IBM Security

2017 年 10 月

白皮书

网络威胁狩猎的觉醒：面向安全和风险的情报分析

IBM

目录

概览问题

如果整个专业团队围着看似无解的问题转，情况将会怎样？想象一下那些永远不会消失、只能加以管理的问题和危机。这种范例就像医学自出现以来一直都在应对的情况 - 在看似永无止境的循环中应对疾病和伤害的冲击。

随着时间的流逝，医师们创建了专门的学科，以此方式推动医学发展，以应对威胁。重大问题由急诊科处理，神经病和心血管病等棘手问题则由各自的专科处理。流行病学家和预防医学专家负责研究长期趋势和模式。现在，现代医学可以运用更具针对性的解决方案来有效地缓解问题。显然，如今的医学专业远比 100 年前（即医学专业诞生之前）更加有效。

同样，网络安全领域也在不断发展。认知分析这一新专业是一个新兴学科，它能够帮助人类安全分析师发现未知信息，从不同的数据集中获得洞察力，尤其是发现高级威胁。

通过对比网络领域的威胁与医学领域的威胁，我们可以从中吸取很多教训。这种创建网络认知分析学科的观点是受到了医学领域的启发，因为医学是一门必须不断学习、不断接受教育培训、追求精益求精的专业。

大家只需要看看新闻，就会了解网络安全领域的日常情况。2017 年 Verizon 数据泄露报告[1] 显示，在 12 个月内共记录了 1,935 例确认的数据泄露事件和 42,068 例安全事故，而涉及的组织只有 1,003 家。我们的公共和商业企业如何会在安全方面达到如此可怕的状态？当前安全危机的主要原因可以分为两大支柱：

支柱 1 - 威胁的演变

- 高级技术商品化。在专家讨论网络威胁的破坏时，通常会提出 80/20 原则，意即：80% 的网络攻击实施者一般不那么精于此道，而前 20% 的网络攻击实施者则非常精于此道，以至于只要有足够的时间和资源，他们便可攻入任何网络。从历史上来看，前 20% 的网络攻击实施者专注于防御和情报社区。现如今，商品化威胁的出现将高级技术传播给了更大的受众。从 2006 年开始，“Web Attacker（Web 攻击者）”漏洞攻击工具包的出现带来了一套打包的工具套件，任何用户都可以使用。[2]
- 多年来一直磨练黑客技术的高级开发人员现在可以将黑客工具包作为软件包出售，进而利用他们丰富的经验获利。漏洞攻击工具包会攻击已知漏洞，提供攻击者所选的恶意有效负载。开发人员正在不断开发具有不同攻击向量和感染技术的新漏洞攻击工具包。在任何给定时间，都有数十种漏洞攻击工具包可供使用，包括 Zeus 变体、FlokiBot、NukeBot 和 GM Bot 等。这些工具的广泛使用提高了各类攻击者的策略、技术和程序水平。
- 不对称威胁的兴起。在不对称冲突中，两个冲突方可能在能量和能力上存在着很大差异，但由于利用了关键漏洞，双方的冲突会持续进行。数个世纪以来，小规模部队已经能够利用地形和战术压制大规模部队。在网络领域也有类似的概念：黑客使用廉价的笔记本电脑，加上价值只有 500 美元的攻击工具包以及一些创新技术，便可以渗透到已投资数百万美元进行安全保护的网络。不对称网络威胁的常见示例包括：通过被劫持的 Twitter 帐户发布虚假推文来影响股票市场，或小规模团队或个人通过勒索软件攻击加密关键信息，进而破坏组织的正常运营。随着个人黑客不断突破通用安全系统，网络领域的持续冲突已成为人类的难题之一。

- **注重机密性。**有效的信息安全是基于三个核心支柱而定义的，分别是机密性、完整性和可用性。数据的机密性是指保证只有经过适当授权的人才能访问系统信息。数据完整性是指系统中的所有信息都是完整且无错误的这么一个概念。数据可用性是指系统正常运行或可供用户访问的时间。
- 攻击者会针对所有支柱进行攻击。他们会尝试通过拒绝服务攻击破坏网络的可用性，对数据进行加密并以此为要挟索要赎金，通过注入或更改电子邮件和其他数据来破坏数据，以及通过彻底盗窃数据来破坏机密性。攻击者所选的武器通常是通过垃圾邮件发送的某种恶意软件。
- 2017 年 IBM® X-Force® 威胁情报指数报告显示，从 2013 年到 2015 年，共发布了 4.31 亿个新的恶意软件变体。[4] AV-TEST Institute 每天注册 39 万个新的恶意程序，这意味着此增长趋势丝毫没有减弱的迹象。[5]
- X-Force 报告还强调，恶意软件是作为垃圾邮件的附件而提供的，与 2015 年相比，2016 年的垃圾邮件数量增加了 400%，而恶意附件的数量也有大幅增加。[6] 通过木马、键盘记录程序、病毒释放器和勒索软件等恶意程序，黑客可以获得系统的远程访问权限，同时隐藏连接，因此很难加以检测。
- 尽管网络犯罪分子会影响信息安全的所有支柱，但大多数安全技术、程序和框架都以可用性以及如何让威胁远离边界为重点，进而会影响提供完整性和机密性的能力。安全行业需要具有更大的灵活性来应对攻击者的战术。

支柱 2 - 不完整的安全响应

- **安全目标错误。**大多数组织都形成了 100% 完美的安全观。在这一追求中，使得“完美”走向了“足够好”的对立面。安全产品已经发展到创造一个所谓的不可渗透的屏障，并且长期以来，安全领域的大部分投资都集中在边界。2017 年的“Gemalto Data Security Confidence Index”就提供了这种思维模式的一个示例，其中 94% 的信息技术决策者认为边界安全技术能“非常有效地将未经授权的用户拒之门外”。[7]
- 在过去的四十年里，网络安全社区并未从根本上改变保护网络的方式。他们在构建下一代防火墙上付出了巨大的努力 - 扩展了围绕网络的虚拟护城河和边界防御技术。当攻击者终于在复杂的系统中发现随机漏洞后，他们就可以在受害者的网络中自由移动了。通常，网络内的监控和可视性最低，这样，攻击者就能“在看不见的地方游走”。例如，如果攻击者要是发现了管理员凭证，他们就可以不受限制地访问所有系统，因为安全设备通常不会记录管理员的登录。由于过于关注将攻击者拒之门外，大多数组织都没有重视弹性，因此无法限制恶意攻击者可能造成的破坏。

- **数据过多，工具过多。**单单是获取适当的数据以实现网络可视性就是一项艰巨的任务。如今，现代网络拥有大量工具和数据存储，用于记录每个日志、警报和脉动信号。数据如此之多，以至于一位分析师需要花一生的时间在不同的数据源中进行筛选才能发现相关事件。而大量令人困惑的安全工具又使得数据过多的问题变得愈加复杂，企业需要持续维护和配置这些安全工具。信息安全团队可能非常了解有关网络攻击的指示器和解决方案，但是现有解决方案的复杂性使其很难实时发现答案，也很难区分重要的数据和数据噪音。
- **缺乏经验丰富的人员。**公共领域和私营领域都在迅速寻求通过合格的人员来提高网络安全级别，但是受过培训的人员根本不够。美国劳工统计局 (US Bureau of Labor Statistics) 数据显示，2015 年有 209,000 个空缺的网络安全岗位，其中约 40,000 个为信息安全分析师岗位。许多岗位要等待 6 个月甚至更长的时间才能找到求职者。针对安全专家培养的教育机会和培训已经大大增加，但是我们还需要花费大量时间才能缩小技能差距，因为预计到 2022 年网络安全岗位需求将增长 37%。[8] 而骨干安全分析师需要花费更长的时间才能积累经验，熟悉技能。没有技能娴熟的团队，企业很难持续跟进安全操作。

角色、责任和术语

要启用由认知驱动的方法，我们必须定义术语并概述特定角色。就像医学领域开始专门研究复杂问题一样，安全行业也必须如此。网络安全必须成为一个需要正规培训、资格和持续教育的职业。我们首先必须区分安全的操作方面和最终创建的产品之间的区别。因此，我们应该定义*分析 (analysis)*、*统计分析 (analytics)*、*认知和情报*之间的区别。

分析 (analysis) 是对相关数据的检查、核查和调查，以便得出结论。通常，这是一个人为主导的手动流程。

统计分析 (analytics) 是对数据或统计数据进行系统化和程序化的计算分析，以生成结果。通常，该流程是自动化的，并且需要计算机的大力协助。

认知是在获取和理解知识、决策和问题的解决中涉及的思维过程。它以事实而非情感为基础。

情报是指有价值的信息集使用某种格式生成的最终结果，它可以作为您制定决策或得出结论的依据。

在这种情况下，分析和统计分析是数据检查的操作流程。该流程的*产物*被认为是*情报*，其目的是支持决策者从混乱的随机性中获得有价值的洞察力。

现在，我们必须探究*信息安全*与*网络分析*之间的区别（图 1）。术语“*信息安全*”通常是指为增强组织架构核心而执行的操作，而“*网络分析*”是指对高级威胁的检查。

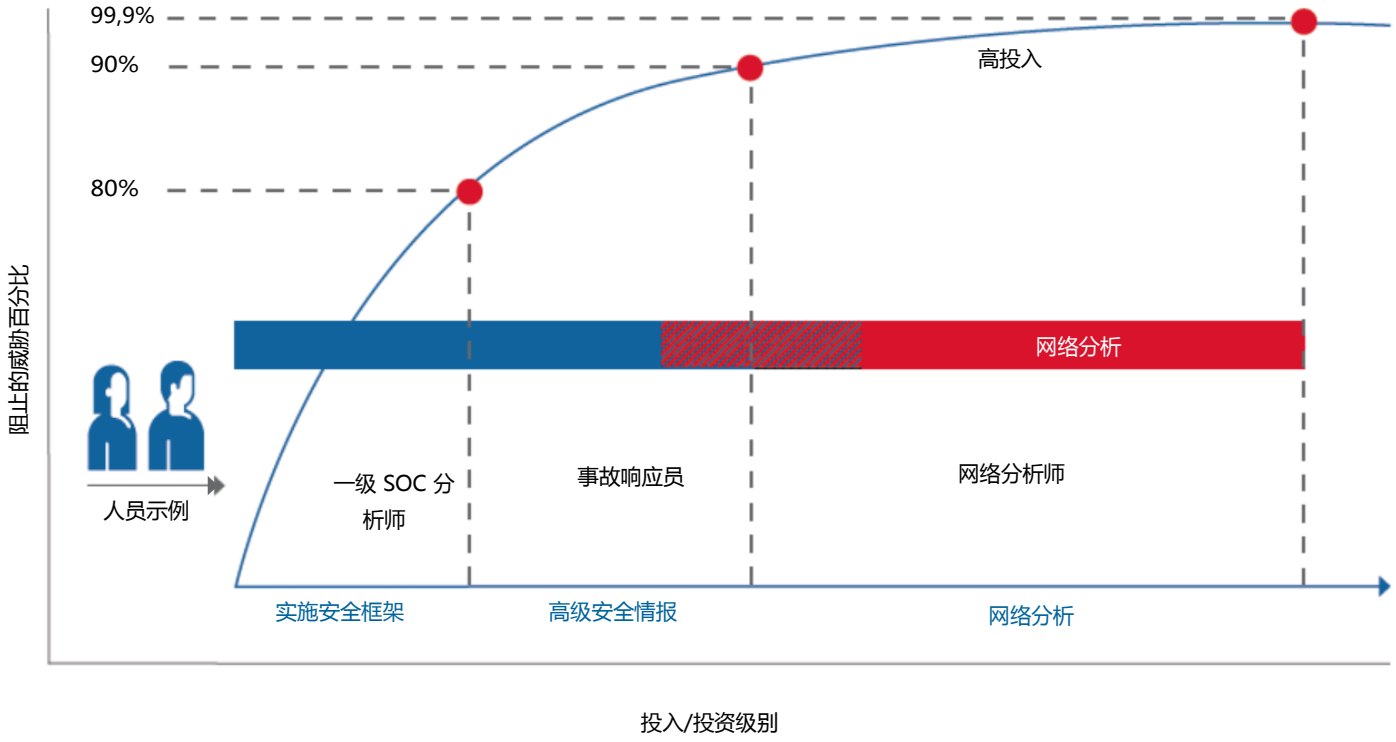


图 1：信息安全领域和网络威胁分析领域的区别。

为了覆盖整个网络威胁范围，组织必须同时兼顾信息安全和网络分析的自然演变，包括使用认知工具，这种做法通常被称为“网络威胁狩猎”。信息安全通过框架利用部分专业知识和技术来构建安全基础。最终，安全流程将演变成网络分析，而网络分析将长期研究恶意攻击者，并生成生态系统可视性。

类比医学，信息安全就是关键问题的“卫生处理和分诊”。而网络分析就相当于医疗和实验室研究，它研究的是更持久的问题（表 1）。

	医学		**安全**	
	威胁示例	**缓解措施**	**威胁示例**	**缓解措施**
一级-卫生	常见医院内感染	洗手、戴口罩、穿外科手术服	商品威胁、个人黑客与广泛使用的工具	更改密码、删除未使用的服务、打补丁
二级-专业化	紧急情况（如胸痛、枪伤）	建立重症监护和预防医学学科	有组织的犯罪、半定制诈骗和犯罪软件工具	可视性、监控、发送警报、响应、实时安全分析
三级-研究	遗传疾病和癌症	研究和定制遗传治疗	高级持续性威胁、国家级攻击、资源密集	网络分析、威胁情报趋势分析、活动跟踪

表 1：该表简要类比了医学和网络行业，以及它们如何制定缓解措施以减轻各级威胁。

不论是信息安全还是网络分析都需要分析和统计分析操作。它们可能都需要人工操作员和分析师来检查数据和警报。此外，这两个维度都使用自动化工具来辅助分析和统计，主要是辅助自动化的重复操作。认知系统充当值得信赖的顾问，它处理的数据比人工处理多得多，从而挖掘新的洞察力、模式和安全情境。在该流程结束时，信息安全分析师和网络分析师都将生成情报，这是帮助领导做决定的最终产品或结论。情报产品的范围和规模可能各不相同。信息安全分析师可能对计算机恢复到易受攻击状态时的特定警报感兴趣。威胁狩猎可能会将上述事件视为长期趋势中的一个数据点。

在所有这些情况中，通过用认知系统补充调查，您可以扩大并提高可用情报的准确性，最终得出更明智的结论。

以下定义阐述了信息安全和网络威胁狩猎之间的区别：

安全分析

该方法指的是汇总、关联和自动化 IT 相关数据，以检测、发现和了解信息安全威胁。该流程大部分由依赖算法和模式识别的自动化工具执行。

网络分析

该方法以人为主导，分析逻辑和物理领域的安全和非安全相关数据，以研究趋势，发掘异常，提供情境，创建关系并发现隐藏的问题。

网络情报

有关安全相关问题的循证知识和可行建议。

安全情报

组织可用的从安全相关数据的分析中得出的可执行信息。

各个组织的术语可能各有不同，因为网络分析和网络威胁狩猎是新兴学科。就像医学领域在社区中不断完善术语一样，网络行业也是如此。一开始的部分网络分析工作始于政府组织，作为军事情报流程的自然延伸。因此，政府部门的从业者倾向于将安全分析、网络分析和威胁研究的整合流程称为“网络情报”。通常，这是因为政府部门利用情报周期作为融合所有数据和创建产品的手段。在私营领域，网络分析师也被称为网络威胁猎人，因为他们通过筛选数据来捕获攻击迹象。

当前方法缺点案例研究

网络领域一直受到恶意攻击者的威胁，包括业余黑客和国家级攻击者。在讨论网络威胁时，请务必牢记攻击者能力和意图的两个因素。例如，恶意攻击者可能拥有最先进的工具，但只有在极少数情况下才会使用它们。从以往来看，拥有先进能力的攻击者和以私营领域为目标的攻击者之间存在着明显的差异。同样，以攻击私人实体为目标的攻击者缺乏影响信息网络的工具、技术和人员。在过去的几年中，我们发现高级威胁局面发生了巨大的变化，这是私营领域极为关注的问题。

低能力、高意图的攻击者也能带来不亚于高能力攻击者的破坏性影响。由于不对称网络威胁的性质，组织必须防御聪明的低能力攻击与高影响力的复杂事件。

以下提供两个案例研究：2014 年的 Sony Pictures 攻击，这是一次高能力事件。另一个案例是 2016 年攻击者成功攻击环球银行金融电信协会 (SWIFT) 的银行网络，窃取了数千万美元。这次危害支付流程的攻击使用了相对简单的技术，取得了巨大的效果。这些研究表明，高级攻击者可以在网络上潜藏数月而不被普通安全方法检测出来。它还表明，如果不将安全性的人为因素纳入分析，低能力攻击者也可以轻易侵入系统并造成相当大的破坏。

案例研究：索尼攻击

2014 年 11 月 25 日，开始有报道称 Sony Pictures 受到了一个勒索软件的攻击，该软件与一个自称 “Guardians of Peace” 的组织有关。[9] 五天后，FBI 协助调查，并最终发布警告，警告称破坏性恶意软件将进一步扩散。在接下来的几周内，公共论坛上出现了数百 GB 的索尼文件包，其中包含个人身份信息、敏感信件和薪酬信息。

2014 年 12 月 3 日，彭博新闻社 (Bloomberg News) 发布了一篇文章，介绍了对索尼网络中发现的恶意软件的早期检查结果。检查结果表明，黑客事先熟悉索尼的网络。通过分析代码，他们发现了索尼内部服务器的名称以及连接网络所需的凭证和密码。该恶意软件用于与欧洲和亚洲的 IP 地址进行通信，这对于试图掩盖自身位置的黑客很常见。这可能表明黑客在网络中潜伏了几个月。

2014 年 12 月 19 日，联邦调查局发布了官方最新的调查结果，[10] 结论是朝鲜政府对此次攻击负责。报告表明，朝鲜的黑客几个月前就潜入了该网络。尽管最初的感染媒介仍然未知，但据信这是一次有针对性的鱼叉式网络钓鱼攻击。黑客在索尼攻击中使用了恶意软件 BKDR_WIPALL.A-F。这个后门包含一个用户名和密码列表，用于在攻击中授权访问受感染机器的系统根文件夹。攻击者在系统中植入后门的方式包括：其他恶意软件在系统中放置文件，或者用户在访问恶意网站时不知不觉下载了文件。结果，放置文件的恶意例行程序会显示在被感染的系统上。它会连接特定的网站以发送和接收信息。2015 年 2 月上旬，索尼宣布初期的修复费用约为 1500 万美元。

案例研究：下一代银行抢劫

2015 年 2 月 4 日，纽约联储 (Federal Reserve Bank of New York) 处理了四个转账请求，从 Bangladesh Central Bank 转账 1.01 亿美元至菲律宾和斯里兰卡的银行。交易是按照 SWIFT 的程序和凭证进行的，SWIFT 是一个国际性联盟，运营着一个值得信赖的封闭式计算机网络，以支持全球成员银行之间的资金转拨。尽管转账似乎有点异常，但由于凭证有效且纽约联储在向孟加拉国当局发出询问请求后并未收到对方的回复，交易得以继续进行。[11]

事后对该操作的检查结果显示，不明攻击者在计划执行前几周就将恶意软件（很可能是远程访问木马（RAT））植入了受害者的计算机系统内。该恶意软件能够收集用户凭证，随后入侵者发现了电子资金转账流程。在收集到足够的信息之后，欺诈者终于开始了他们的行动。该机制还能让黑客删除关键的系统文件并禁用记录了每个转账请求的打印机，这使得银行更难在转账停止之前发现这些转账操作。[12]

此次事故本可能造成更严重的后果，万幸黑客在提交数十笔交易后，由于请求文档中的错别字，除四笔外，其余所有交易均被拒绝。但是，此次事故很重要，因为它引起国际金融机构质疑每日处理数百万次通信的系统。调查人员透露，此次抢劫所使用的恶意软件几乎与入侵厄瓜多尔、越南和菲律宾银行的恶意软件一模一样。

对黑客的调查揭示了罪犯如何获取凭证，了解银行的流程并试图避免被发现。但是，检查还发现 Bangladesh Central Bank 的安全措施相当宽松。他们的网络没有防火墙保护，因此，在网络中植入恶意软件变得更加容易。在许多近期备受瞩目的数据泄露案件中，受害组织缺乏网络弹性，这一点显而易见。回到与医学的类比，这就相当于切开一个可以让病毒进入的小伤口，而最终因忽略了感染症状而导致病患死亡。在这个特定的案例中，如果 2015 年 1 月检测出了恶意软件，他们就可以阻止 2015 年 2 月的事件。

情报运营的概念：新方法

网络威胁狩猎是安全行业的最新领域之一。这个新兴学科融合了情报分析、信息安全和法庭科学的各个方面。网络流量和系统日志是网络威胁分析师的基础数据源，但他们还必须考虑外部信息源和人工生成的信息源。通过使用网络分析，您可以更快地检测到任意来源的入侵。结合利用高级分析和认知平台与人类的智慧是检测入侵的最有效方法。

网络猎人擅长在海量数据集中找到独特的模式。考虑黑客攻击的四个阶段：侦察、扫描、利用和坚持。如果组织整合了系统日志和网络流量，则分析师可以在每个阶段筛选数据。分析师可以将多个来源的事件关联起来，并回放攻击是如何发生的。通过一段时间对模式的追踪，分析师可以确定扫描的签名并将其分配给特定的攻击者。这将有助于预测何时发生攻击。这样，分析师就能快速找到来自后门信标的流量，并在网关处拦截这些流量。数据源无关紧要；分析师可以轻松识别来自内部威胁和互联网攻击的流量。在上述 SWIFT 抢劫案例中，也许通过采用整体情报分析和信息共享方法，分析师就能确定初始模式，抢劫也就不会发生了。

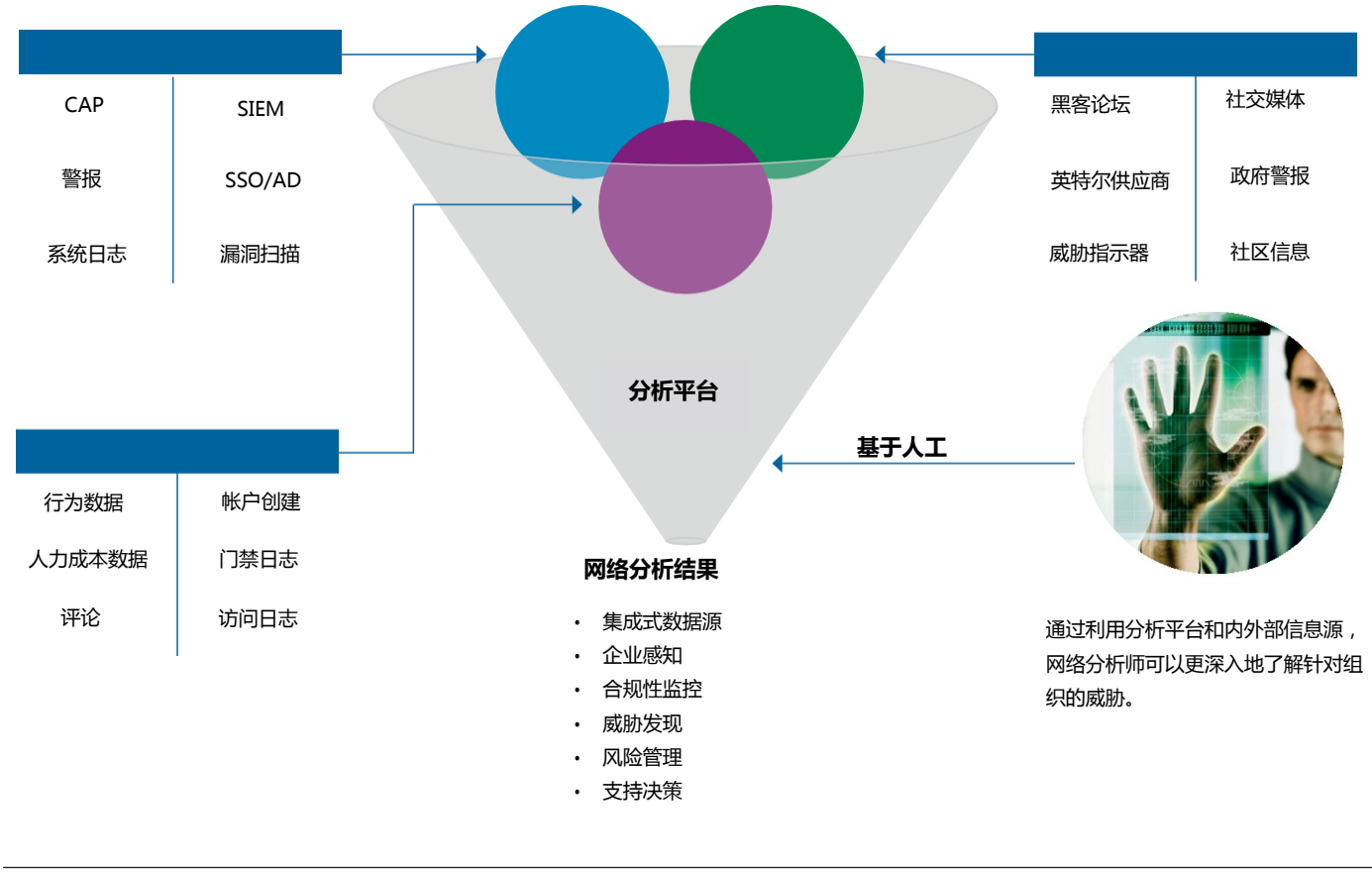


*图 2：*提供网络威胁分析流程的各种组件。

网络威胁分析学科在现代安全运营中心 (SOC) 中发挥什么作用？总体安全运营在时间上分为战术、战役和战略三个阶段。在运营的每个阶段，分析师可能生成数据和情报，为决策提供依据。所有安全范围和关键功能定义如下：

战术阶段。该阶段生成的情报主要供安全操作员在日常战斗中使用。该领域最常见的工具是威胁源或威胁指示器 (IOC)。该阶段可以细分为*当前操作*（0-24 小时）和*未来操作*（1-5 天）。*一级分析师*通常是当前操作中的关键角色，负责不断检查感兴趣的事件并进行分类，以确定关键事件。一级分析师可能需要 1-15 分钟的时间来检查每个感兴趣的事件。二级分析师接收并深入分析一级分析师提交的案例，以确定实际发生了什么以及感兴趣的事件是否可能是事故。二级分析师可以使用系统事故和事件监控 (SIEM) 工具来辅助执行此职能。二级分析师可能需要 1-5 天才能检查出感兴趣的活动。在医学领域，这就相当于急诊室的运转。

战役阶段。此阶段尝试使用高级取证分析来确定攻击的性质。事故响应员或逆向工程师是此阶段的关键角色。他们使用硬盘映像、全会话数据包捕获 (PCAP) 或恶意软件逆向工程等工件，确定事故中到底发生了什么。他们可能使用安全情报或取证工具辅助执行此职能。有时，他们必须收集和分析法庭证据以支持正式调查。此阶段尝试确定事故中出了什么问题，并生成情报以防止未来出现问题。

战略阶段。此阶段尝试查看更大的数据生态系统，以洞悉威胁、漏洞和攻击者的 TTP。在该流程中，网络威胁猎人将结合利用网络新闻资讯、签名更新、角色数据、事故报告、威胁摘要和漏洞警报，最终生成网络情报。战略阶段的情报可以帮助高层领导制定有关安全投资的关键决策，它可以回答谁出于什么原因在攻击我。战术和战役阶段可能收集威胁攻击者攻击类似组织的情报，以提高运营效率。

战略阶段打开了数据的大门，而且检测更长时间范围内的问题。在医学领域，这相当于对遗传疾病的长期研究。比如一些癌症需要很长时间才会出现明显的症状。但是，“噪声基底”中可能隐藏着一些潜在指示器或标识。通过开展研究，识别看似正常的指示器组合，医生可能可以在癌症发展到危险阶段之前发现它。

网络分析和相关平台中可能有各种各样的用例。在最简单的用例中，我们假定事件与相关事故的比率为 100,000:1。从表面上看，这个比率非常小，但是许多组织每天可以产生 20 亿个事件。这样一来，该公司的安全团队每天需要调查 20,000 个事故。

传统的 SIEM 关联工具可能会将噪声降低到错过重要关联的程度。通过利用受过训练的人类专家的经验和认知辅助机器，网络分析平台可以快速识别重要的潜在活动。

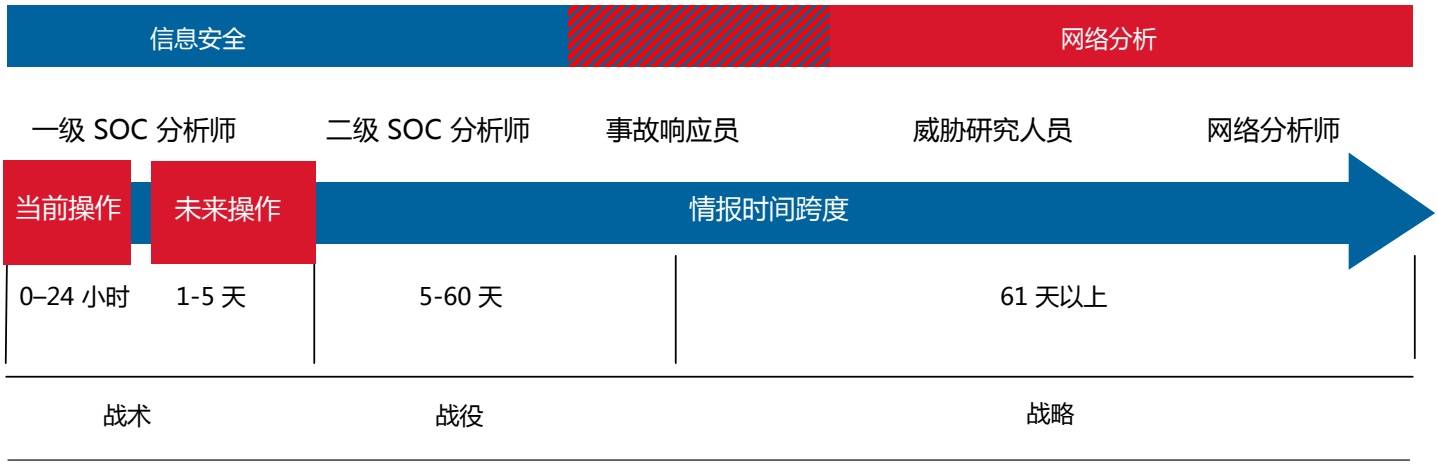


图 3：适用于信息安全和网络威胁分析的情报时间跨度。

以下是使用网络分析的其他用例：

- **捕鲸运动。**通过整合电子邮件元数据、威胁指示源和 Web 代理日志，网络分析功能可以发现针对大型公司高管的“鱼叉式”钓鱼活动，也就是捕鲸。此类活动必须通过分析才能发现，并且它们在个人信息源中并不明显。
- **信标活动。**分析师可能从发现出站到不同位置的异常端口打开活动入手。通过检查代理日志并与外部数据相关联，分析师可以发现最初的感染源，还可能发现遭到破坏的精确数据。
- **发现隐藏的 RDP 会话。**分析师可能会发现定期出现异常的远程桌面 (RDP) 会话。通过提取 HIPS、IDS 和防火墙日志，分析师可以发现在哪些位置边界安全机制未能检测出允许在内部系统上执行的远程漏洞。
- **内部僵尸网络。**分析师可以整合代理日志、防火墙日志和 IDS 数据集。通过将数据集可视化并挖掘数据集，您可能会发现内部僵尸网络控制器在内部业务网络中蔓延。被感染的机器可能会通过看似正常流量的加密会话，向恶意命令和控制节点发出信号。
- **内部威胁。**通过检查人力资源数据库、管理员记录和商业智能数据库，分析师可以发现已离职但仍拥有未撤销的高级管理员访问权限的员工。此外，分析师可以使用时程分析，快速确定哪些员工在下班时间仍在访问关键系统。
- **供应商风险管理。**一些大型组织可能采用成千上万个供应商提供各种类型的服务。成熟的安全程序将尝试了解这些供应商的风险，但往往很难确定风险最高的供应商。图 4 简要描述了网络分析流程如何使供应商风险流程变得更有效。

安全供应商风险管理团队会访问并记录有关供应商的信息。

报告包含详细介绍基础架构和保护措施的信息页面。

定期扫描供应商服务器的漏洞，服务器包含敏感的公司信息。

不断分析各种社交媒体资讯，寻找正在讨论如何对供应商发起潜在威胁的恶意攻击者。

BitSight 提供有关僵尸网络和其他漏洞活动的实时数据，这些活动源自供应商的基础架构。数据服务对每个供应商进行实时风险评级。

通过挖掘各种暗网数据源，安全团队可能会发现某个泄露指示器，该泄露涉及可能包含敏感公司数据的某家供应商。

*图 4：*一个分析流程，可帮助您确定企业风险更高的供应商。

IBM i2 Enterprise Insight Analysis 的验证点

人类分析师是网络分析流程的重要组成部分。分析师将利用直觉和经验发现隐藏的威胁，并随着时间的推移发现威胁活动的模式。为了最大程度地提高分析师的能力并增强工作能力，成熟的安全组织必须使用数据分析工具来充实、生成、可视化和分析信息。IBM 使用 IBMi2® Enterprise Insight Analysis（EIA），这是一款开放、可扩展、可互操作的解决方案。它支持组织快速、大规模地执行分析和高级分析，帮助他们加速推进数据到决策流程。

以下是在 i2 EIA 中创建的特定网络分析和威胁狩猎用例：

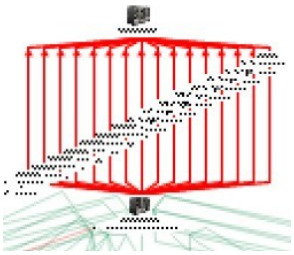
统一 SOC 分析师：随着时间的流逝将蛛丝马迹串联起来

*问题：*数据集中隐藏了哪些潜在活动？随着时间的流逝，您如何压缩不同的事件？

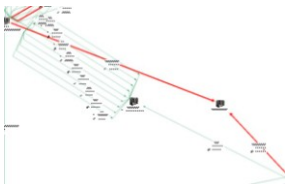
*为什么这很困难：*高级攻击者可能使用简单而缓慢的技术来进行伪装。

*i2 Enterprise Insight Analysis 网络解决方案：*高级攻击者可能使用简单而缓慢的技术来进行伪装。

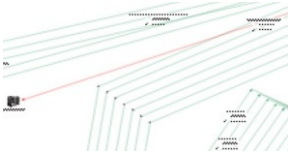
捕获模式是网络分析的环节之一，也就是，寻找通常无法检测到的未知的未知情况。想象一个典型的 SOC，其中有多位分析师，他们每天按两三班倒工作。每个岗位甚至可能分配五名不同的人员。一位分析师可能会发现一个引起关注的事件，然后认为是良性异常而将其忽视。换班的另一位分析师可能会注意到一个具有某些相关属性的相似事件，但无法确定两个问题之间的相似之处。这些难以发现的异常可能就是“简单而缓慢”的攻击的征兆，而这些攻击很难被检测出来。下面，我们研究四个单独的事件，如果这些事件是由不同的 SOC 分析师发现的，则可能看似无关：



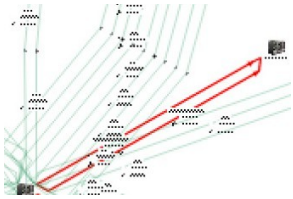
拦截电子邮件流量：分析师注意到来自异常端口上的 DHCP 服务器的电子邮件流量。



端口 81 的流量：HTTP 网络流量记录在端口 81 上；有时它们与 TOR 有关。



端口 80 上的 LDAP 流量：分析师注意到端口 80（而非通常的端口 689）上的 LDAP 流量。



出站 FTP：在端口 20 的网络中发现了奇怪的出站 FTP 流量。

*图 5：*四个看似无关的异常信号可能表示“简单而缓慢”的攻击。

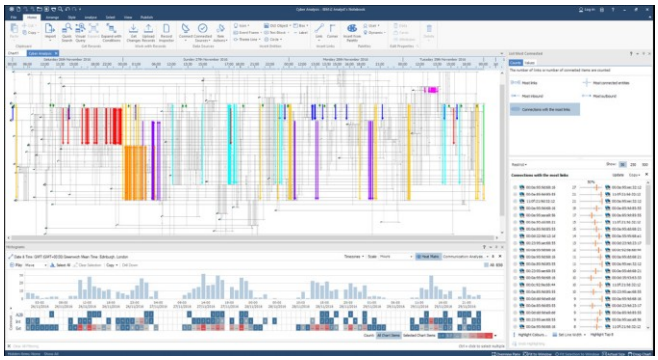


*图 6：*作为了解未知情况的一种方法，i2 EIA 可帮助分析师发现会在更远的将来显现的问题。

跟踪威胁活动：预测谁将在何时攻击您

*问题：*谁在攻击我？我最容易受到攻击的地方在哪里？什么时候可能出现攻击？

*为什么这很困难：*关于攻击者和攻击媒介的数据来自各种孤立的数据源。

*i2 EIA 网络解决方案：*高级分析，比如社交网络分析、可视化查询攻击、数据融合。

网络威胁分析平台的一个主要优势是它能够获取所有外部安全数据，并将其与组织的内部安全运营进行比较。这个角度的信息对于内部网络情报团队来说非常重要，它们能使安全生态系统中的所有数据与组织相关且具有可操作性。i2 EIA 能够摄取多个数据源并提供高级分析工具，从而启用这个战略分析组件。

全局概况：使用 i2 EIA 的分析师发现这些事件是相关的。所有异常都连接到最初被恶意软件感染的 DHCP 服务器。恶意攻击者使用一台服务器向网络中的用户发送网络钓鱼攻击。一旦个别用户被感染，便与 C2 服务器建立 FTP 会话，然后窃取数据。老练的攻击者会使用反常的端口来掩盖与 C2 节点的连接并隐藏内部流量。

打开开口。非结构化和结构化的源数据是从公共数据源、深网、供应商和社交媒体数据源自动导入的。IBM i2 EIA 可以自动执行该流程。在论坛上，攻击者将讨论策略并针对他们攻击的目标发表声明。黑客通常会在合法网站和暗网上使用相同的账号名。这种关联可以用于挖掘个体之间的隐藏关系。您还可以获取与过往攻击有关的 STIX/TAXI 类型的数据，从中挖掘模式。

了解攻击者和攻击方式。借助自动化社交网络分析工具，分析师可以查看威胁攻击者的人际关系、行动、技术和步骤。分析师可能会发现连接到威胁攻击者的地理 IP 地址信息，安全团队可以利用这些信息识别威胁。他们可以了解被特定功能群体瞄准的行业以及他们如何入侵相关的防御系统，并将这些信息与组织当前的安全状态进行比较。

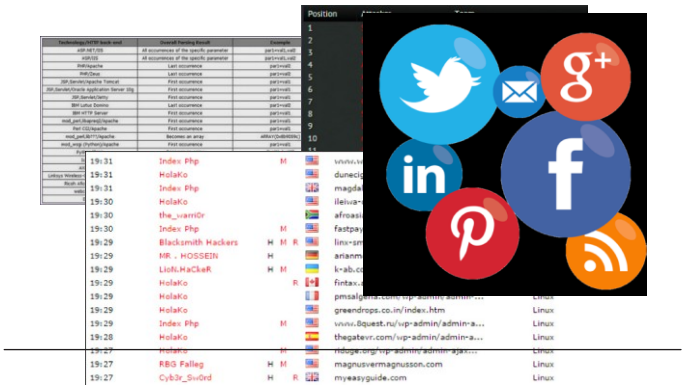


*图 7：*社交网络分析工具

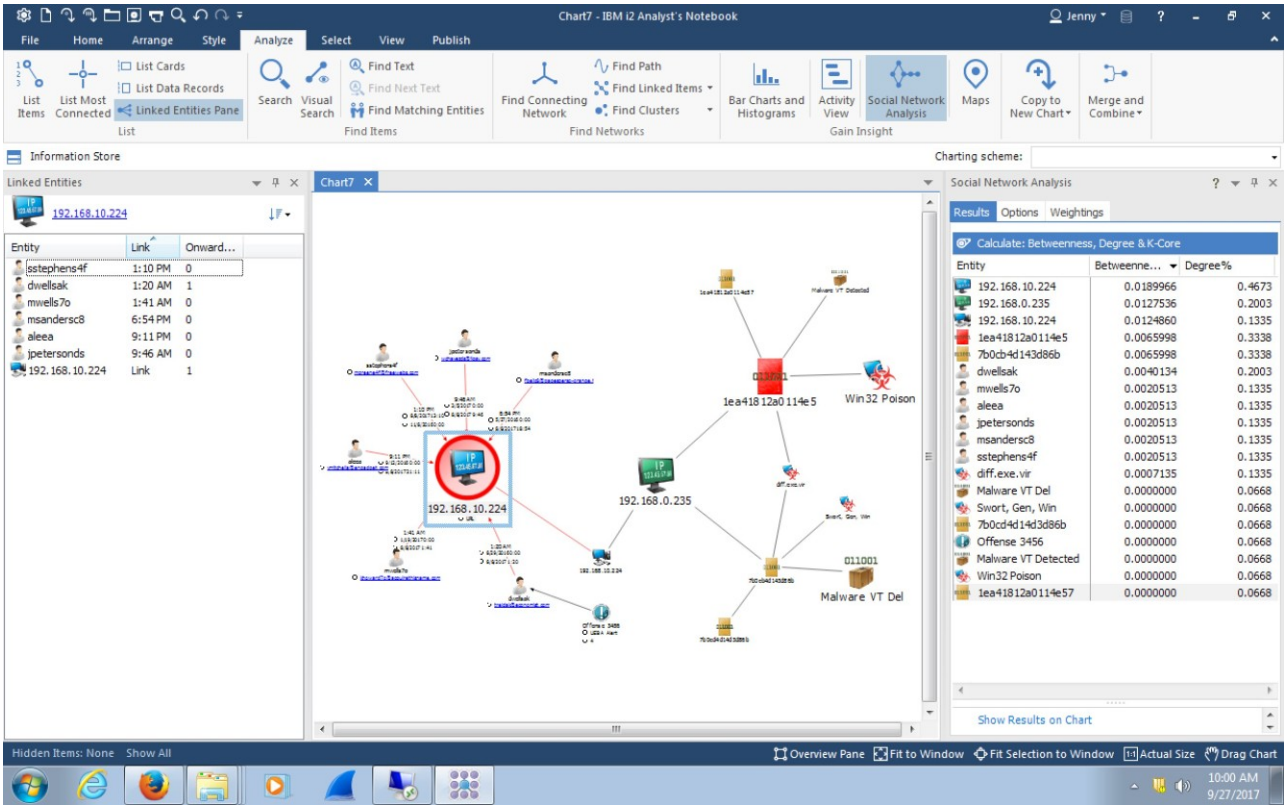


*图 8：*自动化社交网络分析工具可帮助分析师揭示更深层次的联系。

在所有上述案例中，网络威胁猎人都可以使用 IBM 的认知功能，发现不同数据集中隐藏的模式和关系。通过将 QRadar 数据直接推送到 i2 Analyst 的 Notebook 中，IBM i2 QRadar® Offensive Investigator 应用整合了 i2、QRadar 和 IBM Watson™ for Cybersecurity 的元素，利用 i2 中内置的可视化、分析和数学建模功能以及非结构化数据，找到异常安全事件之间的关联。通过主动关联看似无关的事件和详细信息，威胁猎人可以全面了解威胁和威胁攻击者，并且可能发现攻击者正在发起恶意攻击的迹象，并在攻击完成之前将其拦截。

行动指导：需要铭记的关键成功因素

为了成功实施网络分析程序，组织必须采用风险管理战略。情报的真正用途始终是为决策者提供决策依据。决策者应该从战略的角度，利用网络分析生成的网络情报，制定有关网络威胁的风险缓解决策。以下概念是关键功能，它们能够支持网络分析程序。通过构建分析平台（例如 i2 EIA），您可以启用成熟的安全情报程序的以下关键组件。

高级威胁是真实存在的且越来越多

从上面的许多例子可以看出，现在，来自高级攻击者（例如国家级攻击者）的网络威胁已成为私营领域无可回避的现实。更重要的是，信息公开后，顶级攻击者所采取的先进策略往往被技能不高的犯罪集团用于牟利。随着漏洞的不断涌现，需要更多资源（例如社交工程学）的攻击将变得更加普遍。组织必须知道，任何人都可能成为高级攻击的目标，他们不能只是达到应对常见恶意软件的最低安全标准。关键在于，将资源转移至结构化的情报分析，以便更好地应对隐秘的高级威胁。

不要忘记简单的措施

与普遍的看法相反，简单的安全控制措施是阻止大多数威胁攻击者的最有效方法。恶意网络攻击者的资源有限，就像其他任何人一样，他们会将资产投入投资回报率最高的领域。攻击者可能会略过拥有适当安全控制措施的组织，瞄准更容易得手的目标。“The Center for Internet Security’s (CIS) Top 20 Critical Security Controls”文档介绍了五个能帮助您快速制胜的控制措施。这些控制措施可以显著降低风险，应对常见的攻击，且您无需对组织环境实施重大的策略或技术变更。这些简单的风险缓解技术包括补丁、标准系统配置和有限的管理控制技术。通过使用网络分析平台，您可以强制实施安全框架的每个组件。

安全是一个“生态系统”

一些执法人员提到“用网络打击网络”这一说法。组织必须在安全团队、网络分析师和外部威胁研究人员之间建立连接流程。对抗顶级攻击者的主要缓解策略之一是参加各个行业的情报共享小组。较复杂的攻击者倾向于使用类似的策略，他们的攻击目标或攻击活动有共同的特征。通过微调代码或策略，恶意攻击者可以偷偷绕过大多数检测技术。通过访问情报共享网络，“对一个组织的攻击就是对所有组织的攻击”。信息安全专家可以共享发生攻击时的所见，分发威胁指标，并将其与网络分析平台内部的漏洞进行比较。

找出攻击发生的原因很重要

在出现对组织发起的高级攻击时，您需要了解入侵成功的原因，这一点很关键。出现攻击的原因可能有很多，包括策略控制失败，缺乏技术检测功能等。找出根本原因的最佳方法是跟踪决策树，回溯原始攻击以了解导致问题的潜在人为决策。未来，分析平台可以检测这些指标，防止将来出现使用类似技术发起的攻击。

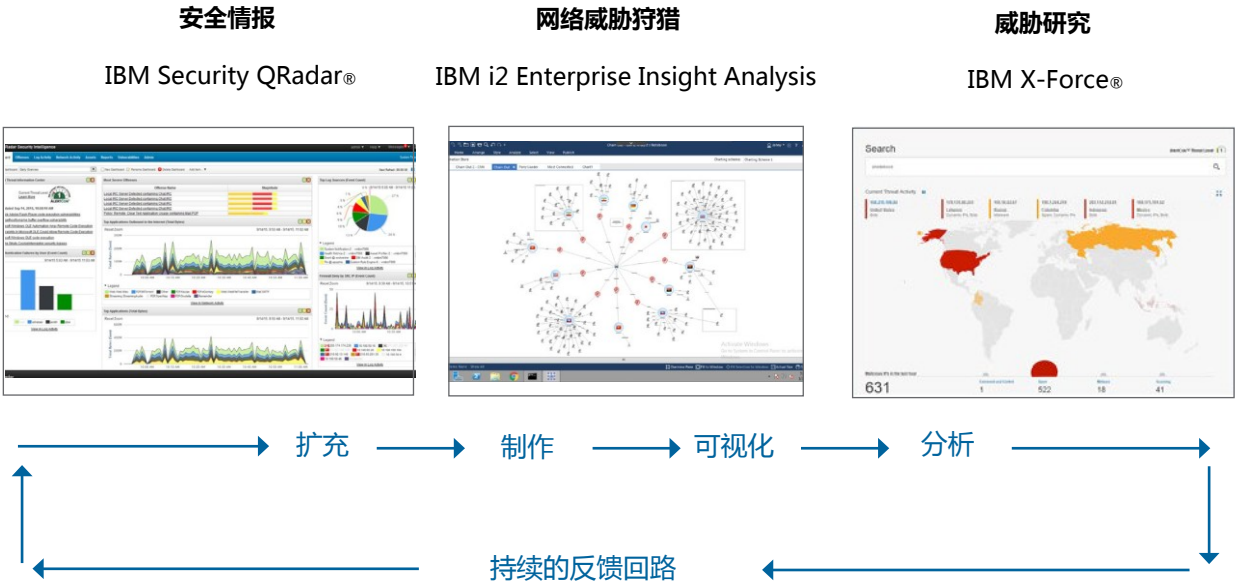


图 9：IBM i2 Enterprise Insight Analysis 网络威胁分析解决方案在与安全情报和外部研究相集成时能够发挥最大作用。

下一步会怎样？

有关更多信息，敬请访问：www.ibm.com/cyber-threat-hunting

IBM Corporation
Software Group
Route 100
Somers, NY 10589

美国印刷
2017 年 10 月

1 2017 年 Verizon 数据泄露报告

2 www.threattracksecurity.com/resources/white-papers/exploit-kits-cybercrimes-growth-industry.aspx

3 https://securityintelligence.com/commercial-malware-makes-a-comeback- in-2016

4 IBM X-Force 2017 年威胁情报指数（2017 年 3 月），第 21 页

5 www.av-test.org/en/statistics/malware

6 X-Force 报告第 10 页

7 www.news.europawire.eu/data-security-confidence-index-companies-under- invest-in-technology-that-adequately-protects-their-business-654321456890/ eu-press-release/2017/07/13

8 www.business2community.com/cybersecurity/booming-job-market-3-reasons-cybersecurity-jobs-will-reign-supreme-01434850#GQ6QQW3CgXv7sDAc.97

9 www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202

10 www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

11 www.bankinfosecurity.com/report-swift-hacked-by-bangladesh-bank-attackers-a-9061

12 www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know

请回收利用

YTW03437-CNZH-04