|  |  |  |  |
| --- | --- | --- | --- |
| 安全巡检word报告-模板 | | | |
| ■ 文档编号 |  | ■ 密级 | 商业机密 |
| ■ 版本编号 | V1.0 | ■ 日期 | 2024-10-15 |

|  |  |  |  |
| --- | --- | --- | --- |
| ■ 版本变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
| 2024-10-15 | V1.0 | 文档创建 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| ■ 适用性声明 |
| 本文档为产品正式部署后输出的安全评估分析报告，适用于相关技术人员对发现的安全风险进行修复时参考。 |

[一 概述 1](#_Toc188395328)

[1.1 评估人员 1](#_Toc188395329)

[1.2 评估时间 1](#_Toc188395330)

[1.3 巡检范围 1](#_Toc188395331)

[1.4 巡检内容 2](#_Toc188395332)

[二 巡检结果摘要 3](#_Toc188395333)

[2.1 Agent管理 3](#_Toc188395334)

[2.1.1 Agent安装 3](#_Toc188395335)

[2.1.2 操作系统类型分布 3](#_Toc188395336)

[2.1.3 Agent业务组覆盖情况 3](#_Toc188395337)

[2.1.4功能插件开启率 4](#_Toc188395338)

[2.1.5事件源开启率 4](#_Toc188395339)

[2.1.6安全建议 4](#_Toc188395340)

[2.2 入侵检测 6](#_Toc188395341)

[2.2.1 历史入侵告警事件统计 6](#_Toc188395342)

[2.2.2 历史入侵告警危险等级分布 6](#_Toc188395343)

[2.2.3 历史入侵告警处理情况 6](#_Toc188395344)

[2.2.4 真实入侵攻击业务组分布 6](#_Toc188395345)

[2.2.5 真实入侵攻击告警危险等级分布 6](#_Toc188395346)

[2.2.6 真实入侵攻击告警类型分布 7](#_Toc188395347)

[2.3.7攻击事件详情列表 7](#_Toc188395348)

[2.3.8 安全建议 7](#_Toc188395349)

[2.3 风险发现 8](#_Toc188395350)

[2.3.1 补丁风险等级分布 8](#_Toc188395351)

[2.3.2 高危补丁风险 8](#_Toc188395352)

[2.3.3 漏洞风险等级分布 8](#_Toc188395353)

[2.3.4 高危漏洞风险 8](#_Toc188395354)

[2.3.5 弱密码风险 8](#_Toc188395355)

[2.3.6 安全建议 9](#_Toc188395356)

[三 总结 10](#_Toc188395357)

1. 概述

安全巡检主要是通过对评估范围内的主机进行安全扫描，对被评估对象进行一系列的安全分析与探测，以发现目标存在的安全隐患并确实的告知修复建议，是安全体系搭建工作中修复安全风险，提升安全等级的重要工作之一。

通过安全巡检工作，可以详细的了解当前服务器中存在的潜在安全隐患，有效发现操作系统和应用软件存在的安全风险、漏洞和威胁，同时梳理安全修复工作，以危害程度高低划分修复工作，阶段性的提供有效、明确的修复方案，为进一步通过技术手段降低或解决发现的问题提供了参考依据和方法。

在本次安全巡检项目中，通过对结果的分析，对目前存在的安全风险以危害程度进行划分，统计并展示各项巡检结果，供相关人员参考。

* 1. 评估人员

**表1.1.1 评估人员**

|  |  |  |
| --- | --- | --- |
| 姓名 | 所属部门 | 邮箱 |
|  |  |  |

* 1. 评估时间

**表1.2.1 评估时间**

|  |  |
| --- | --- |
| 评估时间 | |
| 起始时间 |  |
| 结束时间 |  |

* 1. 巡检范围

本次安全巡检范围，如表1.3.1所示：

**表1.3.1 巡检范围**

* 1. 巡检内容

本次安全巡检内容包括下内容：

* 获取巡检范围内主机的Agent管理信息，包含Agent安装及在线情况，插件安装情况等信息；
* 评估巡检范围内的系统、服务和应用的风险信息，包含漏洞检测、安全补丁以及弱密码等风险项；
* 评估巡检范围内主机的被入侵情况，包含暴力破解、异常登录以及web后门等入侵事件；
* 评估巡检范围内主机的合规性是否达到合规基线标准。

1. 巡检结果摘要

本次安全巡检主要对Agent管理、风险发现、入侵诊断等3方面进行安全巡检，摘要如表2.1.1所示。

**表2.1.1 巡检结果摘要**

|  |  |
| --- | --- |
| 项名 | 说明 |
| 版本 | 5.0.5 |
| 主机总数 |  |
| 发现风险项总数 |  |
| 历史入侵告警总数 |  |

* 1. Agent管理

2.1.1 Agent安装

Agent覆盖率和在线情况能体现您系统安全防护的建设情况和防护状态。本次巡检主机中Agent的在线状态分布如图2.1.1所示。

**图2.1.1 Agent状态情况**

2.1.2 操作系统类型分布

已经安装Agent的主机中，操作系统分布情况如图2.1.2所示：

**图2.1.2 操作系统覆盖情况**

2.1.3 主机业务组覆盖情况

本次巡检中主机业务组覆盖情况如图2.1.3所示：

**图2.1.3 Agent业务组覆盖情况**

2.1.4功能插件开启率

平台的部分功能需要依赖功能插件的开启，例如对用户执行的命令进行审计需要安装Bash插件，未安装Bash插件的主机将无法获取其执行的危险命令信息，存在一定风险；本次巡检范围内Agent插件安装的情况如表2.1.1所示。

**表2.1.1 插件安装列表**

2.1.5事件源开启率

**表2.1.2 事件源开启列表**

2.1.6安全建议

1. 需要关注巡检范围期间的离线Agent，确认Agent离线原因并及时上线以保障该主机安全。若确定离线的Agent不再使用，建议停用该Agent以释放license授权数量；
2. 需要关注巡检范围期间的停用Agent，Agent处于停用状态时，Agent功能均为不可用状态，包括资产清点与入侵检测功能，Agent只保持与服务端的心跳消息与命令下发通道；
3. 需要关注巡检范围内的降级Agent，Agent降级意味着系统内的系统整体负载持续偏高，存在一定风险；
4. 需要关注插件和事件源的开启情况，入侵部分功能需要依赖插件或者事件源的开启，未安装插件的主机部分功能无法正常使用，存在一定风险。检测能力与影响说明详见表2.1.2所示：

**表2.1.2 检测能力影响说明**

|  |  |
| --- | --- |
| 检测能力 | 影响说明 |
|  |  |
| 进程注入检测 | 必须开启audit事件源、ebpf事件源、驱动事件源中的任意一种事件源，否则无法进行进程注入检测。 |
| 恶意模块加载检测 | Linux设备必须开启ebpf事件源或驱动事件源，Windows设备必须安装sysmon插件或者开启驱动事件源，否则无法进行恶意模块加载检测。 |
| DNS域名检测增强 | Linux设备必须安装dns插件或开启ebpf事件源，否则无法监控DNS域名解析。 |
| 勒索防护 | 必须开启驱动，否则无法进行勒索防护。 |
| 恶意驱动防护 | Linux设备必须开启驱动事件源，否则无法进行检测。 |
| 程序劫持检测 | Windows设备必须安装sysmon插件或开启驱动事件源，否则无法进行检测。 |
| 可疑权限变更 | Linux设备必须开启audit事件源、ebpf事件源、驱动事件源中的任意一种事件源，否则无法进行检测 |
| BypassUAC检测 | Windows设备必须安装sysmon插件或开启驱动事件源，否则无法进行检测。 |
| 容器行为模型 | 已购买“容器安全高级版”产品的客户，使用容器行为模型功能时，必须开启ebpf事件源或驱动事件源，否则只能监控文件写和进程启动行为。 |

* 1. 入侵检测

入侵检测实时监控在主机上发生的入侵事件，并根据设定的监控规则进行告警。

2.2.1 历史入侵告警事件统计

各类历史入侵告警类型的分布情况如图2.2.1所示。

**图2.2.1 历史入侵告警类型分布**

2.2.2 历史入侵告警危险等级分布

历史入侵告警的危险等级分布情况如图2.2.2所示。

**图2.2.2 历史入侵告警危险等级分布**

2.2.3 历史入侵告警处理情况

各类历史入侵告警的处理情况如图2.2.3 所示。

**图2.2.3 历史入侵告警危险等级分布**

2.2.4 真实入侵攻击业务组分布

在历史入侵告警事件中，告警状态为已确认或处理中的告警表示一次真实的入侵攻击告警，需要重点关注。本次巡检过程中，受到真实入侵攻击的主机业务组分布如图2.2.4所示。

**图2.2.4真实攻击主机业务组分布**

2.2.5 真实入侵攻击告警危险等级分布

在历史入侵告警事件中，告警状态为已确认或处理中的告警表示一次真实的入侵攻击告警，需要重点关注。本次巡检过程中，受到真实入侵攻击的危险等级分布如图2.2.5所示。

**图2.2.6真实攻击告警危险等级分布**

2.2.6 真实入侵攻击告警类型分布

在历史入侵告警事件中，告警状态为已确认或处理中的告警表示一次真实的入侵攻击告警，需要重点关注。本次巡检过程中，受到真实入侵攻击的告警分布如图2.2.6所示。

**图2.2.6真实攻击告警类型分布**

2.3.7攻击事件详情列表

在历史入侵告警事件中，告警状态为已确认的告警表示一次真实的入侵攻击告警，需要重点关注。本次巡检过程中发现的真实攻击事件详情如表2.3.1所示：

**表2.3.1 攻击事件详细列表Top20**

2.3.8 安全建议

1. 本次巡检发现历史告警中存在被真实攻击的情况，建议尽快处理真实告警；
2. 对于还存在的未查清的攻击事件建议进一步分析。
   1. 风险发现

风险发现主要从漏洞、补丁、弱密码等角度发现当前威胁主机安全的风险项，并统计已修复的风险项。

2.3.1 补丁风险等级分布

本次巡检过程中，发现补丁风险等级分布情况如图2.3.1所示：

**图2.3.1补丁风险等级分布**

2.3.2 高危补丁风险

高危补丁指的是风险等级为危急、高危的补丁。本次巡检过程中，发现高危补丁风险项详情TOP20如表2.3.1所示：

**表2.3.1高危补丁风险详情TOP20**

2.3.3 漏洞风险等级分布

本次巡检过程中，发现补丁风险等级分布情况如图2.3.2所示：

**图2.3.2漏洞风险等级分布**

2.3.4 高危漏洞风险

高危漏洞指的是风险等级为危急和高危的漏洞。本次巡检过程中，发现高危漏洞风险项按照影响的主机数从高到低展示TOP20的漏洞详细信息，如表2.3.2所示：

**表2.3.2高危漏洞风险项TOP20**

2.3.5 弱密码风险

巡检过程中发现存在弱密码的应用详细列表如表2.3.3所示：

**表2.3.3弱密码应用列表**

2.3.6 安全建议

1. 通过安全巡检发现部分主机存在高危风险问题，所以建议优先修复POC验证检测出来的漏洞；建议在不影响业务的情况下尽快修复；
2. 经检测发现主机上存在弱口令问题。弱口令账号非常容易被攻破，一旦入侵者发现弱口令账号，可以在较短时间内攻破该账号，登录到系统，对系统产生较大危害。建议在不影响业务正常运转的情况下加强密码复杂度。
3. 总结
4. 经过本次巡检，确定目前Agent均正常运行，如后续可以考虑接入更多的主机，可联系我司工作人员进行license的扩容；
5. 当前规则日期为2024-01-01，相对较久，建议及时更新规则到最新，增加检测率和减少相关误报率；
6. License到期时间为2024-10-31，与当前日期距离较近，为了保障业务的正常防护能力，请尽快联系我司工作人员重新进行license授权的更新。