

安世加

EISS-2020

企业信息安全峰会 之深圳站

2020.9.10





面向现代攻击面的漏洞风险管理

许晓晨

Tenable技术经理
xxu@tenable.com

基础安全工作仍面临考验

- 去年的攻防演练中，多家单位因攻击面评估不到位等低级错误而被攻破

例1：某单位被物理攻击，通过营业厅的网络接入到内网，再使用已知漏洞拿下护网目标

例2：某单位员工被钓鱼攻击，邮件链接下载恶意代码，后作为跳板进一步拿下内网目标

- 绝大部分情况下，攻击者无需耗费0-day

未修复的漏洞

弱口令

未保护的敏感信息

老旧的资产

未知且不必要的暴露

过度的程序权限

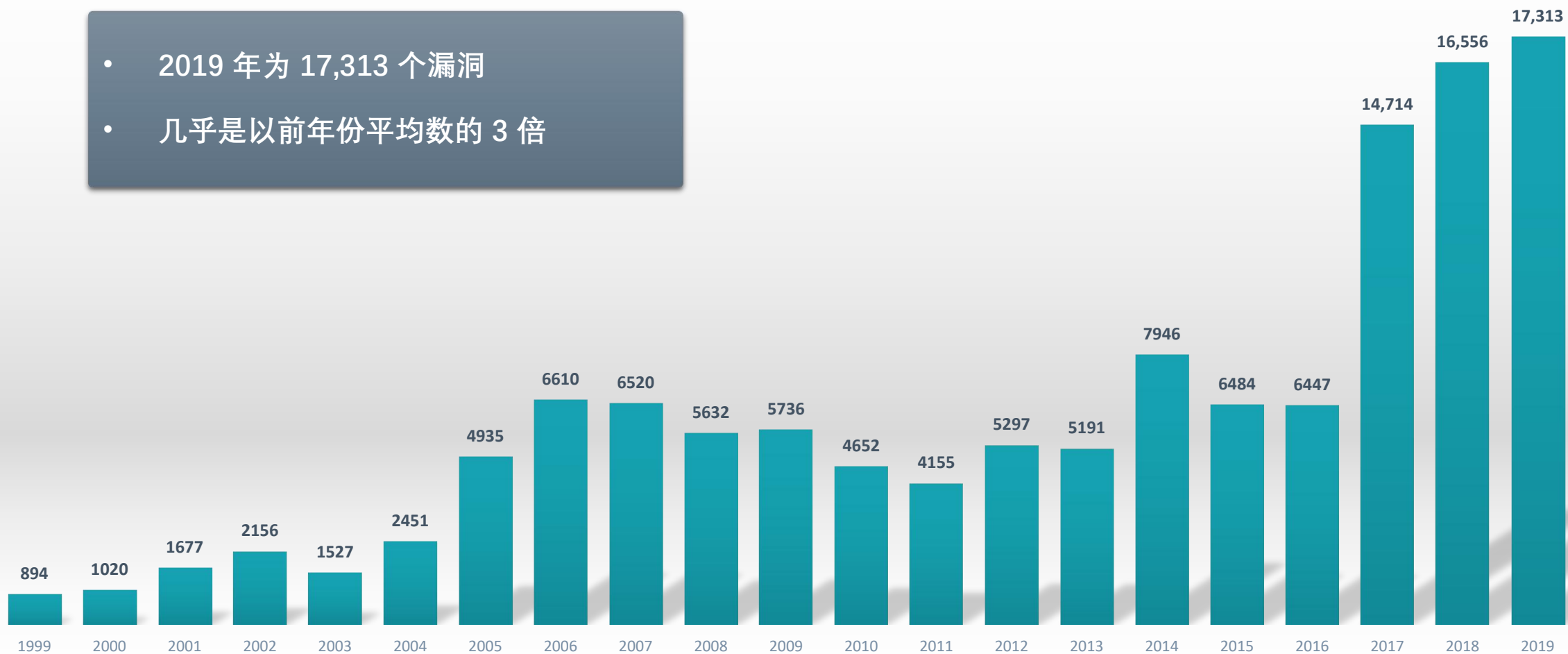
#Low-hanging Fruits

(HW高风险攻击手法)



新漏洞数量持续增长

- 2019 年为 17,313 个漏洞
- 几乎是以前年份平均数的 3 倍



来源：漏洞情报报告，Tenable Research

攻击面的扩大带来了更多的安全隐患



工业 OT



ICS/SCADA



容器



云



企业 IoT



Web App



桌面



笔记本



移动



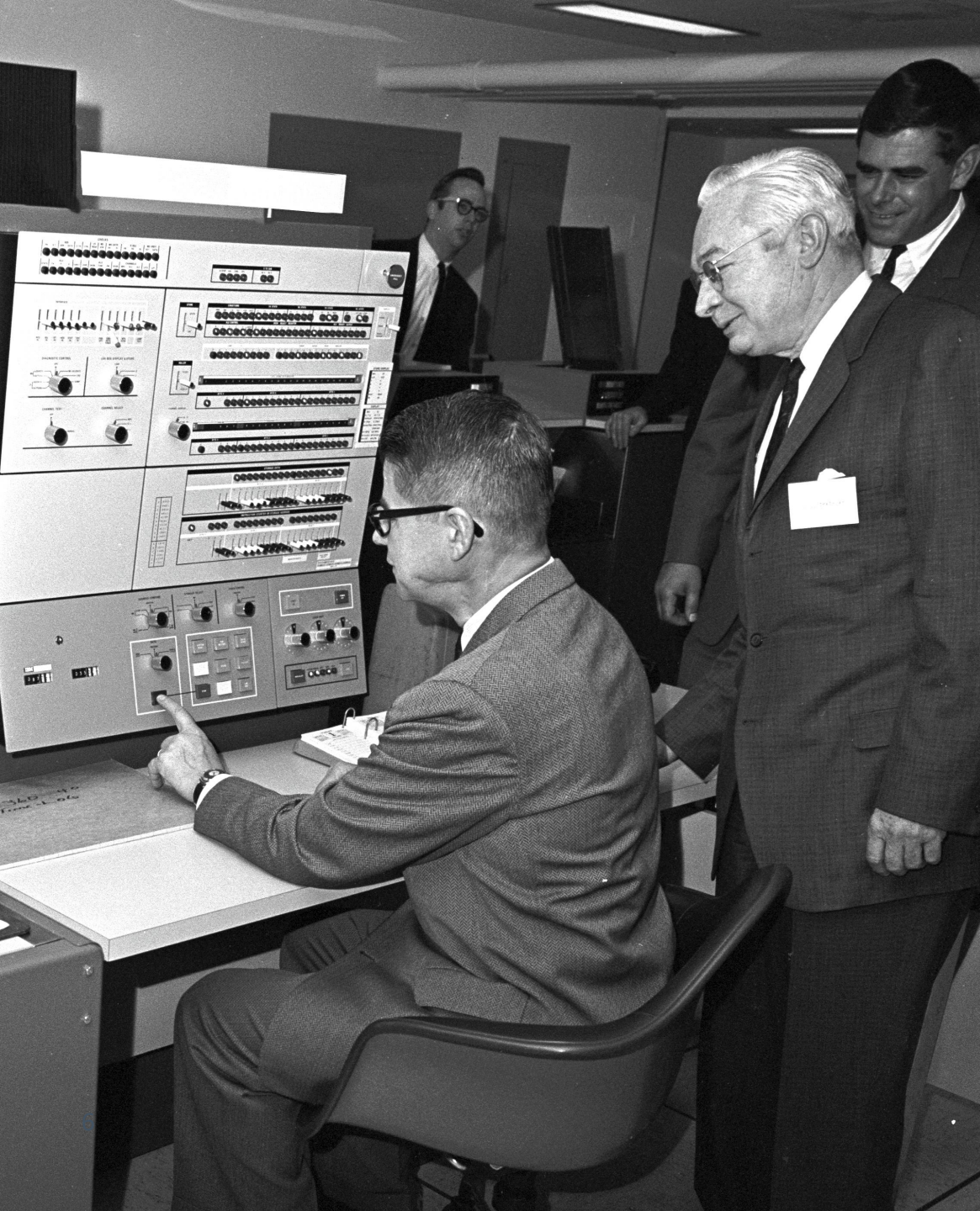
虚拟机



网络



服务器



传统漏洞管理 难以与时俱进



有限的
可见性



低效的
优先级分析



糟糕的
沟通方式

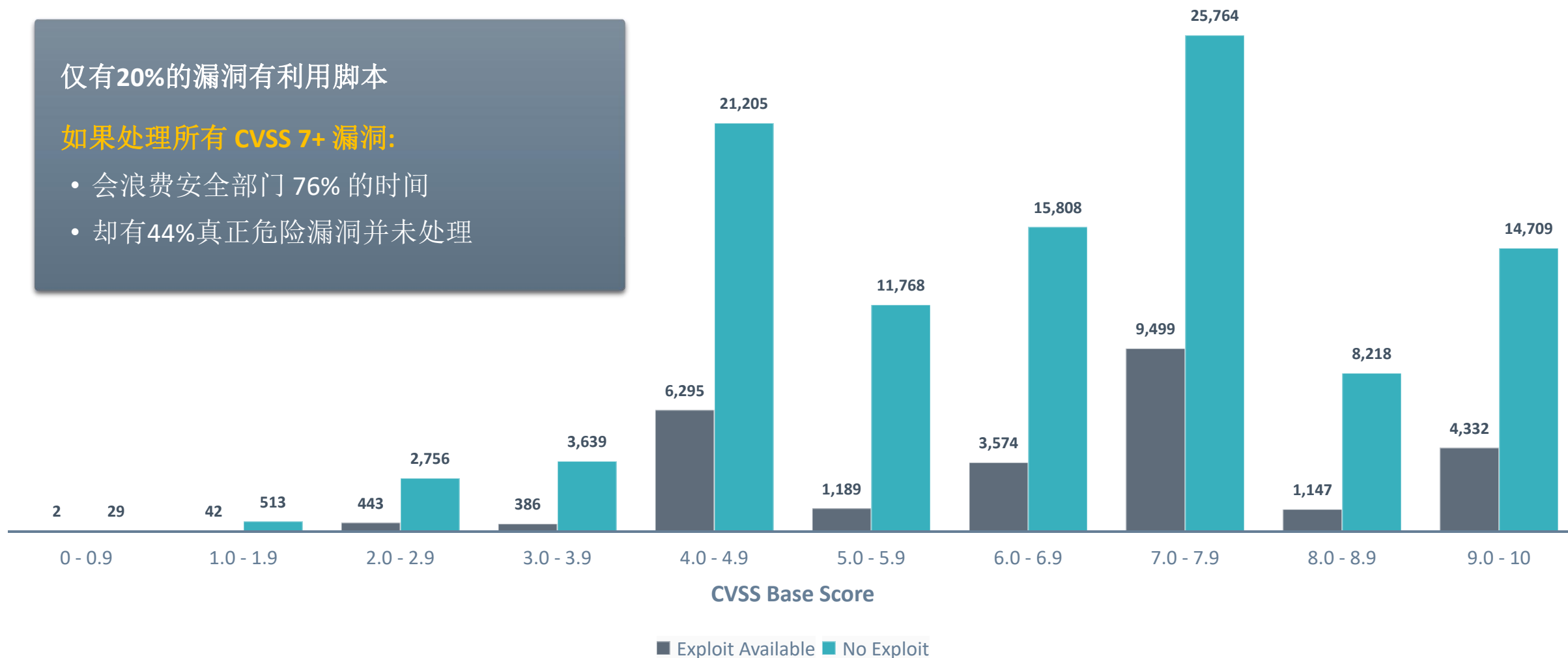
传统工具无法处理现代攻击面

CVSS 是一个较差的风险指标

仅有20%的漏洞有利用脚本

如果处理所有 CVSS 7+ 漏洞:

- 会浪费安全部门 76% 的时间
- 却有44%真正危险漏洞并未处理



问题是

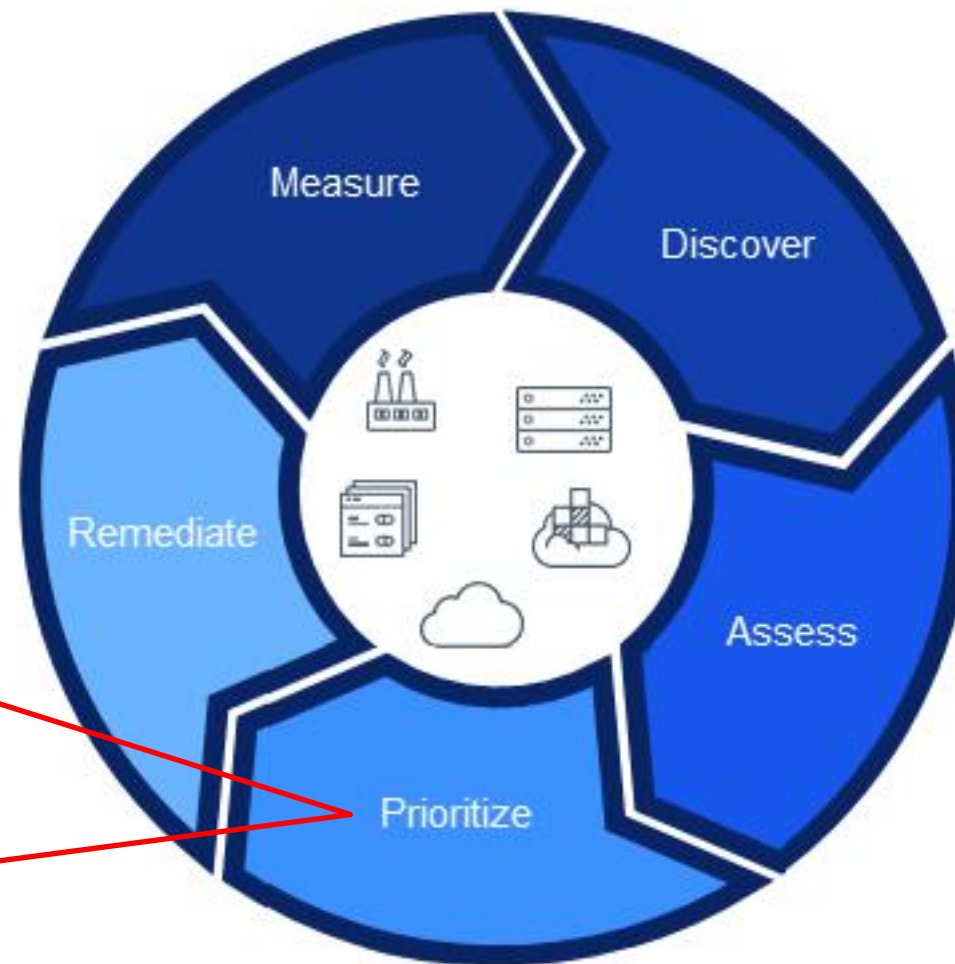
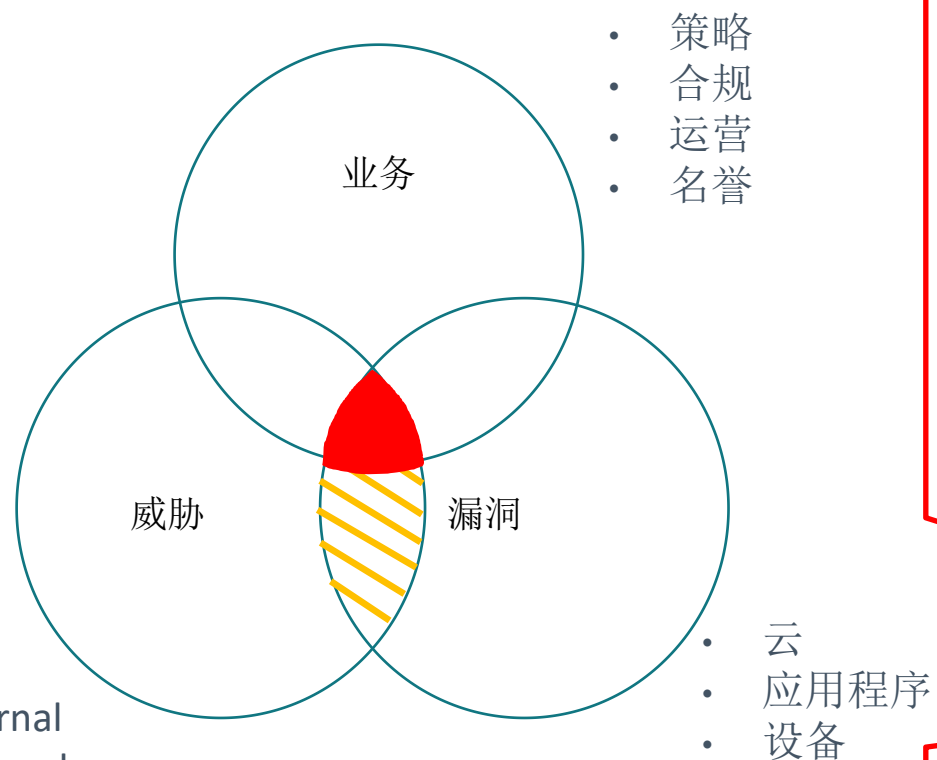
无论公司规模大小，
都可能永远没有足够的资源来补救攻击
面上的每个漏洞。



关注在
最重要的
事情上

利用基于风险的漏洞管理进行优先级分析

假如今天只有一个漏洞需要修复，你会选哪个？



优先关注最重要的

VPR

VULNERABILITY PRIORITY RATING

利用机器学习和威胁情报来预测攻击中可能针对的漏洞

+

ACR

ASSET CRITICALITY RATING

利用机器学习根据业务价值和重要性指标预测资产的优先级

海底可以捞针

研究洞察

对超过109,000个漏洞插件进行大数据分析，以识别漏洞导致的实际风险和理论风险

威胁情报

深入洞察哪些漏洞会遭到有针对性或投机主机攻击者频繁利用

漏洞评级

与缺陷相关的重要性、可利用性和攻击向量

基于风险的 漏洞管理

97%

减少对攻击面有同等影响的待修复漏洞

VPR实际功效——更少修复但同效

False: 计算 VPR 后的 28 天内未发现 IoC（攻陷指标）

Ture: 计算 VPR 后的 28 天内发现 IoC


With IoC	False	True	With IoC	False	True
VPR			CVSSv3		
1-Low	26889	1	1-Low	937	5
2-Medium	28398	63	2-Medium	22252	49
3-High	1259	263	3-High	24892	278
4-Critical	289	102	4-Critical	8760	98

公众号原文链接:

【什么是VPR，它与CVSS有何不同】https://mp.weixin.qq.com/s/JVNfmRX2Qg9Z_Z-EyR0ivg

某金融企业案例背景





演进目标

- 每日全网交叉扫描
- 关键补丁日级运营与响应

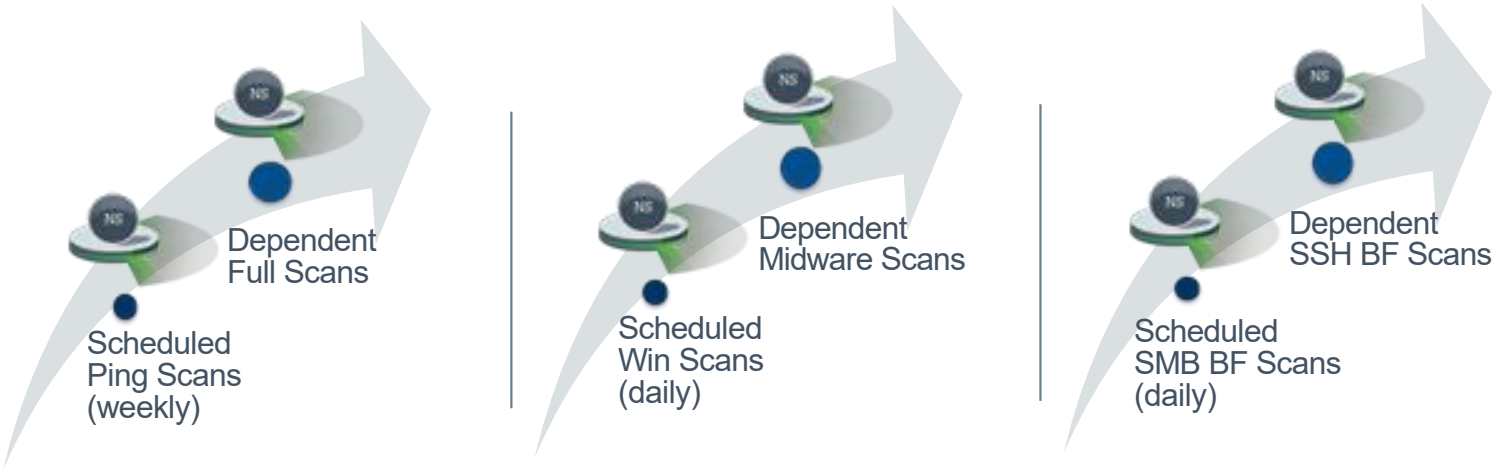
面临的问题...

- 扫描覆盖盲区
 - Agent装机率黑洞
 - 无法接受的扫描耗时
 - 防火墙压力
- 关键补丁抉择
- 自动化程度不足
 - 1 vs 40



自动化工程分解

- 分布式网络扫描器规划
- 漏洞风险优先排序
- 扫描策略的平衡与抉择
 - 特定端口/插件 vs. 全端口/插件
 - 扫描任务 - 分解、分解、再分解
 - 场景、场景、场景

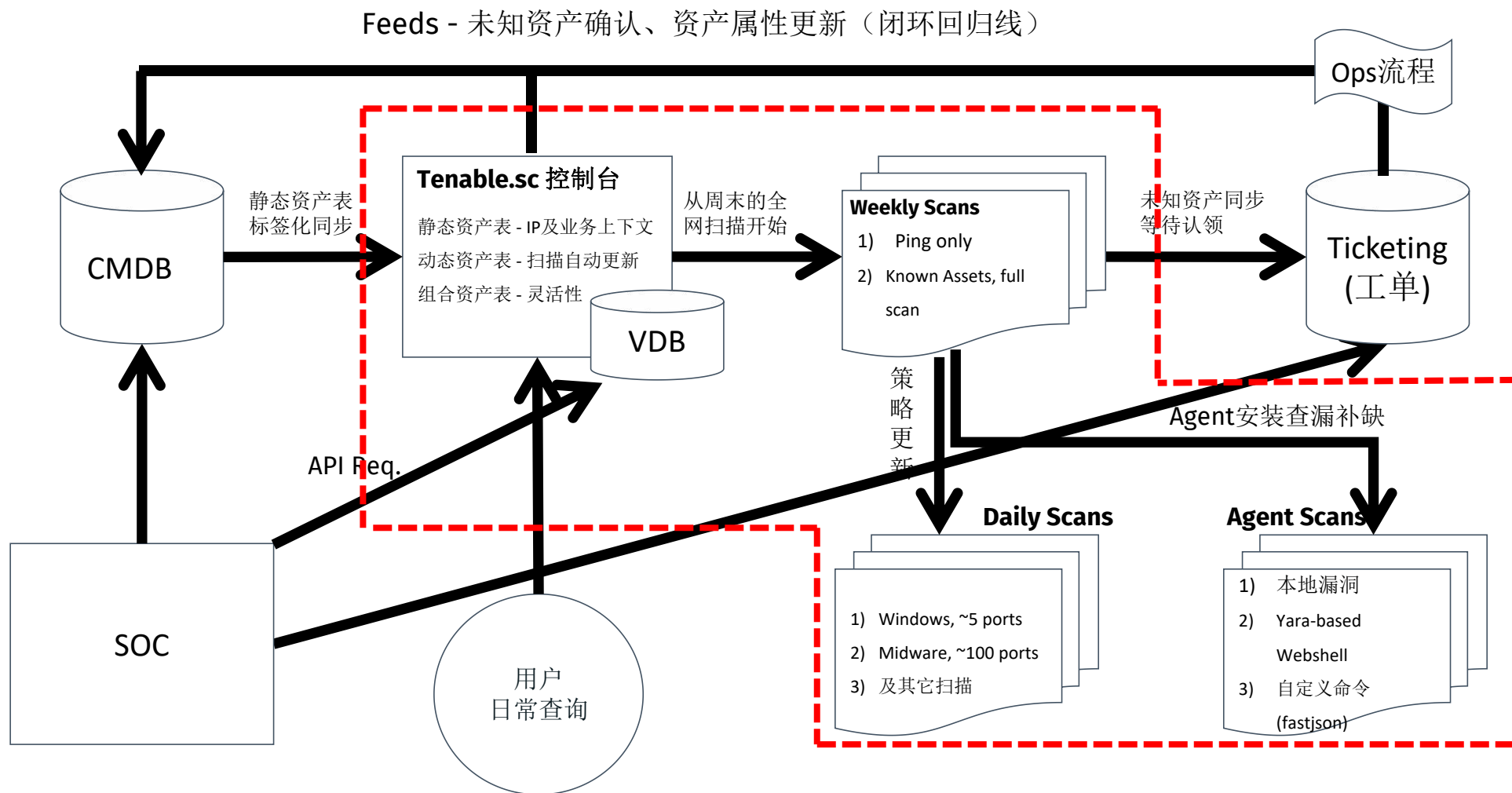


全自动化扫描任务一览表 (部分)

- Set it and Forget it!
 - 以动态资产表(标签)代替IP
 - 定时 vs. 嵌套
 - 业务保护措施

Scan Jobs	Scan Types	Scan Policies	Start Time	Stop Time	Targets
Daily-Scans	Agent	Internal-Scan-Malware-w/o-yara	Every Sun - Thu, Sat	6 hrs	Windows Assets, Middleware Assets, DMZ Hosts
Daily-Yara		Internal-Scan-Yara	Every Sun - Thu, Sat	2.5 hrs	DMZ Hosts
Weekly-Scans		Internal-Scan-Malware	Every Fri 6.30pm	12 hrs	All hosts in Prod
Weekly-Ping-Scans	Remote	Fast_Ping-Scan	Weekly on Fri	Unlimited	XYZ-All
Weekly-Scans		Weekly-Scan	Dependent to Weekly-Ping-Scans	Unlimited	XYZ-All-2d
Daily-Win_Patch-Scans		Win_Patch-Remote-Scan	Every Sun - Thu, Sat	2 hrs	XYZ-Windows
Daily-Middleware-Scans		Middleware-Remote-Scan	Dependent to Daily-Win_Patch-Scans	6 hrs	XYZ-DMZ-14d, XYZ-Core-Middleware-14d
Weak-Passwd-SMB-Scans		Weak-Passwd-SMB-Scan	On Demand	Unlimited	On Demand
Weak-Passwd-SSH-Scans		Weak-Passwd-SSH-Scan	Dependent to Weak-Passwd-SMB-Scans	Unlimited	On Demand
XYZ-互联网扫描每周五		Weekly-External-Scan	Every Fri	Unlimited	XYZ-互联网
XYZ-AWS扫描每周五	Remote	Weekly-External-Scan	Every Fri	Unlimited	XYZ-AWS
XYZ_YYB-互联网IP扫描每周五		Weekly-External-Scan	Every Fri	Unlimited	XYZ-YYB

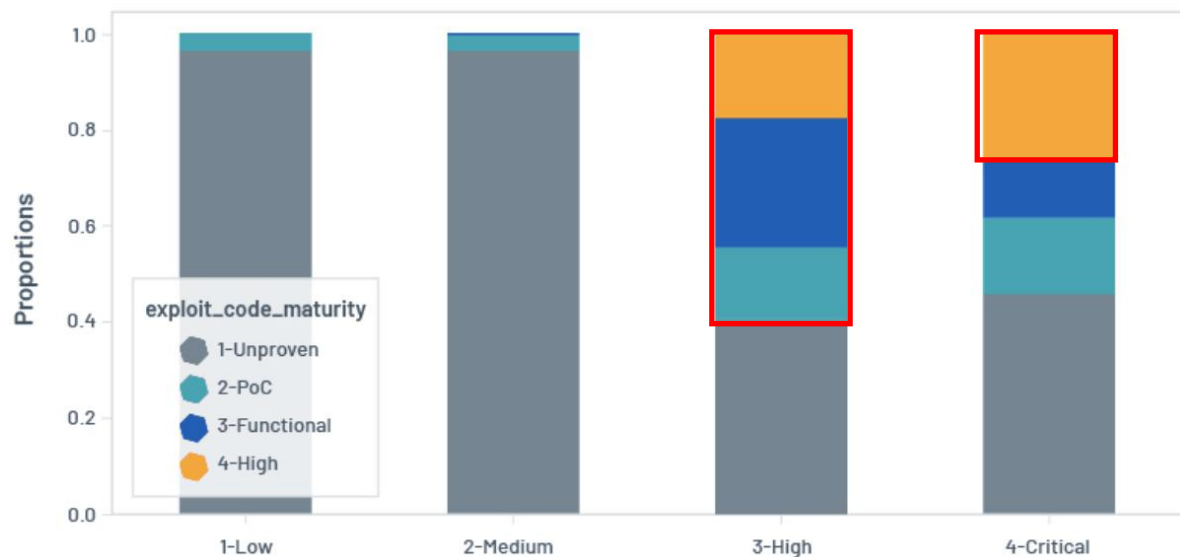
漏洞风险运维 - 自动化基准



折衷的攻击面防护思路

并没有标准方法，适合的才是有效的

Proportion of Exploit Code Maturity by VPR Criticality



- 优先关注面向外联资产
- 优先修复易受攻击中间件、windows关键补丁
- 考虑利用代码成熟度和利用方式
- 本地漏洞(AV:L)主要靠教育和约束
- Linux内核漏洞主要靠加固和防护

HW期间相关技术措施小结

› 自动化攻击面检测(优先顺序↓)

- ①外网侧主机资产及漏洞扫描
- ②互联网Web应用漏洞扫描 (DAST)
- ③内部主机资产及漏洞扫描

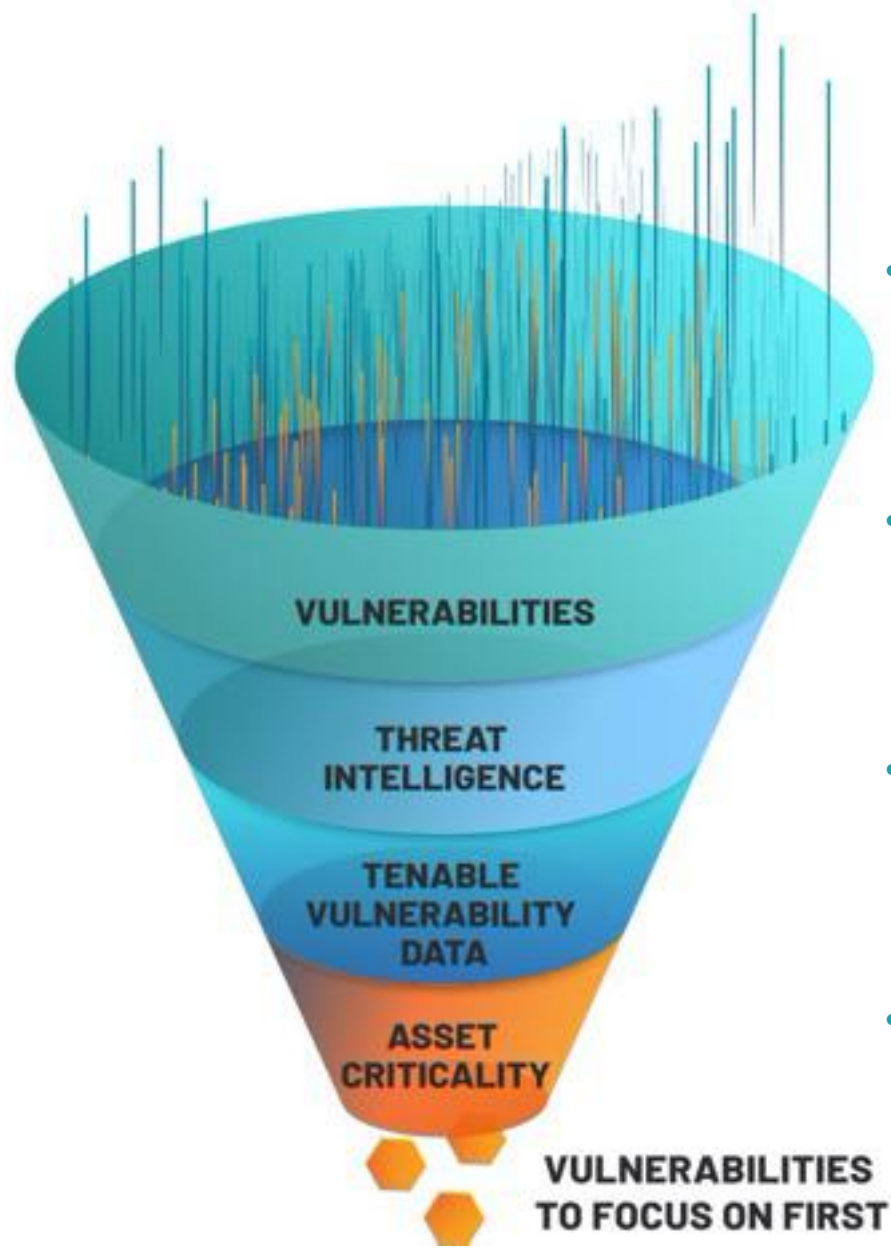
› 主机漏洞优先修复原则

- ①Windows知名老洞 + 当月安全补丁(Patch Tuesday)
- ②脆弱中间件及服务 (相关列表见下链接)
 - https://github.com/shawntns/tsc_asset_query/blob/master/tsc_asset.yml
- ③参考Tenable VPR漏洞情报 (交叉覆盖①、②)
 - 优先规则: **2010年后发布, VPR情报存在利用代码, 网络利用, 无需用户交互或认证, 利用复杂度低**
 - 优先级1: **VPR分数9+**
 - 优先级2: **VPR分数7.0-8.9**

› 其它风险检测

- 弱口令
- 安全配置加固
 - 注重本地敏感信息、程序权限等
- 恶意软件及Webshell (加分项)

基于风险的漏洞管理使您能够首先关注最重要的事情



- 关注**整个**攻击面
- 理解风险**环境**中的漏洞
- **停止**在不会带来风险的漏洞上浪费时间
- 用最少的努力减少最大的业务**风险**



GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

“到2025年，70%采用传统、批量漏洞管理方案的中型都会遭受到已知漏洞攻击。”**

** Gartner, Midsize Enterprises Must Prioritize to Achieve Effective Vulnerability Management, Patrick Long, Mitchell Schneider, November 26, 2019.

“到2022年，若使用基于风险的漏洞管理方式，企业遭受的数据泄露将减少80%”*

* Gartner, A Guide to Choosing a Vulnerability Assessment Solution, Prateek Bhajanka, Mitchell Schneider, Craig Lawson, April 3, 2019.



欢迎关注

微信公众号：“Tenable安全”

- 联系我们
- 体验与评估我们的解决方案
 - 资产发现及漏洞合规管理平台（Tenable.SC）
 - 持续网络安全监控平台（Tenable.CV）
 - 工控安全平台（Tenable.OT）
 - 下一代安全风险可视平台（Tenable.io）
 - 公有云安全
 - 容器安全
 - Web应用安全



安世加 专注于安全行业，通过互联网平台、线下沙龙、培训、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。



官方网站: <https://www.anshijia.net.cn>

微信公众号: asjeiss