10 大网络安全热点趋势

从产品互操作性、第三方漏洞、数据丢失到预防到关键基础设施的威胁，以下是行业领导者在今年 Black Hat 大会上关注的重点网络安全发展趋势。

1. 对新一代 SOAR 的需求

FireEye 首席执行官 Kevin Mandia 在谈起第一代安全运营、分析和报告（SOAR）产品时，认为它们用于检测和汇总大量安全信息的工作时，已经完全没有什么问题，应当准备进入下一个阶段，寻求如何满足客户对于更高互操作性的需求。

大型跨国组织和公司使用的产品相对较多，环境也较为复杂，因此它们对于产品间高互操作性的需求格外强烈，期望能够尽可能缩短问题出现到完成修复的过程。下一代 SOAR 产品需要针对互操作性进行特别优化，这样才能在面对各种纷杂的情况时，具备一定的自动化操作能力。

Mandia 表示，未来的安全运营中心应当通过网络安全中心提供更多的一键功能，将现在很多仍要人来参与的事情变成自动化操作，并增强不同供应商产品间的互操作性，加速网络安全问题的解决进程。

2. 人工智能在行为分析领域的应用

Sophos 首席研究科学家 Chester Wisniewski 表示，人工智能可用于处理输入的数据，降低产生的误报，使得数据更易管理从而助力用户和实体行为分析（UEBA）市场。

由于 UEBA 市场所使用的数据量非常庞大，使得从业人员很难编写出能够通吃所有内容的算法。因此，组织和企业会收到大量误报，这意味着即使检测到异常，安全运维人员也不太可能采取行动，只会把问题标注来，交给安全运营中心（SOC）研究。

得益于人工智能技术的进步，现在误报可以通过工具自动处理和消减，可以预见组织和企业最终会全面开放自动化工具来处理所有告警的情况，同时还能为安全专家腾出时间，用于研究最重要的安全问题。

3. 数据安全已成为核心问题

Digital Guardian 首席执行官 Ken Levine 认为，企业在网络安全方面的投入远远不够，在防范潜在威胁和新型攻击媒介方面已经捉襟见肘。企业网络中的入侵者难以被发现和定位，只有当入侵者能够从公司网络获取数据时，才会引企业的重视。

为了防止企业网络中的数据被窃取，企业必须明确信息的密级基于用户对于这些信息的访问权限。这种方法使得企业能够围绕数据本身构建安全壁垒，而不仅限于在公司网络中排查恶意活动。

4. 基础设施已成为恶意活动的目标

根据 SonicWall 首席执行官 Bill Conner 透露的信息，通过僵尸网络或路由器对基础设施发起的攻击越来越多，目标涵盖能源和公用事业系统，甚至互联网基础设施也在内。

在美国，大约 95％的基础设施都是私有化的，这就导致解决方案提供商在进行修复时需要与公用事业提供商和政府监管机构合作。从实际发生的案例可以看到，一些基础设施的技术提供方或者供应商，如实验室或学术机构，也会成为恶意活动的目标，黑客试着从最基础的地方寻找最薄弱的环节。

随着越来越多的新芯片投入使用，以及针对 PDF 或 Microsoft Office 的恶意软件不断泛滥，基础设施面临着越来越多的安全问题。 Bill 表示，新的攻击工具更善于伪装，使得基础设施供应商在检测和预防网络安全问题是更加费劲。

5. 第三方漏洞应必须被重视起来

按照 BitSight 总裁兼首席执行官 Tom Turner 的说法，来自第三方的风险，或者是有业务往来的组织所存在的风险已成为公司决策者们必须要重点关注和讨论的一个热门议题。去年的 WannaCry 勒索软件攻击是第三方风险进入大家视野的里程碑。举个例子，如果港口遭到恶意活动攻击而导致上游航运公司的船只无法出港，导致的损失将十分巨大。

WannaCry 的爆发让企业高层意识到控制第三方风险对于保持公司业务的正常运行和股票价格的稳定至关重要。

6. 分散的员工队伍带来的数据安全隐患

来自 Micro Focus 安全和信息管理与政府产品部门总经理 John Delk 表示，随着企业用工形式的变化，很多企业的员工队伍越来越分散，这样一来员工们就会通过各种方式将敏感数据带出公司。

如果让员工使用各种各样的接入点来登录公司内网以访问所需的数据，这又会带来非常复杂的安全基础架构设计挑战。John 建议先从简单的方法开始，例如多步身份验证，然后逐步完善用于分布式数据和分散劳动力环境（如数据丢失防护）的网络安全。

7. 化被动为主动

Cybereason 联合创始人兼首席执行官 Lior Div 表示，企业正在从使用被动的网络安全（包括新一代反病毒软件）维护手段转向主动寻找和规避威胁的方式。围绕着企业打造安全的城墙，只能在短期内提供保护，别忘了特洛伊木马的故事。在过去六年了，企业在网络安全领域的投入每年都在增加，但新型攻击的发生率以及企业遭遇黑客入侵的情况并没有发生实质性的好转。

这个时候，企业必须要转变思维采取更积极主动的行动，如引入第三方进行模拟黑客渗透的安全测试，主动化解网络安全隐患。

8. 数据保护业务崛起

Digital Guardian 全球渠道部副总裁 Marcus Brown 告诉媒体说，数据保护业务已经成为网络安全市场中增长最快的领域之一，这是因为云计算技术的发展为企业提供了更多整合数据和资源的途径。

除了偶尔发生的 DDoS 攻击之外，几乎所有在全球发生的漏洞和黑客事件都是对于数据的窃取。数据泄露后造成的严重后果向各个行业敲响了警钟，越来越多的企业将数据保护提升到很高的优先级，由首席执行官、首席财务官和董事会成员全权负责。

司法部门也在加强对数据保护的法规建设，例如欧盟的 GDPR 法规和加利福尼亚的数据隐私法案。鉴于数据泄露对公司的声誉、股价、知识产权保护和竞争优势造成的危害，企业应当加大对数据保护的投入。

9. 传播恶意软件的媒介持续多样化

Mimecast 渠道项目副总裁 Julian Martin 表示，新时代下传播恶意软件的媒介越来越多样化，如电子邮件、网络、即时通讯和社交媒体，这意味着解决方案提供商必须为客户提供全面的产品，应对来自多种渠道的安全挑战。

黑客总是攻击一点，而不会对整个企业或组织的网络安全体系大打大闹。他们将通过电子邮件、社交媒体对用户进行分析，通过某个切入点找到入侵企业的薄弱环节。因此，解决方案提供商应该从传统的思维模式中跳出来，围绕着企业员工的日常生活和工作提供全面的整套安全解决方案。

10. 设备触网越多，风险越高

RSA Security 的美洲区域副总裁 Faraz Siraj 表示，最近几年，物联网的高速发展为企业和消费者提供了将汽车、家用电器接入互联网的各种解决方案。

这些新兴的网络接入方式为用户带来了更多现代化的新奇体验，但随之而来的网络安全威胁也不容小觑，想象一下让黑客非法接入设备所在的网络，随意控制汽车等，这多么可怕。在研发新技术时，设计师最初的关注点总是如何又快又好用，对于安全往往会疏忽一些。Faraz 表示，设计师们应当去寻找既不会减慢整个系统开发进度又可兼顾网络安全的开发方式。