OWASP

Open Web Application Security Project

云管端全面协同检测响应

自我介绍

- 邹荣新：深信服首席安全技术专家
  - 十年以上的安全从业经历，有丰富的安全对抗技术经验
  - 常年奋斗在产品研发一线，关注云、管、端的安全核心技术实现
  - 带领公司进行智安全的核心能力建设，安全闭环体系的能力建设

大纲

- 网络安全面临的新环境
- 安全建设理念的新变化
- 云管端全面协同检测响应

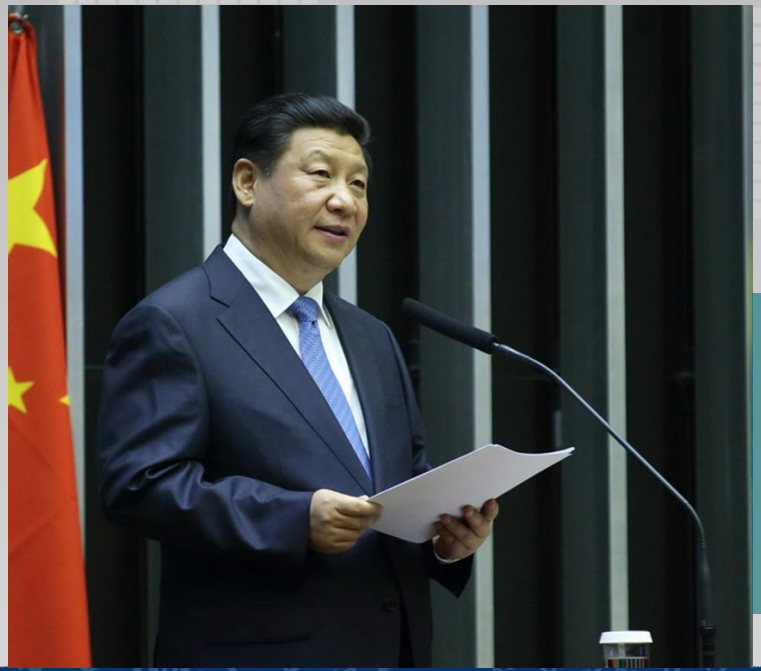
IT基础环境的变化

云化

移动互联网

物联网

国家安全战略的变化—战略高度



网络安全不断升温

上升到国家战略高度

国家安全战略的变化—419讲话

- 第一，树立正确的网络安全观。
- 第二，加快构建关键信息基础设施安全保障体系。
- 第三，全天候全方位感知网络安全态势。
- 第四，增强网络安全防御能力和威慑能力。

法律法规的安全要求—网络安全法

关键信息基础设施
范围扩大

组织、个人的法律责任
经济处罚、停职

法律法规的安全要求—等级保护

等级保护2.0发布，

带来合规建设要求

安全事件的频繁发生

CNCERT持续对“暗云III”木马程序进行监测，截止6月12日，累计发现全球感染该木马程序的主机超过162万台，其中我国境内主机占比高达99.9%，广东、河南、山东等省感染主机数量较多。同时，CNCERT对木马程序控制端IP地址进行分析发现，“暗云III”木马程序控制端IP地址10个，控制端IP地址均位于境外，且单个IP地址控制境内主机数量规模均超过60万台。

根据监测结果可知，目前“暗云III”木马程序控制的主机已经组成了一个超大规模的跨境僵尸网络，黑客不仅可以窃取我国百万计网民的个人隐私信息，而且一旦利用该僵尸网络发起DDoS攻击将对我国互联网稳定运行造成严重影响。

大纲

- 网络安全面临的新环境
- 安全建设理念的新变化
- 云管端全面协同检测响应

安全建设的能力需求

安全建设真正需要的是：安全能力

安全可视

看清看懂
安全现状风险的能力

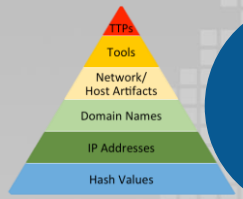
持续检测和响应

持续对抗
新型威胁的能力

高效运维

简化
安全运营的能力

云管端安全防御体系



云平台

威胁情报
安全即服务
云安全资源池

下一代防火墙
上网行为管理
安全感知平台

边界

端点

端点检测响应
SSL VPN
EMM

安全事件响应处置需求

安全事件响应处置案例

自2017年5月12日起，“WannaCry”勒索病毒突然大面积爆发，影响遍及全球100多个国家，超10万台机器。英国医疗系统、俄罗斯电信公司等，国内一些知名高校、能源企业、政府机构也受到波及。

防火墙策略

- 下发445端口访问控制规则，限制该端口的访问
- 根据WannaCry的开关域名加入检测策略，检测到开关域名后告警

端点响应

- 第一时间发布免疫工具，界面友好，一键免疫
- 第一时间发布针对MS17-010漏洞补丁安装建议，让用户主机第一时间得到保护

云端威胁情报联动

- 云端检测事件日志数据分析，联动产品推送解决方案；
- 云端样本数据采集汇总，安全原理分析，输出检测能力。

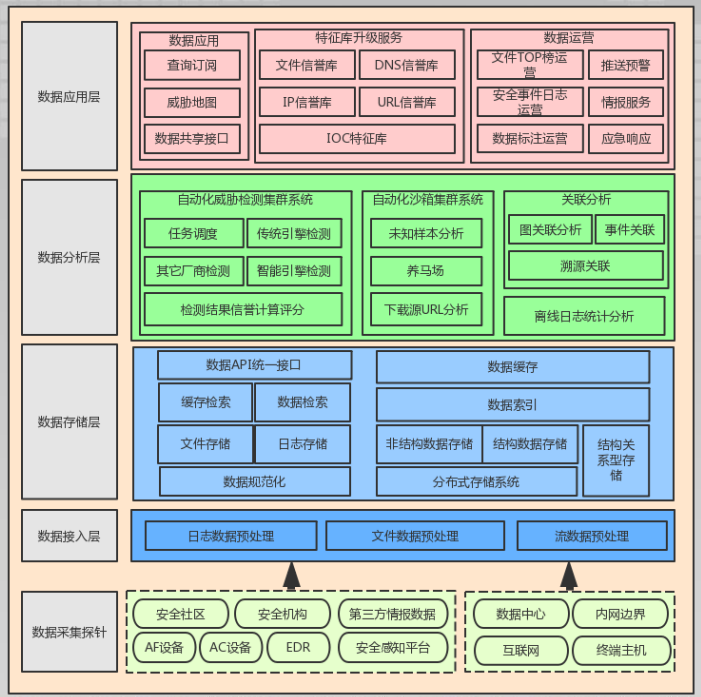
大纲

- 网络安全面临的新环境
- 安全建设理念的新变化
- 云管端全面协同检测响应

云管端全面协同检测响应

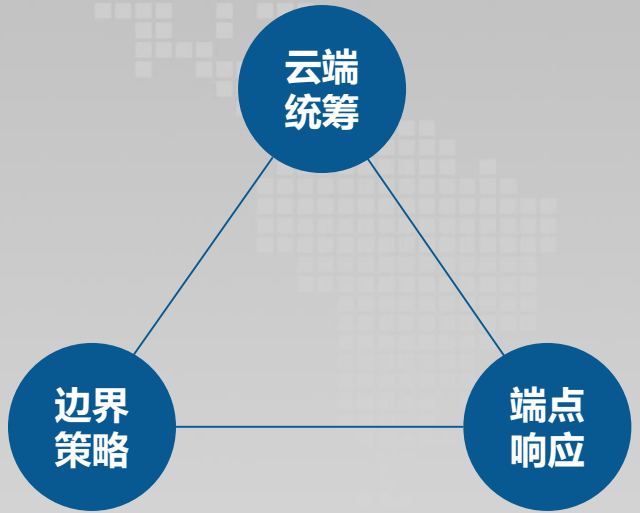
- 云端大数据分析平台
- 多引擎流量检测
- 沙箱蜜网系统
- 机器学习智能检测
- UEBA行为关联分析
- 数据统计分析系统
- 日志关联分析系统
- 威胁情报联动协作
- 端点安全快速响应
- .....

云安全运营体系建设



云安全运营体系建设

深信服基于新的安全建设理念，提供一套更容易落地的安全框架。



融合安全

- “事前、事中、事后”风险闭环管理

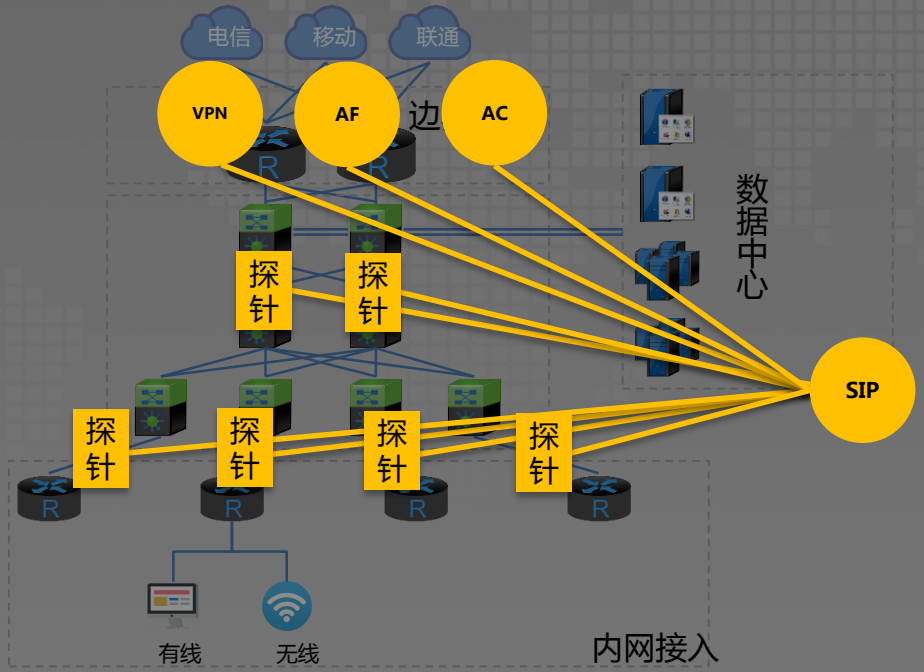
立体保护

- 基于全业务链的整体保护

简单有效

- 部署简单、灵活，产品易用

网络侧安全监测构建



终端侧快速响应处置

端点安全，不只是杀毒

- 日志采集
- 行为采集
- 恶意软件分析
- 云端联动
- 策略下发
- 及时响应
- 范围定位
- 事件取证
- ……