**业务挑战**

企业的安全漏洞管理难度不断增加，企业安全漏洞管理面临三个方面的挑战：

1、 漏洞管理环节缺失

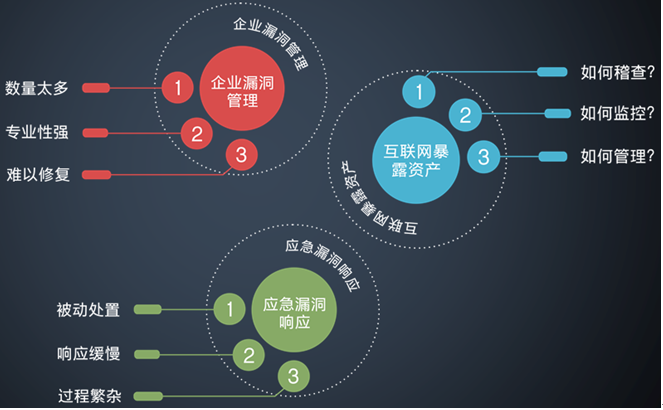
每年被披露的漏洞数量逐年递增，企业业务规模在持续增长，漏洞管理的复杂度不断增加，表现在三个方面：a.漏洞未依据企业实际影响情况进行优先级划分；b.现有手段重扫描轻修补，漏洞修补建议未充分参考软件系统自身的特性；c.现有手段重扫描轻处置，不具备对漏洞管理过程的跟踪和分析，不能支撑量化和优化工作。

2、 应急漏洞响应被动缓慢

紧急漏洞往往传播快、范围广、危害大，如果不及时修补，企业将面临直接的经济和名誉损失；而现有的手段，在漏洞知晓和处置上，都是非常被动和缓慢，也造成了安全主管人员压力大、经常加班，还不知道效果会怎么样，总处于焦虑状况。

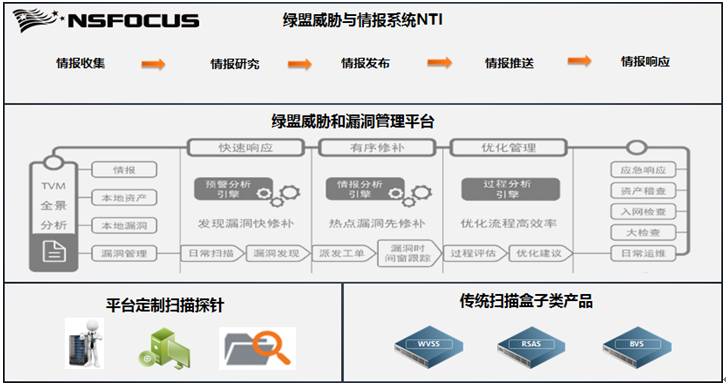
3、 互联网暴露资产缺少监管

对于承载了较多互联网业务的企业，暴露在互联网的资产承受的是直接的外部威胁，而这些海量的资产往往是动态变化的，因此，如何能够全面实时的了解这些资产，成为这类企业面临的一个难点，毕竟这些资产如果出现问题，企业是会被追责的。



**解决方案方案概述**

绿盟威胁和漏洞管理方案（NSFOCUS Threat and Vulnerability Management Solution，简称NSFOCUS TVM）提供漏洞管理的全过程支撑，量化跟踪和分析流程执行情况，促进管理流程持续优化。同时充分利用绿盟科技威胁情报中心的漏洞情报信息，由情报触发流程运转，帮助客户建立快速响应机制，及时有效完成漏洞修补工作。



**解决方案价值**

基于情报的应急响应。实时跟踪热点漏洞事件，紧急漏洞直接定位到客户网络环境资产，对资产风险进行预警。

基于威胁的漏洞管理。根据外部漏洞威胁情报，结合本地资产，找出有可能会被利用的资产及漏洞，给出修复优先级建议。

基于持续监控的资产生命周期管理。全面发现内外网网站资产和IP资产，建立合规资产基线，持续监控资产的上线、变更、转移、销毁状态，及时发现资产变化带来的潜在安全风险。

**解决方案特点**

 **情报驱动快速修复漏洞**

绿盟威胁和漏洞管理方案通过绿盟威胁情报中心获取漏洞披露情报，结合本地资产信息精确分析漏洞对业务的影响，对可能存在漏洞的资产精确预警。运维人员能够快速进入漏洞管理流程，及时发现漏洞并修补。

 **多维度漏洞优先级建议**

绿盟威胁和漏洞管理方案引入漏洞攻防情报，如漏洞炒作热度、漏洞利用活跃度信息，结合本地业务资产重要程度，综合多种维度分析关键漏洞风险，给出漏洞处置的优先级建议。

** 漏洞全过程管理**

绿盟威胁和漏洞管理方案从漏洞披露开始，持续监控资产变化，实时获取漏洞披露情报，对漏洞发现、分析、修补和审核过程进行跟踪，通过对整个管理过程的评估、对比，达到持续优化漏洞管理基准要求的目的。



 **内外网资产持续监控**

利用绿盟威胁情报系统的云端大数据采集能力，能够快速大规模发现企业暴露在互联网上的资产和安全状况。利用本地资产采集设备，全面采集内网资产信息。绿盟威胁和漏洞管理方案持续跟踪网络资产变更，及时发现非合规资产新入网、端口服务变化等问题带来的风险。