漏洞管理技术演变的夏商周

绿盟科技

NSFOCUS

目 录

NSFOCUS

“新基建”下的漏洞管理挑战

NSFOCUS

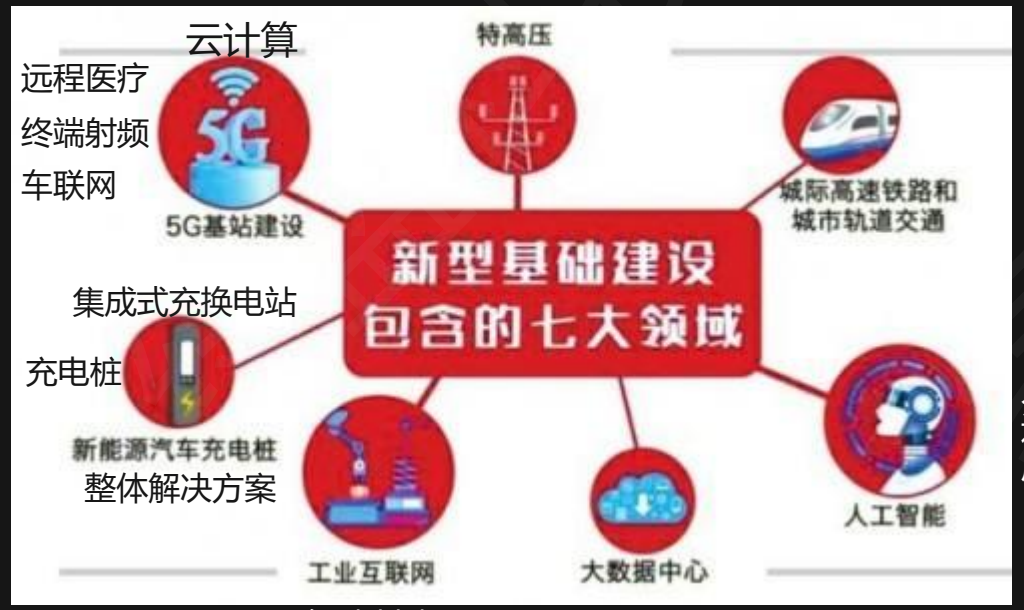
“新基建”下的安全挑战

产业数字化升级

直流交流
断路器
电站监控
高压组合

牵引供电
工程机械

机车车体
轨道铁轨



人脸识别
通用平台
底层硬件

智造制造
互联平台

云计算厂商
运维服务
制冷设备
IT设备

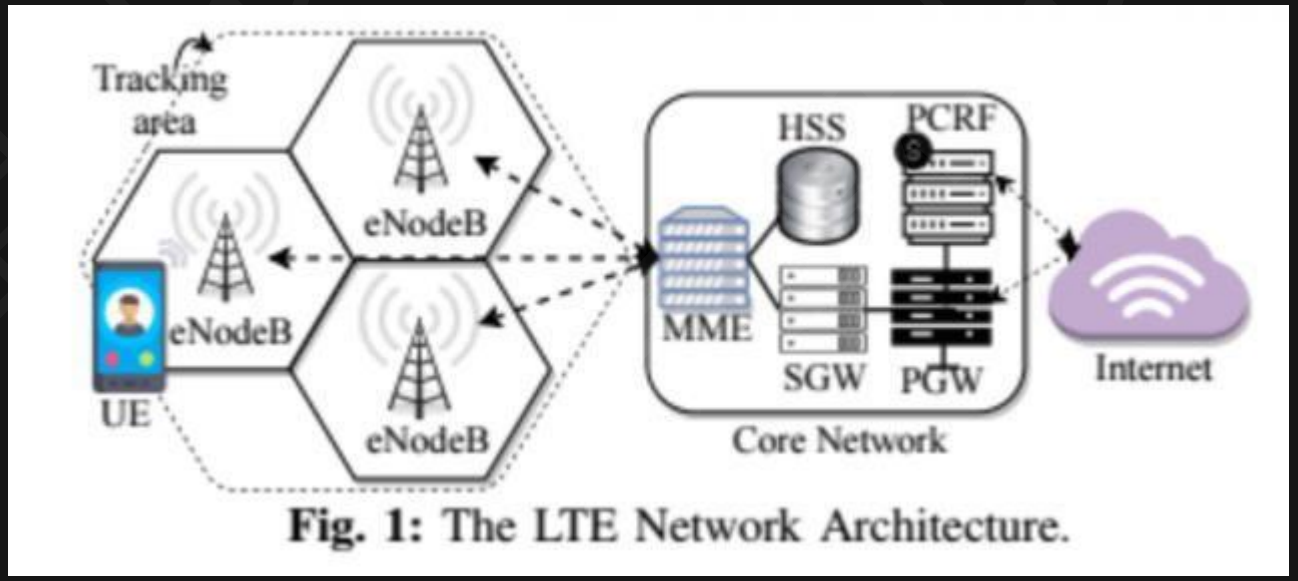


Fig. 1: The LTE Network Architecture.

Torpedo 漏洞

漏洞披露数量仍成上升趋势

- 漏洞数量和影响范围仍然大幅增加，2019年高危零日漏洞占比增长，漏洞消控工作依然任重道远；
- 物联网相关漏洞利用持续高涨，服务器类类漏洞中WEB相关漏洞最受关注；
- 漏洞披露速度增长快，2017年、2018年每天平均有近40个漏洞被报告，2016年每天平均报告漏洞数量仅17个。

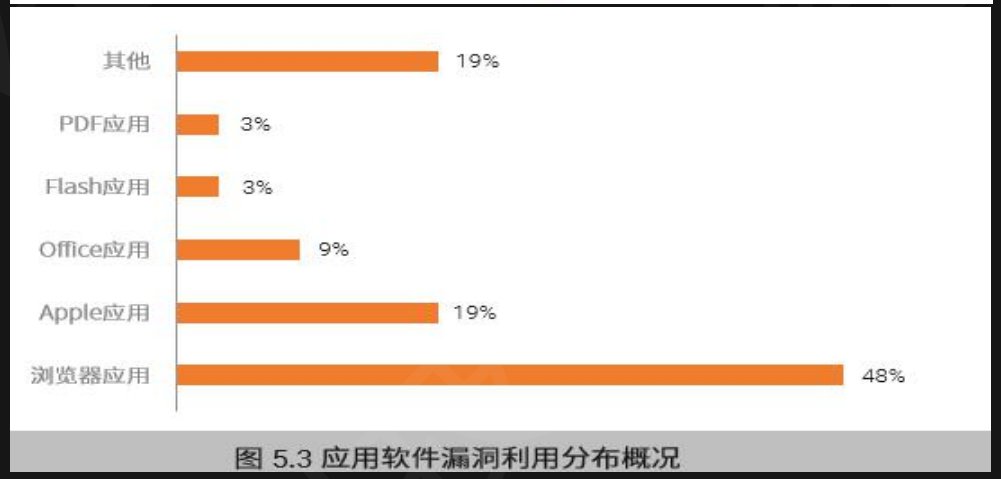


图 5.3 应用软件漏洞利用分布概况

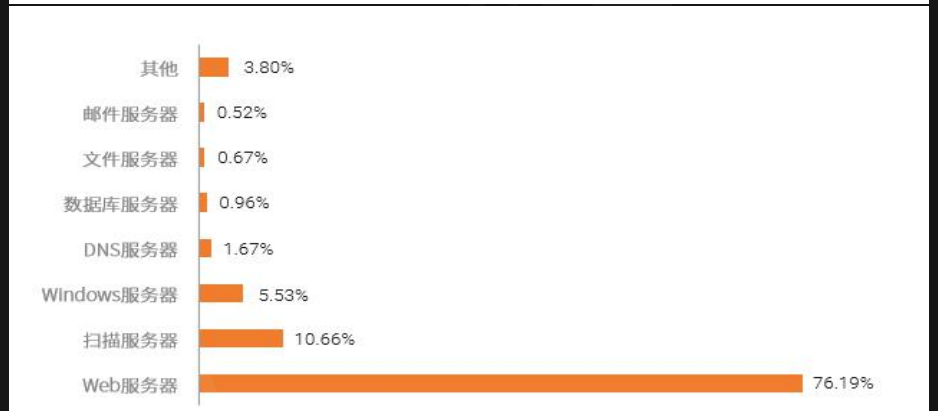


图 5.1 服务器漏洞利用概况

Source：《2019年网络安全观察报告》

漏洞应急常态化

注：绿盟科技漏洞库包含应用程序漏洞、安全产品漏洞、操作系统漏洞、数据库漏洞、网络设备漏洞等；

Zoom会议系统曝出高危漏洞，或影响400万电脑摄像头

- 2020年3月绿盟科技安全漏洞库共收录237个漏洞, 其中高危漏洞113个，微软高危漏洞27个。绿盟科技收录高危漏洞数量与前期相比呈下降趋势；
- 主要分布在微软、Adobe、Moxa、Videolabs实验室、VISAM、Siemens、Rockwell、D-Link、Linux、Vmware等厂商的主要产品中；

NSFOCUS

网络安全漏洞管理规范释放的信号

- 第三条 网络产品、服务提供者和网络运营者发现或获知其网络产品、服务、系统存在漏洞后，应当遵守以下规定：

  （一）立即对漏洞进行验证，对相关网络产品应当在90日内采取漏洞修补或防范措施，对相关网络服务或系统应当在10日内采取漏洞修补或防范措施；

- 第四条 工业和信息化部、公安部和有关行业主管部门按照各自职责组织督促网络产品、服务提供者和网络运营者采取漏洞修补或防范措施

- 第七条 第三方组织应当加强内部管理，履行下列管理义务，防范漏洞信息泄露和内部人员违规发布漏洞信息：

  （一）明确漏洞管理部门和责任人；

  （二）建立漏洞信息发布内部审核机制；

  （三）采取防范漏洞信息泄露的必要措施；

  （四）定期对内部人员进行保密教育；

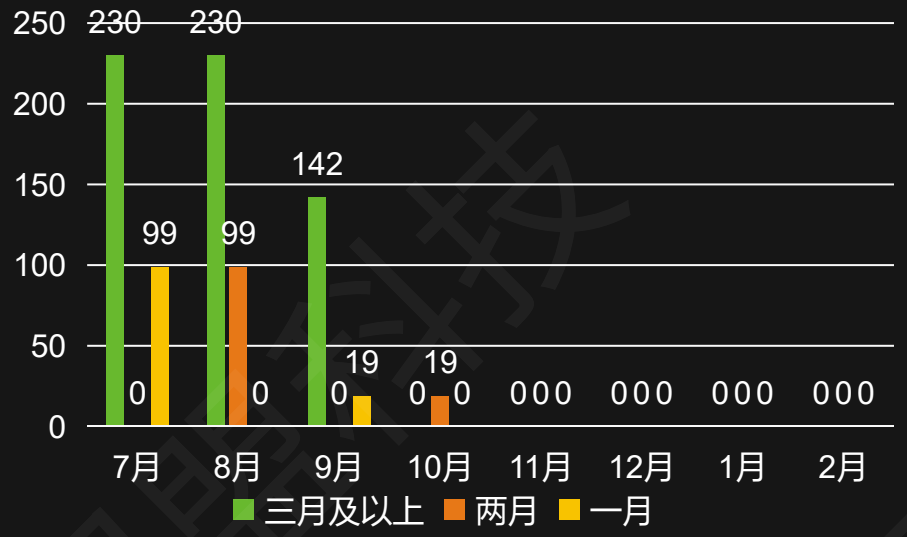
  （五）制定内部问责制度。

处罚主体	责任方处罚	责任人处罚
网络存在较大安全风险或者发生安全事件的	整改	约谈、警告
拒不改正或者导致危害网络安全等后果的	10K-100K并整改	5K-50K
关键信息基础设施拒不改正或者导致危害网络安全等后果的	100K-100W并整改	10K-100K
设置恶意程序； 对风险未立即采取补救； 擅自终止产品、服务的	50K-500K并整改	10K-100K

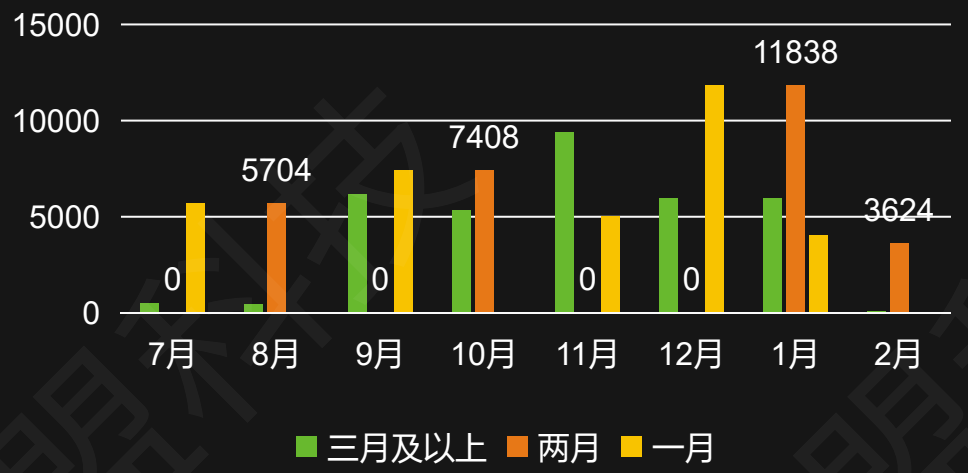
- 未按本规定采取漏洞修补或防范措施并向社会或用户发布的，要对其进行处罚，包括约谈、罚款、判刑等方式。

某央企安全运营实例

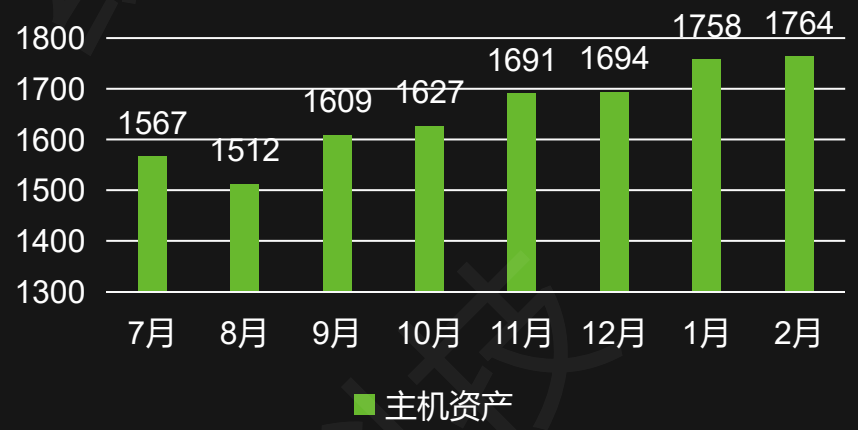
外网漏洞滞留情况



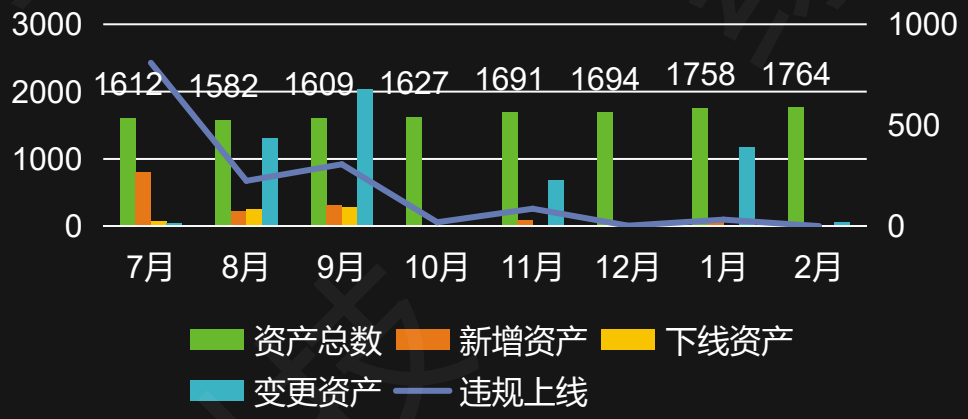
内网漏洞滞留情况



资产整体情况



历史资产变更情况



NSFOCUS

漏洞管理问题与挑战

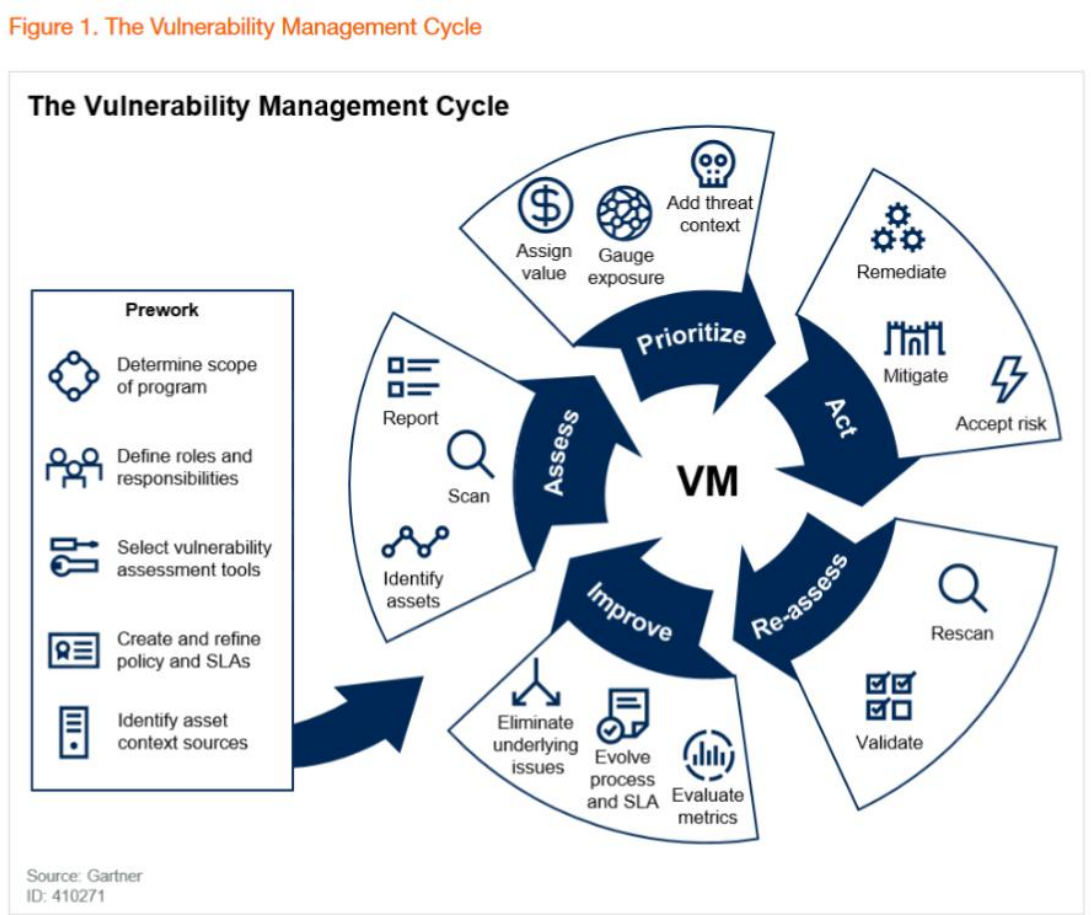
- 随着企业安全体系发展，海量漏洞，漏洞种类多样化；
- 漏洞管理是需要流程+人+工具一体化的工作；
- 专业性强，难以修复
- 漏洞管理与企业的目标范围强依赖，全局视角下的漏洞管理；
- 应急响应常态化是无法接受被动处置，响应缓慢，繁琐过程的现状

02

漏洞管理模型及技术变化

NSFOCUS

2019 Gartner定义的漏洞管理流程



From Gartner《A Guidance Framework for Developing and Implementing Vulnerability Management 2019》

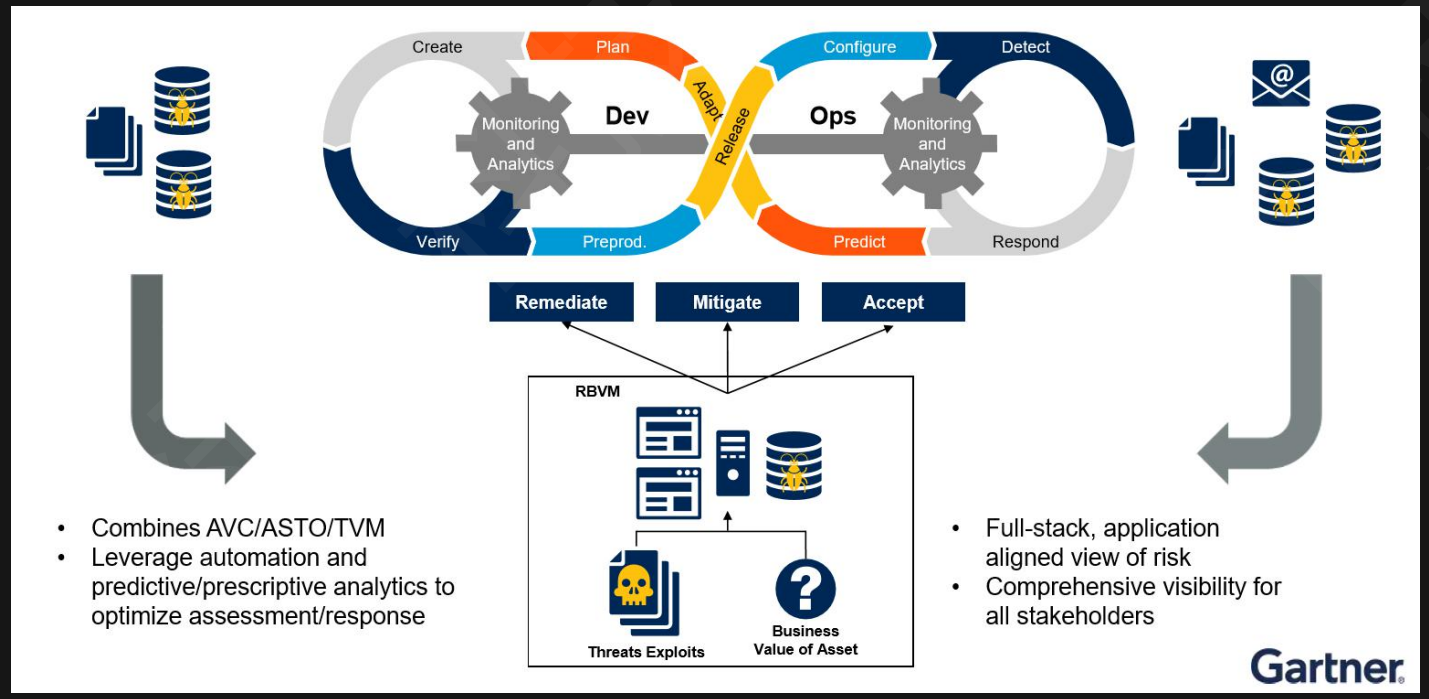
- **预处理阶段**
  - 定义管理的范围
  - 定义角色和职能
  - 选择漏洞评估工具
  - 创建或精炼策略和SLA
  - 识别资产上下文源头
- **漏洞管理流程**

  评估->**优先化**->采取行动->验证->**改进**（循环往复）

定义和优先化环节缺失和修复成本高为主要问题

NSFOCUS

基于风险的脆弱性管理



关键点

- 漏洞管理范围将扩至应用程序漏洞相关性、应用程序安全测试编制、威胁和漏洞的合集
- 有效将漏洞管理转化为业务语言，评估范围覆盖企业脆弱性类型，整个过程为优化和减少资源消耗才能简化企业漏洞管理工作

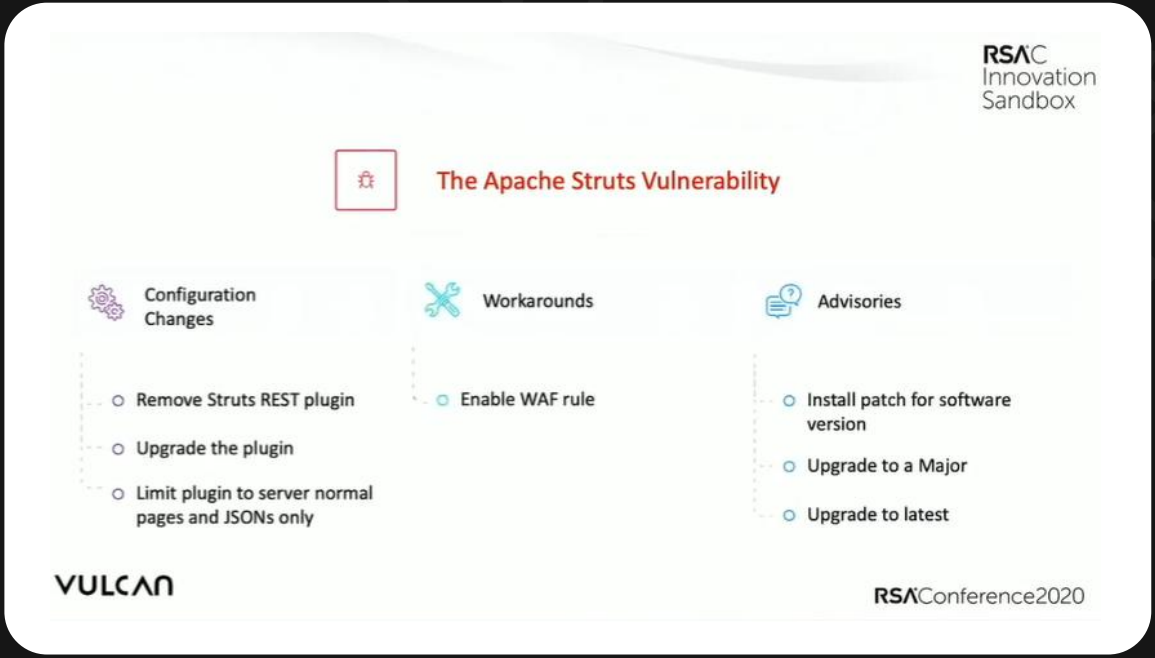
NSFOCUS

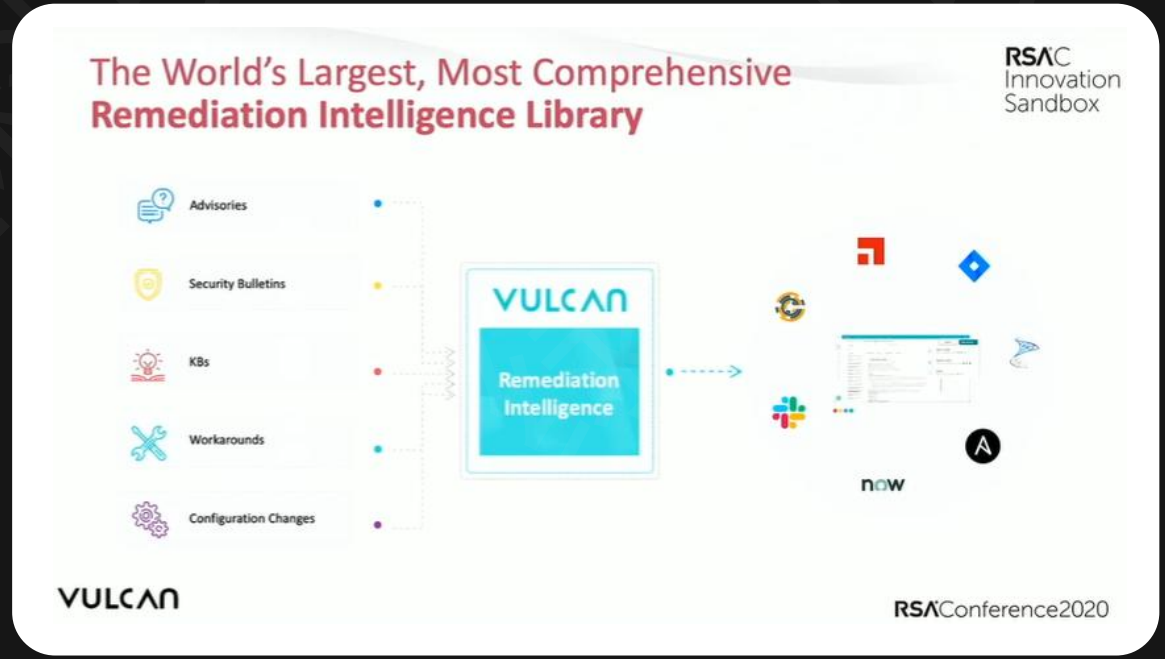
回到原点：网络安全风险三要素

漏洞管理的转变

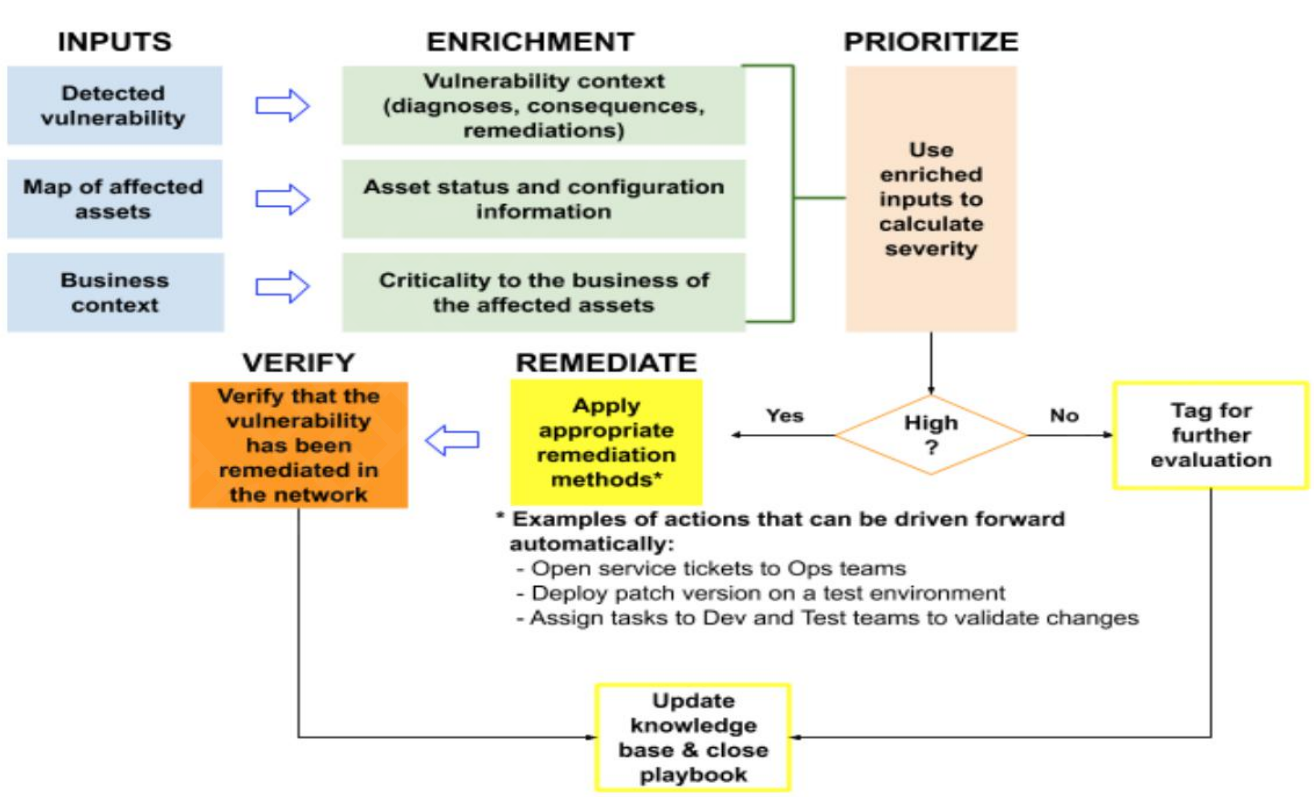
2020 沙盒——以色列 Vulcan Cyber

漏洞缓解机制知识库建立，漏洞编排及自动化响应。





漏洞缓解补偿控制措施



漏洞处理三种选择：

补救措施：完全修复或修补漏洞，让攻击者无法再利用该漏洞，这通常是在可能的情况下最可取的选择。

缓解措施：如果无法完成补救措施，组织机构可能会选择次佳方案，即通过实施补偿性控制措施来降低利用漏洞的可能性。这种解决方案应该是临时的，实在为组织机构最终补救该漏洞争取时间。

风险接受：如果某个漏洞是低风险漏洞，或者其修复成本要比漏洞被利用的成本还要高，这时组织机构可以选择不采取任何措施来修复该漏洞。

03

思考及应对之策

漏洞管理思路-绿盟威胁和漏洞管理方案

基于以威胁为中心的风险自适应管理解决方案，**整合**多源脆弱性数据，**聚焦**关键风险，**量化分析**风险管理指标，建立快速漏洞预警响应机制，提供漏洞管理的过程支撑，及时有效建立和完善漏洞管理补偿体系。

漏洞管理全局观

情报驱动应急响应

绿盟威胁情报中心实时跟踪热点漏洞事件，TVM获取后直接定位到客户网络受影响资产范围，给出漏洞预警，帮助安全运维人员尽快完成确认、分析、修复工作，并确认修复效果。

漏洞事件

- 因为安全事件突然被广泛关注的漏洞

外部

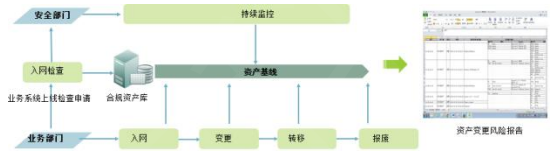
资产风险

- 新增资产
- 资产变更

内部

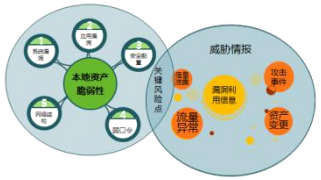
全网资产持续监控

对采集到的情报、脆弱性数据进行预处理，排除重复、无用数据，尽量消除误报信息，使最终评估分析结果更为精确。



利用情报聚焦关键风险

利用外部威胁情报，快速定位影响本地资产安全的关键风险点，结合业务系统资产重要等级，给出更为有效的风险评估分析。



漏洞威胁

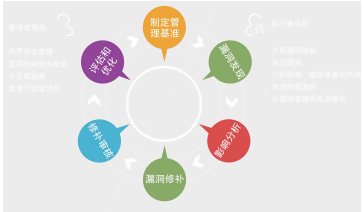
- 漏洞有POC代码
- 被渗透代码利用
- 被恶意软件利用

漏洞管理

- 管理制度
- 管理指标
- 管理考核

漏洞管理过程支撑

内置漏洞闭环过程处置引擎，成为漏洞闭环管理的技术支撑，对漏洞处置跟踪分析和量化，并支持多用户协作修复，和经验共享。



NSFOCUS

写在最后-漏洞管理建议

解决人的弱点

- 漏洞不仅限于技术，也存在于组织机构内的人为因素中。安全团队必须与IT运营和应用程序开发小组合作，以便更快地识别和修复各种漏洞。同时，用户培训和模拟可以提高组织抵御网络钓鱼和其他社会工程攻击的能力。

加快流程

- 实现漏洞管理流程的自动化对于正确管理企业面临的大量风险至关重要。人工决策在每个漏洞管理计划中都扮演着至关重要的角色，但是自动化可以帮助简化在这些关键决策点之前和之后所做的重复性工作。

持续评估漏洞

- 基础架构和应用程序可以每天甚至每小时都在发生变化。因此，必须不断扫描环境，确保尽早识别新漏洞。许多漏洞管理解决方案包括端点代理和其他集成，可以为您实时提供整个环境中漏洞状况视图。

善用补偿措施

- 在决定是否打补丁前，明确收益和风险，从CIA三要素入手，用边界防护加强针对物理攻击和数字化攻击的两方面防御，用隔离的方式阻断威胁的横向移动，并将安全事件限制在某一区域，避免整个组织受到攻击。

谢谢！

NSFOCUS