什么是主动网络安全

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	What Is Proactive Cybersecurity?		
原文作者	迈克·埃尔根（Mike Elgan）	**原文发布日期**	2021 年 10 月 20 日
作者简介	迈克·埃尔根是一位专栏作家。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/what-is-proactive-cybersecurity/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	积极和被动的网络安全方法，要求企业寻找“攻击信标”（IoC，表明已经发生攻击和网络犯罪的迹象）。但是，主动网络安全方法寻找的是“行为信标”，即用户采取的行动的集合。主动网络安全是一种整体性的安全方法。它不仅涉及具体的方法和实践，还涉及一种进攻性网络安全的心态。毕竟，企业为什么要等到被攻击才进行响应呢？他们可以立即采取行动以防止攻击发生。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

什么是主动网络安全

迈克·埃尔根

2021 年 10 月 20 日

大多数企业采取“积极的”（active）网络安全方法；他们时刻做好准备，一旦发生攻击，他们就能迅速采取措施。有的企业则采取“被动的”（reactive）网络安全方法，在攻击完成后才能采取行动。“主动的”（proactive）网络安全策略是指在攻击发生之前就采取行动，这是一种良好的网络安全准备就绪状态。

接下来，我们将分析主动网络安全的策略、工具和实践。

主动 vs 被动和积极审查

安全工具、协议、策略和实践的创建和审查，通常是一个“设置然后忘记”的过程。然而，世界是在不断变化的。主动的安全方法是不断审查这些内容，着眼于新出现的威胁、新工具和新想法，并及时更新所有内容。网络安全意识培训也是如此——企业应至少每季度审查员工网络安全意识培训“课程”。

道德黑客

与其坐等被攻击，不如自己发起攻击。经过认证的道德黑客可以使用与恶意攻击者相同的方法和工具，来探查企业的防御系统，寻找其中的漏洞和防御弱点。通过红队/蓝队演习、渗透测试和其他模拟，企业员工可以从网络攻击中学习经验教训，但不会真得受到攻击。

自动化智能工具

企业可以使用自动化工具，深入了解其网络上发生的事情并自动做出响应。主动安全方法意味着，企业已经确定并加载了尽可能多的修复方法。智能软件可以全天候地搜索攻击和异常行为，时刻准备在发生某些事情时进行隔离和修复。这更像是一种进攻而非防御。

零信任策略

通过使用“积极的”安全方法，企业可以在系统检测到入侵者时切断攻击路径。但是通过“主动的”安全方法，企业可以在攻击者到达之前就切断攻击路径。

零信任策略力求验证试图访问企业资源的每个设备、应用和用户的身份，并为其授权。

对于攻击者来说，即使能够窃取密码，他们也无法入侵企业网络，这是因为他们没有获得授权的设备。许多远程办公人员都在使用家庭办公室，他们在物理安全未知的空间和质量未知的网络中使用办公设备；因此，这种通过零信任模型主动锁门的方法更为重要。

零信任模型是动态的，能够持续、主动地进行监控、学习和适应。

端点监控中的主动与被动

主动安全意味着主动进行端点监控。随着物联网设备、云基础设施和远程工作设备的普及，主动安全比以往任何时候都更加重要。企业应实现端点监控的自动化，以最大限度地提高每台设备的安全性。

行为信标（IoB）

积极和被动的网络安全方法，要求企业寻找“攻击信标”（IoC，表明已经发生攻击和网络犯罪的迹象）。但是，主动网络安全方法寻找的是“行为信标”，即用户采取的行动的集合。

举例来说，通过寻找 IoB，安全团队可能会发现有人将业务数据下载到外部存储设备，或将代码上传到未知的云服务。IoB 可能是权限的更改，也可能是个人台式 PC 的网络从内部 Wi-Fi 切换到移动宽带热点。通过收集成百上千个这样的信息，安全团队可以从行为的角度更清晰地了解企业的薄弱环节。基于 IoB，安全团队可以以最小的中断进行行为更改。例如，企业可以提前让使用 U 盘的用户找到更安全的方法，然后主动禁用 U 盘连接。在员工出现危险行为时，安全团队还可以隔离特定设备或端点，并对其进行密切监控。

主动与被动是一种心态

主动网络安全是一种整体性的安全方法。它不仅涉及具体的方法和实践，还涉及一种进攻性网络安全的心态。

毕竟，企业为什么要等到被攻击才进行响应呢？他们可以立即采取行动以防止攻击发生。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com