# 安全反思-主动数据泄漏监测

* Protecting themselves from a targeted data breach is a top priority for most (if not all) organizations and their IT departments. The concern rises up to the board of directors level, where many have it as a standing agenda item. None of the anxiety is unwarranted, given that the recent breaches at the Office of Personnel and Management (OPM), the White House and even that of the loathsome Hacking Team demonstrated the grave consequences of a targeted data breach.
* 对于大多数公司以及他们的IT部门而言, 防止敏感信息被泄漏占据了所有工作中的最高优先级. 这样的顾虑会上升至在主管级别, 并在他们的常设议程保持一席之地中. 这样的顾虑自然并非杞人忧天. 在近期发生的人事管理办公室数据泄漏事件的背景下, 白宫以及那些可恶的黑客团体证明了目标数据泄漏所能导致的严重后果.

Most organizations are primarily focused on preventative security and have little or no effective ability to detect an active data breach quickly or accurately. The average attackers’ dwell time in the target’s network – around six months - is evidence of this deficiency. What’s more, according a security report from Trustwave, only 19 percent of organizations discover the breach themselves. Most of the breaches are discovered by a third-party, long after the damage has been done.

大多机构将关注点主要集中于防御性安全, 而缺乏对主动数据泄漏有效及时精确的监测能力. 攻击者在目标网络中的平均停驻时间长达六个月也足以证明了这方面能力的不足. 此外, TrustWave的一份安全报告表明, 只有19%的机构有能力独自发现数据泄漏. 而余下的大多数的数据泄漏都是在造成系统损害后很久才被第三方揭露出来.

The information security industry has been focused on singular events since its inception. Security has been oriented towards a specific file, a particular network connection, a protocol anomaly, and similar things. However, while identifying those technical artifacts is crucial for preventing a specific intrusion attempt, they usually provide very little context as to the broader attack process, which remains a concern for post-damage investigation.

信息安全行业从最初期就重点关注单一事件. 安全被直接导向到对一个特定的文件, 一个特殊的网络链接, 一个异常的端口这类的独立事物的关注. 尽管标识这样的技术构件对于防止某些特定入侵企图至关重要, 然而他们针对那些更广泛的攻击过程却只能提供极为有限的应对, 因此仍然是损害后的调查的顾虑之一.

As a result, an organization may detect and block thousands of intrusion attempts without realizing they are under a targeted attack. To find these attackers requires a re-thinking of some of the most basic tenets of security.

结果就是, 一个机构可能探测并阻挡了成千上万个的入侵尝试, 却仍然没能发现自己已经被针对性攻击了. 若想要发现这些攻击者, 我们需要对安全的一些根本原则进行反思.

Many of the technologies in place today labeled as “detection” are really some form of “prevention”. Sandboxing, for instance, and Intrusion Detection/Prevention (IDS/IPS) is another form of detection—it is based on statically defined elements from a singular bit of software. The flawed assumption is that stopping a breach involves stopping this one bit of malicious software. It is also flawed in that it is based on spotting something malicious thanks to a known signature or “technical artifact”

目前许多被标记为监测的技术实际上可以归类为某种形式的防护. 而例如沙盒 (Sandbox) 以及入侵监测/防御 (IDS/IPS) 则属于另一类基于特定软件中预定义静态元素的防护措施. 这是基于一个有瑕疵的假设, 即只能通过停止这样的恶意软件的执行来阻止数据泄漏. 这样假设的另一个疏漏在于它是基于对已知签名以及特定技术构件的匹配来发现恶意对象的.

Other systems that are designed to flag anomalies produce an overwhelming number of alerts—hundreds or thousands each day— that are heavily dominated by false positives. Often times, there is an indicator of an active breach among these alerts, but it would be like finding a needle in a haystack to actually locate it

其他 (防护) 系统则被设计为在发现异常后产生过多的警报 -- 每天数百或数千个 -- 而误报又占了警报中的大多数. 尽管在很多时候, 这些警报中确实存在主动泄漏的明显标志, 但是定位这样的标志就如同大海捞针一般艰苦.

When you stop to consider it, attackers have a nearly unlimited number of attempts to break into a network. The attack surface is too big and too complex to fully protect, particularly with employees susceptible to social engineering or increasingly clever spear phishing, which makes them often the weakest link. A defender has to be successful 100 percent of the time to prevent a breach. An attacker needs to be successful only once to break into the network. The odds are clearly in the attacker’s favor.

当您停下来思考时也会发现, 攻击者们有着几乎无限次数的机会来尝试入侵网络. 这样的攻击面实在太庞大太复杂以至于很难能够全面防护到位. 尤其是员工还会受到社会工程学以及越来越聪明的鱼叉式网络钓鱼攻击, 他们很容易成为全局防护中最薄弱的一环. 一个防护者只有做到100%防护成功才能防止一次数据泄漏, 而攻击者只需要一次的成功入侵即可. 这样的对比明显对攻击者更为有利.

Once inside a network, an attacker should be at a disadvantage. He or she needs to explore and understand the new, unfamiliar network, locate assets and work towards accessing them. All of these activities can be detected, if one knows what to look for and at. Unfortunately, since most organizations do not have an effective way to quickly and accurately find an active intruder, the advantage that should belong to the defender once again goes to the attacker.

一旦攻入网络后, 攻击者理应处于劣势一方. 他或她需要探索来理解这个全新的未曾熟悉的网络, 从而定位资产, 获取到它们的权限. 倘若如果有人懂得正确的关注点与监控点, 所有的 (攻击者) 活动都能够被监测到. 然而不幸的是, 由于大多数机构没有一个发现活跃入侵者的有效途径, 使得这一本应属于防护方的优势再一次归结到了攻击者一侧.

Detecting an active data breach requires a blend of new strategies, tools and procedures.

监测一个主动数据泄漏需要的是一系列的新策略, 新工具以及新方法.

In terms of strategy, there are several things to consider. First of all is the notion that breach detection after an intrusion is viable and necessary. This may seem like an obvious point, but there is already a tremendous amount of self-defeatism in the security field when it comes to data breaches. Many discussions revolve around more stringent data access, acquiring cyber insurance and developing contingency, post-damage communications and incident response. Most dialogs that I have witnessed do not include breach detection. Organizations need to see that early breach detection is possible and commit budget and resources to it. Companies accept the fact that they likely will be breached, but they have not committed to true breach detection, largely out of ignorance. The ability to find an active data breach and the tools that can accomplish this are relatively new.

就策略方面而言, 有若干个角度值得思考. 首先要做的是确立一个观念, 即入侵后的数据泄漏监测是可行且完全必要的. 这一点看起来似乎是再明显不过, 然而安全领域在对待数据泄漏问题时, 自我放弃主义做法 (放弃数据泄漏监测) 却是屡见不鲜. (行业中的) 许多讨论都是围绕着如何制定更为严格的数据访问权限, 包括购买网络保险, 建立应急机制以及损害后的通讯与事件响应. 而我所了解到的大多数谈话却均没能涉及数据泄漏监测. 企业们需要了解到早期的数据泄漏监测是可行并且应该为之提供资源与相应的预算. 但公司们虽然理解他们可能会被泄漏这一事实, 却出于无知没能做出任何监测泄漏行为的努力. 这样发现一个主动数据泄漏的技术或是拥有这样技术的工具的确是相对较新的.

Another strategy involves personnel. Most organizations have a limited security operations team, and fewer have trained, experienced security analysts. It’s amazing how many large companies have security responsibilities shared by a small IT team responsible for other operations as well, including networking, storage and applications. To effectively detect a data breach, the organization must be comfortable with—and even value—a certain amount of automation. The “investigate everything” mentality of a SIEM or IPS and other devices must go.

另一种策略则是与人事管理相关. 大多数机构只拥有一个十分有限的安全运营团队, 拥有训练有素, 经验丰富的安全分析师的企业可谓是少之又少. 更为人惊奇的在于许多大公司都把包括网络, 存储和应用程序在内的安全任务交给了一个同时还负责其他公司的小型IT团队负责. 此外, 倘若要高效监测数据泄漏, 机构必须坦然乃至重视一定程度上的自动化. 对于SIEM, IPS以及其他设备那样"排查一切"的心态必然会遭到淘汰.

A breach detection system must provide smart, careful analysis to pinpoint a potential breach with a high level of accuracy and actionability. Instead of hundreds or thousands of alerts, a breach detection system should produce only a handful each day to maximize the procedural work done by personnel and minimize wasted time. Team productivity is key so they can spend time on the most important activities.

一个泄漏监测系统必须能够提智能, 周全的分析成果, 从而以高准确率及可操作的标准指出潜在的泄露风险. 这样的泄漏监测系统只会产生少量而非以往成百上千个的警报, 并尽可能地完成了过去需要人力完成的程序化工作, 减少了被浪费的时间. 而团队效率的提高使得他们能够将时间花在那些更为重要的任务当中.

Personnel efficiency will become an even greater concern over the next several years. There is a shortage of security professionals already, and it will become acute before we enter the next decade. Don’t send a team on a daily wild goose chase. Let them focus on real threats and issues, and give them time to become more proactive.

人员效率因素在未来数年中将会变得越发重要. 而目前就存在的安全专家稀缺问题也将会在下一年代也将变得更为严重. 与其让小组陷入每日的鸡毛蒜皮小事, 不如使他们专注于真正的威胁与问题, 并有时间变得更为积极主动.

Finally, another strategy consideration involves shifting from a heavily malware dominated mentality to one that is focused on attack behaviors from a live intruder. While malware is clearly bad, hunting for it does not generally uncover a data breach.

最后, 另一种策略围绕着从以恶意软件为重心到以线上入侵者攻击行为为重心的思路转变. 尽管恶意软件的确是可恶的, 但搜寻它通常并不能发现数据泄漏行为.

Often, malware is not used in an attack, or its role is not readily discernible. Many security organizations have gone “malware crazy” to the detriment of being able to see the larger threats. It may seem like an obvious point, but the organization needs to prioritize the detection of much more insidious threats

通常, 恶意软件没有被用于攻击过程之中, 或是它在攻击过程中的角色难以分辨. 但许多安全组织已经为恶意软件着魔以至于难以看到更大威胁所能造成的损害. 有一点看起来很明显, 即相对于那些潜在的威胁, 机构需要把监测放在优先级更高的位置上.

\*What’s important in a breach detection system?\*

### 一个泄漏监测系统, 何者重要?

To meet the challenges of targeted breaches, a breach detection system needs to be highly accurate and enable an operator to be highly efficient. In this way, even an IT or networking professional without much security experience should be able to detect an active breach and stop the attack in an early phase. Breach detection requires four main capabilities to provide the accuracy and efficiency needed by today’s organizations that are trying to prevent theft or damage to assets:

• Broad set of inputs

• Continuous behavioral profiling

• Comprehensive attack detection

• Actionable breach indicators.

为迎接针对性泄漏所带来的挑战, 泄漏监测系统必须高精度且能使运营人员高效工作. 这样一来, 即便是一个没有太多安全经验的IT或网络专家, 也能够监测到主动泄漏并于攻击早期阶段就能予以阻止. 泄漏监测系统需要四个主要功能来提供当今企业为防止资产失窃或损坏所需要的高效及准确性:

\* 全面的输入数据

\* 持续性的行为分析

\* 全面的攻击监测

\* 可操作的泄漏标志

* Endpoint intelligence can associate processes or applications with the specific network behaviors and also see prevalence—what might be unique or rare for that particular endpoint as compared to the others.
* 终端智能可以把进程和应用程序关联到特定的网络行为并且观测其出现频率 -- 对于一个特定的端口而言, 哪些 (网络行为) 是相对独特或是罕见的.

### Broad set of inputs 全面的输入数据

To detect an intruder, it is essential to look at internal connections and operations, administrative tasks and outbound communication. In particular, the internal “affairs” are the most telling for breach activity. This means that breach detection has to start with the network.

为监测入侵者, 查看内部连接, 内部操作, 管理任务以及出站连接是极为关键的. 特别要注意的是那些能够标识泄漏行为的内部事件. 这也意味这泄漏监测已经开始实施于这个网络.

While complete coverage of all networks and subnets is not necessary, it is important to view network activity at a deep level to be able to accurately profile the activity of all users, applications and endpoints / devices. This is accomplished by deep packet inspection (DPI) looking at traffic in the core of the network.

虽然全面覆盖所有网络及子网络是没有必要的, 但深层次查看网络活动来准确分析所有用户, 应用程序以及终端和设备的活动仍是十分重要的. 这是通过监控网络核心中流量情况的深度包审查 (DPI) 来完成的.

Network DPI enables a detection system to strongly associate network activity to specific users and devices. This is critical to enable accurate behavioral profiling of all users and all IP-connected devices on the network. In addition, network DPI provides a great deal of application metadata. For instance, it can show the particular interactions with a database or details about file access, including share and directory information.

网络DPI (深度包审查) 使得监测系统能将网络活动与对应的用户及设备联系起来. 这对网络之中的全部用户及IP相关设备的审计是极为关键的. 此外 ,网络DPI (深度包审查) 提供了大量的应用程序元数据. 例如, 他能够显示与数据库的特殊交互行为, 或是包括共享及目录信息在内的文件访问相关细节.

A system limited to network flow data can only see Layer 4 information, which might be helpful in seeing massive, noisy activity, but is generally useless in spotting a quiet active data breach. Flow data is limited mainly to IP addresses and ports. A port may give an indication as to the type of application being used, but even that is mostly uncertain, and it lacks important investigative metadata.

一个局限于网络流数据的系统只能获取到第四层 (传输层) 信息. 这样的信息可能对观测大量嘈杂数据有所帮助, 但对于发现不起眼的主动数据泄漏来说却意义不大. 流数据大都集中于IP地址以及端口. 端口也许能提供一些应用程序类型方面的证据, 但几乎也是最不确定的证据, 同时还遗漏了关键的调查元数据.

Input from endpoints helps corroborate suspicious network behavior and adds important investigative details. It adds to the overall accuracy of determining breach activity and provides actionable details for investigation and remediation.

终端输入能够确认网络中可疑行为并增加重要的调查细节. 它提高了判断泄漏行为的总体准确性并为调查与修复提供了可操作的详细内容.

Endpoint intelligence can associate processes or applications with the specific network behaviors and also see prevalence—what might be unique or rare for that particular endpoint as compared to the others. It can also see if the process or application is new or never before used. All of this information is extremely helpful in boosting the accuracy and efficiency of breach detection.

终端智能可以把进程和应用程序关联到特定的网络行为并且观测其出现频率 -- 对于一个特定的端口而言, 哪些 (网络行为) 是相对独特或是罕见的. 他也会观测进程或者应用程序是否从未被使用过. 所有的这些信息对于提高泄漏监测的准确性和效率来说都是极为有帮助的.

Breach detection cannot be limited to endpoint details. It’s critical to start with behaviors on the network and then use endpoint as augmentative. A view of the endpoint only will tend to miss most of the signals or activities of an active intruder. It may be possible to see a suspicious operation from the endpoint, but it will likely be singular and lack the detail needed to accurately detect a breach

泄漏监测不应被限制于终端的细枝末节. 对它 (泄漏监测) 来说, 以网络活动作为基础才是最重要的, 此后才可以辅之作为增强的终端 (智能) . 仅仅以终端的角度只会漏掉大多数在线入侵者的信号或是活动. 当然, 通过终端也有可能发现可疑操作, 但是这样的观测太过单一而缺失了对准确监测泄漏行为必要的具体细节.

Of course, most networks are noisy and crowded, perhaps even a bit chaotic, and always in flux. This makes the detection of breach activity even more difficult. Every network generates a huge amount of traffic and data and contains a countless variety of executables on endpoints.

当然, 多数网络嘈杂而又拥挤, 还有些混乱, 总是处于不断变化的状态. 这使得泄漏行为监测变得更为困难. 每一个网络都有数量庞大的流量与数据, 并含有终端上数之不尽的可执行文件.

The problem of monitoring such complex environments is significant. Alone, taking in such broad inputs tends to emphasize gathering and storing of all this vast data.

监控如此复杂环境中出现的问题也是层出不群的. 仅此一项, 接受如此大量的输入也倾向于强调收集存储这些所有的大数据.

Data science can channel this data into ongoing profiling of users and devices and change the problem from being a classic big data problem to one of machine learning and continuous intelligence. The intelligence is channeled into developing profiles of normal activity and the detection of anomalous activity.

数据科学可以将这些数据引导至对用户及设备的分析, 同时从典型大数据问题转变为机器学习与持续化智能问题上来. 而智能则指向到对正常行为的分析与对异常行为分析两方面.

Broad inputs also enable much better detection coverage across the entire lifecycle of a data breach. A data breach consists of many different activities over time, and it is best detected by an ability to see multiple activities and, ideally, how they work together.

全面的输入同时也使得整个数据泄漏生活周期中的泄漏监测覆盖的更为全面. 一次数据泄漏活动由一段时间内多次不同的行为组成, 因此, 最好能以多个活动甚至理想情况下它们之间协同关系的角度进行监测.

Seeing a single anomaly may not provide much value for a fast, accurate detection of a breach. Seeing multiple anomalies that are connected increases the speed and accuracy of the overall detection.

观测单一异常可能无法为快速准确的数据监测提供多少价值. 但观测多个互相关联的异常却能在整体监测中提高速度与准确度.

* Most networks are noisy and crowded, perhaps even a bit chaotic, and always in flux.
* 多数网络嘈杂而又拥挤, 可能还会有些混乱, 总是处于不断变化的状态.

### Continuous behavioral profiling 持续性的行为分析

Critical to successfully detecting breach activity is the continuous behavioral profiling of users and devices. Using a broad set of inputs, the goal is to establish what “normal” looks like for users and devices, by taking into consideration group, role, history, and other factors. This profiling can help reveal which users usually access which machines, for what purpose, where machines usually connect, who performs administrative operations, which machines are servers, and which workstations, and a near-endless number of other important observations.

对用户和设备的持续性行为分析对于成功的数据泄漏监测而言尤为关键. 通过利用全面的输入数据, 根据用户组, 角色, 历史记录等其他因素, 可以建立针对不同用户和设备的正常行为库. 这样的分析也能帮助展现哪些用户通常访问哪些机器, 又有何目的, 从何处建立连接, 何人进行管理权限操作, 以及分辨哪些机器是服务器, 哪些是工作站等这些几近无穷的重要观测数据.

Profiling must be an automated process based on machine learning. It would be an impossible task to manually build profiles for all users and devices with the associated network and application activity. Keeping them constantly updated and evolved would be an even greater nightmare.

分析也必须是一个基于机器学习的自动化过程. 手动为所有用户及设备建立相关网络和应用程序活动的分析日志将如同天方夜谭一般. 更别提还要迭代更新和维护了.

Profiling needs to be build on baselines of what is normal across ever-expanding time windows: what is the average per minute for the last hour, per hour for the last day, per day for the last week, per week for the last month, etc. This enables detections across vastly different timescales as appropriate, but without burdening the system with the external storage costs that plague other approaches.

分析还需要建立一套跨日益扩大时间窗口的常规基线: 比如最近一小时中每分钟的平均值, 最近一天内每一小时的平均值, 最近一个月里每星期的平均值. 这样才能使得在不同时间尺度下都能得到恰当的监测结果, 同时也无需更多的系统外部存储以免拖累到其他方法.

Profiles are specific to each company, department, role, individual, season, etc. The profiles must be created from “scratch” - there can be no boilerplate profile to start the process or assumptions about anything. To be accurate they must be built based on real behaviors. While this represents a lot of work, it also means that such an approach cannot be “gamed” by an intruder, nor can the activities stay hidden.

此外, 对于不同公司, 部门, 角色, 个人, 季节等因素的分析都是特定的. 分析必须从零创建 - 即对于任何事物, 都不能从任何分析模版起步. 他们必须基于真实行为才可以确保准确. 虽然这代表着极大的工作量, 但同时也意味着这样的方式即无法被入侵者预料, 也不会漏过任何活动.

Once a baseline of normal is developed, the system should be looking for anomalous behaviors—significant deviations from the established profiles. The key is to not “cry wolf” with every anomaly. It’s important to differentiate between a benign anomaly and malicious one.

一旦建立好一个正常基线, 系统就应当开始寻找异常文件 - 即对于建立的分析而言明显的异常. 关键还在于防止对任何异常都大叫"狼来了". 分辨良性异常与恶意异常也至关重要.

### Comprehensive attack detection - 全面的攻击监测

After an attacker spreads through the network, there are numerous operational activities they need to perform. To be sure, these are human-led functions. This is not an automated process such as might be used to establish a botnet or create a malware delivery service. Real cybercriminals are behind these targeted breaches, and they are in direct control of each step and sequence of the attack. With comprehensive, accurate profiling from a broad array of inputs, these activities are difficult or impossible to hide.

当一个攻击者渗透入网络后, 他们就需要实施相当数量的操作行为. 当然, 这些都是手动完成的操作. 还没有能够用来建立僵尸网络或创建恶意软件注入服务的自动化进程. 这样的针对性泄漏背后都有直接控制攻击的每个步骤和顺序的真实网络罪犯的身影. 通过对广泛的输入内容进行全面精准的分析, (攻击者) 将难以甚至不可能隐藏这些的行为.

There are four basic types of breach activities after the initial intrusion. The two most commonly understood are communication and control (C&C) behaviors and exfiltration. C&C is the so-called “phone home” activity that enables an external attacker to learn about the network, orchestrate the ongoing breach and install any software that would be useful in conducting the breach. Exfiltration is the act of moving data out of the victim’s network and to a site controlled by the attacker. This stage of the attack is late in the process, and should obviously be avoided. Breaches should be identified and stopped prior to exfiltration.

初始入侵之后的泄漏活动可以分为四大类. 最为人普遍了解的两类分别是通信与控制 (C&C) 行为和渗出. C&C 也叫做"电话中心"活动 , 能够使得一个外部攻击者了解网络, 协调正在进行的泄漏以及安装有助于实施泄漏的任何软件. 渗出则是将数据从受攻击网络中移出至攻击者控制的站点上. 然而这已经处于攻击的晚期阶段了, 并且显然应该避免. 泄漏行为在渗出之前就应当被识别并制止.

Even so, there is tremendous value in deploying a breach detection system even late in the breach process. While exfiltration may have been accomplished, there could likely be follow-on steps to the breach, including addition theft, damage, extortion or leap frogging to a partner, customer/client, supplier or any other entity connected to the victim.

尽管如此, 在泄漏行为的晚期阶段部署泄漏监测系统仍然拥有可观价值. 即便渗出已经完成, 它依然可能成为泄漏后续工作的突破口. 这些后续工作可能包括盗窃, 损伤, 敲诈甚至传染给合作伙伴, 客户, 供应商等任何连接到受害者的实体上.

While being the most widely understood breach activities, C&C and exfiltration are also the two activities that can be best obscured by an attacker. Once an attacker has a foothold in the network and owns the “home base,” they can carefully manage these communication processes and hide communication flows in tweets, Gmail messages and other seemingly benign activities. They can sometimes be difficult to spot.

C&C 与渗出不仅是最为广泛认知的泄漏行为, 同时也是可以被攻击者隐蔽的最好的两个行为. 一旦攻击者在网络中站稳脚跟并建立"大本营", 他们就能够谨慎控制这些通信过程并利用推特, Gmail消息等看起来正常的活动来隐藏通讯流. 这样依赖就很难被发现了.

The two other active breach activities are sometimes known as “East-West” activities. They go hand in hand and help the attacker get to know the network and identify assets and key vulnerabilities (reconnaissance) and move to gain additional points of control and to get positioned to access target assets (lateral movement)

另外两种主动泄漏行为有时也被称为 "孟焦" 行为. 他们一同出现并能帮助攻击者熟悉网络, 定位资产与关键漏洞 (侦查) , 转变角色以获取更多权限, 以及转移位置来访问目标资产 (横向移动) .

Successful breach detection requires seeing the forest and not just the trees. The trees can be seen by a good breach detection system, but discerning a real active data breach generally requires seeing multiple activities, perhaps at different points in the attack lifecycle

成功的泄漏监测需要的是纵观全局而非一叶障目. 优秀的泄漏监测系统自然需要关注那些独立的细节, 但分辨出一个真实的数据泄漏还需要关注可能存在于攻击生命周期中不同阶段的多个行为.

### Breach indicators - 泄漏标志

Due to the failure of legacy systems to detect an active breach and the well-known frustration of mountains of security alerts, I like to think in terms of “breach indicators.” Rather than simply an alert of something anomalous and without context or confidence, a breach indicator presents a probable indication of a breach with a high level of assurance and with contextual details to show why such an assessment was made. These breach indicators should be based on multiple events or actions, ideally over a span of time.

鉴于以往系统在主动泄漏监测以及广为人知的海量安全警报上的失败, 我更倾向于"泄漏标志"方式. 相比于忽略背景及可靠性的异常行为警报, 泄漏标志代表的一个是具有更高准确率及能解释评估理由的背景详情的标志. 这样的标志应当基于一段时间内的多个事件或行为.

The detection of advanced attackers within live production networks poses a significant challenge. Many legacy security vendors are attempting to shift their focus to this broadlyrecognized problem, but most are ill-suited to the task. Most unfortunately combine both a limited degree of visibility (inputs) with an analysis model that cannot drive highly accurate or actionable alerts. An effective breach detection system learns what is normal on your network through profiling, and then detects active attackers based on anomalous behavior.

对于在线产品网络中更高级的攻击者的检测则是一项更有意义的挑战. 很多安全厂商都试图把重点转移到这个广泛认可的问题上, 但大都没能胜任这一任务. 程度有限的输入数据与无法提供高精度及可操作警报的分析模型共同造就了这些不幸的发生. 一个有效的泄漏监测系统必须先分析了解对于您的网络而言何为常规, 然后才能基于异常行为来监测在线攻击者.

Only through a new approach to breach detection can organizations win against a targeted attacker. Prevailing against an attacker is certainly possible, but it requires new strategies, plans and system.

想要防范针对性攻击者, 我们需要的是采用新方法进行泄漏监测, 战胜攻击者是完全可能的, 但它需要的是新的策略, 新的计划以及新的系统.