量攻击，通过路由协议对IP地址进行牵引并清洗，秒级响应。

4、真安全，清洗业务可以在只有大流量攻击时才牵引，大部分时间流量只过本地，流量仍然在用户的有效掌控之中，而不必担心自身业务的安全私密性。

5、真智能，本地清洗时，本地清洗设备ADS进行实时检测和清洗。当攻击流量超过本地设备设置阈值后，本地设备ADS自动联动云清洗中心进行Cloud DPS清洗服务。

6、真划算，基于DDoS攻击历史统计数据，10G以上大流量攻击仅占全部攻击的50%以内，推出灵活的按次清洗服务，避免用户承担昂贵的包月或包年的云清洗服务。用户根据自身遭受的攻击情况，可灵活购买服务，将服务利用率最大化。

智能云呼救，“云地人机”四维一体全面抗D

2020年，绿盟科技抗D整合了云清洗和本地设备的能力，实现了智能切换流量路线的云地联动整体方案。并且可以根据流量大小和实际攻击情况自动切换，在流量超出本地处理能力时，ADS才会发出呼救信号，将流量牵引上云清洗，对付大流量攻击，让云地两端协同作战，真正的实现了云地人机的方案结合。既能最大程度上的保障客户业务流量的安全性和私密性，又能在真正大流量攻击到来的时候保障客户的业务的可靠性，在云端部署防护服务，一键呼救，秒级牵引真正做到零延迟的智能防护。绿盟ADS和绿盟Cloud DPS在线防御的强强联合消除了针对用户和基础设施的所有DDoS攻击。这一组合使服务提供商能够双管齐下以适当的投入保障用户业务的健康运行。

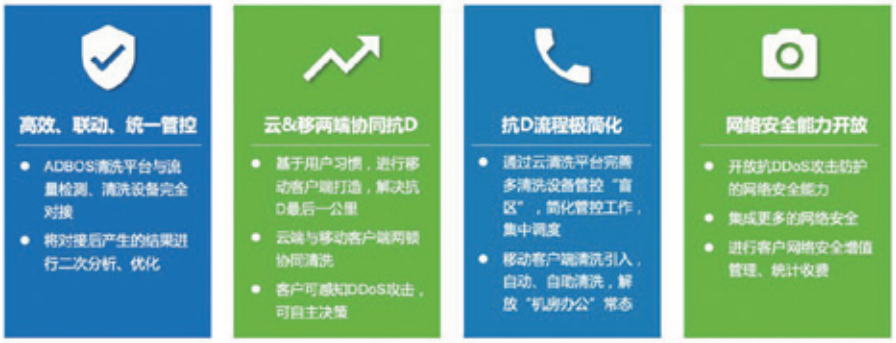
正如今年RSA的主题一样“Human Element”，DDoS攻击可谓是最古老最容易人为造成的一种安全事件，绿盟科技也在不断的探索怎么才能更有效的对DDoS攻击进行防护，利用人类行为分析找出部署薄弱点进行防护，利用情报（Threat Intelligence）利用威胁情报和共享的力量来做攻击前的防护部署，利用自学习功能更智能的完善安全策略Security S Strategy，这些都是我们的探索的方向。让我们在不断的探索行进过程中，使得DPS进化的更加强大。

RSA 2020 | 还在担心 DDOS 运营？绿盟 ADBOS 带你玩转 SOC

不断加剧的互联网市场竞争，使得网络服务提供商企业告别了用户高速增长的黄金时代。随着整个网络带宽的提速降价，数据流量增长和网络服务提供商的增收不成比例。在新兴的互联网领域，网络服务提供商的产业链控制优势已不复存在。阿里云、腾讯云等新兴互联网巨头通过提供具有DDoS防护的云上主机和带宽租用，吸引着市场上大量的残余客户资源。此外，一系列监管方面的挑战使得网络服务提供商的传统业务“疆土”也在不断收缩。

但在数字化变革的大潮中，网络服务提供商的传统优势遭到侵袭和面临转型压力的同时，也面临着变革带来的新机遇。如新增的市场规模非常可观，有望匹敌传统电信服务市场。国内网络服务提供商的当务之急是积极寻找新增市场，从单纯卖带宽向数字化增值服务转型。云清洗服务市场正在成为网络服务提供商业务数字化转型的主战场之一。

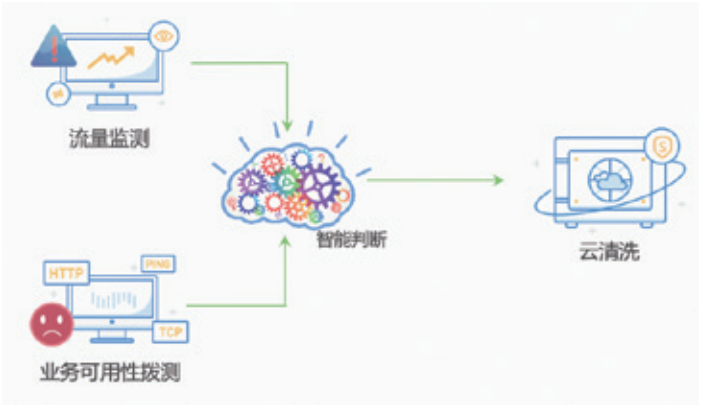
开拓服务市场，运营平台就是不可或缺的服务工具，绿盟流量清洗业务运营系统ADBOS在这个契机下应运而生。绿盟流量清洗业务运营系统ADBOS（Anti-DDOS Business Operation System）是一款专业的、基于抗DDoS产品设计的管理、运维及运营综合平台，通过智能管理、多点拨测，流量调度等方式，使部署在不同地方的流量清洗设备和检测设备可以进行统一管理及资源调用。并且，ADBOS能迅速准确地对各类DDoS攻击流量进行过滤，利用各个节点设备，展示并处置不同厂商的抗D设备，通过丰富的功能，给客户提供流量调度、运维管理、运营增值等功能，同时确保正常业务的可用性和客户的增值收益。配合云清洗开发的手机APP，帮助客户随时随地了解业务情况、网络情况，打通安全和业务件的最后一公里，有效地降低了运维复杂度，高效利用时间。



为了能够满足市场需求的多样性、更好地适应全球市场的不断变化、真正地解决客户痛点，ADBOS作为产品的设计理念核心围绕以下几项关键特性：

◆ 智能

业务检测为客户提供实时“心电图”，云流量检测则为客户提供实时的流量趋势图及异常告警信息。业务检测+云流量检测双重保障攻击智能检测的准确率。在多重智能监测下，可以保证清洗节点的优化利用，一旦判断自动进行流量调度，无需人员干预。客户也可以选择自助清洗进行一键调度指令下达，流量会根据指令进行智能调度。



◆ 敏捷

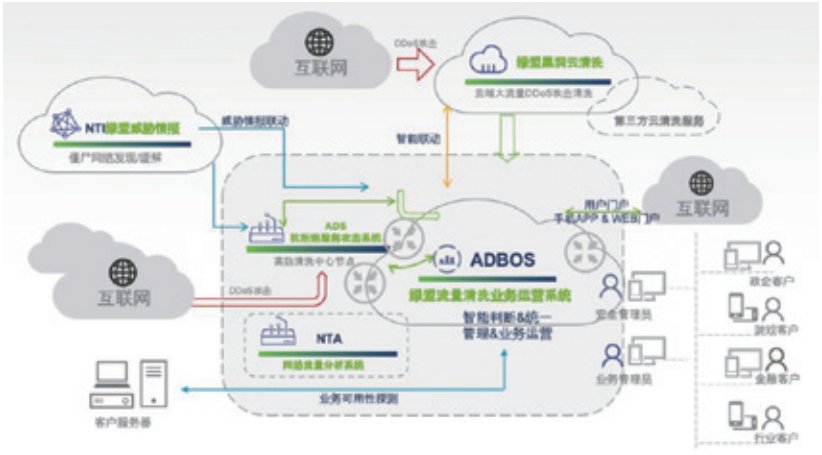
绿盟流量清洗业务运营系统ADBOS提供多样化的自助服务形式，不仅提供传统的Web Portal形式的自助服务，而且提供移动终端App形式的自助服务，方便预警消息推送、运维，提高用户感知与运维效率。主动防御，达到攻击防护“秒级”响应。客户可通过移动终端便捷获取实时信息。

◆ 可运营

ADBOS的服务可视化能力可以降低维护的工作量，实现云清洗业务大规模推广。通过对流量监控和清洗的统一管控、可视化展示、业务开通、统计报表等集中安全运营能力，实现云端统一管控。同时通过多种计费模式，极大的提升了运营&增值的关联性。

一、ADBOS的抗D智慧安全防御体系

云清洗中心不是孤岛，它与云端情报系统、安全专家、客户及设备紧密协同。绿盟提出的“云地人机”体系，做到了“云”中有“人”、有“机”。当云端监控DDoS攻击态势感知平台的安全专家发现有DDoS攻击苗头时，会及时联动相关的抗D系统采取有效的防御策略。本地清洗中心的驻场安全专家或工程师获取到攻击情报或发现攻击后，也可以通过本地的抗D系统采取有效的防御策略。实现真正的云地人机的完美配合。



匹配RSA的热点关键词“SOC”来看，ADBOS也正好符合了市场的期许。ADBOS将安全能力嵌入到系统中。把SOC和用户需要用到的产品和服务交付做到“简单”，除了部署更简易、运维便捷、响应自动化程度更高外，还从客户角度，强调能更容易感知到安全的有效性。结合ADBOS平台上线部署具备短周期、优体验、高适配、高契合、轻型化的特点，能够在短期内快速部署上线，并且实现了安卓、IOS、Windows多平台协同。数据接口适配绝大多数抗D设备，契合当前安全能力增值趋势，节约企业自身运营人力成本，可以为各类用户提供低成本、高效率的抗D防护。不仅为网络服务提供商行业抗D能力快速商业化提供了解决方案，在金融、互联网等规模部署流量清洗设备的行业也可进行推广。

二、精准、智能、便携、个性化缺一不可

前瞻性SOC团队正在转向智能安全运营，以使安全操作现代化、自动化、可视化为目的，并利用不断增长的数据量来检测和响应网络威胁。在适应市场、满足需求、解决痛点的同时，ADBOS也在不断快速迭代和进化。致力于在精准度、智能化、移动互联、云适配等方面进行深耕。

1、为进一步降低误报，DDoS监测与防护平台还采用业内先进的基于业务状态与流量监测告警双重结合、智能判断的自动清洗方式，通过不同类型告警权重，综合智能判断分析后进行告警，从而解决单一探测误报导致的乱牵引、分钟级拨测周期、多种协议探测（包括HTTP/HTTPS、TCP、ICMP、DNS）的问题，避免影响客户业务，提高服务质量与运维效率。

2、DDoS监测与防护平台针对移动网络中客户众多、对DDoS防护需求不同的特点，为了降低运维的成本，使用探针对防护对象中各种服务的流量进行自动学习，并根据学习的结果生成防护策略。

3、针对移动互联网时代的普及和移动互联办公化影响，ADBOS采用了移动互联协同安全防护，通过移动终端实时业务可用性监控、感知DDoS攻击态势、牵引防护策略下发、客户业务启停等功能，更加人性化、便捷化的随时随地抗D。

4、DDoS监测与防护平台提供本地防护产品云化，在云端为每个客户独立提供一套流量监测、流量清洗、拨测系统，可按需进行弹性扩大清洗需求、轻松实现抗D需求。

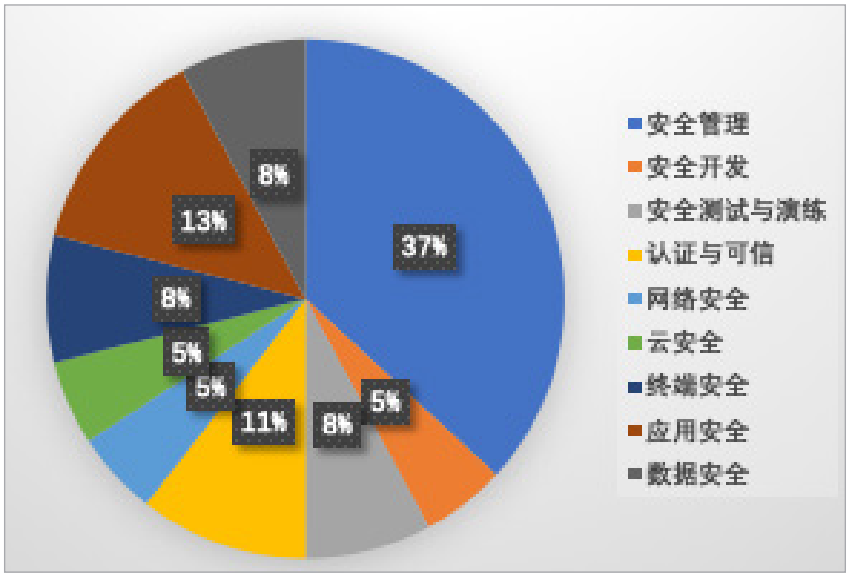
三、过亿威胁情报源，助力运营

在市场需要智能运营的今天，安全运营中心SOC，可以使用ADBOS借助绿盟威胁情报收集的海量IP信誉情报源在收到攻击前研判威胁、预置防御策略、主动规避威胁；事中，攻击情报能及时通过ADBOS下发到ADS，增强防御能力，同时结合威胁情报和持续监控，可以实时感知威胁发展态势，以便及时调整防御策略、快速响应；事后，ADBOS收到的攻击数据，通过威胁情报提供的亦可以支撑对攻击行为和攻击者进行全面的追溯、取证和反制。

绿盟科技作为国内网络安全厂商，拥有品质一流的抗D产品、强大的清洗中心运维平台、完整有效的抗D方案以及安全专家和运营经验，愿意与网络服务提供商开展双赢合作，协助其通过业务和技术的不断创新，在云清洗市场完成增值业务、智能运营的华丽绽放。

RSA 2020 新品调研：解密改善安全运营效能的“法宝”

RSA 2020在旧金山落下帷幕。大会期间共有41家安全厂商发布了新产品，涉及安全安全管理、威胁情报、安全开发、安全演练与测试、安全认证与可信环境、网络安全、云安全、应用安全、终端安全和数据安全11个领域，基本上覆盖了企业网络安全所有需求。其中安全管理类产品、服务和平台共计14款，占比37%，是技术和产品演进速度最快的一个领域。



2020年RSA大会发布新品分布情况

接下来绿盟君将以安全运营的视角，盘点、总结下新产品和服务，看看它们可以帮助企业解决哪些问题，带来什么样的变化。

RSA 2020大会期间发布的新产品主要有两个特征：第一，过去两年在大会上的热点产品与技术已趋于成熟，例如SOAR、MDR服务、MSS服务；第二，传统的产品和技术在进一步演进和更新，例如具备可信验证功能的认证产品与技术，攻击模拟和靶场技术与安全管理平台。

企业和机构在构建和完善安全运营体系可以考虑：

第1，对于已经趋于成熟产品与技术，企业和机构可以考虑大规模引入到企业的安全运营体系，例如SOAR、MDR服务、MSS服务。

第2，考虑对一些传统设备进行升级和替代，引入或扩展新的安全机制和

能力。例如采用具备可信验证功能的产品替换单纯的认证，引入靶场和攻击模拟技术实现安全运营体系的验证和评估。

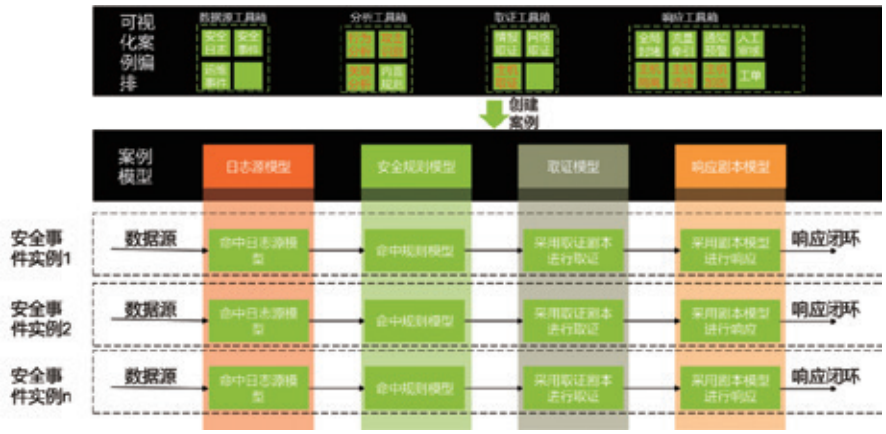
一、安全管理类

1、SOAR

SOAR仍然是此次在大会议题中的热点。会议期间，知名厂商CISCO和Palo Alto都发布和更新了SOAR产品，此次发布的新品可以SIEM及威胁情报相互集成和融合，标志着SOAR技术已经融入安全技术体系。

SOAR技术可以帮助用户逐步实现安全响应的自动化、流程化，用户可以根据已有的应急响应预案结合自身网络环境及安全设备，预先设置威胁处置和事件处置的剧本（Playbook），将威胁和安全事件响应周期缩短到至准实时成程度。

SOAR的部署和实施将极大提升用户安全攻防与对抗能力，一方面它可以将威胁监测与研判人员的精力从数量庞大常见攻击行为工作中释放出来，集中精力处置没有预案的高危行为。另外一方面，SOAR的实施也将大幅提升攻击者探测、攻击、进一步渗透等环节时间成本和曝光率，对攻击行为起到震慑和压制作用。



图：SOAR实现架构图

2、威胁自动化分析与研判

飞塔发布的FortiAI是一个独立的产品，FortiAI主要应用于威胁和可疑事件的分析研判阶段，通过自动化分析和研判，大幅度提升可疑事件的分析研判速度。在攻防演练和对抗中，此类技术可以大幅提升威胁分析师的分析效率和分析能力，确保分析能力不会成为对抗的瓶颈。

FortiAI采用自学习的深度神经网络（DNN）技术，并且作为一个独立的产品发布，也一定程度上反映了大数据分析和机器学习技术在威胁分析领域的应用已经逐步成熟。

图：威胁自动化分析与研判的应用

3、靶场技术与攻防演练

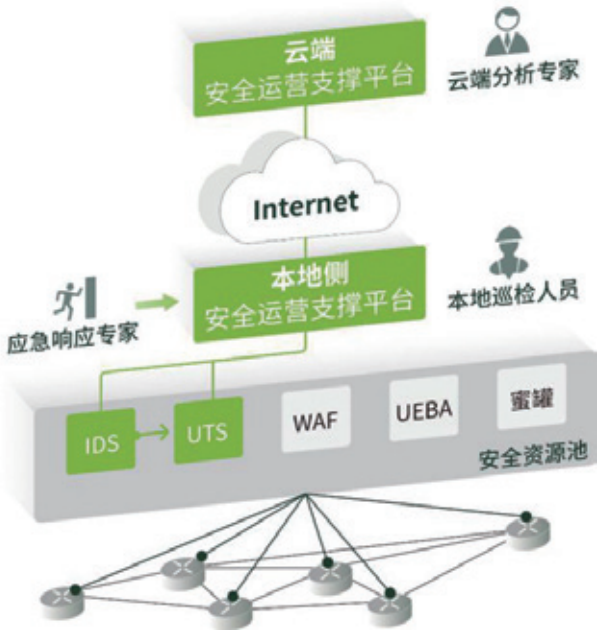
KeySight发布的Breach Defense平台，集成了攻击模拟的功能，用户可以使用该功能对网络进行模拟攻击行为，对网络安全防护有效性进行验证和评估。从安全管理角度看，在相对接近真实环境中进行攻防演练，可以更真实地反应和暴露网络安全防护中存在的问题，根据演练的结果进行整改和改造，更具备针对性和有效性。当企业面对复杂和庞大的安全框架无从下手时，采用靶场技术和攻防演练评估下一步优化和改进的内容将是一种最好的选择。未来，企业和机构的日常安全运营体系需要构建安全度量和安全验证机制，在技术上将安全管理平台集成或对接“靶场”与模拟攻击技术将是一种趋势。

图：靶场系统的样例

4、SIEM-aaS、MSS和MDR

此次大会期间，McAfee、CrowdStride、Secureworks等知名服务商相继对MDR、SIEM-aaS、MSS服务进行升级，基于云端的服务日趋完善。McAfee的MDR服务及CrowdStrike通过合作和平台开放，扩大服务的地域范围；Exabeam在SIEM-aaS（基于云端的事件管理自服务平台）整合UEBA（行为分析）能力；SentinelOne的XDR平台具备容器安全的检测与防护能力，SecureWork MSS服务增加了资产配置检查与管理功能。

云端远程服务逐步具备了替代和超越本地化部署的产品，企业和机构的安全运营将有更多的选择。大型企业和机构可以选择自建安全运营中心，开放安全能力，向下级单位输出MDR、MSS和SECaaS服务，中小型企业可以选择使用MDR、MSS及SECaaS服务构建补充自己的安全能力。



MDR服务示意图

二、认证与可信类

大会期间，各大厂商共发布了4款认证相关的新品，其中GreatHorn发布的解决方案和CyberArk的Endpoint Privilege Manager产品比较有特点，这两款产品和解决方案在认证的基础上增加了可信验证的功能。GreatHorn发布的帐号接管保护是一种基于生物识别技术解决方案，能够识别受感染的帐户并根据用户的输入模式鉴定接管尝试，进一步通过用户行为判定用户是否可信。CyberArk 的Endpoint Privilege Manager增加了特权的防欺骗功能，通过可信验证机制在工作站和服务器上的凭证被盗时帮助用户快速检测并主动关闭正在进行的攻击。

传统认证机制在特定场景下（例如帐号被盗用、弱口令被猜解、开放未授权访问机制的应用）会失效，认证技术逐步融合可信验证功能是一种趋势。

三、检测与防护类

1、加密流量检测

Juniper 对SRX防火墙系列产品和云进行了升级，两类产品无需在不解密的情况具备加密流量检测功能和能力。加密流量检测是网关类检测设备的盲点，由于网络性能降低和私有协议难以解析的原因，网关类检测设备难以通过解密来对加密流量检测。这导致企业只能依赖于终端检测技术对攻陷主机进行检测。Juniper在SRX产品实现加密流量检测后，企业可以通过该网关类设备在边界实现非法外联主机的检测与发现，网络运营商可以具备识别被黑客控制的僵尸主机和IoT设备的能力。

2、机器人防火墙

Imperva发布的 Advanced Bot Protection新的解决方案，采用的机器人防火墙技术，用户能够识别并且拦截没有攻击特征的异常行为，例如CC攻击（DDoS攻击的一种，借助代理服务器生成海量合法请求进行攻击）。采用机器人防火墙技术可以有效对网络抓取，交易欺诈，竞争性数据挖掘，未经授权的漏洞扫描，以及

网络和移动API滥用进行防护。

3、终端恢复

CrowdStrike发布的Endpoint Recovery Services，是通过远程方式帮助用户在入侵后恢复业务运营的一种服务，该服务可以加速事件恢复生命周期，以最大程度地减少中断，减少企业的损失。

四、绿盟安全运营解决之道

1、绿盟智能安全运营中心介绍

绿盟智能安全运营中心（NSFOCUS Intelligent Security Operation Center，iSOC）是遵循绿盟智慧安全2.0理念，以运营为中心，智能化、全场景的统一安全管理平台。iSOC以大数据框架为基础，结合威胁情报系统，通过对攻防场景的机器学习、威胁建模、场景关联分析、异常行为分析以及安全编排自动化、可视化呈现等技术，帮助客户建立和完善安全态势全面监控、安全威胁实时预警、资产及漏洞全生命周期管理、安全事故紧急响应能力。通过独有的自适应体系架构，为安全运营提供可靠的信息数据支撑，协助客户快速发现和分析安全问题，并通过运维手段实现安全闭环管理。

2、绿盟靶场平台介绍

绿盟网络靶场通过SDN、Docker、流量仿真、虚实结合、APT知识图谱，大数据安全态势感知等技术构建各种云、大、物、工等各类环境的仿真场景，实现网络安全实训、竞技比赛、APT仿真演练、护网演练、攻防武器测试、产品测试评估和技术研究验证，满足用户进行人才培养、攻防演练和测试研究的需求。

3、绿盟机器人防火墙介绍

绿盟科技机器人防火墙主要解决客户Web系统、业务平台等Bot流量的管理以及安全防护的，可以解决暴破、爬取用户信息，撞库等安全问题。帮助客户实现API请求防护和管控、机器人流量管理。能够通过对各个业务接口的保护实现打击窃取用户隐私、撞库、薅羊毛、黄牛党等恶意行为，有效拦截自动化攻击、针对API的手动参数篡改两大攻击方式，提升攻击者的攻击难度，保障业务系统稳定运行、实现业务能力提升。

4、绿盟MDR服务介绍

绿盟一体化安全运营解决方案（简称MDR服务）是以资产为基础，实现威胁、脆弱性管理闭环，并通过服务工具提升检测及防护效果的一站式安全运营解决方案。通过为客户提供从规划、建设到运维的全价值链，贯穿预警、防护、监测、响应和处置的安全闭环流程，以持续降低企业的安全风险。

NSFOCUS

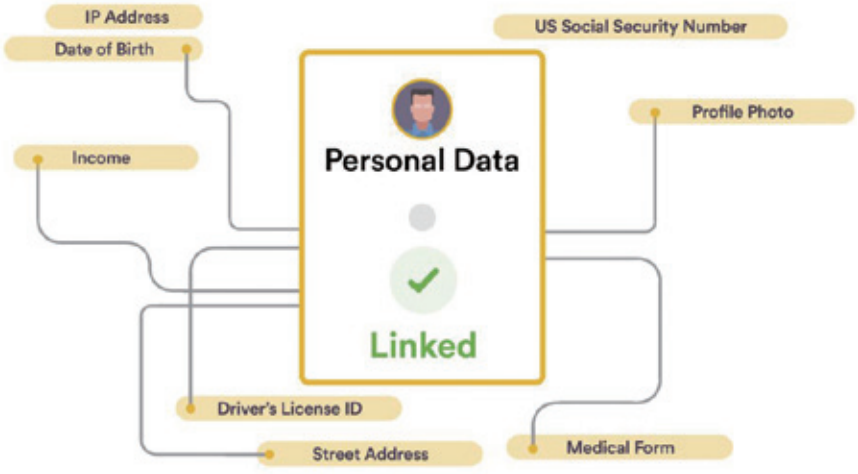
创新沙盒

Securiti.ai 为何成为 2020 RSAC 创新沙盒冠军得主?

2020 RSA 创新沙盒大赛尘埃落定，冠军花落Securiti.ai公司。作为本次大赛冠军，Securiti.ai是如何从十大“劲敌”中脱颖而出的呢？之前，绿盟君已经为大家分析过Securiti.ai的产品特点，今天，绿盟君再次带大家详细了解一下这所公司的与众不同。

一、情理之中的冠军得主

总体而言，今年Securiti.ai夺冠是情理之中：于大势而言，数据安全、个人信息、敏感数据的识别、防护是国内外最重要的合规性要求，市场空间可期；于技术而言，通过技术手段对个人数据识别，使用People Data Graph构建面向人的知识图谱，为后续的分析提供模型支撑，通过聊天机器人实现智能化的交互；于方案而言，针对客户的数据安全难以落地的痛点，提供了整套解决方案，构建个人数据链接，实现消费者数据权利请求-响应的流程自动化处理，生成合规性审查报告，分析第三方风险。前年GDPR的发布引发了数据安全的关注，如果说BigID那次夺冠很大程度上是因为GDPR的颁布“蹭热点”，这两年已经有很多起违反GDPR罚款的案例，可以说这次Securiti.ai发布的产品和解决方案更加接地气，也更加全面，能够满足企业的数据安全合规性要求，本次夺冠更让人心服口服。



如果我们把安全行业的创新划分为两个维度：攻防技术的创新和以及行业的创新，那么从入选2020年创新沙盒决赛的公司和产品来看，今年的攻防技术创新在于模糊测试、响应技术、人工智能落地，而行业的创新集中在敏捷开发、数据安全等热点领域。此外，今年大会主题是以人为本，所以创新企业中也融入了人性的创新。下面以这三个维度进行分析。

以人为本的创新

随着这几年的安全事件逐渐曝光，越来越显示出，只追求完善的安全制度或先进的安全防护技术，并无助于避免企业安全事件。因为人往往是企业安全中最薄弱的一环，所以如何提高员工的安全水平和安全意识，可能是今后企业安全中非常重要的一环。人、流程、技术，相辅相成，缺一不可。

◆ 数据安全

Securiti.ai主要是在数据安全领域，如今个人信息和敏感数据的合规性要求已经非常强了，之前绿盟君已经为大家做过分析做过分析（点此回顾）。GPDR、CCPA等法律的严格执行，使得近两年个人信息领域，特别是如何识别、如何匿名化、如何评估个人信息，成为行业一大热点。简单而言，Securiti.ai根据数据安全法律的合规性要求，特别是数据权利请求、第三方风险评估、许可生命周期管理等，通过技术的手段，自动化、程序化地进行监控、处理，从前端而言，整体感觉用户友好，可视化、易用性较好。

亮点：直击个人信息合规性问题，持续监控、链接、评估个人信息

◆ 安全意识培训

Elevate Security主页的标题是“人的风险：度量、影响、减少”，非常讨巧地切合了大会主旨，印象中这也是RSAC近年来第一家在安全意识培训（SAT）方面的创业公司。通过技术手段促进安全治理，发挥员工的主观能动性，能够更好地提升安全防护的效果。

亮点：技术手段提升员工参与能动性

◆ 邮件安全

国外的电子邮件使用率远高于国内，所以邮件安全的重要程度可能高于其他

安全领域。传统邮件安全网关通过发件人地址、内容是否包含恶意IOC，以及附件等网络安全角度去检测邮件的安全性，但这些无法抵御基于社会工程商业电子邮件犯罪（BEC）。INKY虽然在传统的邮件安全领域，但解决的是跟人密切相关的问题，它试图通过从人的感知的角度去分析其中的内容是否存在欺诈，所以能够检测出传统手段无法检测到的0day攻击。

亮点：AI助力人脑很难识别的视觉欺诈

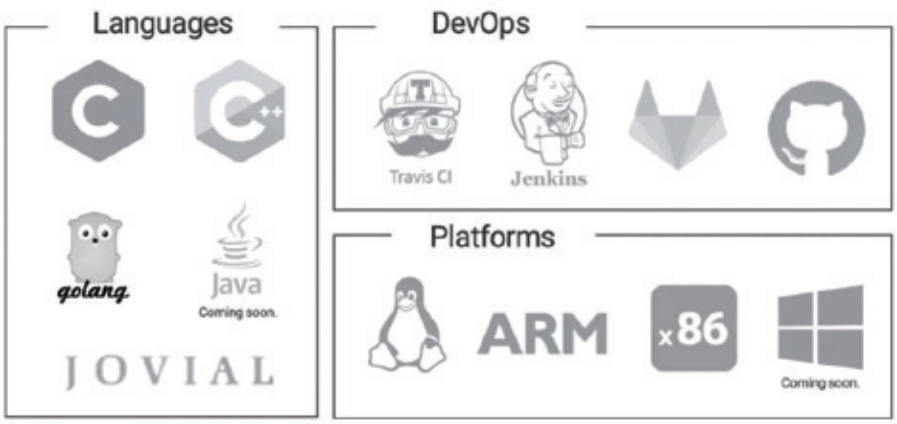
行业创新

◆ 敏捷开发

总体而言，DevSecOps是一个新兴的方向。今年创新沙盒有三家是DevSecOps方面的：ForAllSecure、Vulcan、BluBracket。其中Vulcan下文中会详细分析，BluBracket成立一年，内容较少。

ForAllSecure聚焦在DevSecOps，有一支来自卡耐基梅隆大学科研团队，通过“下一代”模糊测试技术结合使用“符号执行”技术和“导向型模糊测试”技术，能够针对测试发现的安全漏洞自动化生成概念性验证（PoC）和补丁，在一定程度上避免传统白盒测试的高误报和黑盒测试的盲目性，具有很高的创新性和价值。该团队在DARPA CGC 2016中夺冠，足以验证其技术实力。

亮点：DevSecOps+Fuzz，技术实力很强



DevSecOps成为了越来越多企业中开发者的选择，其中代码安全已经成为了非常重要的安全方面，开发阶段解决安全问题，远比运行时检测、响应的投入划算得多，所以看好未来几年代码安全相关的创新企业。

◆ 云安全

无论在国内还是国外，云计算已经成为了普适的基础设施，云安全已经成为了传统的安全问题，例如云上配置、访问控制、检测响应等。

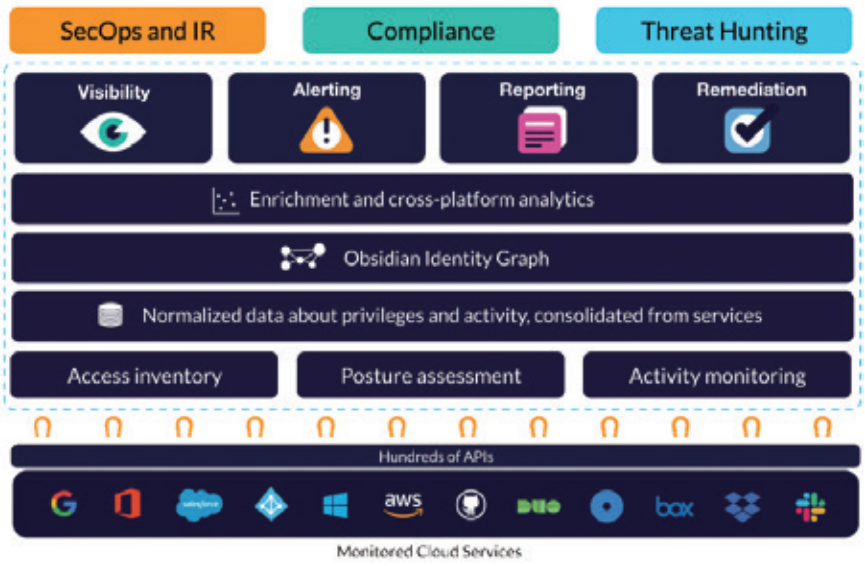
随着各种云上安全事件频繁，SaaS、PaaS的数据泄露已经成为这两年很热的话题，Gartner将该细分市场称为CSPM（Cloud Security Posture Management），目前大部分公司的配置核查主要是对如存储资源的访问凭证进行检查，避免弱口令或无口令拖库的事件。下面两家公司则更进一步，既然攻击者能够无凭证或获取弱凭证，那就需要监控云端服务的访问行为，聚焦在看似合法的访问，而非以往关注恶意攻击，有点像前几年内网持续遭到渗透后，业界开始聚焦在合法用户的异常行为，所以出现了UEBA。总体而言，这个方向的技术难度不大，借鉴的现有技术不少，创新不多，但市场空间大，所以创业公司的前景还不错。

AppOmni实现了公有云上的配置和访问控制策略的持续核查和监控，更多的是从合规性角度、安全策略可视化和监控方面更出彩。

亮点：SaaS持续访问控制监控

Obsidian实现类似的功能，但在RBAC基础上增加了检测和响应功能，通过监控用户的登陆、操作等事件，分析其中异常的行为操作，可以理解为xDR在云端SaaS的应用。本身创新度不大，主要还是新技术与云安全的融合。

亮点：xDR+SaaS融合



传统安全的创新和微创新融合

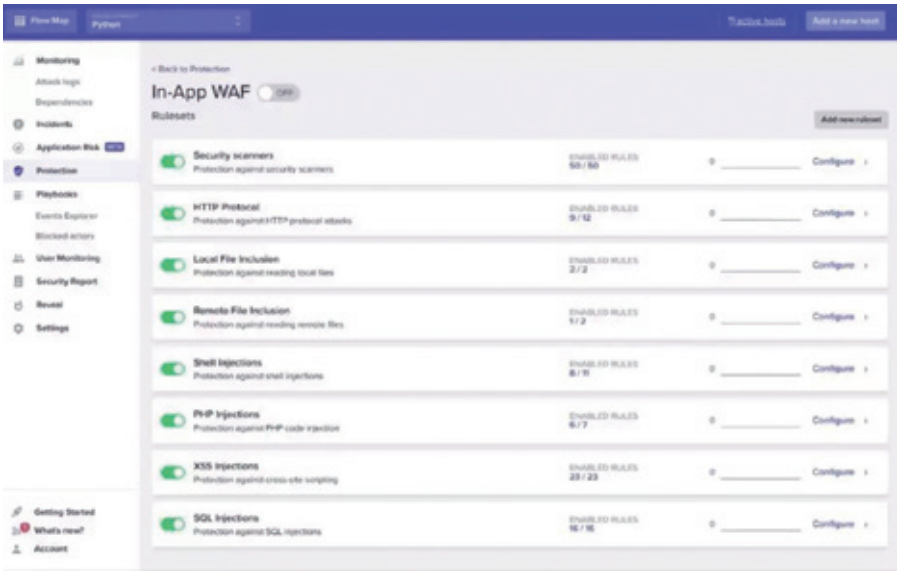
Sqreen、Tala Security和Vulcan Cyber三家均出现在Gartner的Security

and Risk Management Cool Vendor 2019中，所以严格意义上说 这三家不算太新的公司，而且这三家在细分领域中没有突破性的创新，需要与成熟的厂商竞争。

Sqreen和Tala Security聚焦在Web安全领域，既传统的WAF，以及近年开始流行的RASP，都已然是服务端Web安全的标配。所以这两家公司不管是部署方式，还是功能层面，虽然有所创新，但均属于微创新。

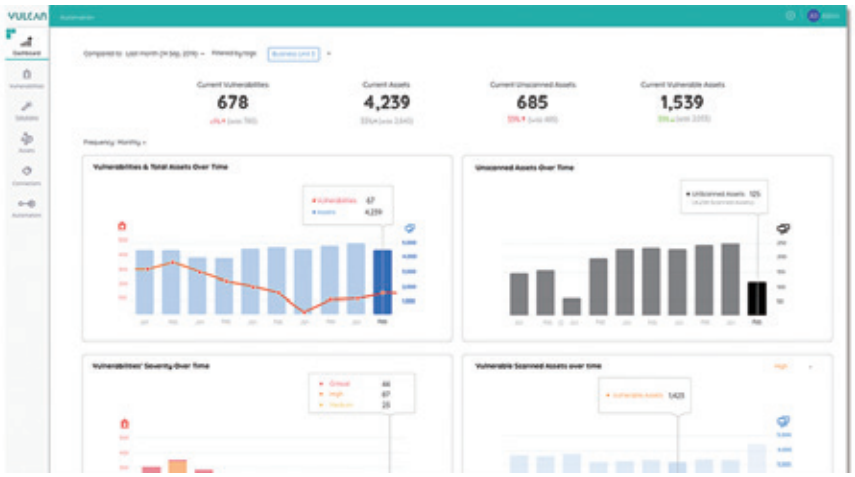
Sqreen是以微代理的方式实现了RASP和In-App WAF，从功能上没有突破当前WAF和RASP。当然他们宣称捅过内嵌无侵入SDK的方式，可以做到对业务应用的无缝、可扩展防护，无论企业有多少服务，服务是基于什么语言，Sqreen都能嵌入，对上形成统一的视图，从而进行监控、分析和防护。借用Service Mesh的概念，Sqreen也提出了Security Mesh。

亮点：切近业务无缝对接



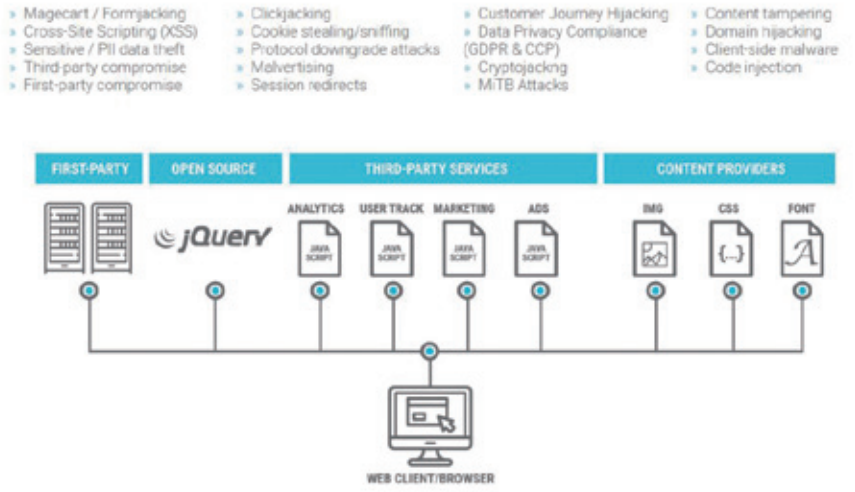
Vulcan Cyber将威胁脆弱性管理平台TVM融入了这两年热门的“响应”元素，通过编写剧本Playbook，将TVM与SOAR结合，自动化缓解高风险的漏洞，解决漏洞生命周期管理运维成本高的问题。决赛中Vulcan举了一个如何缓解Apache Structs的多种方法，通过SOAR实现workload的自动运行，这样就解决了大规模业务环境下漏洞管理的可扩展性和响应速度。

亮点：漏洞管理和SOAR融合



Tala Security聚焦在客户侧的Web应用防护，通过CSP机制抵御如XSS、挖矿等针对客户端浏览器的攻击，主要面向金融交易的安全防护。这是传统Web安全缺失的地方，如果没有威胁情报，服务器端安全机制无法判断网站中的第三方引用是否存在安全问题（因为第三方的流量不会经过WAF）。Tala Security通过客户端浏览器CSP的安全策略，覆盖了传统Web安全的短板，有一定的新颖之处，是传统服务端Web安全有益的补充，但本身替代不了WAF，两者应该是互为补充，最终形成端到端的Web安全方案。

亮点：客户端的Web安全机制



二、总结

从技术点上看，自动化似乎贯穿了很多公司的产品特点，如PrivacyOps、SOAR、xDR、API Driven等等，原因是当前的攻防到了争分夺秒的阶段，而安全运营也面临规模化、复杂化的挑战，只有通过自动化提升整体的安全防护效率，才能应对这些挑战。

而从安全防护体系来看，人的因素的重视程度一直在提升，如何降低所有员工中安全防护水平的短板，如何利用人的积极性提升整体防护水平，也是创业公司通过技术驱动完善制度、符合合规性要求需要考虑的重要问题。

总体而言，网络安全的创新一直在进行中，但从这几年的创新沙盒看，没有哪个行业，也没有哪个技术是全新、闻所未闻的。尽管国内的网络安全企业与国外的差距在逐渐缩小，但需要指出的是，国外的IT环境在很大程度上跟国内是有差异性的，例如云计算、电子邮件等，所以当我们思考相关的安全创新也需要考虑到国情，避免邯郸学步。

AppOmni：面向 SaaS 数据泄漏的持续性监控和告警防护

2020年2月24日-28日，网络安全行业盛会RSA Conference将在旧金山拉开帷幕。前不久，RSAC官方宣布了最终入选今年的创新沙盒十强初创公司：AppOmni、BluBracket、Elevate Security、ForAllSecure、INKY、Obsidian、SECURITI.AI、Sqreen、Tala Security、Vulcan。

昨天绿盟君已经向大家介绍了Elevate Security 和Sqreen两家厂商，今天，我们要介绍的是厂商是：AppOmni。

一、公司介绍

AppOmni成立于2018年，总部位于旧金山卡本代尔，该公司致力于保护、管理和监控公有云上的应用程序（SaaS），从而解决了绝大多数企业SaaS产品上云后面临的安全风险。目前公司人数大约40-50人左右，公司的创始人大部分来自Salesforce、Palo Alto Networks公司，在今年1月28日，该公司已经筹集了1300万美元的A轮融资，投资者以ClearSky牵头，Inner Loop Capital公司也参与了这一轮融资。

二、背景介绍

随着云技术的蓬勃发展，企业纷纷选择上云。然而，面临复杂多变的云环境，企业也因担心数据泄漏问题而经常问云服务商“你的云安全吗？”

随着技术的不断积累，云计算的技术手段越来越成熟，虽然如今的云环境逐渐趋向于稳定和安全，但是企业上云暴露出来的安全问题仍然层出不穷，归根到底是什么原因？

Gartner曾预测到2022年，至少有95%的云安全问题是客户的过错。因为技术提升的同时，云上应用变得普适广泛，云上的业务复杂性也在提高，我们知道在一些规模比较大的生产级IaaS、PaaS平台上，通常会有上百个配置选项、每日千万级的API调用频次以及各种数据访问模型。云服务面临的安全挑战不在于云自身的安全，而在于有效的安全管理、技术控制、实施安全策略等。所以问题不应该是“你的云安全吗？”而是“你是否有安全的使用云？”

SaaS安全防护面临的问题

SaaS服务在IT成熟市场已被广泛应用，相关数据表明，到2024年全球SaaS的市场规模将达到1800亿美金，年复合增长率超过20%。与此同时，SaaS的安全问题也成为技术人员讨论的热点，近年来大规模的数据泄漏事件已造成数以万计的损失，综合原因不外乎以下几点：

1、云端不安全的访问控制

访问控制、包括特权用户访问是数据泄漏的最大原因，而根源在于不安全的默认配置以及对访问控制的滥用造成，比如旧的用户未删除或过度使用管理控制等。面对以上这些问题，一些企业采用RBAC机制来管理用户的权限访问控制，这看上去是没问题的，但在实际运用当中，没有良好安全基础背景的运维人员是很难做到完全可控的，毕竟随着企业规模的增大，人员会越来越多，角色权限也会增多，没有一个统一的管理平台光靠专业的维护人员去管理未免要求太高。

2、错误的云存储配置

许多企业选择将SaaS服务部署在公有云上，却对云上的存储配置并不关心，他们认为这是云服务商的责任。但现实很残酷，在购买云服务商服务时大多数中小企业甚至没有仔细阅读过条款。据Macfee调查声称99%的云端和IaaS错误配置都是在终端用户的控制范围内，而且并不为人所知，造成这一现象的主要原因是“公开数据”在很多云服务中是云数据存储配置的默认访问设置，所以企业需要受过良好教育的架构师和安全人员对服务进行适当的管理，以免数据泄漏的惨案再次发生。

3、SaaS服务缺乏持续性的监控告警

当服务被黑客攻陷导致数据泄漏时，持续的监控告警可以将用户的损失降到最低。目前企业大多数使用云服务商提供的监控告警，但因为服务商针对的是普遍用户群体，所以其安全功能存在单一性、反馈用户信息不够友好、缺乏持续性的监控等不足，最终导致了黑客入侵造成了不可收拾的局面。为保证SaaS服务的安全，企业急需一个专业的云告警平台处理所有入侵事件。

2018年9月，Veeam公司客户数据泄漏，有200GB与4.4亿条客户记录相关的数据在网上公开。2019年12月，雷锋网报道了 Elasticsearch 服务器 12 亿个人数据遭泄露的事件，造成如此之大的损失原因竟然都是因为错误的云实例配置导致，想起来让人唏嘘不已。

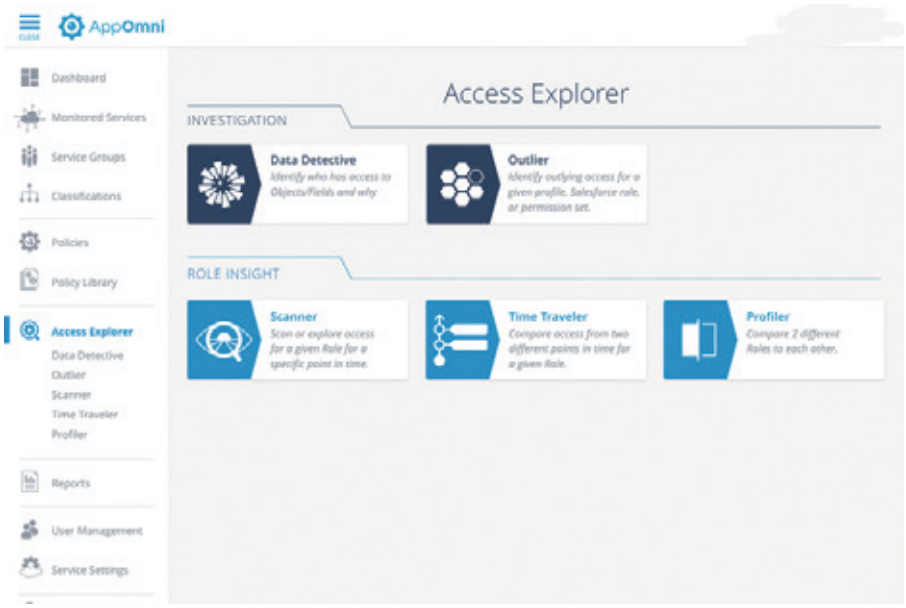
综上，相关领域如云中的数据的可访问性如何实现，用户访问控制，跨云的应用程序安全性和数据访问策略成为了客户侧安全防护面临的最大问题。

三、产品介绍

AppOmni平台是由一个具有丰富经验并了解安全性、合规性、IT团队需求的专家团队设计和构建的。通过使用AppOmni自研的策略引擎深度扫描SaaS服务的API和配置，可在数分钟内识别出数据泄漏，并生成相应报告；其次，AppOmni还持续提供监控用户的SaaS程序是否发生安全事件并产生相应告警；最后，AppOmni的“SaaS权限建模” 专利可使用户能够立即、切实并可行的洞察对SaaS应用程序中关键业务数据的有效访问权限。综合以上三点，AppOmni在访问控制、数据泄漏、数据访问策略方面均有着一定程度的创新，从而为SaaS服务全力保障护航。

四、产品特点

AppOmni 的解决方案主要是：安全自动化、合规控制和IT管理，我们逐一进行介绍。



安全自动化

1、配置防火墙

AppOmni支持配置防火墙功能，并可以定义数据访问的安全规则，以防止数据暴露给第三方或公共网络。

2、一致的访问控制

基于角色的访问控制（RBAC）仍然是对SaaS用户访问权限控制和授权的行业标准策略，在大型企业必须支持成千上万内部用户时，IT团队将不得不面临授予访问权限的压力，并且此时很容易造成配置权限超越了其自身原本应有权限的事件发生，而且不正确的删除权限可能会对业务造成严重影响。AppOmni遵循RBAC的原则，提供可视化的角色用户管理界面，可以显示哪些用户共享同一权限哪些不共享，并且可以标识异常的用户权限绑定，使运维人员清晰的对用户及角色进行有效分配。

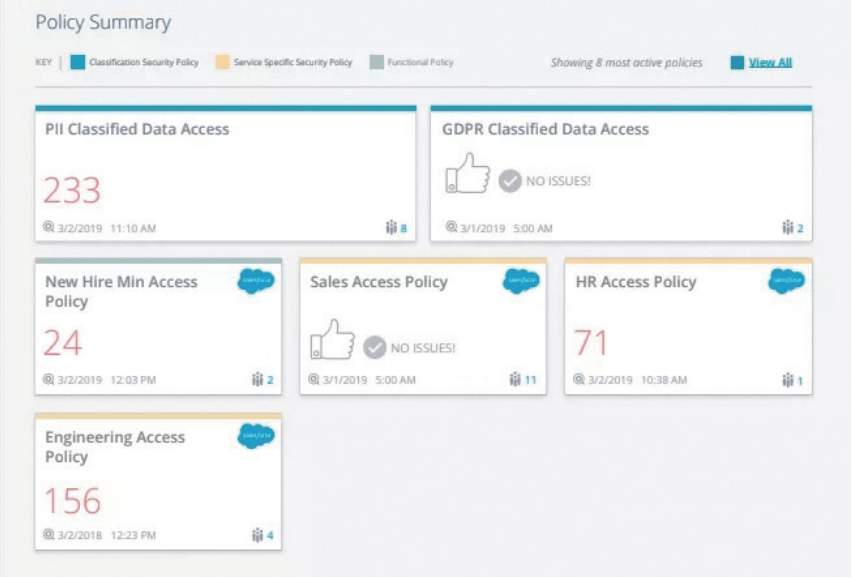
3、24*7的持续监控

有了一致的访问控制往往还不够，一旦SaaS应用程序处于已知良好的访问控制状态，就需要不断的保持这种良好的状态并将一致性延续下去。AppOmni提供了24*7的持续监控，其内部通过“权限模型”可以评估SaaS应用程序配置和有效访问，与设置的安全策略或绑定的用户权限有任何偏差都会立即告警并进行相应的处理措施。

合规控制

1、合规报告

AppOmni支持在“数分钟”内执行对SaaS的访问检查并导出对应合规性报告，这在企业中是非常必要的，因为企业会不定期的查询当前部署的SaaS服务是否一切合规。



2、数据清单

AppOmni会根据类型、业务需求、合规性需求对数据进行分类提供用户可视化数据清单，并且可以将数据接入任何SIEM系统（SOAR）、日志管理系统、漏洞管理系统做进一步的数据分析。

3、控制匹配

AppOmni中提供了业界的一些标准，例如ISO 27001、PCI、NIST等，作为基线与SaaS的应用程序进行匹配，从而可以看出SaaS应用程序使用是否合规。

IT管理

1、配置管理

AppOmni可以配置用户角色权限、防火墙安全策略、配置文件等，为用户、云环境和应用程序创建了良好的基础配置模版。

2、功能测试

在IT流程中，将自动化测试纳入其中可以在用户升级和部署新的应用程序时不担心会出现影响线上版本的事件发生，AppOmni具备这项能力。

五、总结

AppOmni在官网未说明其使用的扫描引擎运用了哪些技术，只是说是一项专利，但可由此推断这一定是AppOmni的核心卖点。毕竟在数分钟内即可扫描完SaaS服务并输出相应的合规性报告及数据清单，同时又可以做到24*7的持续性服务监控和告警并且不会太影响性能，试问谁不好奇AppOmni是怎么做到的呢?

对于公有云上的配置进行核查，Gartner将该细分市场称为CSPM（Cloud Security Posture Management），目前大部分公司的配置核查主要是对如存储资源的访问凭证进行检查，避免弱口令或无口令拖库的事件，AppOmni的创新之处在于结合合规性要求，可视化地还原业务层面的访问逻辑关系，并通过持续性的监控告警保证访问策略随着业务迁移和人员变更后的一致性。

AppOmni可提供持续的监控和告警这一优势使得用户层面具备了“即时可见性”，从而在很大程度上改善了云中的安全现状。另外，AppOmni平台通过用户定义的安全策略评估数据暴露风险，以提供警告和见解，为用户节省了大量的补救时间。在企业发展业务速度跟不上上云引起的安全问题这一普遍趋势下，AppOmni可以说是该领域的首批着眼于解决如何安全的使用SaaS云的公司，未来随着业务越发复杂，云中面临的安全问题只会越来越多，希望AppOmni可以保持其创新性和优势，继续努力，同时也祝愿AppOmni在2020年RSAC创新沙盒十强赛中可以取得好的成绩。

参考链接

[1] https://appomni.com/
[2] https://appomni.com/appomni-raises-10-million-in-series-a/
[3] https://appomni.com/using-roles-for-continuous-saas-security-monitoring/
[4] https://appomni.com/is-the-cloud-secure/
[5] https://www.infosecurity-magazine.com/news/orgs-failing-protect-data-cloud/
[6] https://www.cbronline.com/news/iaas-misconfiguration-mcafee
[7] https://thehackernews.com/2019/10/data-breach-protection.html

BluBracket：让安全的保障和代码迭代一样快

2020年2月24日-28日，网络安全行业盛会RSA Conference将在旧金山拉开帷幕。在RSAC官方宣布入选今年创新沙盒十强初创公司中，绿盟君已经为大家介绍过了Elevate Security 、Sqreen、AppOmni、Tala Security、ForAllSecure、INKY六家厂商，今天为大家介绍的是：BluBracket。

一、公司介绍

BluBracket于2019年成立，总部位于美国加州，是一家专注于代码安全的初创公司。当前由Unusual Ventures、SignalFire、Point72 Ventures和Firebolt Ventures共同投资650万美元作为其种子资金，当前处于种子轮。

BluBracket在其官网上指出，公司的定位是：提出当前业界首个也是唯一一个全面的代码安全解决方案。作为一家成立刚刚一年的公司就能进入创新沙盒决赛，必有其过人之处。

二、背景介绍

在具体介绍其产品前，我们先看一下公司的董事会成员以及背景经历。

Prakash Linga，公司的创始人兼CEO，2007年于康奈尔大学获得Computer Science博士学位。之后在Moka5作为技术总监工作了4年（Moka5是一个成立于2005年的桌面虚拟化公司，于2015年停止运营）。然后就开始了其创业之路，从其在Linkedin上的资料来看，从2011年至今，已经创办了三家公司：

第一家公司是RAPsphere（2011.4—2012.5），Linga作为创始人、CTO和技术VP，从网上仅存的一些介绍中，大概可以看出，RAPsphere主要提供移动安全、应用和设备管理服务，为企业和员工的移动设备提供安全的设备控制、管理和可见性。很不幸的是，这个公司只存活了一年多。

然后其在2014年又创立另一家公司，Vera Security，主要做数据安全。Vera提供了一种数据安全的解决方案，使各种规模和位置的企业能够轻松地跨所有平台和设备保护和跟踪任何数字信息。通过全面的数据安全和实时控制，允许人们使用任何想要的平台和设备，同时确保最高级别的安全性、可视性和控制。

在2018年8月，Linga离开了Vera，创办了BluBracket，任CEO，从其履历和Linkedin上的自我介绍来看，Prakash Linga这个印度小伙将自己定位为一个连续的创业者和天使投资人。

Ajay Arora，BluBracket的另一个合伙人，同样给自己的标签也是连续的创业者和天使投资人，Ajay Arora可以算是Prakash Linga的老搭档了，从RAPsphere的Co-Founder、COO和产品VP，到Vera的CEO、Co-Founder，甚至二者还曾经共同就职于AppSence分别担任VP。从Ajay Arora的履历中可以看出来，从产品、解决方案管理，到市场运营管理，可以说是什么都做过了。但是除了前文提到的这几个创业公司之外，其他就职过的公司似乎很少是做安全相关的。

BluBracket董事会的另外两名成员，从其个人简历介绍中，并未提及BluBracket的任职职务，其中Jim Zemlin当前是Linux基金会的执行董事，另外一位John Vrionis是BluBracket投资方Unusual Ventures的创始人。

三、产品介绍

接下来我们看一下BluBracket的产品，公司成立于2019年，是此次创新沙盒所有公司中“最年轻”的一个，也是融资金额最少的一个（650万美元）。从其官网上看，对公司的各项介绍都少的可怜，也可能是因为成立时间太短，公司的主要精力还集中在产品的研发上。

BluBracket对其产品的定位是：当前业界首个也是唯一一个全面的代码安全解决方案。公司的口号为“Security at the speed of code”，绿盟君理解应该是“让安全的保障和代码迭代一样的快”。

为了支撑这样的定位，BluBracket当前提供CodeInsights和CodeSecure两款产品，组成其代码安全解决方案。

CodeInsights

从产品介绍上看，CodeInsights主要提供的是代码的管理功能。

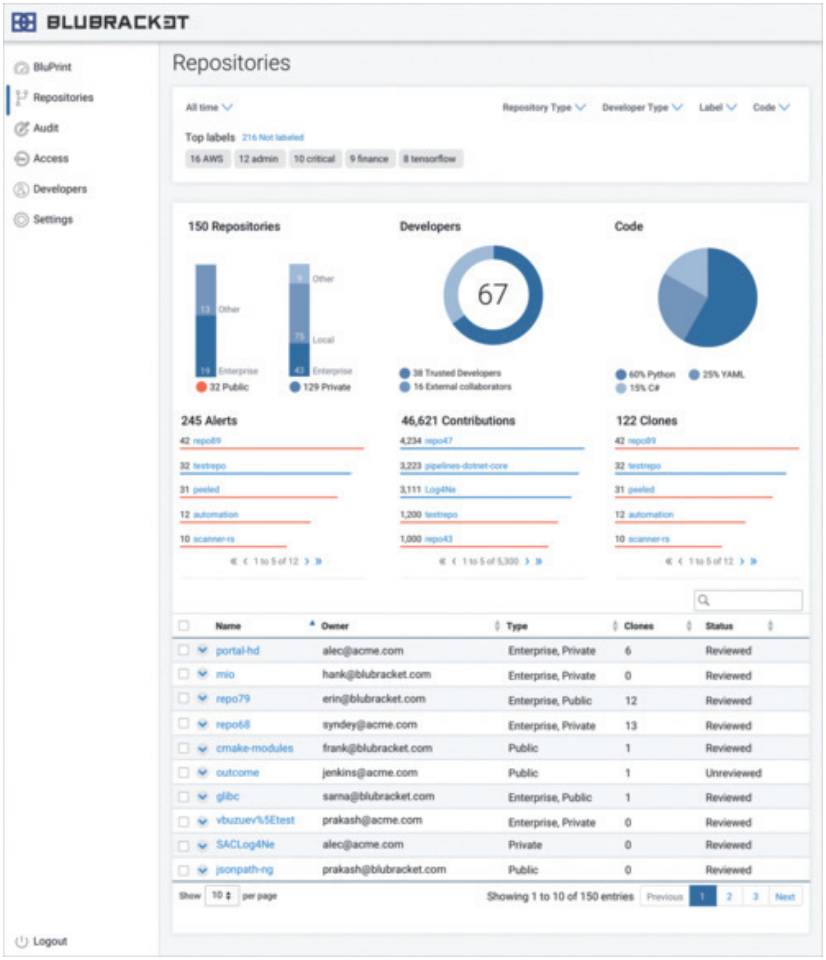
当前无论是敏捷开发，还是DevOps，任何一个软件项目，其代码管理都是一个重要问题，尤其是从安全的角度来看，大量的开源项目应用、大量的开发人员不断进行代码的更新，以及快速的代码迭代。能够对整个项目的代码进行全视角的查看和追踪，无论是对代码的规范性管理还是脆弱性管理，都有着重要的意义。

如今协作式编码工具，为研发管理提供了极大的便捷性，但是同时也导致了代码扩散不清晰的问题。CodeInsights主要为企业提供了代码环境视图（BluPrint），这样用户就可以知道自己的代码在哪里，无论是组织内部还是外部，谁可以访问它。最重要的是，用户就可以对最重要的代码进行分类，这样就可以为任何审计或规范性要求显示详细的追踪链。

CodeSecure

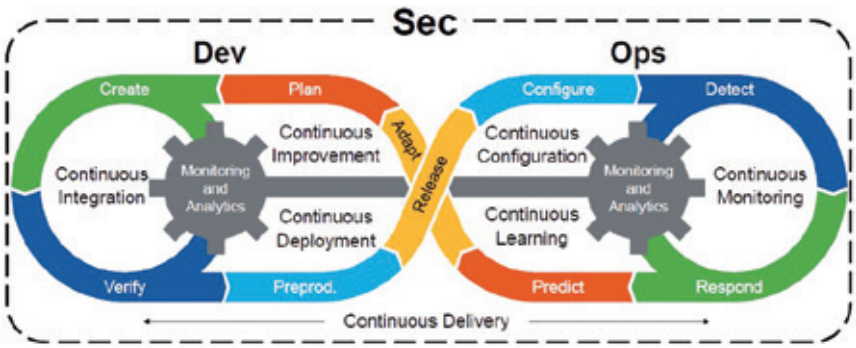
BluBracket提供的另一款产品叫CodeSecure，从名字理解，是保证代码安全的。通常，使用Stack Overflow、Github或其它开源的代码协作工具，通常会对企业安全构成严重的威胁。CodeSecure可以检测代码中的密钥，并确保代码中没有敏感的密码，或者是令牌被盗用、错误的处理或误用。CodeSecure还可以让用户识别、预防甚至阻止代码从企业中意外或恶意的流出，保证企业代码的隐私性。

下面的两张图是其官网上贴出来的产品界面截图，从截图上，我们可以大概的看一下它具体的功能，比如能够在代码仓库中识别到AWS的token，能够识别出代码仓库中存在的密钥，能够识别代码仓库的访问权限等安全告警。还能够对代码仓库、开发者、开发环境等信息进行集中的管理和监控。



四、历届创新沙盒与DevSecOps

代码安全更广义的范畴，可以划分到DevSecOps里面。DevSecOps的理念和架构，近年来越来越多的为人们所青睐。Gartner从2016年起，就持续的将DevSecOps列入其年度Top10安全技术和项目中。下图是Gartner发布的经典DevSecOps闭环模型。



随着敏捷开发、DevOps的飞速发展，DevOps全流程自动化的工具链相对来讲已经比较成熟和完善，在众多规模性的企业得到了较好的应用和推广。然而要想实现DevSecOps闭环模型，还需要重点解决以下几方面的

问题：

（1）切实有效的安全工具，实现每个阶段对应的安全能力；

（2）能够友好的集成到DevOps工具链生态中，实现完全的安全自动化；

（3）要能够保证其效率与性能，使得安全能力的接入，不会影响到DevOps流程的性能。

在市场和技术的推动下，近年的创新沙盒中，多次出现DevSecOps相关产品，比如今年的ForAllSecure，2019年的DisruptOps（云基础设施检测与修复）、ShiftLeft（软件代码防护与审计）等。

DisruptOps

多云和敏捷开发是云计算的热点，DisruptOps以SaaS化的服务方式，通过对用户的多个云资源进行安全与操作问题的快速检测并自动修复，一方面节省了客户上云的成本，另一方面实现对云基础架构的持续安全控制，在安全、运营和成本等方面，给用户带来最大的收益。此外，借助自动化和服务编排的技术，推动云原生应用和DevSecOps的落地。

ShiftLeft

ShiftLeft创新性的提出基于多层图表的代码分析方法，将全部应用代码进行多层次的、可扩展的图的方式展现。图能完整包含代码的多种元素，完整展现代码细节，比如语言、自主开发代码、开源代码（OSS库、SDK）、不同类别，方法等。从而可以从图中清晰的理解数据流动，快速识别数据泄露，关键漏洞等。而且扫描速度极快，10分钟分析50万行代码，适用于DevOps场景，能够直接和CI/CD无缝结合，发现每个产品版本的问题，效率极高。通过将代码分析和ShiftLeft的应用微代理结合起来，能够深刻理解漏洞，并针对漏洞进行优先级排序。

四、总结

首先从市场来看，随着云原生、微服务、敏捷开发DevOps等越来越多的实现落地应用，代码安全确实是一个亟需解决的问题。前文也有提到，在整个DevSecOps闭环中，如何高效的实现开发阶段的代码安全，对于整个DevSecOps有着重要的意义。所以说，这个产品在定位上应该是紧紧抓住了当前的热点同时也是痛点的问题。

其次，从产品本身来看：在功能上，BluBracket提供了代码管理和安全检查两个功能，但是从仅有的资料来看，安全检查上似乎功能点并不是十分的吸引人，只能看出来可以对代码中存在的密钥、权限等的检测，对于代码的脆弱性、漏洞、恶意文件等敏感的问题，从产品介绍上似乎都看不出能实现这些能力，可以说功能上并不突出。另外再从技术上看，所有的介绍中并找不到任何关于产品实现技术的描述，也没有相关的技术博客介绍。

最后，从公司的核心创始人来看，官网公布的4个核心成员，除去其中一个投资人，其余的除了CEO有明确的职责外，另外三个人很难看出明确的职责分工，比如技术负责人、市场负责人、销售负责人等。另外核心成员的履历背景相对来看也不是特别的好看。所以，在绿盟君看来，BluBracket尚处于发展初期。

参考链接

[1] blubracket，https://www.blubracket.com/
[2] DisruptOps，http://dwz.date/wH7
[3] ShiftLeft，http://dwz.date/wJg
[4] https://www.crunchbase.com/organization/blubracket

Elevate Security:“以人为本”的安全行为改善平台

2020年2月24日-28日，网络安全行业盛会RSA Conference将在旧金山拉开帷幕。大会的创新沙盒环节备受瞩目，成为全球网络安全行业技术创新和投资的风向标。

前不久，RSAC官方宣布了最终入选今年的创新沙盒十强初创公司：AppOmni、BluBracket、Elevate Security、ForAllSecure、INKY、Obsidian、SECURITI.AI、Sqreen、Tala Security、Vulcan。

绿盟君将通过背景介绍、产品特点、点评分析等，带大家了解入围的十强厂商。今天，我们要介绍的是厂商是：Elevate Security。

一、公司介绍

Elevate Security于2017年1月创立，总部位于美国旧金山湾区。两位创始人Masha Sedova和Robert Fly都是前Salesforce负责安全和信任管理的高管，有丰富的安全管理经验。公司经过两轮融资，目前处于A轮融资阶段，融资规模1000万美元。区别于多数重点关注技术（Technology）与流程（Processes）的安全创业公司，Elevate基于对当前网络安全风险的洞察，提供针对人（People）的安全行为改善平台及定制化方案，能够通过对员工行为的评估测量、数据可视化提供对企业多层次的风险监控，进而提供个性化的员工评级反馈以及增强的安全培训。Elevate Security正契合今年RSAC的“Human Element”主题，有些“应运而生”的意思，想必这也是助力它进入了创新沙盒决赛的一大因素。

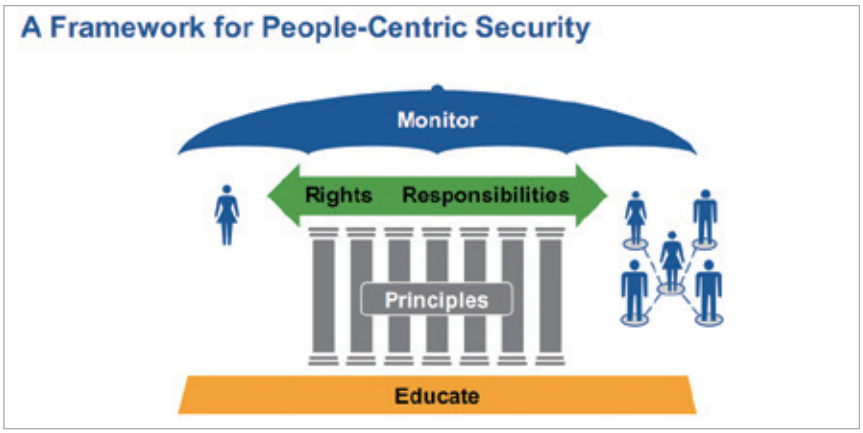
二、背景介绍

2014年IBM安全服务的一项研究表明，95%的网络安全失陷是人为错误造成的。而近期卡巴斯基的研究则表明91%的涉及公有云用户数据泄露事件的公司声明社会工程学是其所遭受攻击活动的一个环节。人为因素一直以来都是网络空间安全的重要一环。随着各种安全防御自动化技术、产品、平台的涌现，大幅提升了攻击者入侵的难度。然而，在安全、利益攸关的关键场景下，由利益驱动的攻击者无缝不钻，高级持续攻防的战场逐渐浮出水面。当前，即使是前沿的人工智能驱动的防御手段，也愈发强调“human-in-the-loop”的人机闭环协同能力。人既是防御环节的重要组成，也同时可能成为

攻击者突破防御的脆弱点。

随着网络安全成为全球各方的关注热点，网络安全从业者愈发感受到所处行业对世界的影响力。而这种影响力也逐渐通过各类安全教育、突发的安全事件、常规化的安全律法，深入到所有人的工作生活中。正如普通人愈发认识到到个人的健康管理尤为重要，大中小型企业乃至个人的网络安全意识、安全习惯、安全行为，将深刻影响到个人以及所处组织的安全基础。然而网络安全文化氛围的形成任重而道远，从业者对安全能力提升和发展的认识也逐渐从追逐更快、更准、更智能的技术、产品，转而更加关注“以人为本”的技术、流程、法规甚至习惯和文化的新层次。

Gartner在自适应安全的体系中，明确地将People-Centric作为了一个重要原则，在整个以人为本的安全体系内，安全教育是基石，只有提高员工的安全意识和安全技能，才能有效减少各种安全机制运行的开销，提升整个安全体系的运转效率。

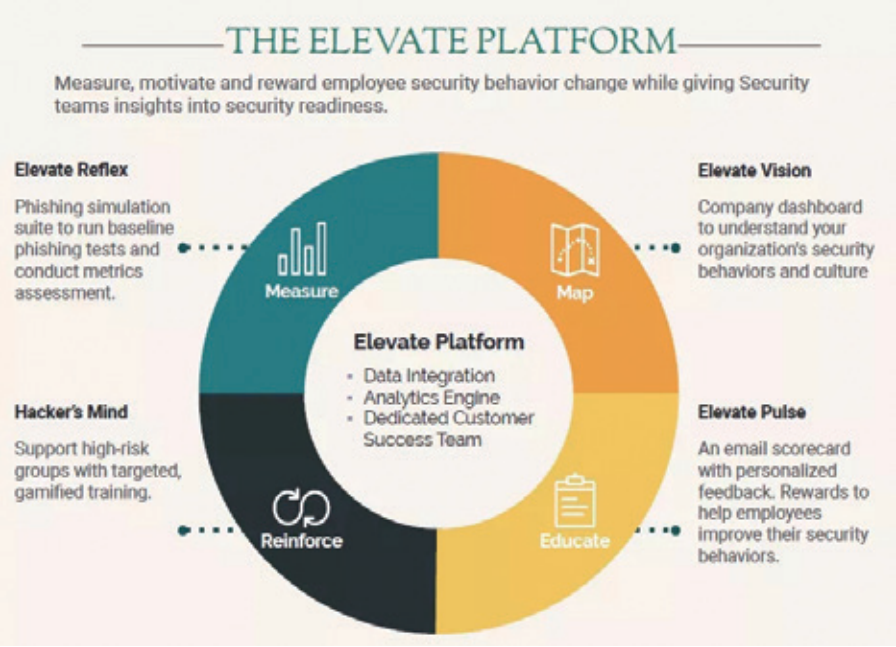


行业已经有不少公司做安全意识培训（Security Awareness Training），Gartner也发布过魔力象限。大部分传统安全意识培训产品的主要竞争力在于系统的、科学的培训内容，以及与内容相匹配的计算机培训辅助系统。而这些内容和工具则主要是围绕通过“培训”以提升“意识”的目标而构建的，这导致安全意识的提升过程更类似对机器打补丁升级的过程，难以明确度量个人在这一过程中的行为变化，而潜在的风险正蕴含于诸多人的行为细节当中。

Elevate Security提供的平台旨在通过统一的可视化手段，监测、管理员工的安全行为，并提供助于提升企业安全文化的邮件反馈和安全教育资源，以可量化的方式促进员工安全行为的改善，帮助企业管理者有效降低员工人为因素关联的安全风险。有了评价指标，就能形成闭环，帮助企业迭代地改善员工在安全防护中的主观能动性，提高企业整体的安全防护水平。

三、产品介绍

Elevate平台主要提供以下四个功能模块，Reflex提供网络钓鱼邮件攻击模拟及相关结果评估；Vision是一个仪表盘，将钓鱼邮件攻击模拟结果及通过API集成的其他员工人为因素相关安全数据统一整合及分析，具备部门级和个人级的下钻视图；Pulse提供可配置的、基于邮件的员工评级反馈系统，以个性化的方式向员工提供整体的以及多个内容模块的安全行为评级；Hacker’s Mind提供攻击者视角的安全培训，以针对性提升关键部门、高风险员工的安全意识和防护能力。

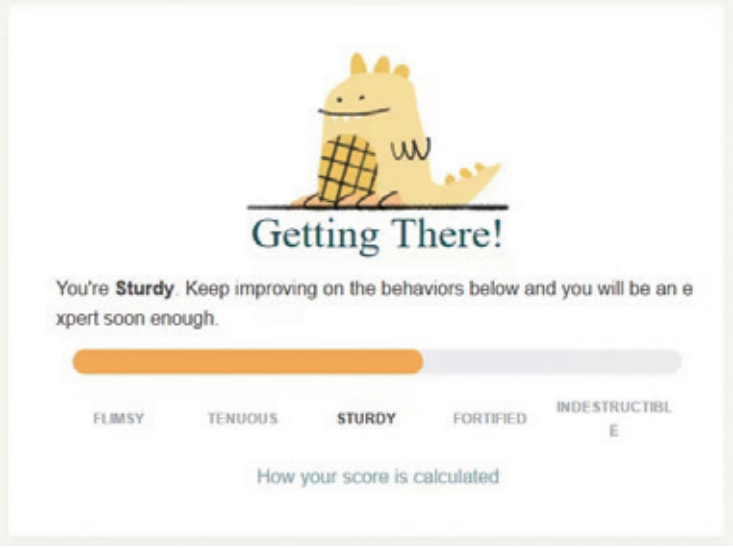


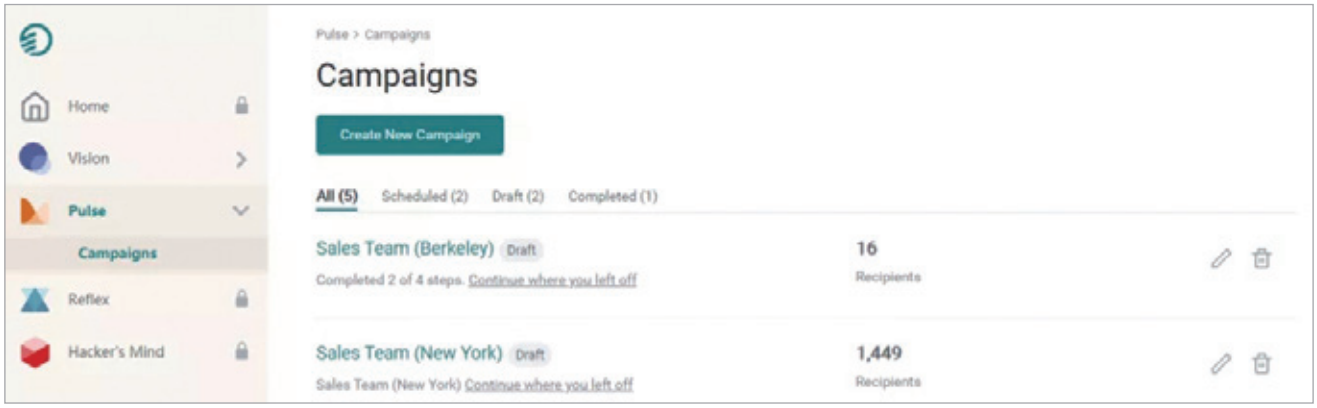
基于以上四个功能模块，提升组织内部人员安全意识、培育安全文化可以分步进行，即通过Reflex完成钓鱼邮件攻击模拟，建立安全基线评级；通过Vision仪表盘分析并跟踪企业各层级人员的整体、总体安全行为风险；通过Pulse邮件评分卡机制反馈人员行为评分，激励行为改进；最后，针对高风险个人或部门，提供针对性个性化的安全培训强化。

Elevate提供了平台的基本试用功能，在此简单介绍。该互动式Demo主要包括Vision和Pulse两部分。可以看到Vision Dashboard提供的视图很简约。从部门级别上，包括总体安全风险值、风险分布、部门评分以及行为映射。行为映射（Behavior Map）是以部门为单位，对所收集的安全行为数据的整合评级，直观反映部门在各维度上，包括整体、桌面清理、恶意软件、密码安全、钓鱼攻击测试、培训等维度的风险等级。从当前信息看，该Elevate Demo所集成和展现的大部分数据源需要通过外部API接入，平台内部只提供基于Reflex的钓鱼邮件攻击模拟的评级数据。

Vision视图下还提供各部门内部的总体和个人评级及排序，提供更细节、直观的安全风险视图。

管理。在Demo中，只能够向试者用邮件发送样例反馈邮件，包括不同等级评分的三份邮件。以一份评级为“Sturdy”的反馈邮件为例，评分分为Phishing & Reporting、Password Manager、Training、Malware、Clean Desk这五个部分，对应Vision仪表盘中集成的五项内容。每一项内容都有对应具体内容，例如对于Phishing & Reporting，包含钓鱼邮件攻击的具体时间、员工个人评估结果以及与同部门其他员工的横向对比结果。当然，如果某一项评估达标，邮件中会有类似于徽章的激励机制，以鼓励员工集齐所有安全徽章，完成对应的完全行为标准。





在Pulse标签下，提供Campaigns功能。该功能应可提供可配置的，基于邮件的安全评级反馈及

四、公司解读

“以人为本”，以人及其行为为核心，关注人员因素在网络空间安全中的关键作用，从组织、策略、流程、法律法规等角度持续管理、监控企业安全风险，进而针对性、系统性的发现脆弱性，降低安全风险，已成为网络安全防御的关键一环。国内许多大型企业的安全管理部门也开始具备包括职工安全培训、安全评估检查等能力。Elevate Security基于平台提供的钓鱼邮件攻击模拟、可视化分析、邮件反馈系统及场景式的安全培训能力，向业界提供了一个企业安全文化培育的平台化范本，能够给各类型组织对个人安全行为的管理机制和方法提供有力的模板。同时，以面向人的安全行为因素在网络安全场景下的风险管控闭环为主题，讲述了一个完整并且切中管理痛点的好故事。不止于此，Elevate Security提供的不止是思路和机制的创新。该公司基于已有平台，提供面向各客户组织的定制化解决方案，包括数据接入、安全流程等层面的定制和咨询，这些平台技术之外的能力补充同样是该公司的核心竞争力。

从现有资料来看，Elevate平台提供的功能可以用简约而不简单来概括。Elevate平台所展现的功能一目了然，也没有呈现复杂的流程，平台背后所使用的技术不是其核心竞争力。“Let's target security behavior change, not awareness.”Elevate的核心功能路线很清晰，以员工安全行为的改善作为目标，提供包含定制化的数据测量、集成、分析、反馈、行动（培训）的流程迭代和闭环，以及持续的、量化的风险评估机制与平台，提升管理者对企业整体到员工个人的安全风险等级的洞见、监控和管理能力。以量化的方式关注人的安全行为改善而不停留于填鸭式的安全培训，Elevate Security是打破传统安全意识培训产品形态固有思路的先行者。相信未来Elevate平台会提供更多的平台化组件，满足各类型组织对内部人员的动态、持续、自适应的安全行为风险量化评估与安全行为提升需求，以适应更高级的攻防场景、更严谨的法律法规要求。

参考链接

[1] https://elevatesecurity.com/
[2] https://www.crunchbase.com/organization/elevate-security
[3]《Understanding Security of the Cloud: from Adoption Benefits to Threats and Concerns》
[4] https://www.gartner.com/doc/3950454
[5] Top Cybersecurity Trends for 2016-2017, Gartner Security & Risk Management Summit 2016

ForAllSecure：融入 DevSecOps 的“下一代”模糊测试技术

2020年2月24日-28日，网络安全行业盛会RSA Conference将在旧金山拉开帷幕。今天绿盟君将介绍创新沙盒十强初创公司之一：ForAllSecure。

一、公司介绍

ForAllSecure是由来自卡耐基梅隆大学的ForAllSecure安全研究团队于2012年创立的公司，工作地点包括宾夕法尼亚州匹兹堡、旧金山湾区和弗吉尼亚州水晶城。创始人David Brumley、Thanassis Avgerinos和Alex Rebert均来自卡耐基梅隆大学并拥有相关专业背景。公司在A轮融资中获得1500万美元，由New Enterprise Associates领投。其主打“下一代”模糊测试技术，并基于此技术实现模糊测试系统Mayhem，凭借Mayhem的出色表现以大幅领先优势在美国国防部先进项目研究局（DARPA）于2016年主办的网络超级挑战赛（CGC）中一举夺魁。ForAllSecure还在2017年被「麻省理工科技评论」选入“全球最聪明的50家公司”榜单（位列第35名）。

公司提供Mayhem模糊测试解决方案，将自动化持续性安全测试融入DevOps流程，力求在早期发现漏洞、修复漏洞，以提高软件安全性。与传统模糊测试技术相比，该“下一代”模糊测试技术结合使用“符号执行”技术和“导向型模糊测试”技术，能够针对测试发现的安全漏洞自动化生成概念性验证（PoC）和补丁，在一定程度上避免传统白盒测试的高误报和黑盒测试的盲目性，具有很高的创新性和价值。

二、背景介绍

根据Cybersecurity Ventures的应用安全报告显示，应用程序的攻击面正在以每年1110亿行代码的速度增长，另外，0day漏洞利用程序被公布的速率已经从2015年的“每周一个”增长到2021年的“每天一个”。

与此同时，DevOps正在被越来越多的团队和组织接受和采用。然而，绝大多数应用安全工具并不能跟上DevOps的脚步。例如，由于其居高不下的误报率，“静态代码分析”工具大大限制了安全、开发和测试人员的生产力。

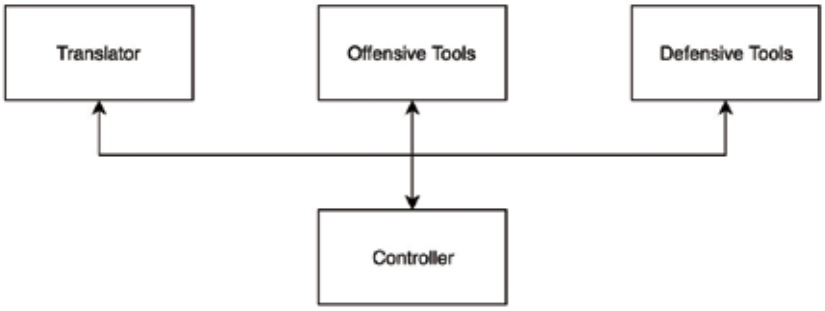
另一方面，企业级漏洞管理方案则是有限应对策略。例如，“软件组成分析”工具只能检测那些已经被公开并分配了CVE编号的漏洞。

面对这些限制和问题，ForAllSecure提供“下一代模糊测试”安全方案Mayhem，兼具导向型模糊测试的可靠性和符号执行技术的创造力，帮助企业在软件开发生命周期中更早地发现安全风险并快速消除。

三、产品介绍

Mayhem是一个帮助企业以机器级速度和规模测试软件的辅助型智能行为测试解决方案。它结合使用符号执行和导向型模糊测试技术，通过监控目标程序的行为来动态生成测试用例。

官方并未直接给出Mayhem的架构组成。绿盟君根据官方公开资料整理出的大致架构如下：



其中：

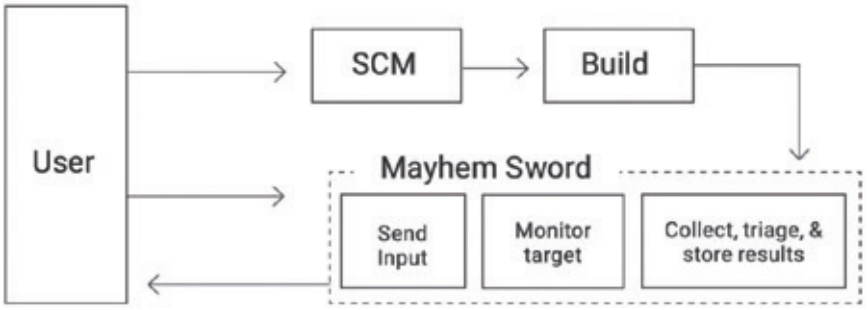
Translator用于将二进制程序翻译为易于分析的中间表示；

Offensive Tools用于寻找漏洞并构建PoC或ExP；

Defensive Tools用于生成补丁；

Controller用于统筹整个流程；

Mayhem的工作流程如下：



我们可以看到，上述流程正是DevOps的一部分：

1、用户向SCM（代码仓库）提交应用代码；

2、系统自动基于SCM最新代码构建应用；

3、系统自动将构建的应用提交给Mayhem进行测试，而Mayhem的测试又可分为三个相辅相成的逻辑模块：

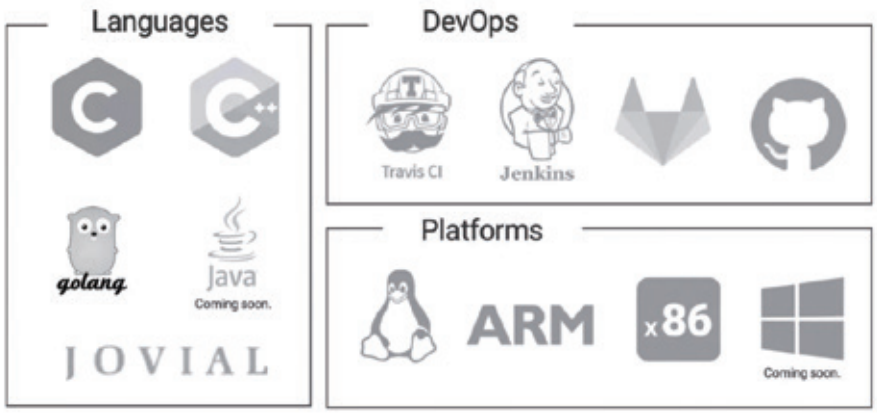
发送测试数据

监视目标行为

收集、分类并储存结果

4、用户与Mayhem交互，查询应用的风险情况并进行下一步处理。

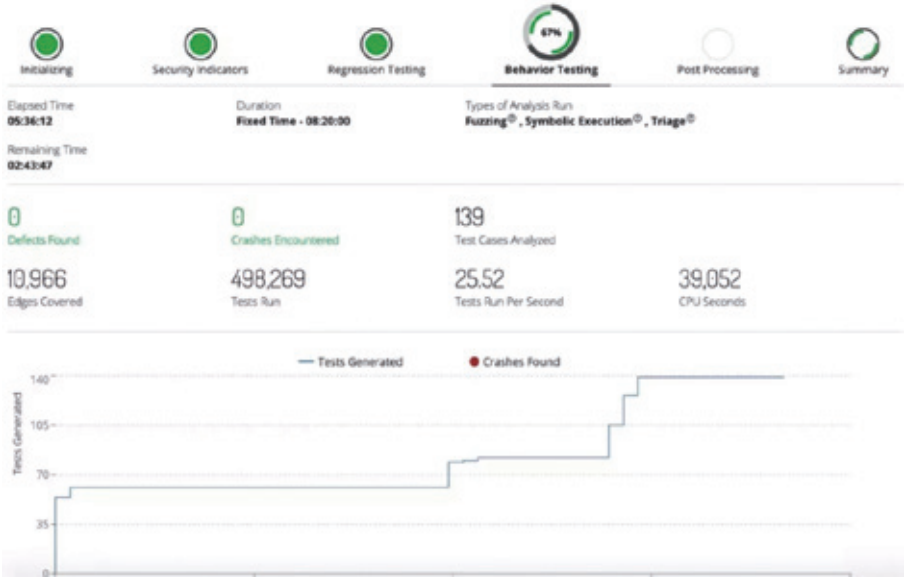
另外，Mayhem支持多种语言、平台和DevOps环境，能够满足不同用户的需求：



接下来，我们展示一个具体的应用案例。借助这个案例，我们能够真正触摸到Mayhem，对其工作流程有深层次的理解；另一方面，也能够在一定程度上体会到它的实力和价值所在。

开始测试

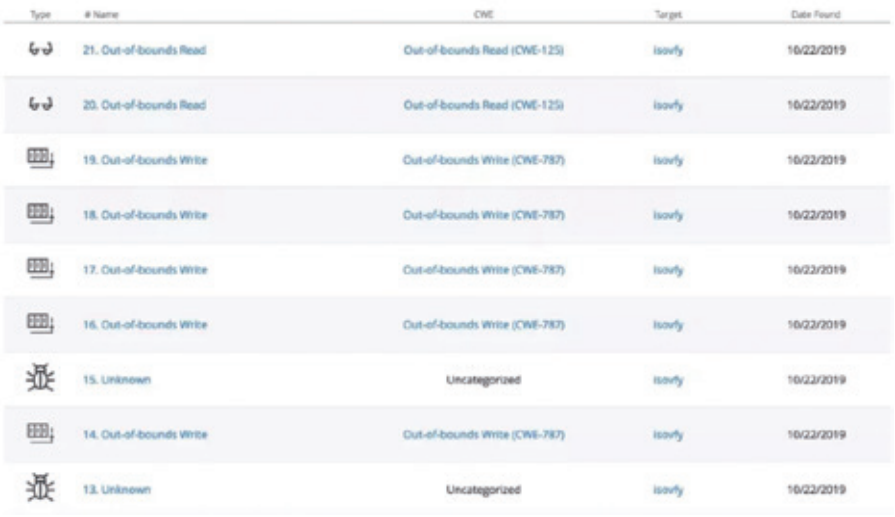
Mayhem提供了友好的用户交互界面。初始化完成后，正式进入测试阶段，可以看到测试正在进行：

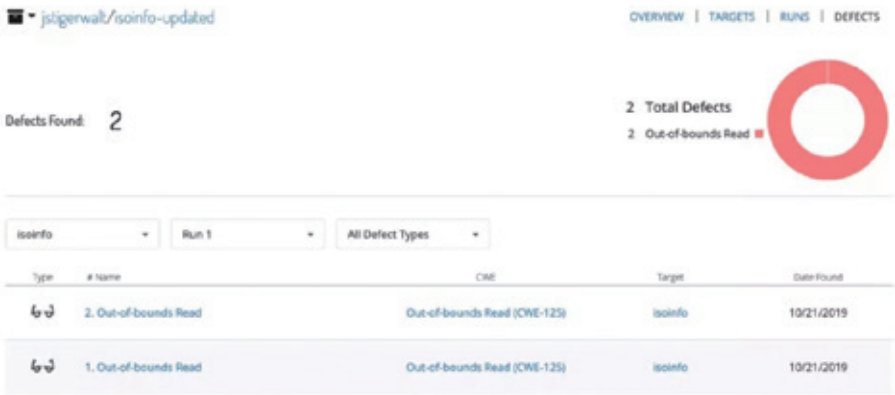


查看基本测试结果

测试结束后，可以查看测试结果，了解应用的脆弱点：

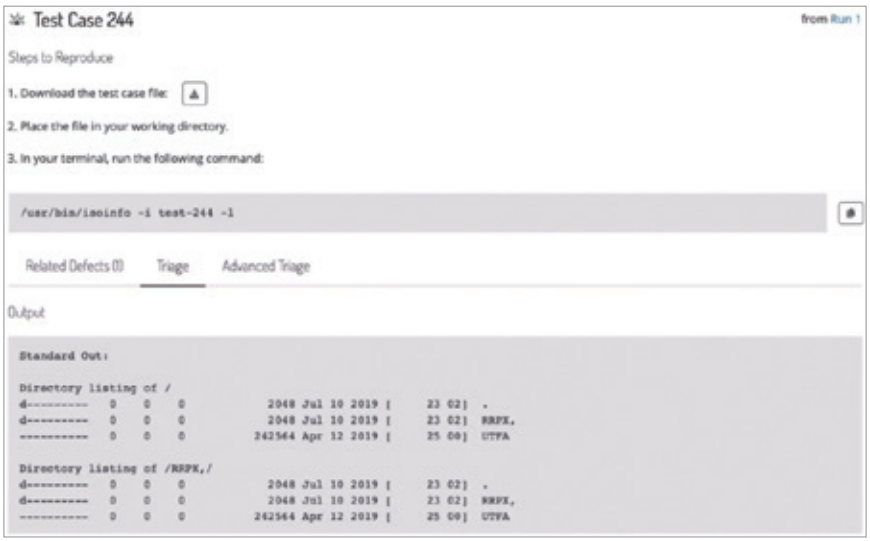
值得注意的是，Mayhem根据CWE对脆弱点进行了分类：

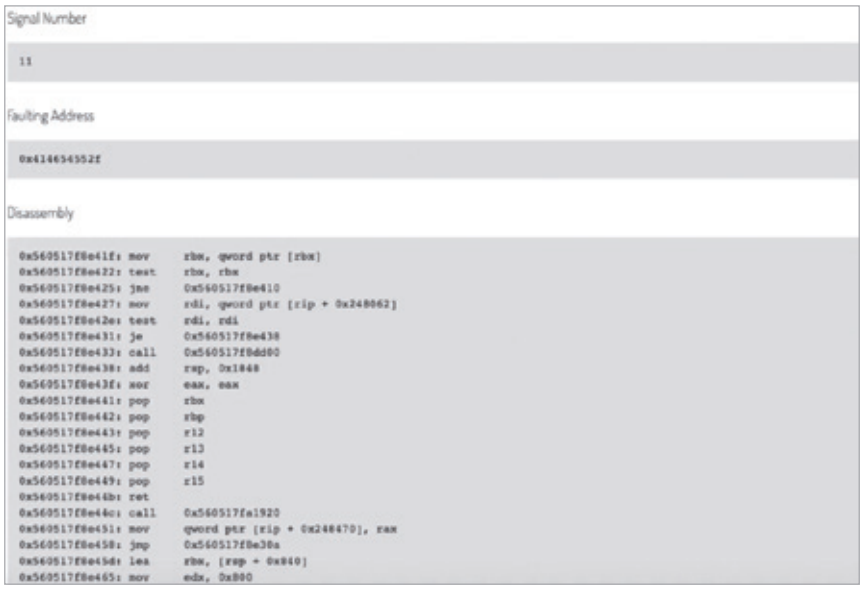




查看详细测试结果

我们还可以查看具体测试用例的输入输出，从而精确定位问题（甚至可以看到反汇编后的代码）：





ForAllSecure强调Mayhem的优势之一是零误报。那么如何做到零误报呢？从上面的测试结果我们可以略知一二。Mayhem自动构建的测试用例等效于研究人员手工验证漏洞时编写的PoC。一般来说，如果能够导致程序出现崩溃或其他异常（代码逻辑预期之外的行为），我们便认为PoC是有效的，同时认为漏洞存在。

四、产品特点

持续性深度分析：随着目标程序知识的积累，Mayhem的分析将逐渐深入，代码覆盖率将逐渐提升。

零误报：Mayhem报告的所有缺陷均是准确的（因为它会自动生成PoC去测试）。

自动化生成测试用例：基于团队在卡耐基梅隆大学的专利技术，Mayhem能够利用目标反馈在运行时自动化生成测试用例。

安全左移：在安全开发流程中，Mayhem将动态分析、模糊测试及威胁建模等测试与验证步骤左移，帮助企业控制修复成本。它能够直接插入到CI流水线中，将持续性测试作为DevOps工作流的一部分。

软件供应链管理：Mayhem能够对应用依赖的开源或第三方代码进行威胁评估，以减少软件供应链中存在的风险。

五、总结

在整个调研过程中，绿盟君能够从各路媒体报道和ForAllSecure官方对Mayhem技术原理的概括性描述中感受到其团队拥有的深厚技术积淀。抛开立场不一的媒体，三个事实足够证明他们的雄厚实力：

1、公司未立，技术先行：作为一支来自卡耐基梅隆大学的科研团队，其技术的诞生时间比公司成立时间早很多年；

2、以绝对优势获得DARPA CGC决赛第一名：挑战赛集合了全球安全领域的顶尖团队，ForAllSecure从104支队伍中脱颖而出进入七强杀入决赛、并获得冠军，这是硬实力的体现；

3、获得New Enterprise Associates领投的1500万美元融资：这是资本的评估和认可。

另一方面，ForAllSecure对当前安全测试技术的痛点把握得十分到位。安全从业者往往会有这样的感受：自动化白盒测试（如静态代码分析等）具有不小的误报率；自动化黑盒测试（如漏洞扫描等）既有一定的误报率，同时也有自身的局限性——受限于漏洞知识库；人工渗透测试虽然效果显著，但自动化的缺失导致其无法融入DevOps流程；而传统模糊测试技术的主要玩家通常是职业或半职业的漏洞猎人。

在此形势下，ForAllSecure给出了一个支持DevOps的企业级模糊测试方案，并在一定程度上证明了该方案的有效性（DARPA CGC），这无疑是令人振奋的。

然而，我们也要提出问题：Mayhem是否真如ForAllSecure描述的那么优秀？他们是否在把握住痛点的同时较好地解决了难点？

符号执行和模糊测试本身并不是新技术，人们对两者的优势和缺陷也都早有研究。符号执行技术更多地具有理论上的先进性，但是在应用到复杂程序时往往会遇到路径爆炸等问题；模糊测试的结果则与输入集的数量和质量有着密切的关系。

通过DARPA CGC，我们看到了Mayhem在漏洞检测和验证上的有效实力，但是我们也注意到，在比赛中Mayhem需要大量的水来进行冷却（CGC决赛为七支队伍配备了180吨水进行水冷）和大规模的算力、能源支持，这些都是前述技术局限性在具体实现上的客观反映。有时候，产品和方案的优秀并不完全由技术上的优势决定。安全行业的特点决定了成本与效果——也就是性价比往往才是最重要的。因此，Mayhem的成本和市场定位也许是需要初创团队考虑的问题，也是客户关心的问题。

滚滚长江东逝水，浪花淘尽英雄。ForAllSecure真的能够推动DevSecOps发展，还是仅仅昙花一现？Mayhem到底是学术界的玩物，还是真的能够成为业界一大杀器？这些都需要时间的检验。然而，就本次创新沙盒竞赛而言，综合考虑技术实力与团队背景，绿盟君认为ForAllSecure具有极强的竞争力，同时看好他们的后续发展。让我们拭目以待。

参考文献

[1] Mayhem, the Machine That Finds Software Vulnerabilities, Then Patches Them
[2] MIT Technology Review Reveals 50 Smartest Companies List in Annual Business Issue
[3] ForAllSecure
[4] ForAllSecure: About us
[5] DARPA网络超级挑战赛情况及思考
[6] 符号执行技术总结（A Brief Summary of Symbol Execution）- wcventure

注：第3节引用了来自VDA Labs的资料Using-Next-Generation-Fuzzing-Tools.pdf；第4节参考了ForAllSecure官方资料FY19 DS Mayhem General v3.7.pdf。

INKY：基于机器学习的恶意邮件识别系统

2020年2月24日-28日，网络安全行业盛会RSA Conference将在旧金山拉开帷幕。绿盟君已经为大家介绍过入选今年创新沙盒的十强初创公司：Elevate Security 、Sqreen、Tala Security和AppOmni四家厂商了，今天将为大家介绍的是：INKY。

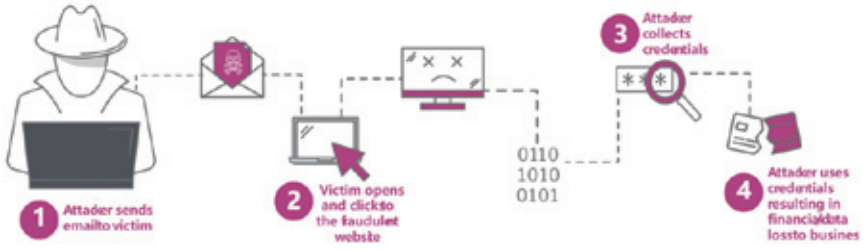
一、公司介绍

INKY公司的总部位于马里兰大学公园，凭借独特的计算机视觉、人工智能和机器学习技术，INKY在电子邮件防护领域处于行业领先的地位。目前，该公司已经完成了三轮融资，共筹集了1183.5万美元。其最近的一次A轮融资在2019年11月，融资金额为600万美元。公司创始人Dave Baggett还与他人共同创立了ITA Software公司（ITA Software公司是业内领先的机票搜索公司，于2011年被谷歌以7.3亿美元收购，目前为谷歌Flights®提供支撑）。

INKY Phish Fence是该公司的旗舰产品，该产品是一个基于云计算的电子邮件安全平台。该平台能够像人一样理解电子邮件，分析其中的欺诈、钓鱼等恶意行为，以防止企业被恶意邮件攻击。

二、背景介绍

钓鱼邮件是最常见的网络威胁之一。大部分网络攻击都是以钓鱼邮件为切入点。Gartner的数据显示78%的网络安全事件中涉及到钓鱼邮件。传统钓鱼邮件的原理如图所示。



攻击者首先伪装成一个可信的实体给受害者发送邮件，并欺骗受害者点击电子邮件中的恶意链接或者下载恶意附件，从而导致受害者的主机被安装恶意软件，进而导致受害主机被勒索软件攻击或者数据泄露。

然而，当今网络钓鱼邮件正变得越来越具有迷惑性，所以即使经验丰富的安全人员也无法有效的对其进行分辨。其中，商业邮件失陷（Business Email Compromise ，BEC）每年造成12亿美金的损失。BEC攻击通常通过正常的商务流程，但会伪装成企业的员工、商业伙伴或供应商，通过社工手段窃取企业的资金或敏感数据。与传统的钓鱼邮件包含恶意链接或附件不同，

BEC攻击者的邮件内容等是正常的，所以网络安全层面的检查无效。因为邮件安全引起的业务损失较高，应对BEC相关的安全产品成为Gartner 2019年十大项目之一。在相关的产品中，机器学习技术越来越多的被用来识别恶意邮件，并取得了较好的效果。

三、产品介绍

INKY Phish Fence是该公司的主打产品。该产品是基于云的电子邮件防护软件。基于特定领域的机器学习和计算机视觉技术，该产品可以识别并阻止多种恶意邮件，包括钓鱼邮件，诈骗邮件等。同时，该产品可以和多种电子邮件服务组件相结合，包括Exchange、Office 365、G Suite，为其提供全方位的防护。

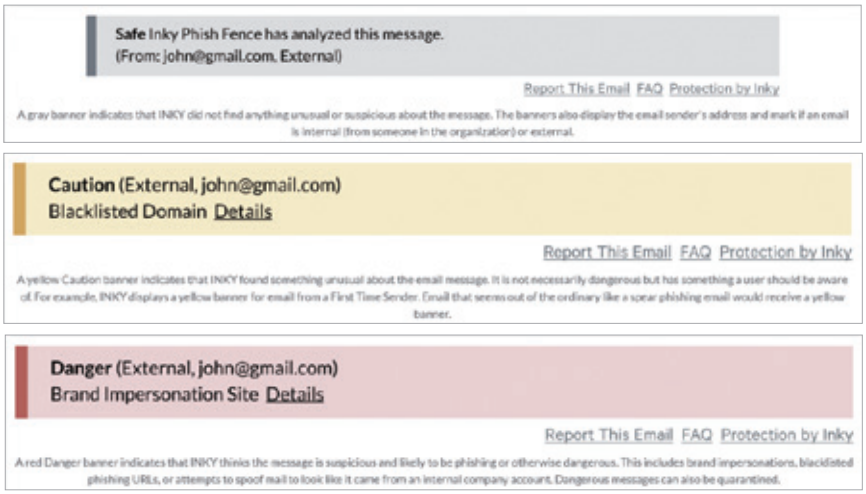
1、Exchange：Exchange 是微软公司的电子邮件服务组件。INKY可以与Exchange无缝集成。INKY通过自动扫描所有内部和外部的电子邮件，寻找其中的钓鱼邮件、恶意邮件、垃圾邮件等。恶意电子邮件会被隔离。

2、Office 365：Office 365 是一种订阅式的跨平台办公软件，基于云平台提供多种服务。Office 365是很多钓鱼邮件攻击的主要目标。由于钓鱼手段的巧妙和狡猾，Office 365本身和传统的第三方安全系统并不能有效的检测到。INKY可以与Office 365无缝集成，具有针对Office 365平台的自定义实现。它集成起来又快又容易。INKY还可以分阶段部署，易于实施。

3、G Suite：G Suite是Google 在订阅基础上提供的一套协作软件工具。INKY可以与G Suite无缝集成，实现对恶意邮件，钓鱼邮件的准确检测。

INKY Phish Fence过滤每一封电子邮件。在最终呈现给用户的邮件中，该系统会在每一封邮件的顶部加上一个横幅（banner），来对邮件的安全性进行说明。

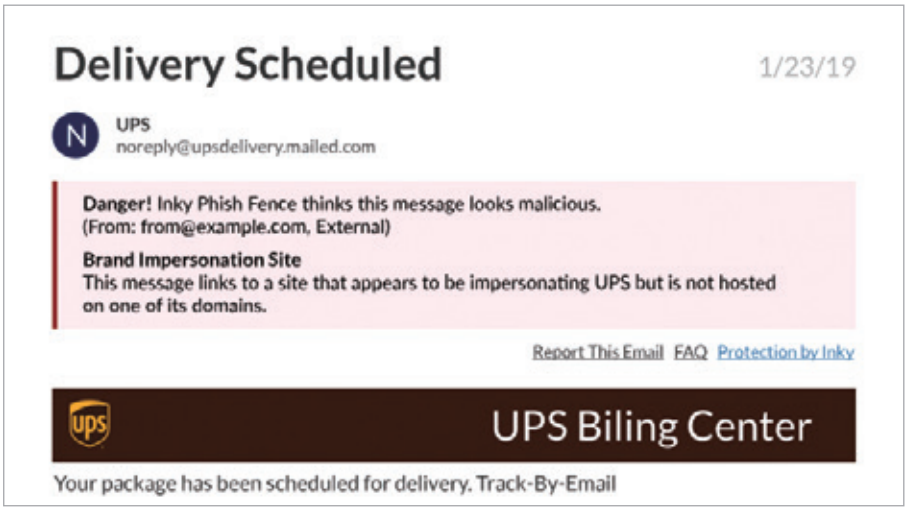
横幅是INKY Phish Fence的一大特色，如图所示。



不同风险程度的邮件用不同的颜色标识。其中，灰色横幅用于标识安全的邮件，黄色横幅用于标识谨慎打开的邮件，红色横幅用于标识危险邮件。在黄色和红色标识中点击“Details”链接可以进一步查看对邮件的描述。这些信息可以让用户了解他们的收件箱中存在的威胁。另外，这些信息可以让用户学习到更多的钓鱼邮件相关的知识，这往往比钓鱼邮件模拟测试更加有效。横幅中的“Report This Email”链接允许终端用户报告来自任何终端设备的有问题的电子邮件，而不需要特殊的客户端软件。INKY甚至整合了自然语言处理(NLP)算法来识别敏感内容，如电汇或发票付款请求、密码相关的电子邮件等，并在横幅中标注客户可配置的策略来对用户进行指导。

四、核心技术

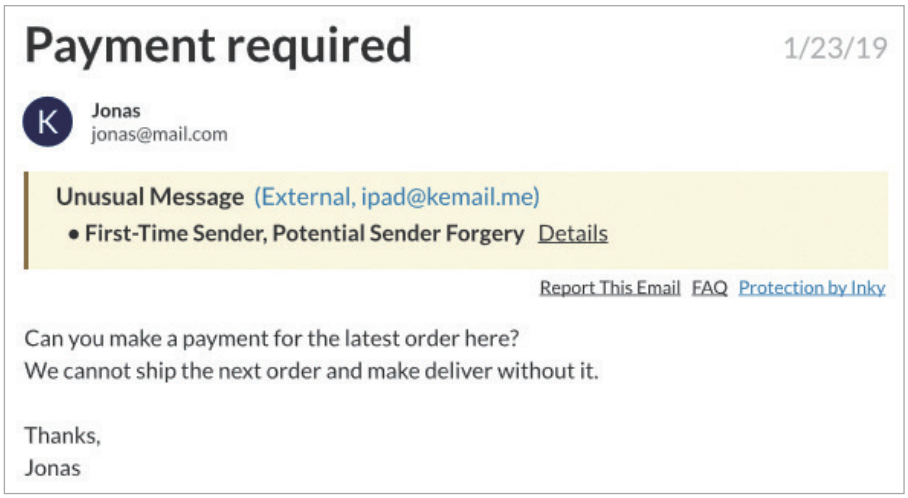
传统的电子邮件安全解决方案通常只依赖于已知的攻击者数据库。INKY除了使用最新的数据库外，还使用机器学习和计算机视觉技术来检测钓鱼邮件，甚至捕捉零日的BEC钓鱼诈骗。超过24个计算机视觉和文本分析模型能够像人一样“看到”邮件信息，并捕捉人类可能会忽略的文本、类型和图像的异常。通过智能分析，可以检测出有问题的电子邮件。



钓鱼邮件检测：钓鱼邮件中往往包含有恶意链接。INKY对收到的电子邮件中包含的每个链接进行模拟点击，并检查相关的网页是否有钓鱼或其他恶意内容的特征。含有恶意网站链接的电子邮件会被标记告警或隔离。

恶意代码检测：HTML为电子邮件提供了更高级别的可配置性，但也使得在电子邮件中嵌入恶意可执行代码成为可能。默认情况下，INKY能够标识并阻止执行跨站点脚本攻击（XSS）、JavaScript和CSS攻击的代码。

可疑发件人检测：INKY的机器学习引擎可以通过行为特征和社交网络图谱来识别可疑的行为或身份。通过观察邮件在组织中的流动情况，INKY可以为所有的人创建行为档案。当INKY看到一封电子邮件的发件人的特征与学习到的特征不匹配时，它会发出告警，如图所示。



结果上报：INKY产品的一个独特的功能是可以在每封电子邮件中点击“Report this Email”链接。这意味着用户可以在不需要安装特定软件的情况下报告来自任何设备（web、手机、任何电子邮件客户端）的有问题的邮件。而大多数电子邮件保护软件只能在已安装特定软件的系统上工作。这样，INKY可以随时收到用户对检测结果的反馈，进一步完善其检测模型。

四、总结

随着钓鱼邮件越来越具有迷惑性，传统的基于规则的检测方法已经无法有效的进行检测。INKY公司的产品INKY Phish Fence采用机器学习技术对邮件进行智能分析，可以更加有效地识别钓鱼邮件。而部署在云端的检测系统使得企业部署更加灵活。同时，该产品可以与Exchange，Office 365和G Suite等办公软件无缝集成，能够为企业提供更加全面的防护。

参考链接：

[1] Gartner 2019十大安全项目：https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2019/
[2] https://www.crunchbase.com/search/funding_rounds/field/organizations/num_funding_rounds/arcode
[3] https://www.inky.com/
[4] Gartner Security & Risk Management Summit 2019

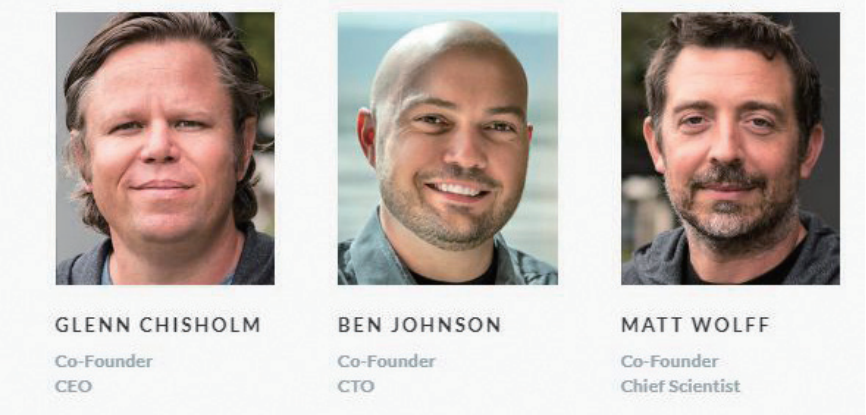
Obsidian：能为 SaaS 应用程序提供安全防护云检测与响应平台

2020年2月24日-28日，网络安全行业盛会RSA Conference将在旧金山拉开帷幕。今天，绿盟君将继续为大家介绍入选今年RSAC创新沙盒十强的初创公司：Obsidian。

一、公司介绍

Obsidan Security公司成立于2017年，于2017年7月完成A轮950万美元融资，现总融资额已达2950万美元，主要由Greylock Partners、Wing和GV投资。

Obsidian公司是一家为企业提供云检测与响应的公司，总部位于加利福尼亚州纽波特海滩。创始团队来自于Cylance、Carbon Black和NSA，Cylance前任CTO格兰·奇什霍尔德创立并出任CEO，Cylance前任首席数据科学家兼NSA计算机科学家马特·沃尔福担任CTO，Carbon Black公司前CTO兼联合创始人以及NSA计算机科学家本·约翰逊则担任首席数据科学家。



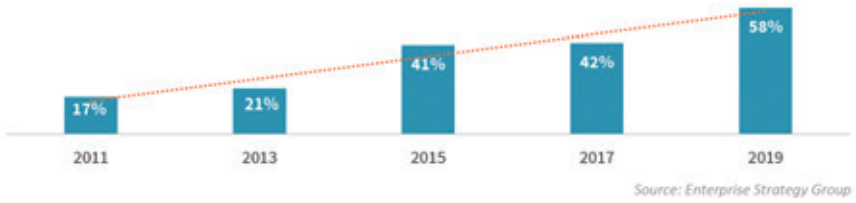
Obsidian提出了一个新的理念-CDR(Cloud Detection and Response)能为SaaS应用程序提供安全防护，并能帮助安全运营团队检测并响应入侵和内部威胁。旨在快速发现、调查和响应SaaS应用程序中的漏洞和内部威胁，在不影响业务的情况下实现持续的监控与分析。

二、产品介绍

◆ 产品背景

在过去的十年中，SaaS和公共云服务的使用取得了巨大的增长。组织已经或正在将其业务系统（包括电子邮件，协作，HR，销售，市场营销和运营）迁移到云中。在2019年ESG研究调查中，三分之二（67%）的参与者报

告，现在超过20%的应用程序基于SaaS，而超过58%的组织在2019年报告使用了IaaS。



2011-2019年使用基础架构即服务（IaaS）的组织百分比

◆ 云检测与响应（CDR）

云检测与响应是Obsidian提出的一个新的理念，也是当前云安全体系中缺失的一部分。

云访问安全代理（CASB）之类的解决方案采用的是预防策略。CASB在结构上像云环境的防火墙，充当组织基础架构与云服务之间的中介，主要是通过阻止访问来防止数据丢失和泄露以及恶意软件暴露。

但是，正如Gartner在自适应安全的理念中提及，预防性（Prevention）控制并不足以保护云环境免受攻击。即使有了最好的预防性安全解决方案，攻击者仍可以穿透或绕过防御获取对云资产的访问权限。在云中，安全团队需要快速检测（Detection），调查并响应威胁（Response），这就需要可视化和丰富的用户上下文信息，以便实时的检测和响应可疑行为。而如今，这正是SaaS和云服务所缺少的功能。

与EDR相比，云环境中的可视化问题有所不同，并且更为复杂。因为用户针对不同应用程序有不同的权限，因此SaaS应用程序需要在平台内进行授权管理。比如安全管理员想查看用户可以在Salesforce中访问的内容或他在G Suite中的操作，则管理员必须先获取相应权限和行为日志，并了解每个服务的授权模型和行为日志格式，然后再确定根据这些信息确定是否发生可疑的攻击事件。大量的访问记录和行为信息使得威胁检测变得异常复杂，通常相关的上下文数据会产生TB级数据，这使得真正的威胁或攻击事件空间被淹没在大量的数据流中。

针对以前的需求，提出了云检测和响应（CDR）解决方案，CDR通过不断收集，规范化和分析来自SaaS和云服务的大量状态和行为数据，为安全专业人员提供了检测，调查和响应云中威胁所需的全面的可视化信息。

因此，CDR需要提供以下核心功能：

1、全局可视化

CDR需要提供一个全局可视化视图来显示用户跨云服务的访问和行为信息。这种全局可视化视图融合了状态和用户行为数据，并集成了威胁情报和相关上下文信息（位置、设备、浏览器等）。基于这种可视化视图，安全团队可以有效的实现不同阶段的威胁检测，并快速实现事件调查和响应。

2、自动检测

CDR所要分析的数据通常比较大，因此，当前云环境的问题是威胁或是攻击行为通常会被淹没在大量的数据与告警中。因此，CDR利用机器学习和规则分析可以帮助SOC从大量的噪声数据中提取有价值的信息。

3、威胁预测

CDR除了具有对已经威胁和攻击的检测能力外，还可以预测云环境中下一步可能发生的异常或威胁行为。这可使安全管理者能提前针对要发生的威胁行为做预防。

◆ Obsidian平台

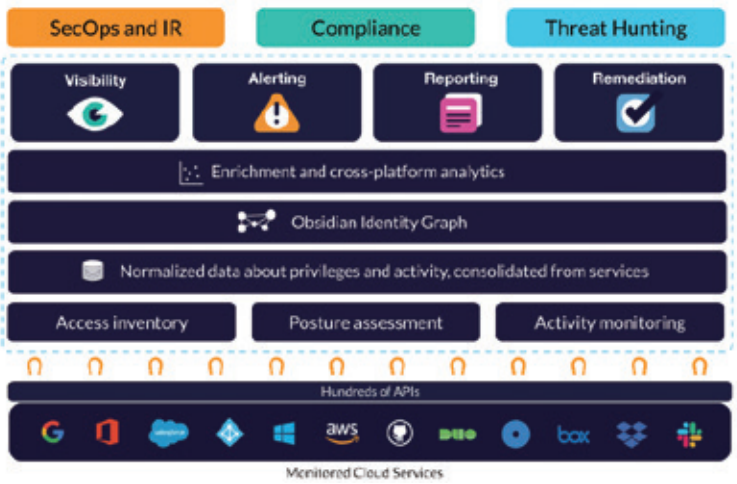
Obsidian云检测和响应为SaaS提供了无缝的安全性。利用一种独特的以身份为中心的方法和机器学习，阻止云中的高级攻击。平台能为SaaS应用程序提供安全防护，并能帮助安全运营团队检测并响应入侵和内部威胁。旨在快速发现、调查和响应SaaS应用程序中的漏洞和内部威胁，在不

影响业务的情况下实现持续的监控与分析。

Obsidian是通过API集成作为SaaS服务的，由于不需要部署任何东西，解决方案可以在几分钟内启动，在几小时内就可以产生结果。

Obsidian自动的收集并标准化云应用的相关数据，并基于威胁情报和上下文来丰富这些数据。Obsidian会基于机器学习和规则针对违规和内网威胁行为生成告警，并不断的从个人和群体行为模式中学习如何来访问数据资产。

基于用户权限和行为的统一视图，Obsidian平台可以实现事件响应、调查和威胁狩猎。平台会建议通过删除过期的账号和修复错误配置从而增强云安全应用的安全性。



Obsidian平台功能

1、可见性

Obsidian首次提出云中的用户、数据和应用程序的统一视图，并可以持续监视用户和服务帐户的行为，对威胁和卫生问题发出告警。可见性主要的功能如下：

a) 每个服务的访问权限和特权清单

b) 特权用户活动

c) 跨SaaS应用程序的活动监视

d)可通过API下载的规范化数据模型

2、告警

根据基于规则的触发器和机器学习，可以获得关于违规、危险行为和策略违规的警告。Obsidian平台可以发现SaaS持久性、OAuth令牌滥用和其他相关异常

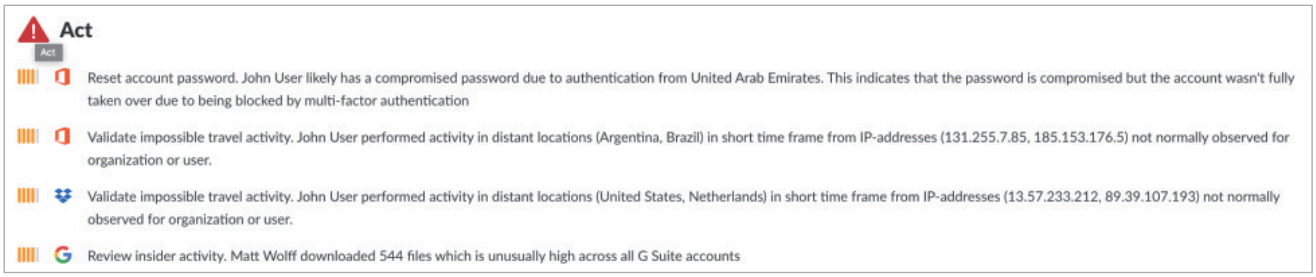
信息。该功能模块包括：

a) 内置规则实现对策略冲突和异常行为发出警报的内置规则

b) 利用机器学习实现异常行为检测

c) 优先处理警报，以减少超负荷的安全团队的警报疲劳

d) 与SOAR和服务管理的可集成性



3、报告

可以根据不同角色，获得关于应用程序使用、新出现的威胁和风险行为的独特见解的报告。因此，平台具有如下功能：

a) 根据组织中不同角色的需要定制报告和仪表板

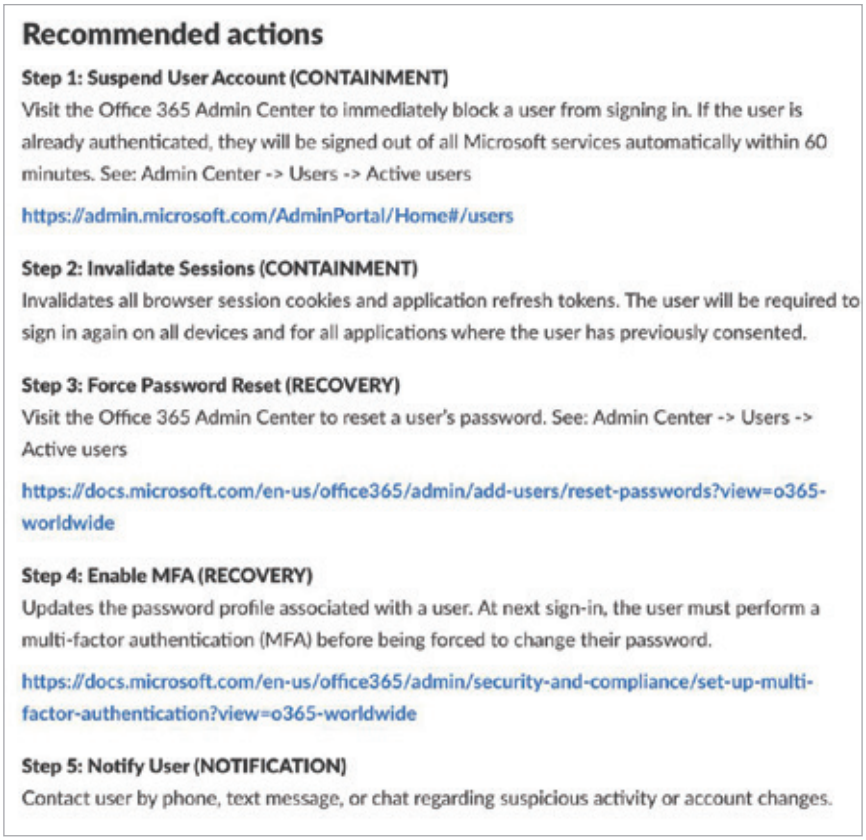
根据需求导出不同格式的数据

4、响应行为

平台基于用户和其行业的统一视图，实现快速有效的异常检测和内部威胁识别，并通过追踪账号共享和文件上传与访问的历史行为来识别用户的横向移动。并能通过平台内置功能，阻断数据泄露和禁止账户滥用。因此，平台需要如下功能：

a) 基于时间关联用户行为和其上下文信息实现异常检测和威胁识别；

b) 提供推荐行为以指导处置。

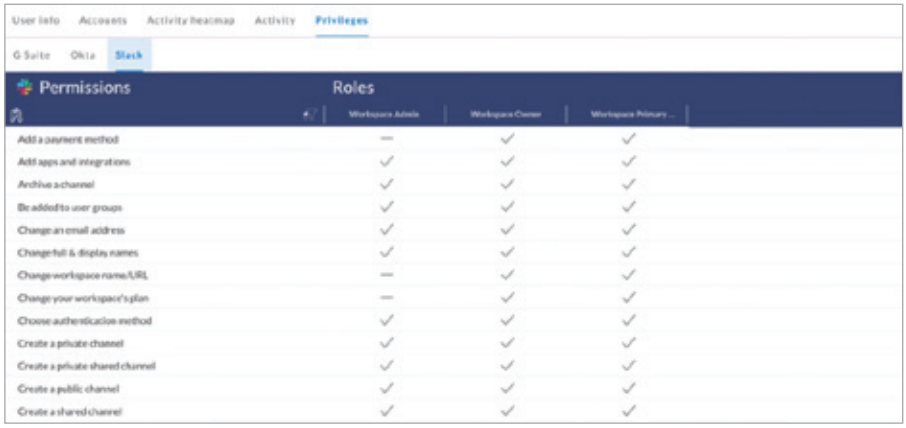


案例

1、账号保护

a) 保护SaaS帐户不被破坏和滥用

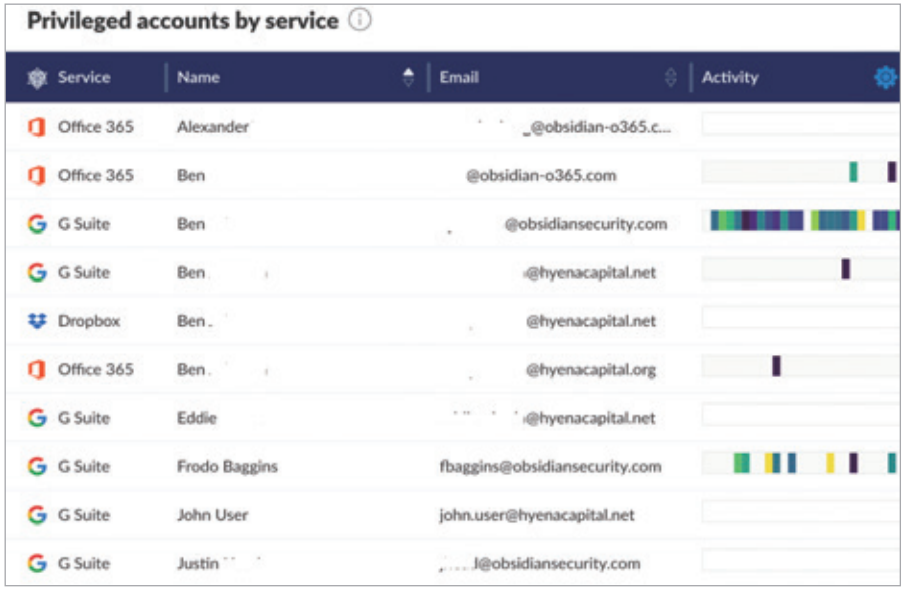
云环境下的关键是如何在不影响合法用户体验的情况下保证云资产的安全。通过全局可见性，Obsidian可以展示哪些用户可以访问SaaS应用程序，以及访问的级别。平台还可以持续监控用户在这些应用程序中做了什么，并删除不活跃的帐户，以缩小攻击面和降低成本。



上图可以看到每个服务上谁拥有什么特权，它们是否处于活动状态，以及它们如何使用这些特权。

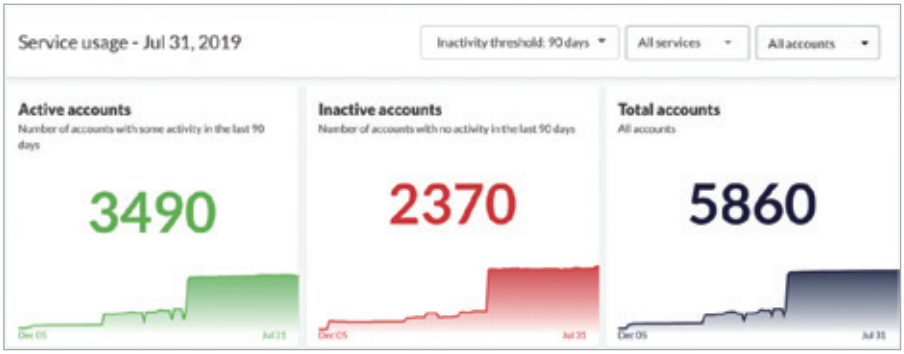
b) 访问特权帐户的目录

获取每个服务中具有特权的帐户清单。



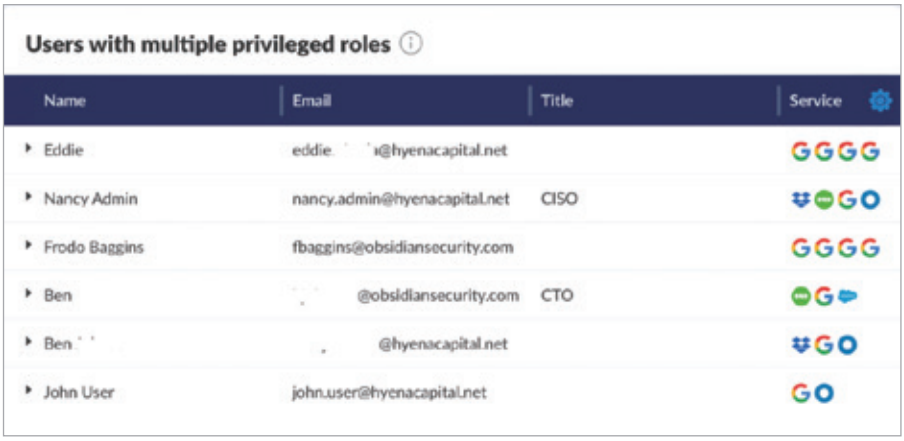
c) 活跃账户与非活跃账号

Obsidian能通过服务获得活动帐户和非活动帐户的粗略视图，其中包含活动情况的历史变化。并且基于这些账户的活动信息，清理不活跃的帐户，以改善身份日常清理和降低成本。



d) 具有多种特权角色的用户

一个用户具有多种特权，可能会对组织构成更高的风险。



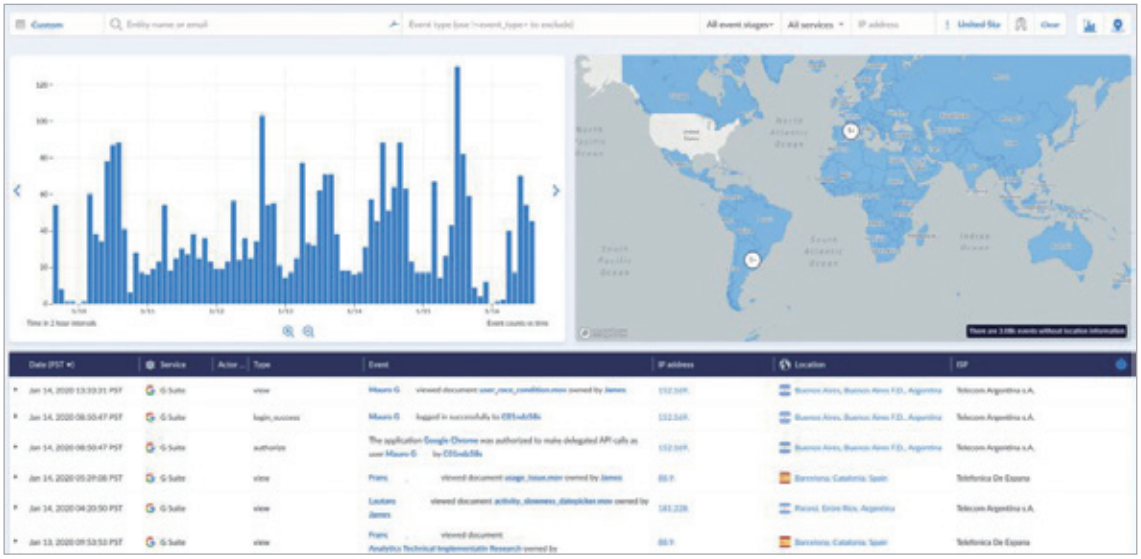
e) 不活动帐户的陈旧用户监控

Obsidian可能监控账户的活跃情况，以便查用户是否已切换角色或离开公司。

2、威胁狩猎

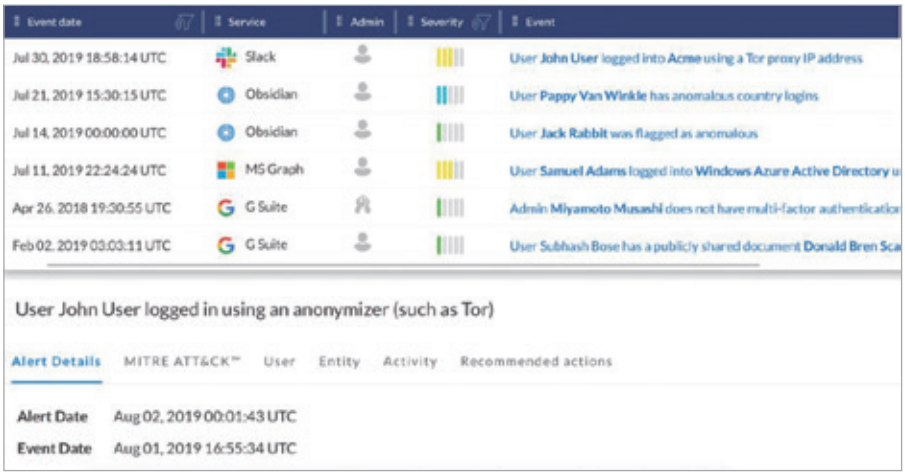
a) 纠正违规和威胁识别

SaaS环境中的威胁检测非常困难，SaaS应用程序本质上是多云环境。Salesforce、G Suite、Slack和其他应用程序都有独特的身份和访问模式，并将有关权限和活动的信息保存在silos中。Obsidian提供了威胁检测、违约修复和安全加固的统一可视化,可以快速检测异常登录、SaaS持久性、数据过滤、横向移动、OAuth令牌滥用和其他威胁的指标，并迅速纠正违规、识别威胁。



b) 警告

Obsidian在不需要进行任何配置的情况下，能够获得各种威胁的告警。Obidian的告警涵盖了众所周知的恶意攻击，并实现了告警严重度排序。

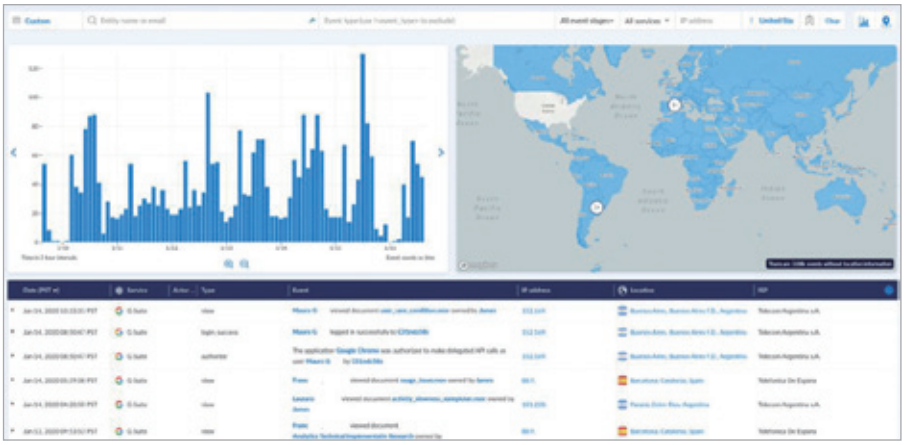


c) 位置记录

Obsidian可以监视用户从何处登录。检测异常登录和活动迹象等。

d) 威胁狩猎的活动视图

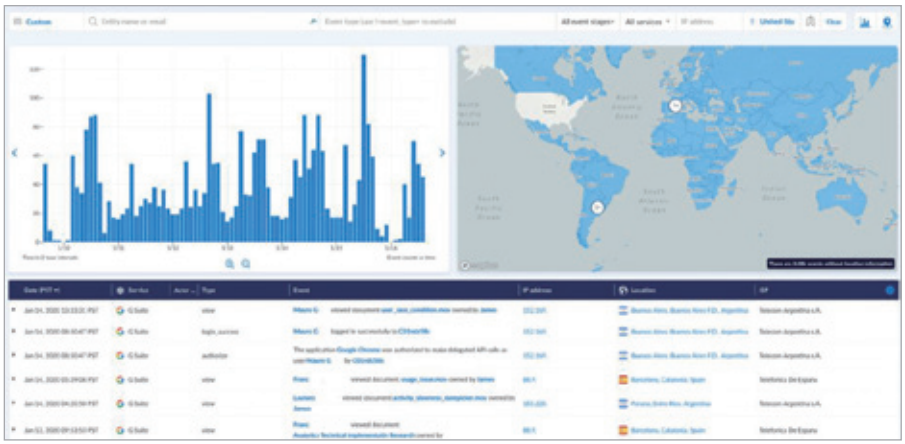
Obsidian通过位置、事件类型、ISP、设备、特权、访问历史等方面的特权、活动和上下文的统一视图，积极主动地检测SaaS环境中的未知威胁。



3、事件响应

a) 基于全局可视化的快速响应

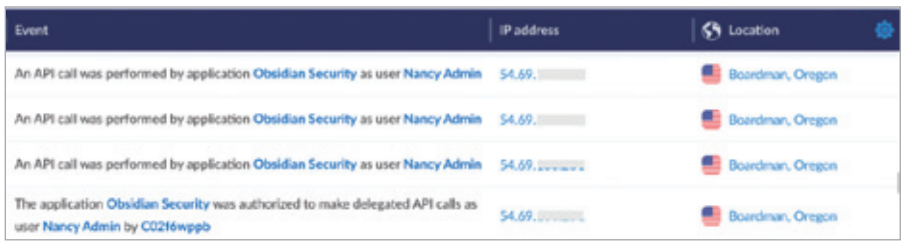
事故响应小组能在不影响系统运行的情况进行检测，识别根因并快速评估影响。Obsidian通过收集、规范化和存储来自SaaS应用程序的大量状态和活动数据，从而实现快速的云事件响应。



通过使用关于用户、特权和活动的统一数据，Obsidian能有效地进行信息检索工作。平台将用户、访问和特权与活动联系起来，并通过位置、事件类型、IP地址和设备丰富了这一功能。

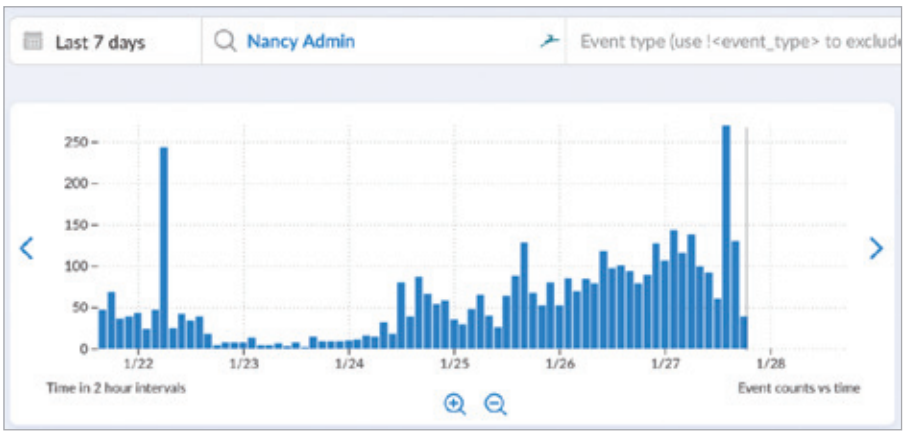
b) 通过IP搜索

搜索已知的恶意IP和感兴趣的IP地址，以查找与该地址相关的其他活动。



c) 根据用户或文档搜索活动日志

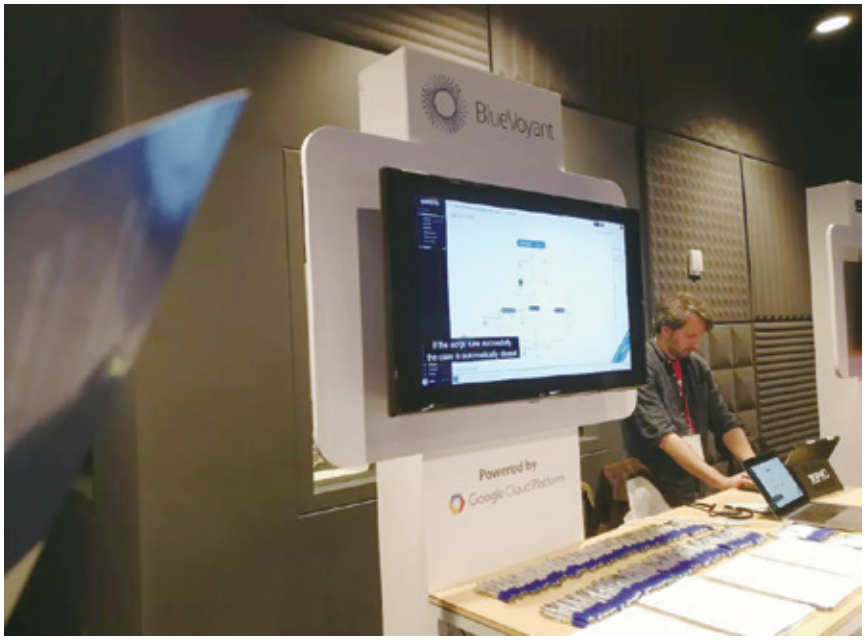
搜索与特定用户相关的所有活动，或在相关文档或资产上执行的所有活动。



三、创新点和挑战

云访问安全代理（CASB）之类的解决方案来采用预防策略，但并不足以保护云环境免受攻击。即使有了最好的预防性安全解决方案，攻击者仍可以穿透或绕过防御获取对云资产的访问权限。云检测与响应是Obsidian提出的一个新的理念，将xDR的理念应用在云端，云安全团队需要快速检测，调查并响应威胁。这就需要可视化和丰富的用户上下文信息，以便实时的检测和响应可疑行为。而如今，这正是SaaS和云服务所缺少的功能。云检测和响应（CDR）解决方案通过不断收集，规范化和分析来自SaaS和云服务的大量状态和行为数据，为安全专业人员提供了检测，调查和响应云中威胁所需的全面的可视化信息。Obsidian的创新，主要包括云环境的可见性、自动化检测和安全风险监控，都是SaaS的核心需求，解决了云安全的痛点。

当然也需要看到其商业化有很大的挑战，xDR产品的成功应用需要用户安全团队有较高的安全运营能力，否则无法发挥其应有的作用。如果上云的企业（特别是中小企业）没有相关的运营能力，那应该要考虑支持云端应用的MDR服务，例如去年RSA会场外，Google组织的生态圈会展中有一家BlueVoyant公司，能够提供面向公有云的MDR服务，通过绝大部分能够自动化的Tier 1服务和基于数据科学的Tier 2后台服务，可以为大量的云客户提供可扩展的安全运营服务。



四、总结

Obsidian的创始人来自Cylance和Carbon Black，分别有云端零信任和终端EDR的成功经验，相信能够将该产品能够理解云端SaaS应用的真实风险，基于检测和响应技术解决客户上云的痛点，也许CDR会是“后CASB”的新型产品，帮助客户及时发现并缓解威胁。

参考链接

[1] CLOUD DETECTION AND RESPONSE IS THE MISSING ELEMENT OF CLOUD SECURITY, https://www.obsidiansecurity.com/cloud-detection-and-response-missing-element/

[2] Obsidian官方网站，https://www.obsidiansecurity.com/

Sqreen：WAF 和 RASP 综合解决方案

2020年2月24日-28日，网络安全行业盛会RSA Conference将在旧金山拉开帷幕。前不久，RSAC官方宣布了最终入选今年的创新沙盒十强初创公司：AppOmni、BluBracket、Elevate Security、ForAllSecure、INKY、Obsidian、SECURITI.AI、Sqreen、Tala Security、Vulcan。

绿盟君将通过背景介绍、产品特点、点评分析等，带大家了解入围的十强厂商。今天，我们要介绍的是厂商是：Sqreen。

一、公司介绍

Sqreen公司是一家来自美国的网络安全初创公司，总部在美国湾区，公司创立于2015年，目前完成三轮融资，最近是A轮融资，累积金额1800万美元。其创始团队中CEO为Pierre Betouin，CTO为Jean-Baptiste Aviat，都来自前Apple的攻防团队。Sqreen聚焦于面向企业用户的应用程序安全防护解决方案，目的是在应用开发以及安全运营的场景下对应用程序进行实时监控并进行自主防护。目前Sqreen的产品被700多家客户所采用，并在2019年被Gartner评选为安全和风险管理方面的Cool Vendor，2020年入选RSA大会创新沙盒决赛。

二、背景介绍

攻击应用程序一直是网络攻击的一种常见入侵行为，随着移动互联网的发展，如今越来越多的应用架构迁移到客户端，对应用程序进行保护是很多企业和个人都要面对的重要问题。Gartner预测到2022年，超过50%的针对点击劫持和移动应用的攻击都可以利用In-App解决方案进行防御。内置应用程序（In-App）保护是对客户端应用程序使用自我保护技术，包括RASP等技术，这种技术跟传统WAF最大的区别在于其部署在服务器端点上，而非网络侧，所以有更好的可视度（Visibility）和上下文细节。Sqreen为企业提供应用程序安全服务，通过一个微代理（Microagent），以模块化的方式提供In-App WAF、RASP、虚拟补丁等安全防护能力，并可进行自动化监控，并通过安全管理平台可管理的应用程序安全。

三、产品介绍

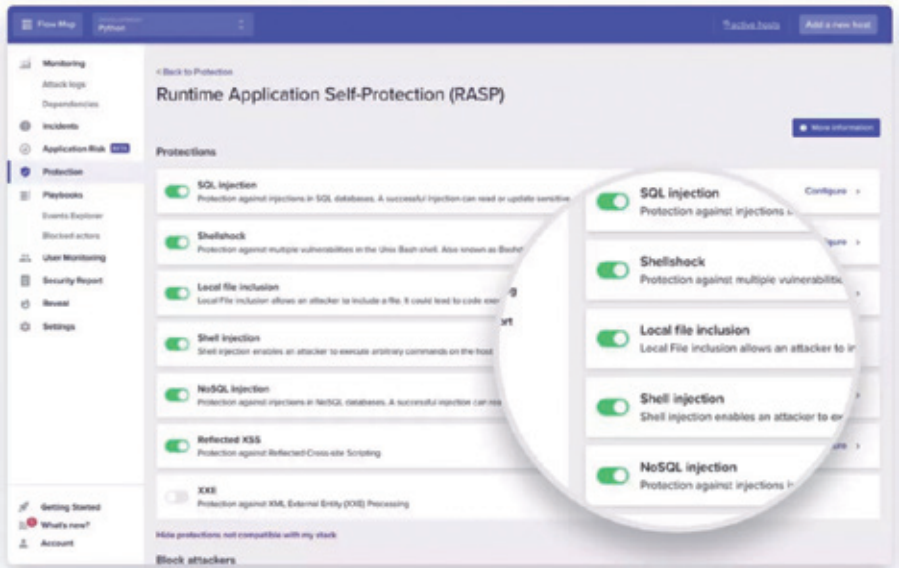
Sqreen产品平台主要包括应用程序运行时自我保护（RASP）以及In-App Web应用防护系统（In-App WAF）。

Sqreen RASP

Sqreen的RASP防护模块可防护OWASP Top 10漏洞（例如SQL注入，XSS攻击，代码注入等），从而降低数据泄漏带来的风险。该RASP架构可以在传统的HTTP层防护外，有更深入的可视度和防护能力。启用RASP很简单，以代码为nodejs语言的服务为例，可以运行以下命令安装对应的sqreen微代理：npm install sqreen

然后在代码开始处加载以下代码，并重启服务即可：require("sqreen")

由于RASP是跟服务代码紧贴的，所以可以观察到程序运行的所有上下文，如请求响应、变量和堆栈等信息，进而通过利用请求的完整执行上下文信息来识别在运行时实际利用漏洞的攻击，在阻止关键攻击同时并不产生误报。

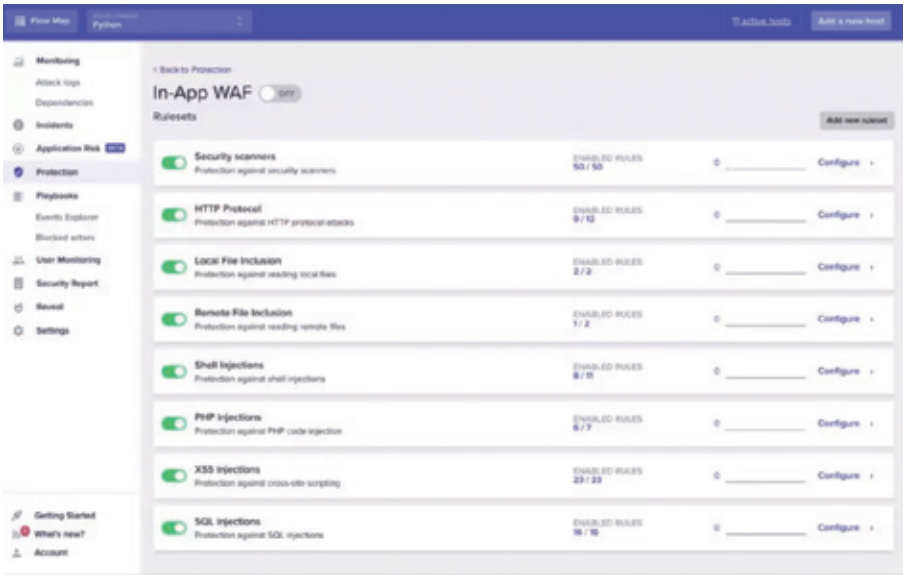


该模块不依赖签名和模式匹配来防御，因为签名和模式匹配容易造成绕过攻击或者阻止正常流量。通过上下文分析判断异常或恶意行为，所以其防御模式可以防护0-day攻击而不触发误报。

Sqreen In-App WAF

Sqreen的In-App WAF防护模块利用前述获得的应用程序的完整上下文，结合传统WAF的策略，最终形成了贴近业务的云原生WAF，拥有WAF功能的同时，误报较低，且不需要频繁的调整策略。与传统WAF相比，In-App WAF部署简单（见上），无需重定向流量，上下文丰富，节约了安全运维时间，并保证防护的安全性。

Sqreen的微代理试用智能堆栈检测机制来学习堆栈信息，并不断的根据变化的Web应用程序调整防护策略，无需事先配置。这种便捷的自定义WAF规则机制使得小型企业避免应用程序遭受高级业务逻辑威胁。



四、产品特点

1、Sqreen的产品采用微代理的结构，企业用户部署快速便捷。

用户只需要安装Sqreen的微代理，在服务器上安装插件即可。完成安装后即可帮助用户对应用程序进行运行时安全监控，报告可疑用户活动并在活动时阻止攻击，无需代码修改或者进行流量重定向。这种低成本并且快捷可靠的方式吸引了很多小型网络公司成为其客户。

2、Sqreen的产品能够自动化防御攻击，产品采用各个安全模块进行防护，包括RASP以及In-App WAF等。

这些模块不需要复杂配置即可适应于客户的应用程序。可以防御OWASP Top10攻击（例如注入攻击，XSS攻击等），0-day攻击，数据泄漏等攻击。可以创建应对高级业务逻辑威胁的安全自动化处置策略。

3、Sqreen的产品具备可扩展的协作安全特点。

Sqreen为工程师和安全团队提供了一个中心平台，将安全性分散到所有的应用程序和微服务中。安全流程图能够帮助用户了解当前风险并确定修复补救工作的优先级。不需要修改以及部署代码就可以轻松的启动新的模块进行安全防护。

五、总结

WAF和RASP已经是当前Web安全防护的重要产品，特别是WAF，已成为大部分企业部署Web安全机制时都会用到的安全防护产品。但是由于传统WAF以及RASP在防护部署过程中往往面临部署困难、防护策略调整复杂问题占用了企业客户的时间成本。

Sqreen提供了微代理的部署方式，这种方式部署快捷，可扩展性强。而且不用重定向流量，因此保护过程不会引入网络延迟。在Sqreen的防护模块的安全监控下，检查HTTP请求是否存在恶意行为并检查应用程序的执行流程，对关键文件、网络访问、命令执行、SQL查询等进行分析，确保不会触发漏洞。同时对用户身份进行监控，发现可疑用户上报。一旦识别出攻击就采取阻断，并在事后调查阶段为开发人员和安全人员提供堆栈跟踪信息，以便后续修复安全问题。

Sqreen的应用程序安全防护微代理具备快速部署的优势，并且其技术壁垒高、商业化落地性比较好，有很强的应用前景。

在当前敏捷开发、微服务、服务网格、云原生的大背景下，应用的复杂度也是大大增加，应用安全的重要性日益增加，如何做好应用安全也是非常大的挑战。虽然前景光明，但Sqreen同样存在挑战。笔者认为有如下几点：

1、虽然Sqreen始终在强调部署方便，但即便是微代理，也还是一种代理（Agent），在终端上部署安全机制会是很多客户存在顾虑的地方。例如代理是否会占用业务服务器的各种资源，虽然没有流量牵引的延迟，但本地分析各种上下文是否也会带来额外的开销；此外，安全应用和业务应用部署在同一个地方，会不会对业务团队的日常运营带来困扰？

现在云原生安全中比较火的istio项目，就是使用了sidecar envoy的方式，在业务侧旁挂一个安全代理，所有的安全处理对业务是无感知的，这是真正的云原生。Sqreen自己宣称的“云原生WAF”，除了可以扩展的特点外，其他还需要经过真正的考验。

2、Sqreen虽然在提In-App WAF，但其形态中就是主机WAF（HWAF），跟主流的网络侧WAF不是一个技术路线，是否能够真正挑战成熟的WAF市场还存疑。目前WAF的购买者通常认为Web安全是安全方案，而将应用安全归为开发团队负责的解决方案。虽然这种局面随着敏捷开发和DevSecOps的不断推进会有改善，但尚待时日。

总而言之，绿盟君认为Sqreen不仅在本次RSA创新沙盒的竞争中非常具备竞争力，而且对Sqreen未来的发展前景看好。

参考链接

[1] https://www.crunchbase.com/organization/sqreen
[2] https://www.gartner.com/doc/3970013
[3] https://www.businesswire.com/news/home/20190806005980/en/Intertrust-Recognized-Gartner-Market-Guide-In-App-Protection

Tala Security：高效检测和防护各种针对WEB客户端的攻击

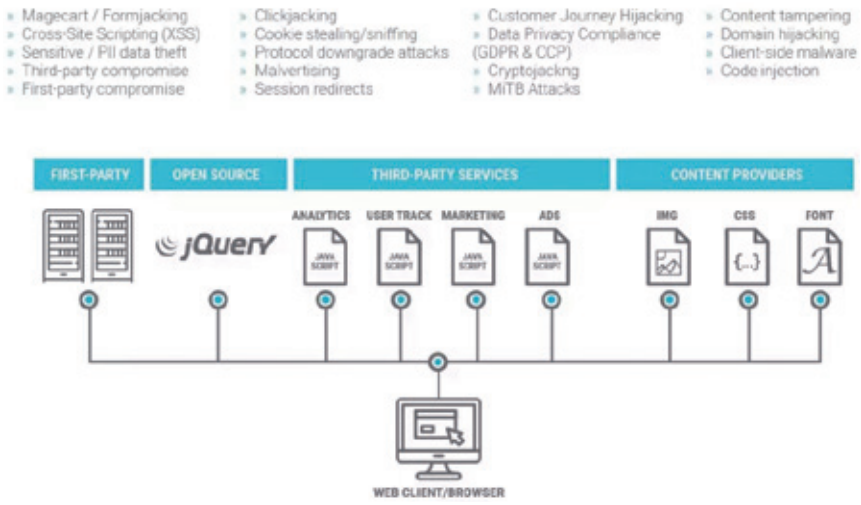
2020年2月24日-28日，网络安全行业盛会RSA Conference将在旧金山拉开帷幕。绿盟君已经相继向大家介绍了入选今年创新沙盒的十强初创公司：Elevate Security 、Sqreen和Tala Security三家厂商，下面将介绍的是：**Tala Security**。

一、公司介绍

Tala Security公司成立于2016年，总部位于美国加利福尼亚的弗里蒙特。其创始人兼CEO——Aanand Krishnan曾是Symantec（赛门铁克）产品管理的高级总监。据owler.com的数据显示，Tala Security自成立以来已经过4轮融资，总共筹集了850万美元。但crunchbase.com的数据则表明Tala Security已经得到了1460万美元的融资。

二、产品介绍

Tala Security的官方网站上展示的唯一一款产品是“Client-side Web Application Firewall”（下简称“Tala WAF”）。产品宣称“具有强大的预防能力、自动化决策能力和无与伦比的性能，可抵御XSS、Magecart，以及最重要的，抵御明天的攻击”。按照官方网站的宣传，Tala WAF的主要功能是检测和防护各种针对WEB客户端（浏览器）的攻击。



三、技术分析

注：以下所有结论均通过公开资料整理推测得出，并非基于对实际产品的研究，可能并不反映Tala WAF产品的实际情况，仅供参考。

整体运作机制

从官方白皮书来看，Tala WAF的运作主要依靠一些浏览器内置安全机制。具体包括：

1、内容安全策略（CSP）

由服务端指定策略，客户端执行策略，限制网页可以加载的内容；

一般通过“Content-Security-Policy”响应首部或“<meta>”标签进行配置。

2、子资源完整性（SRI）

对网页内嵌资源（脚本、样式、图片等等）的完整性断言。

3、iFrame沙盒

限制网页内iframe的表单提交、脚本执行等操作。

4、Referrer策略

避免将网站URL通过“Referer”请求首部泄露给其它网站。

5、HTTP严格传输安全（HSTS）

一定时间内强制客户端使用SSL/TLS访问网站，并禁止用户忽略安全警告。

6、证书装订（暂译，Certificate Stapling）

服务端会在SSL/TLS协商中附带OCSP信息，以证实服务端证书的有效性。

如果能够得到正确配置，CSP等客户端安全机制无疑是应对各类客户端侧攻击的有效方法。官方白皮书中称Tala WAF的核心功能是“在所有现代浏览器中动态部署并持续调整基于标准的安全措施”。

由此推测，Tala WAF的关键机制有二：

1、自动化生成和调整上述安全策略

和大部分的ACL一样，要严格配置这些安全机制并不是一件容易的事情。

2、收集和分析这些安全策略的执行记录

由于CSP具有Report机制，要收集其执行记录应该不算复杂。

最关键的部分是生成安全策略和分析执行记录的算法。对此，但绿盟君没能找到任何有价值的公开信息。仅有的叙述来自官方网站：“Tala利用AI辅助分析引擎来评估网页体系结构和集成的50多个独特指标”。至于具体使用了何种模型则不得而知。

细节分析

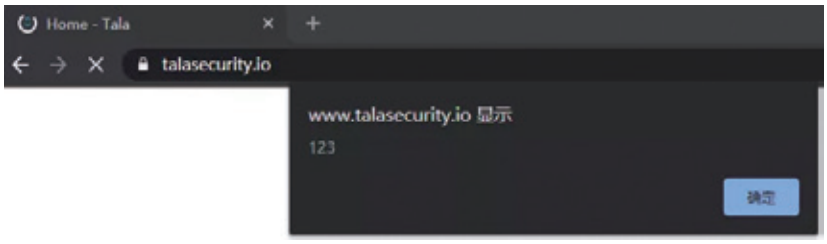
特别声明：我们不会在未经授权的情况下对他人网站采取任何进攻性行为。以下测试仅通过查看和修改本地通信来测试浏览器CSP的实现效果，并不能表明Tala Security网站存在或不存在任何安全漏洞。

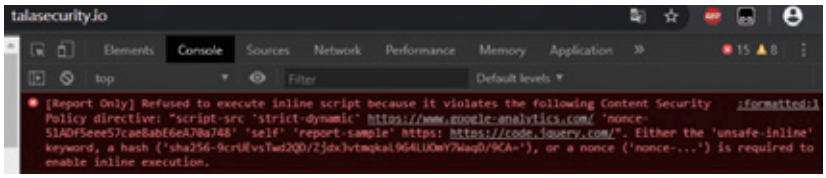
直接访问Tala Security官方网站，可见该网站的CSP配置如下：

可见是一组非常复杂的CSP，我们猜测Tala Security官方网站大概使用了Tala WAF。如果猜测属实，其中有一些细节值得注意：

CSP响应首部

我们首先发现，响应首部中配置的是“Content-Security-Policy-Report-Only”而非“Content-Security-Policy”。这意味着即使页面元素/脚本违背了CSP也不会被阻止，而是仅仅产生一条Report信息：





上图可见，即使<script>标签缺少“nonce”属性也能正常执行，只是会产生Report信息。

由此猜想，Tala WAF可能也无法以非常高的信心生成严格的CSP（而不影响网站正常业务）。Tala WAF可能会像态势感知系统那样，针对收集到的CSP Report信息使用某种异常检测模型。

CSP中的report-uri

Tala Security官方网站的report-uri指向站外地址“https://pilot.tsrs.cloud/r/7d9925a3e964e7eb0ed12fa82e9a3f891ae28372”。该网址不知为何无法正常访问，也正好避免测试过程产生虚假告警。绿盟君多次尝试删除Cookie并更换IP地址后刷新页面，但report-uri始终不变。

由此猜测，Tala WAF可能是以云服务形式提供的，report-uri中一长串的hash可能唯一标识一个被保护的网站。如此一来，用户本地就能实现轻量化部署，且几乎不产生性能损耗（官网宣称的“no signatures, no agents”），但也意味着用户的CSP Report信息可能会被Tala Security公司收集。

CSP的粒度

Tala Security官方网站的大量页面（包括HTML、JS、CSS、甚至是图片资源和302跳转响应）都使用了相同的CSP配置。以下为测试中的部分记录：

可见除了script-src中随机生成的nonce值之外，其它字段全部相同。

由此猜测，Tala WAF可能是对网站整体的资源引用情况进行分析，并产生一组静态策略，随后通过修改WEB中间件配置等方式应用到整个网站中。按理说，这是一种相对粗粒度的方法，当网站业务构成比较复杂时，可能难以有效发挥防护效果。但也不能排除有其它机制来适应这些场景。

四、特征对比

优势和创新点

Tala WAF似乎并不关注像SQL注入、任意文件上传这样的漏洞攻击，但它能够将客户端安全机制活性化，从而检测和阻止大部分常见的对客户端攻击，诸如XSS、挖矿脚本、广告注入等。即使攻击者能够运用各种五花八门的bypass技巧，在一套严格配置的CSP面前也会非常苦恼。

绿盟君曾在应急响应中多次遇到通过推广平台发起的网页篡改攻击，其中大多数属于黑产流量变现（可以简单理解为薅羊毛的一种）。由于广告代理商层层外包，即使是一些看上去很正规的推广平台也可能会提供包含恶意代码的广告内容。这些恶意代码会嵌入到所有呈现该广告的网站页面上，并大面积攻击访问这些网站页面的用户。目前的常规WEB应用防护体系很难与之对抗，但Tala WAF的方法理应可以有效防范此类攻击。

又例如有些XSS的Payload不会出现在通信流量中，一种常见情况是URL中“#”后面的部分（通常用来控制页面自动滚动定位）所构成的DOM型XSS。常规网络防护依赖对通信流量的检查，因此很难发现这种XSS。但正确配置的CSP能够阻止此类漏洞利用。

整体来说，Tala WAF相对适合互联网行业，尤其是电商零售领域的网站，因为这些网站往往具有大量的第三方资源引用。Tala WAF可能会成为现有WEB安全防护体系中一个非常重要的补充。

劣势与挑战

从公开的资料来看，Tala WAF并不具备对常规漏洞入侵的防御能力，因此可能不适合单独部署使用。Tala WAF可能也难以在企业内网环境中发挥优势——内部网站的内容资源大多可控性很高，且接入云服务也很困难。

此外，Tala Security也面临一些外部挑战。引用Gartner高级总监分析师Dionisio Zumerle的观点：“Tala Security面临来自提供替代方法的供应商的竞争。一些应用内置保护的播放器提供客户端JavaScript监控。一些RASP和WAF供应商将CSP和SRI功能作为端到端应用程序安全平台的一部分来提供。此外，网站运营者对客户端应用程序的保护意识普遍不足。”

五、总结

长期以来，大多数网站安全建设都着重于防止服务器被入侵或泄露数据，而Tala Security的思想确实弥补了现有体系的一个短板，当之无愧为2020年度RSA大会的10大Sandbox创新厂商之一。不仅仅是CSP，如何能够快速而精确地调整各种安全策略配置，如何能够最大化地利用好现有的防护机制，都是值得我们深入思考的问题。

参考链接

[1] https://www.talasecurity.io/

Vulcan Cyber：化被动为主动的云端漏洞响应自动化平台

2020年2月24日-28日，网络安全行业盛会RSA Conference将在旧金山拉开帷幕。绿盟君相继为大家介绍了进入今年创新沙盒十强初创公司，今天为大家介绍的是：Vulcan Cyber。

一、公司介绍

Vulcan Cyber是创新沙盒十强中唯一的一家以色列公司，在2019年曾入选Gartner 在Security and Risk Management的Cool Vendor。在公司的三位联合创始人中，CEO Yaniv Bar-Dayan与CPO Tal Morgenstern都曾在以色列军方任职，有丰富的网络安全实战经验。公司成立于2018年，目前已经获得了两轮共1400万美元的融资，最近一次是由Ten Eleven Ventures领头的1000万美元A轮融资。Vulcan Cyber为企业提供了一套自动化漏洞威胁缓解（Automated Vulnerability Remediation）解决方案，通过对已有开发、运维工具的集成与整合，实现对突发安全漏洞的快速响应，将企业受到安全威胁的时间窗口从数周、数月缩短到小时级。

Vulcan Cyber自称为业界自动化漏洞缓解概念的先行者。绿盟君认为，将企业资产整合、针对安全事件进行自动化响应的思想可以追溯到2017年Gartner提出的安全编排自动化与响应SOAR（Security Orchestration, Automation and Response）。但作为SOAR概念的实现者，切实为企业解决了安全痛点，未来可期。

二、背景介绍

随着网络安全攻防对抗的日趋激烈，企业的安全团队与运维团队面临着日益严峻的考验。安全事件、安全漏洞日益增多，越来越复杂且有针对性。企业针对不同业务的开展，部署、维护来自不同供应商的资产设备，持续增多的安全告警与误报增添了应急响应团队的工作负荷。

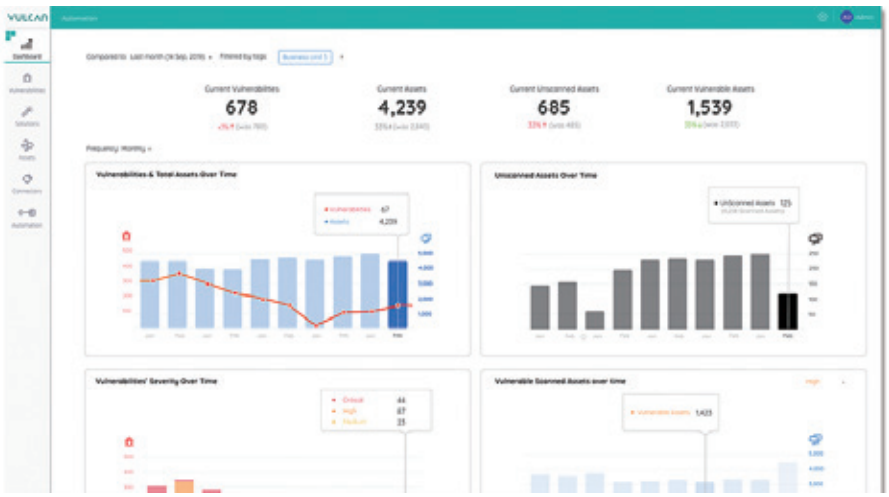
这些年来，检测与响应类的产品受到了极大的关注，尤其是对未知恶意行为的检测功能已经成为近年终端防护产品的标配。这些产品和技术使用户获得了更低的MTTD（平均检测时间Mean Time to Detect），能够更快、更精确的检测入侵和攻击，但对用户而言，解决问题与发现问题一样重要。一个现状是，企业的安全团队与运维团队不能保证在任何时候都能找到缓解漏洞的措施，同时也不一定能够准确评估缓解措施对业务造成的影响。Vulcan Cyber提供的解决方案旨在弥补企业的这一能力空白。

三、产品介绍

Vulcan Cyber的解决方案与公司同名，下面我们将简称其为Vulcan。Vulcan是一套部署在云端的漏洞响应自动化平台（Vulnerability Response Automation Platform），它的设计目标是将应用漏洞、错误配置等一系列安全问题转化为可执行的解决方案，从而使企业的安全团队能够专注于解决最有威胁的安全问题，化被动于主动。Vulcan将漏洞信息的收集、风险评估过程进行自动化，最终以一个补丁、配置文件改动或其他形式提供一个对生产环境影响最低的最佳解决方案。

Vulcan具有三大核心功能：风险信息聚合、威胁分析、自动化漏洞缓解。

风险信息聚合：提供完整的资产视图



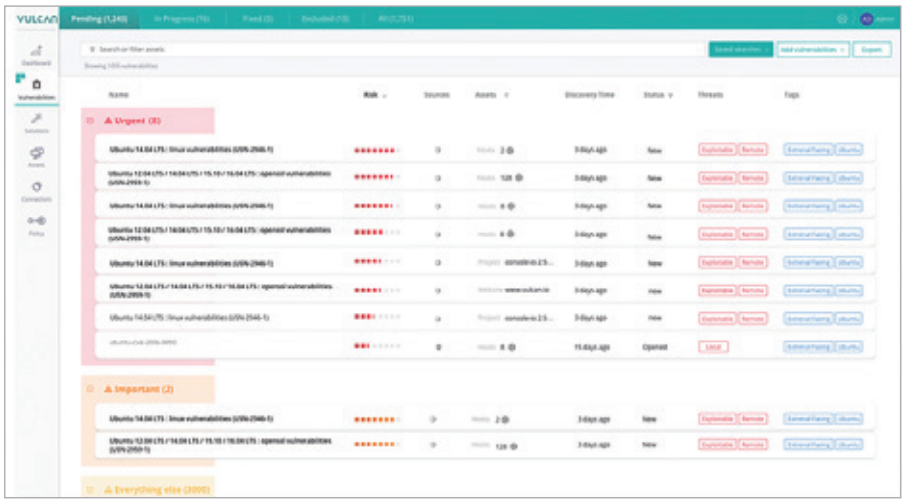
一个现代的漏洞管理平台能够完整的呈现企业的资产与这些资产之间的关联关系，只有当企业对其网络中所有的组件有完整的认知，应对漏洞的缓解措施才能完美的解决问题。Vulcan会对网络进行扫描并对结果进行收集汇总，找出其中可能存在的暴露点、配置缺陷。

除此之外，当我们评估一个漏洞缓解措施的潜在风险时，我们也需要知道资产之间的联动关系，从而确保对漏洞修复过程所导致的副作用（如意外停机）进行完整的预判。

在整个修复过程中，Vulcan会跟踪何时、何地、哪些步骤使用了哪些维护工具，以及这些工具由谁使用。通常不同的工具与业务系统分散在不同的平台

上，Vulcan提供对多种云平台与维护工具的支持，包括AWS Inspector、Microsoft Intune、Tenable Nessus、Ansible等，也支持通过Vulcan Gateway将用户私有云的监控数据上传到Vulcan云端。

威胁分析：基于风险的威胁优先级排序



传统的TVM厂商倾向于依赖客观评分，如CVSS分数，对漏洞的危害程度进行定级，但实际上，不同漏洞对实际业务的危害程度，还是依赖安全团队的主观判断。因此，Vulcan引入了多种要素来评定一个安全事件的实际风险。

1、应用安全性。包括Qualys、SourceClear等DevSecOps工具产出的代码规范性、覆盖率等数据。

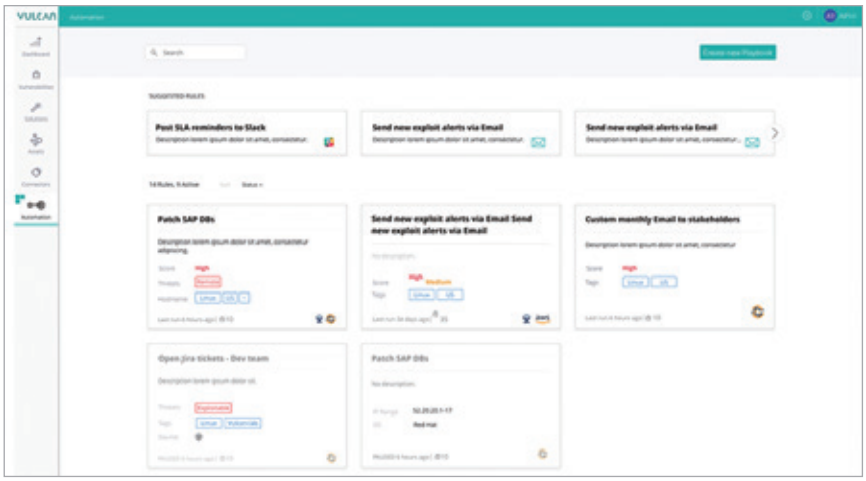
2、业务影响力。与企业的CMDB联动，将应用服务的商业价值纳入到风险评价指标中。例如储存用户信息、交易记录的数据库对公司至关重要，这些资产关联的漏洞与安全事件的处理优先级就是最高的。

3、资产分布情况。通过与应用部署工具、资产管理系统的集成，对漏洞所波及的资产数量进行定位与统计。

4、威胁情报。Vulcan接入了超过50个威胁情报源，查询发现的漏洞是否存在已知的IOC。

当然，这些维度的存在，除了纳入Vulcan的算法，输出威胁定级之外，也能够为安全团队处理安全事件提供更多的参考。

自动化漏洞缓解：对应用组件进行批量修复



Vulcan通过自动化的方式来减少事件响应所需的人力与时间，排除误操作的风险，提供更高的可靠性。用户可以预先定义一些Playbook，从而将满足特定条件的事件处理半自动或全自动化，在官方的案例分析中，Vulcan可以将某些组件的漏洞信息推送到Slack的聊天频道中，并在Jira中创建一个Issue，从而调动相关人员进行处理。除此之外，Vulcan还维护了一些常见的自动化指令，比如使用Ansible或Chef等工具对Linux服务器安装补丁，或操作WAF、终端防护软件设置规则阻断恶意软件传播等等。

四、优势与挑战

Vulcan的一大亮点是，通过漏洞评级之外的更多维度，衡量漏洞的风险程度，帮助安全团队在海量告警与安全事件中定位最重要的安全问题；更重要的是传统TVM产品只具备管理漏洞生命周期功能，大部分的漏洞缓解、系统升级都是人工处理，耗时耗力，在大规模的系统中不可扩展，而Vulcan使用了自动化编排的方式，高效解决问题，这一点是很多TVM产品所不具备的，解决了用户一大痛点。

但同时，Vulcan也存在一些不完善的地方。作为一个漏洞管理的集中平台，它需要能给用户提供足够的灵活性以将更多种类的资产纳入平台中。Vulcan只提到了支持与某些应用的集成，但不支持什么，我们并不知道。其次，应对复杂多变的企业环境，在数据的展示上给用户定制的空间也是非常必要的。如Rapid7 InsightVM与FireEye Helix提供了多种可定制的界面元素，不同的团队可以从不同的视角进行监控。Vulcan目前看来还缺少这样的功能。

五、总结

Gartner 曾预测，到 2020 年底，拥有 5 人以上规模安全团队的公司企业中，15% 都将采用 SOAR，而现在 SOAR 的采用率只有 1%。Vulcan Cyber将SOAR的概念进一步推向落地，并展示了一个切实可行的解决方案，减少了事件响应过程中重复性任务的人工干预，帮助加速问题的解决。正如去年创新沙盒获胜者Axonius在网络安全最基础的资产管理方面有所创新得到评委垂青，今年Vulcan是否会在同样基础的漏洞管理方面自动化提升安全运维效率而得到行业的认可？我们拭目以待。

绿盟邮件高级威胁解决方案

轻松应对APT攻击、勒索病毒攻击等高级邮件威胁

邮件高级威胁净化器

全面 | 精确 | 及时

适配通用邮件网关，
隔离APT攻击邮件，
未知勒索软件等高级威胁

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为金融、政府、运营商、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

NSFOCUS绿盟科技

安全月报

绿盟科技金融事业部出品

主办/绿盟科技金融事业部
地址/北京市海淀区北洼路4号益泰大厦3层
邮编/100089
电话/010-59610688-1159
传真/010-59610689
网站/www.nsfocus.com
客户支持热线/400-818-6868
股票代码/300369
月报电子版下载/http://www.nsfocus.com.cn/research/list_145_145.html