SKYBOX SECURITY

Cyberworld

解决方案简介

基于风险的漏洞优先级排序和修复

Skybox 漏洞和威胁管理

企业的数字化转型在加速，已将大多数IT工作负载迁移至云端。但随之带来的挑战是如何应对日益增长的攻击面。如今，恶意行为者的攻击手段越来越复杂，而且新的漏洞在陆续增加。安全性已上升为董事会级别的关注点。

安全团队现有的安全计划不能再依赖于简单的优先级划分工作和大量的补丁管理，而是要识别并修复对业务构成最大风险的漏洞。

有效的漏洞管理应通过多因素来确定优先级排序，该优先级以暴露风险分析为中心，考虑混合网络环境，并包括所有潜在攻击路径的模拟。至关重要的是：准确地说明暴露情况，并将修复措施集中于消除最大的风险。

业务挑战

安全团队正在应对不断扩大的技能差距、越来越分散的网络、日益增长的攻击面、陆续增加的工作负载、可视化和修复差距、无效且不完整的扫描结果。

随着新漏洞数量不断增加，原有的传统修复措施对那些风险最高的问题已不适用，优先级排序和修复会变得非常困难。

大多数企业都拥有传统老旧的基础设施、日益增加的不同类型的产品和设备、以及一长串无人管理的漏洞，这些漏洞却增加了网络风险。据统计，2020年75%的攻击所利用的漏洞至少存在了两年。[1] 此外，高级和多阶段的攻击数量正在增加。全球勒索软件攻击数量也在不断增加，预计每 11 秒就会发生一起事件。[2]

注1：
网络安全漏洞统计：https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/

注2：
Cybersecurity Ventures 报告：
https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

简介

解决方案

Skybox漏洞和威胁管理解决方案提供了一种集中式、自动化、与多种供应商产品和服务兼容的方法，可跨混合和多云基础设施实现全生命周期漏洞管理。

商业挑战

+ 新漏洞数量不断增加
+ 新技术和新设备数量激增，可视化效果变差
+ 资源有限

商业效益

+ 提高漏洞评估的准确性
+ 确定优先级并采取最佳修复方案
+ 降低整体网络风险
+ 投资保护

商业价值

+ 缩短修复时间
+ 降低资源成本
+ 减少网络威胁暴露
+ 加速实现价值
+ 使用[漏洞管控云版]减轻运营负担

基于当下的形势，企业安全团队需要凭借更精准的评估、优先级划分和修复能力，来进一步消除被用作潜在攻击的特定漏洞。如果不能及时地、准确地识别高风险漏洞，就算修复工作最终消除了大量漏洞，也无法降低商业风险。

漏洞管控云版是一种可扩展的现代化解决方案，用于管理混合环境中的漏洞暴露和风险。从而享受投资保护，加速实现价值，减轻运营负担。

传统方法存在缺口

传统方法是没有考虑影响漏洞风险的所有因素的。这使得安全团队将资源浪费在恶意行为者可能永远找不到或不知道如何利用漏洞的问题上。由于每周都会陆续发布大量漏洞，单单依靠电子表格和手动分析来获得见解，这会徒劳无功。此外，扫描和修复方法往往忽略了漏洞管理工作流程的关键要素，尤其在如何设置修复优先级方面。如果扫描器无法提供对网络拓扑的全面了解，就无法识别实际的暴露情况。

迄今为止，通过 CVSS 评分和可利用性级别对漏洞进行优先级排序是最常见的技术。然而，这种方法并没有解决以下问题：

+ 这项资产对企业而言有多重要?
+ 由于该漏洞已暴露给内部或外部的恶意行为者，是否构成了迫在眉睫的威胁?
+ 假设漏洞暴露，恶意行为者利用它并通过网络横向移动的速度有多快?
+ 在收到漏洞存在警报或发生违规事件时，能否快速关闭关键的、暴露的资产，使其免受威胁?

基于风险的漏洞优先级

为了可以智能地确定漏洞修复的优先级，Skybox采用了一种基于对暴露和商业风险分析的方法。

除了通过基于风险的漏洞优先级划分，帮助客户将修复工作扩展到补丁管理。Skybox还提供修复选项的优先级列表，尽可能以最有效和最高效的方式消除暴露风险。

可以从多个角度（包括资产重要性、野外威胁活动、暴露于威胁来源）查看漏洞，Skybox使您能够在最要紧的地方采取行动，主动降低攻击风险。

基于风险的漏洞优先级排序方法，可以通过以下方式得到增强：

+ 根据 CVSS 严重性、资产重要性、可利用性和暴露程度等因素，自动地进行漏洞分析。
+ 将简单明了的、可追踪的风险评分分配给漏洞、资产和组。
+ 优先修复对业务构成最大风险的漏洞。

全生命周期漏洞和威胁管理

Skybox漏洞和威胁管理解决方案提供了一种集中式、自动化、与多种供应商产品和服务兼容的方法，可跨混合和多云基础设施实现全生命周期漏洞管理。Skybox威胁和上下文感知分析引擎聚合了多个来源的广泛数据，包括扫描器、安全和网络基础设施、各种配置数据库和不可扫描资产。

Skybox不仅提供这些数据和信息，还根据资产优先级、可利用性和暴露分析，提供风险评分和漏洞修复优先级。安全团队使用Skybox，可以自动映射和可视化其攻击面，确定最佳修复选项，从而持续地减少网络安全风险。

Skybox 漏洞和威胁管理

智能的全生命周期漏洞和威胁管理方法

可视化

+ 所有扫描数据*
+ 补丁和EDR数据*
+ CMDB数据*
+ 安全控制*
+ 网络数据*
+ OT漏洞*
+ 威胁情报

*** 指 Skybox 对传统漏洞管理计划的补充**

漏洞发现

主动扫描是漏洞发现的重要组成部分，但可能会在“不可扫描”的网络区域和设备、快速变化的云环境中留下盲点。准确的漏洞优先级分析始于良好的数据可视化。 Skybox 威胁和上下文感知分析引擎聚合了 150 多种来源的数据，包括扫描器、安全和网络基础设施、配置数据库、不可扫描资产。这些广泛的数据都是网络模型的基础，能使该模型精确地、有针对性地解决最高风险。

Skybox漏洞发现方法整合了来自第三方扫描器、APP和Web扫描器、OT平台等结果，增强了数据可视化。Skybox还使用被动评估技术来填补盲点，该技术可以检测禁区网络范围和设备中的漏洞。

此外，Skybox还会获取有关漏洞利用特征的信息——野外活跃的漏洞利用、样本漏洞利用代码、打包在分布式犯罪软件中的利用。Skybox的威胁情报是持续从公共和私有来源获取的，由Skybox研究实验室进行分析和审查，并通过Skybox情报源传送到Skybox产品。

优先级

+ **业务影响***
+ **暴露情况***
+ 可利用性
+ 严重性
+ **分布密度***
+ 存在时间
+ **位置***

*** 指 Skybox 对传统漏洞管理计划的补充**

漏洞优先级

Skybox根据资产重要性、CVSS评分、可利用性和暴露分析，确定漏洞的优先级排序。漏洞情报来自已知的漏洞信息数据库，这有助于生成准确的风险评分，其中包括以下详细信息：

+ 操作系统、版本、其他已安装的应用程序等会影响漏洞可利用性的触发条件。
+ 对机密性、完整性和可用性 (CIA) 值的利用效应。
+ 对漏洞进行研究，例如 NVD 列表、安全供应商公告等。
+ 漏洞变化的历史记录，它与严重性、利用、可用补丁等相关。
+ 修复和缓解解决方案。
+ 来自 NVD、IBM X-Force、扫描供应商等严重性评级和通用漏洞评分系统 (CVSS) 分数。

漏洞上下文

通过对存在漏洞的环境进行建模，安全团队能了解暴露于威胁来源的漏洞。这是基于风险的漏洞优先级排序的关键组成部分。

Skybox构建了一个网络模型，该模型是混合环境的动态表现，包括企业网络、私有云、公有云和OT。它了解环境中的所有设备、漏洞和配置，可用于运行评估和攻击模拟。

该网络模型能让安全团队分析网络、云、IT、OT和安全配置，以主动获取完整的上下文并了解攻击面。Skybox跨安全、云和网络技术聚合数据集，包括：

+ 网络拓扑（路由器、负载均衡器、交换机）
+ 安全控制（防火墙、IPS、VPN）
+ 资产（服务器、工作站、网络——传统 IT、多云和 OT 环境）

暴露分析和攻击模拟

漏洞分析最关键的步骤是确定漏洞在网络中的暴露程度。当不同的数据存储库（例如补丁和资产管理系统、配置数据、威胁情报源和网络安全设备）汇集在一起，并对数据进行标准化和建模以推断漏洞的存在时，就可以进行暴露分析。此暴露分析能精确地指出内部和外部恶意行为者可以访问的资产。通过了解暴露情况，将资源投入到恶意行为者能够访问的漏洞上，确定缓解选项以切断攻击路径。

Skybox通过模拟网络模型的攻击来确定漏洞的暴露程度。通过网络模型，企业可以提高攻击模拟功能，以纳入更深入的攻击上下文和见解，探索所有可能的攻击路径，查看攻击者可能接触的设备，并确定防止违规的最佳行动方案。

自动模拟从所有威胁源（入口点）运行，并评估所有网络路径，以确定是否可以到达易受攻击的资产。此类漏洞会被标记为直接暴露。

直接暴露的资产在二次模拟中用于代表受损的资产（就像多步骤攻击中的情况一样）。在这些二次模拟中发现的漏洞会被标记为间接暴露。

修复

计划：

+ 评估补丁选项
+ **评估非补丁选项***
+ **缓解建议***

任务：

+ 生成工单
+ ITSM工作流程
+ **提供上下文***
+ 提供SLA
+ 与运营团队沟通

*** 指 Skybox 对传统漏洞管理计划的补充**

智能和自动化修复措施

Skybox提供了最有效的解决漏洞或受影响最严重的资产的选项。通过Skybox新的解决方案视图，团队可以立即看到解决方案，最大程度地提高资产风险评分。

Skybox提出对防火墙规则的更改、IPS签名的更新和其他替代方案，以选择最适合您独特环境和变更管理流程的修复方法。所以，客户可以受益于灵活性的提高、平均修复时间的显著缩短、以及最重要的是业务风险的降低。

Skybox还与第三方工单管理系统集成，实行闭环修复责任制。根据上述要素，对漏洞进行优先级排序后，企业可以快速修复最高优先级的漏洞。

区别于传统的漏洞管理程序，Skybox是通过基于对网络基础设施的深入见解，以及对通信路径、攻击路径、潜在爆炸半径和恶意行为者复杂程度的了解，提供上下文修复选项。这能使企业安全团队采用替代方法来处理关键任务或无法长时间离线的系统。

使用Skybox智能修复措施，客户能受益于：

+ 实现自动化修复，快速消除漏洞。
+ 从集成的数据中获得见解，加速决策。
+ 模拟网络漏洞与攻击，制定主动防御。
+ 关联修复流程，打破安全堆栈中的孤岛。

审计与监督

当您采用成熟的漏洞管理程序时，会持续验证和完善数据聚合流程，构建和维护企业网络模型。另外，准确的报告和对长期趋势的了解将提高可预测性，这有助于预防攻击。

使用Skybox，执行报告简单易行，完全可定制，能查看与业务最相关的见解，让决策更明智。跨职能团队可以引用单一事实来源来获取所需的见解。

Skybox提供随时间变化的趋势报告，并强调可能对风险评分产生负面影响的下降趋势，例如：

+ 扫描频率降低。
+ 扫描的机器数量减少。
+ 高危漏洞或暴露漏洞增多。

关于 Skybox Security

全球500多家注重网络安全的大型企业依靠Skybox获得所需的见解和保障，以降低风险。Skybox应对动态变化攻击面的能力始终处于业界领先地位，Skybox安全态势管理平台提供完整的可视化、分析和自动化功能，可快速映射、确定优先级并修复漏洞。