计算机世界/2020 年/8 月/31 日/第 005 版
产品潮流汇

企业需紧跟安全自动化趋势

Stacy Collett Maria Korolov 编译 Charles

处于压力和紧张中的 IT 安全部门希望通过自动化技术缓解来自检测和响应系统的大量警报。

网络工程师 Jose Arellano 承认,“ 我每天最棘手的工作 ” 是保证伊利诺斯州 West Aurora 129 学区 1.27 万名学生、1900 名员工和 1 万多台连网设备的安全。仅有两个人的安全部门的主要工作是让网络尽可能安全、高效地运行,为教师和学生提供服务。在学校有限的资源和预算下,Arellano 说: “ 我们的精力都集中在内部网络。”

然而,一场 DDoS 攻击使该学区的网络瘫痪了 6 个星期,他们很难找出问题所在。现在,他不得不把注意力从单纯的预防方法转到检测和响应上。他说: “ 这是一项极其困难的工作。”

越来越多的安全专家也和 Arellano 一样感到沮丧,部分原因是每年报告的漏洞数量实在太多了。威胁情报公司 Risk Based Security 仅在 2020 年第一季度就记录了近 5000 起新发现的漏洞。对于捉襟见肘的安全部门来说,很难评估这些漏洞带来的风险。

几乎所有参加 Dimensional Research 公司 2020 年 SecOps 和自动化调查的受访者都表示,太多的警报给安全部门带来了问题,83%的受访者表示,自己的部门已经对警报麻木了。很多员工数量超过 1 万人的公司每天都会收到 1 千多条警报。

WannaCry 勒索软件攻击事件标志着犯罪分子们在全球发起了新一轮恶意软件、勒索软件、网络钓鱼等各种恶意攻击,而且是不加选择的攻击各种目标。很多企业,不管规模大小,每天都会从其监控系统收到数以万计的安全警报。例如,据研究公司 Ovum 的数据,大约 37%的银行每天都会收到 20 多万次可能是攻击的安全警报。

猛烈的攻击只会让安全部门越来越头疼。企业不仅要对数据进行筛选,按先后顺序处理数以千计的警报,而且还要采取行动,让那些人手严重不足的网络专业人员动手开展调查。Oxford Economics 公司代表 ServiceNow 进行的一项调查显示,81%的受访者表示,他们担心不能很好地解决检测到的安全漏洞。Cybersecurity Ventures 的一份报告估计,到 2021 年,将空缺 350 万个网络安全工作岗位,高于去年的 100 万个。

Forrester 高级分析师、安全和风险专家 Joseph Blankenship 说,大量新出现的自动检测和事件响应技术虽然有所帮助,但很多企业仍不愿意让安全实现自动化。Blankenship 说: “ 在过去,自动化给我们带来了问题。合法的数据流被阻断,造成了中断。在采取自动化措施的过程中,如果没有人去查看并进行验证,会出现很多问题。”

现在,有的人可能又有些乐观了。Blankenship 说: “ 直到最近我们才开放了 API,我们不仅能把数据从简单的日志数据中提取出来,而且还能推送回去。平台之间的共享越来越多了,我们已经创建了这一自动的流程编排层,这要归功于 API 能够让我们更自由地交换数据。”

Jon Oltsik 是 ESG 的高级首席分析师,也是该公司的网络安全服务创始人,他说: “ 流程编排和自动化有可能是不错的解决方案,但你真的只能浅尝辄止,因为它不会解决所有的问题。有时候这也意味着要改变工作流程。”

据 Dimensional Research 的调查,使用自动化技术来处理警报过载的企业逐步看到了成效。虽然 34%自动化程度较低的安全部门能够在一天内处理大部分安全警报,而 65%的安全部门报告说,他们是通过自动化技术来处理一天内的警报。大多数受访者(92%)表示,自动化是处理大量警报的最佳解决方案。

企业有大量可供选择的自动事件响应解决方案,当然不会有万能的解决方案。三家企业分享了

他们自己遇到的网络安全挑战和应对策略。

管理海量的安全数据

对于完全托管服务提供商 CareWorks 来说,其分布在美国 88 个地区和 6 个国际地区的安全工具收集了太多的安全数据以至于很难处理,该公司首席信息官兼首席技术官 Bart Murphy 说:“ 即使我们的 IT 部门人员配置得很好,也很难处理这些数据。我们需想办法以少胜多 ”。

Murphy 开始寻找方法来收集其漏洞扫描器、安全分析软件和端点解决方案中的所有数据,然后至少把一些工作流程进行自动化。

CareWorks 已经采用了 ServiceNow 的平台即服务来实现企业 IT 运营的自动化。因此,在 2017 年 3 月,该公司增加了供应商的安全运营模块。虽然仍然在早期应用阶段,但该公司已经集成了 Symantec、Nessus、LogRythm 和 Tanium 等工具,目的是识别出能够自动化的流程。Murphy 说:“ 我们最终会利用流程编排工具来让流程自己去真正地应对威胁,并返回报告。”

目前,SecOps 模块可以跟踪与潜在或者实际的安全事件相关的所有活动,而无需人工去查阅各种各样的日志。目前还不能确切地知道节省了多少时间和人力。现在,Murphy 的目标是 “ 确保我们能够尽可能地保护和预防我们所知道的 ”,但他说,在安全自动化方面建立信心需要时间。

他说: “ 随着时间的推移,要通过一定程度的验证才能适应这种自动化。在今后 6～12 个月的时间里,我并没有不切实际地想把所有一切都实现自动化。我宁愿有 10 个经过深思熟虑和经过测试的自动化流程,而不是 100 个随意的流程。确保各部门了解目标,不要为了自动化而自动化。”

安全工具越少越好

对于网络安全,Finning 国际公司首席信息安全官 Suzie Smibert 的做法就是能简则简。总部位于温哥华的这家公司是全球最大的 Caterpillar 产品和支持服务供应商,Smibert 也是该公司的企业架构全球总监,对于网络响应技术,Smibert 指出, “ 现在有太多的供应商。”

Finning 每天收到成千上万的安全警报,服务器和网络覆盖了 3 个地区,全球有 1.3 万多名员工,每名员工都有一台以上联网的设备,所有这些因素都使得警报越来越复杂。Smibert 说: “ 添加更多的安全工具并不能提高安全性。反而会使得情况更糟,因为如果采用 100 种不同的安全小工具来管理复杂的环境,会带来虚假的安全感。” 更重要的是, “ 如果 10 台设备只完成一项网络安全功能,那么你就要付出 10 倍的培训和费用。”

Smibert 选择少量的多功能安全工具来检测并响应网络攻击,这包括,能够自动防御攻击的网络、云和端点相结合的安全平台,云实现的端点防护解决方案,以及分析驱动的 SIEM。

她的部门现在每天能查清楚数以千计的警报,但只处理那些需要调查的——每天大约 20～40 个。Smibert 说,好在有人手足够的经验丰富的安全专业人员来完成人工处理工作,所以她没有急于进行更多的流程编排和自动化。

她说: “ 对于企业非常关键的系统数据和功能,我不太愿意以自动的方式去保护它们 ”,特别是老应用程序, “ 但并不意味着这不会发生。其中一些系统并不太适合进行自动化。如果自动产生了一个误报,或者自动产生了连锁反应,那么其负面影响要比小规模的、可控的安全事件的影响大得多。”

网络流量分析让两个人的部门感觉就像 200 人的部门

K-12 学校不像私人企业那样有网络安全工作人员和相关的预算。West Aurora 129 学区转向采用事件响应软件,以帮助填补这方面的空白。

由两个人组成的 IT 部门负责管理该地区 18 所学校的基础设施。在 2016 年 8 月开学之初,该学区的无线网络崩溃了,没有人(甚至包括该学区的 ISP)能够找到问题的根源。Arellano 回忆说:

“ 我们的设备都是思科的,但我们缺乏很多功能,而这些功能是可以通过固件更新(通过思科 Smartnet 服务)来获得的,我们的网络可见性很差。”

他说,ISP 提醒我们,学区可能会成为大规模攻击的试验场, “ 这让我们感到害怕 ”。这个问题持续了 6 个多星期,直到 Arellano 安装了事件响应软件,分析数据流,对数据进行取证,以找出中断的根

源。

使用 Plixer 的网络流量分析系统 Scrutinizer,Arellano 立刻看到了泛滥的 DDoS 警报。通过抓取数据包,他发现很多 DNS 响应来自美国消费者产品安全委员会(CPSC)。他回忆说:“我们由此确定了是哪一类攻击。”利用 DNS 反射攻击,黑客欺骗学校的地址,并要求 CPSC 向学校发送大量的记录。下一步就是去阻止它。

通过现在可见的时间戳和 IP 地址,Arellano 缩小了事件范围,只提取与事件有关的数据。所有证据指向了学校二楼的一个网络教室。“我们注意到一名学生在删除旧记录。我们拿到学生的 ID 之后,我们挖掘出记录,发现他使用一个网络压力网站来发动攻击,这个网站每月收费 10 美元。自那以后,又阻止了两起类似的袭击事件。”

技术总监 Don Ringelestein 说:“21 世纪版本的‘拉响火警’发动了 DDoS 攻击。过去我们处于被动的环境中,但现在我们要主动多了。”他说:“在很多情况下,我都能发现问题,并采用事件响应工具,在造成破坏性之前将其阻止。”

外部安全服务提供商可以提供帮助

很多企业面对网络安全威胁感到人手不足或者束手无策,他们正在寻求服务提供商的帮助,为他们提供自动化和流程编排服务。到 2020 年,Gartner 预测,15%的中型企业和大企业将使用托管检测和响应等服务,而 2016 年这一比例不到 1%。

IDC 安全战略副总裁 Pete Lindstrom 表示:“我非常信任服务提供商,因为对很多企业来说,每年都有一、二次这样的事件发生。只有通过服务提供商我们才能了解风险到底在哪里。”他说,Trustwave、FireEye 和其他 20 多家供应商都是如此。

有助于实现安全自动化的 5 种机器学习技术

据 ESG 去年秋天进行的一项调查,2/3 的企业认为安全分析和操作的自动化是首要任务,39%的企业已经部署了机器学习技术来帮助应对这一挑战。那么这些机器学习技术到底是什么?

1.异常检测

机器学习技术的一种常见用途是异常检测。如果一家公司拥有网络流量或者用户行为的基准数据集,那么机器学习可以用来发现不合常规的事件。例如,如果一名员工一般都是在正常工作时间工作,从工作计算机上登录,那么下班后从国外登录就是不正常的——而且可能是恶意的。

机器学习系统通常是在历史数据集上进行训练,然后去寻找任何新的或者不正常的东西。员工、网络和其他系统会随着时间而变化,因此,需要定期更新训练。然而,虽然异常检测系统会报告异常事件,但它不会告诉你这些事件是否存在恶意活动的迹象。

2.聚类分析

另一种常见的机器学习算法是聚类分析。例如,利用规模很大的用户行为数据集,聚类分析能确定有一组员工经常出差并且有某些共同的行为,而另一组员工倾向于在同一个地点工作。

与人类相比,聚类算法能观察到更多的各种因素和行为,并实时更新聚类。通常还是需要有人去观察这些聚类或者异常情况,并确定究竟有什么含义:是因为公司朝着新方向发展,还是因为发生了一些可疑的事情而导致出现了行为怪异的聚类?

3.分类

如果有足够大的数据集并预先划分为不同的类别,那么,机器学习可以识别出新数据属于哪一类别。例如,如果已经把大量的软件划分为恶意软件和合法应用程序,那么机器学习系统就能判断以前没见过的应用程序是不是恶意的。

随着数据集越来越大,算法越来越智能,错误率也随之下降,这项技术对网络安全越来越有用。同样的技术可以应用于各种各样的安全难题,而不局限于对恶意软件进行分类。例如,如果有足够的历史数据表明哪些异常最终是恶意的,那么可以将分类系统与异常检测系统结合起来,从而减少了需要安全专业人员处理的事件数量。

4.预测

网络安全情报的下一步是让学习系统监视安全专业人员怎样处理事件。对于某一安全问题,典型的反应是什么?

这里的难点是怎样收集足够的历史数据来做出适当的预测。每家公司都略有不同,即使在一家公司内部,不同的分析师也会以不同的方式来处理问题。然而,这一领域不仅数据集越来越好,算法也越来越善于从数据中得出分析结果,而且供应商也在努力从客户数据池中创建匿名数据集。现在,网络安全平台可以智能地预测对特定事件会有什么样的反应,并将其转化为一系列建议。

5.自动修复

在将来的某个时候,一旦公司对所提供的建议感到足够满意,该技术就可以开始自动地对那些对公司风险最低或者效益最高的建议进行修复。要做到这一步需要时间——系统需要时间才能变得足够智能,变得实用,公司也需要时间来学会信任它们。

在公司能够自动化其安全响应之前,必须打好基础,包括编排框架、安全规程和收集安全响应的过程。编排允许一个安全系统在不同的系统中触发一个操作,而不需要人登录到各个系统中并手动执行命令。这通常是通过使用 API 和某种编排架构或者平台来实现的,要么完全自行开发,使用开源组件进行组装,要么从第三方供应商处购买。

下一步是创建规程——如果发生某种事件,则执行一系列步骤。这些规程通常是根据安全人员的专业知识和经验手工编成的。通过自动化最常见的任务,这些规程能够立即减少工作量并加快响应速度,同时帮助企业发现其集成和编排框架中的漏洞。

过渡期间

Oltsik 建议,打算将事件响应自动化的安全领导们在解决好自己的运营难题之前,先不要购买单点工具。“ 和自己的人谈谈,找出最大的痛点在哪里。解决某个问题为什么需要 2 个小时的时间?让员工们合作的难点在哪里,为什么很难得到调查取证所需的数据?从这些地方开始采用流程编排和自动化工具。这些工作不能是强制性的。必须让员工们参与进来,每个人都朝着同一个方向努力。”

Oltsik 说,只有做好自动化准备工作,结果才能唾手可得。“ 如果威胁情报告诉你某一 IP 地址或者网络域有问题,而且有 80%的把握,那就不应该再分配这些地址或者网络域。”

Oltsik 说,下一步,花时间去进行流程编排。假设你有了安全流程,或者花时间去梳理了与流程相关的所有任务,那你就知道怎样应用技术更好地做出响应。“ 这可能需要一段时间。”

他说,应该对任何新的自动化或者编排流程进行大量的检查,这一点也很重要。“ 是不是错过了不应错过的?下次能做得更好吗?是不是应该有这样的流程,或者应该有额外的步骤,还是遗漏了某些步骤? ”

Smibert 认为,事件响应自动化广泛应用的过程与云应用的过程相类似。“ 5～10 年前,每个人都害怕云技术,但业界已经证明,当你采用一种战略性的、深思熟虑的方法来使用云技术时,就会创造奇迹。我认为安全自动化也是如此。一旦业界达成共识,而且我们已经有了成功的早期采用者,那么我们会有更多的应用,而更多的应用将带来更多的创新。我们将看到安全自动化就像今天的云一样流行。”

Stacy Collett 是《计算机世界》、CSO 和《网络世界》的特约撰稿人,他的文章涉及各种安全和风险问题。

Maria Korolov 过去 20 年一直涉足新兴技术和新兴市场。她曾对俄罗斯、印度和阿富汗进行报道,在中国的新闻机构工作了五年之后,最近回到了美国。