第四届全国网络与信息安全防护峰会

安全行业的运营升级

攻防对抗技术民用化的思

演讲者：

深圳市极限网络科技有限公

XDef2015 对话·交流·合作

公司简介

公司地址：深圳市南山区高新
技园南区深南大道9789号德赛
技大厦1001B室

公司研发中心地址：深圳市罗
区松园路九号茂源大厦707室

业务

1. 安全产品定制研发
2. 安全服务解决方案
3. 漏洞挖掘、底层技术研究

提纲

面对日趋严峻的网络安全形势，堵漏洞、作高墙、防外攻的“被动式防御”已经远远不能满足企业安全运营的需求。病毒和攻击技术的不断更新，使得人们的防御措施不断的跟在安全威胁的后面跑，被动挨打的局面显而易见。那么，如何变被动为主动呢？

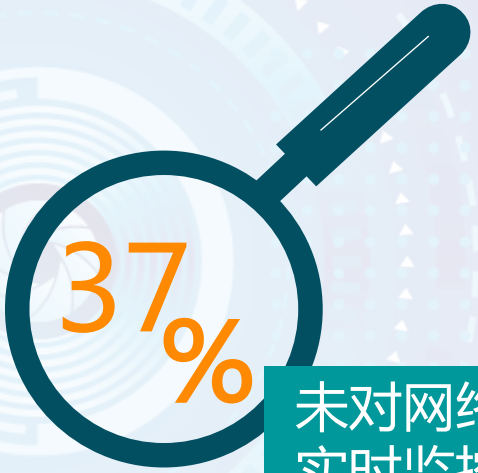
本次议题从网络安全的本质——攻防对抗技术出发，思考如何有效的将攻防对抗技术民用化，以帮助企业有效地应对日新月异的网络攻击技术，优化企业安全运营的能力，彻底摆脱防御和安全运营一直处于滞后状态的现状。

目录

数据有话说

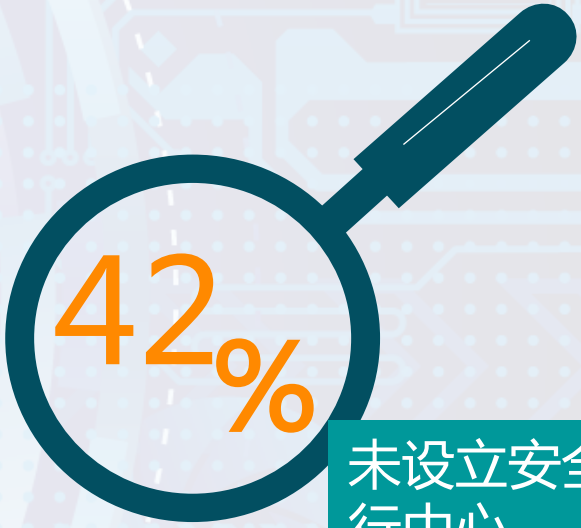
5%

企业设立了网络威胁情报信息团队



37%

未对网络风险进行实时监控



42%

未设立安全运行中心

缺乏敏捷性

对于目前明确存在的危险，企业采取的行动尚不够迅速
仅有36%的企业对网络风险进行实时监控，27%的受访者表示只是“偶尔”监控
企业在构建基础网络安全方面仍十分滞后。

缺乏网络安全技能

- 成熟的企业不仅会做好自身防御工作，使其免遭网络攻击，还会使用智能分析预见他们可能面临的风险。
- 但是，专业技能人才缺乏是一个常态化的问题且愈演愈烈。

络威胁新形势

攻击手段日益复杂、智能化

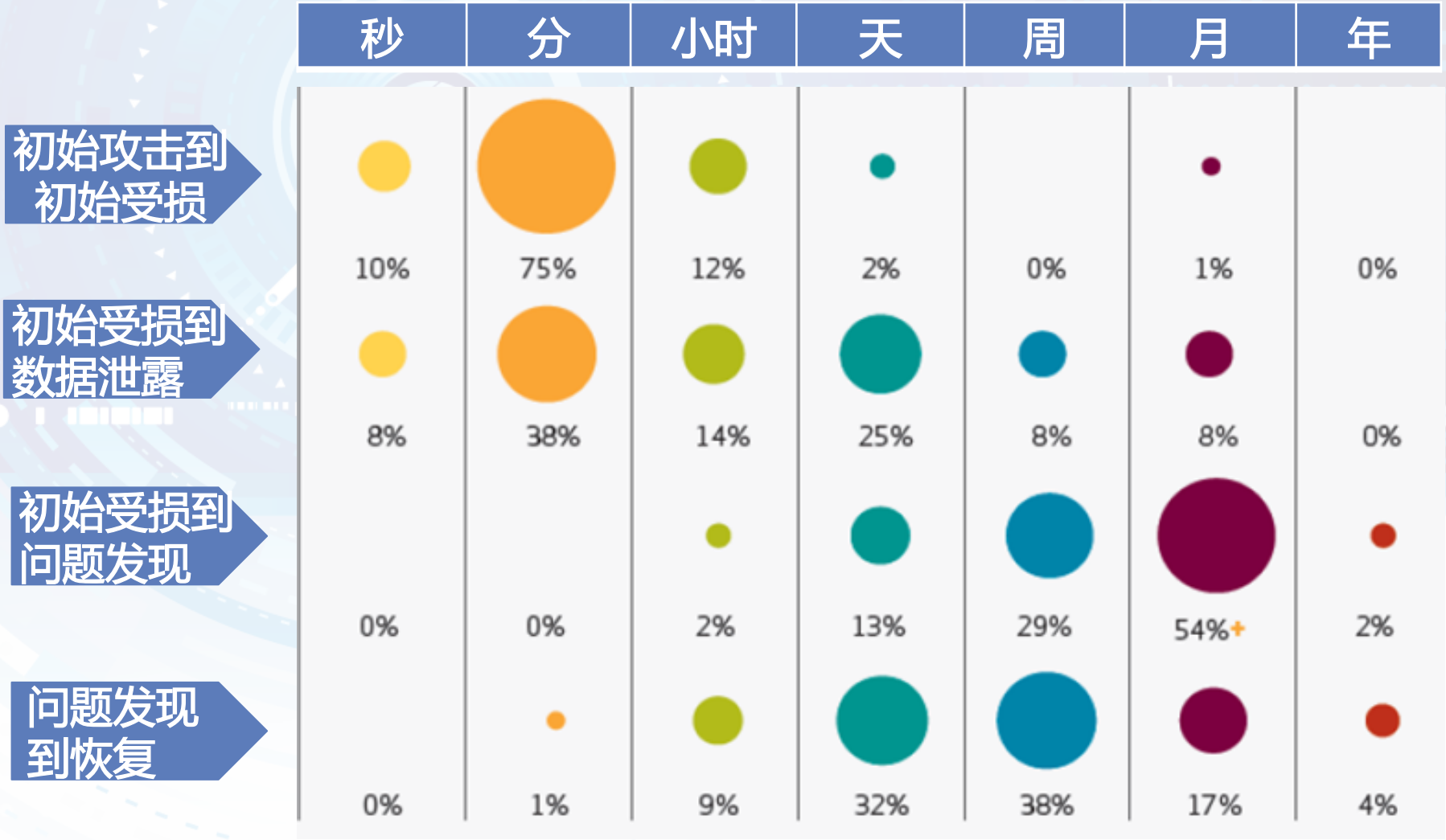
新的攻击手段、工具被不断地开发利用，利用漏洞进行的网络攻击更是层出不穷。

攻击者利用安全漏洞发动攻击的速度越来越快。目前，许多攻击工具已经具备了反侦破、动态行为、更加成熟等特点。

网络攻击的自动化程度和攻击速度不断提高

- 大量的网络自动化攻击工具的出现，网络攻击变得越来越平民化。
- 目前，分布式攻击工具能够很有效地发动拒绝服务攻击，扫描潜在的受害主机，对存在安全隐患的系统实施快速攻击。

络安全防护体系落后于攻击技术发展



01 网络攻防形势分析

02 案例分析

03 攻防对抗技术民用化应用场景

04 反思总结

方程式”攻击分解

- EquationLaser
  最早木马
- EquationDrug
  上传和卸载的模块插件
- DoubleFantasy
  验证式的木马
- TripleFantasy
  全功能的后门程序
- Fanny
  USB蠕虫
- GrayFish
  驻留木马

DoubleFantasy　验证式的木马

- 确定目标是否为感兴趣的目标，如果是，则将恶意代码升级EQUATIONDRUG或GRAYFISH。
- 作为一个后门长期潜伏在感兴趣目标的电脑上。

行为分析

第一步：DoubleFantasy首先通过访问Microsoft.com域名，以确定是否可以连接网络

第二步：如果可以连网，它接着访问timelywebsitehostesses.com并向其发送POST数据请求。

第三步：接着DoubleFantasy会探测目标内网的存活主机，通过发送NBNS、NBSS、SMB协议数据探测目标局域网的所有主机计算机名称以及开启相关共享服务的主机。我们怀疑它具有通过局域网共享漏洞传播自己的功能，但这可能在得到C&C的指示命令后才进

方程式”攻击分解

EquationDrug

上传和卸载的模块插件

，受害者不会直接被EquationDrug
，攻击者首先让目标感染
bleFantasy，这是一个验证目标
的插件。如果受害者被确认为攻击
兴趣的目标，EquationDrug才会
装到目标电脑上。

行为分析

第一步：EquationDrug同样探测目标内网的存活主机，
着发送NBNS、NBSS、SMB协议数据探测目标局域网的
有主机计算机名称以及开启相关共享服务的主机。

第二步：那些从目标PC机上收集到的准备传输给C&C的
息，被加密后保存成.FON后缀的文件，存储在受害者计
机的Windows\Fonts文件夹下。

第三步：收集完信息后，EquationDrug接着访问C&C，
会轮询内置的多个域名，直到有一个能验证成功。轮询的
程中除了尝试HTTP协议外还尝试HTTPS协议。

GrayFish

驻留木马

，它的目的是提供一个有效的（几乎
隐形”）持久性机制，在Windows操
系统内隐藏存储和执行恶意命令。它
容微软所有主流操作系统版本

行为分析

GrayFish运行后先轮询内置的多个域名，直到有一个
验证成功。在轮询的时候除了尝试HTTP协议外还尝试
HTTPS协议。验证过程中，GrayFish会随机生成一些请求
面访问域名服务器。

程式”攻击生产周期和特性

过蓝牙设备 入侵监狱系统

Hack WPA2——攻击WPA2

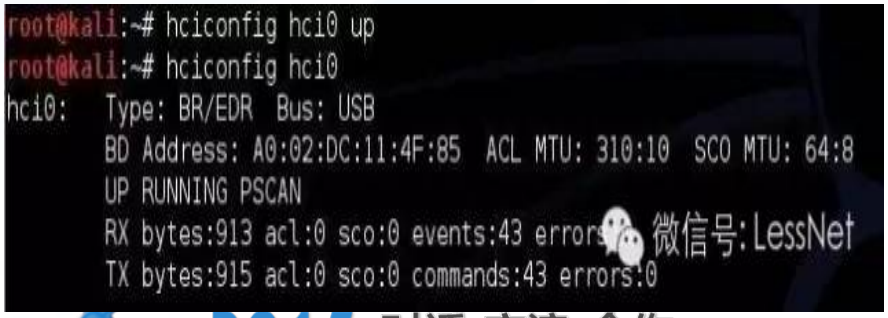
安装Wi-Fi扫描应用，获取监狱所有无线AP，发现都是WPA2加密

扫描过程中，发现一辆监狱警车及一个蓝牙连接

开启蓝牙服务

渗透前在Linux渗透系统上开启蓝牙服务
『kali > servicebluetooth start』

激活蓝牙设备并检查蓝牙是否正常工作，以及性能



注意第二行“BD Address”
这是蓝牙设备的MAC地址

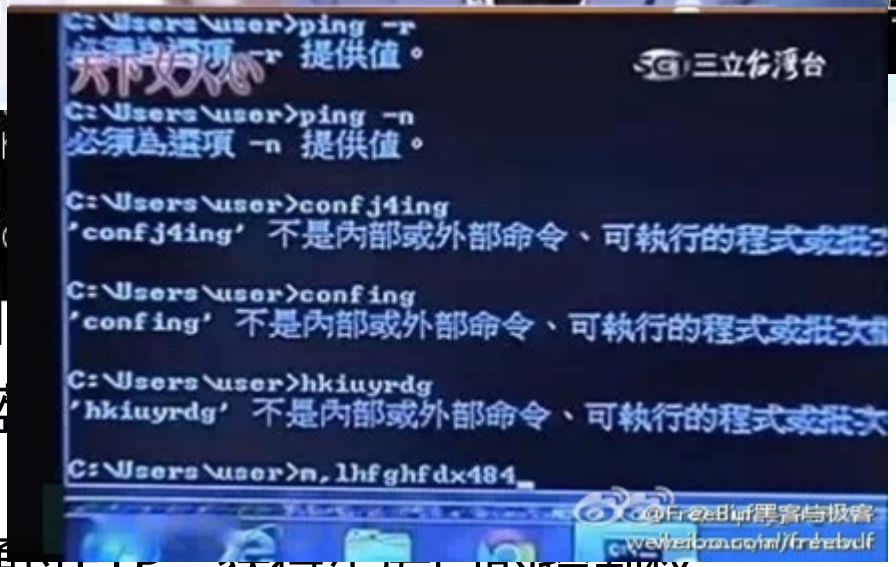
过蓝牙设备 入侵监狱系统

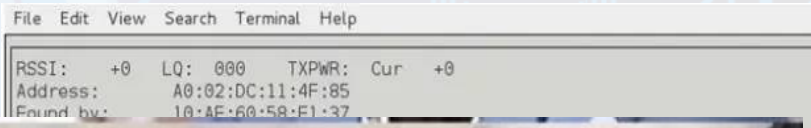
扫描蓝

欺骗键盘

连接蓝
的笔记

入侵监狱系统





围蓝牙设备

名为“Tyler”

C地址和蓝牙设

i内置欺骗蓝牙

键盘

过连接键将蓝

- 利用控制到的狱警电脑上传恶意软件通过IP，获得牢房门的控制权。
- 这些工业系统的PLC基本上是数字控制器，恶意软件感染了它们获得了控制权

01 网络攻防形势分析

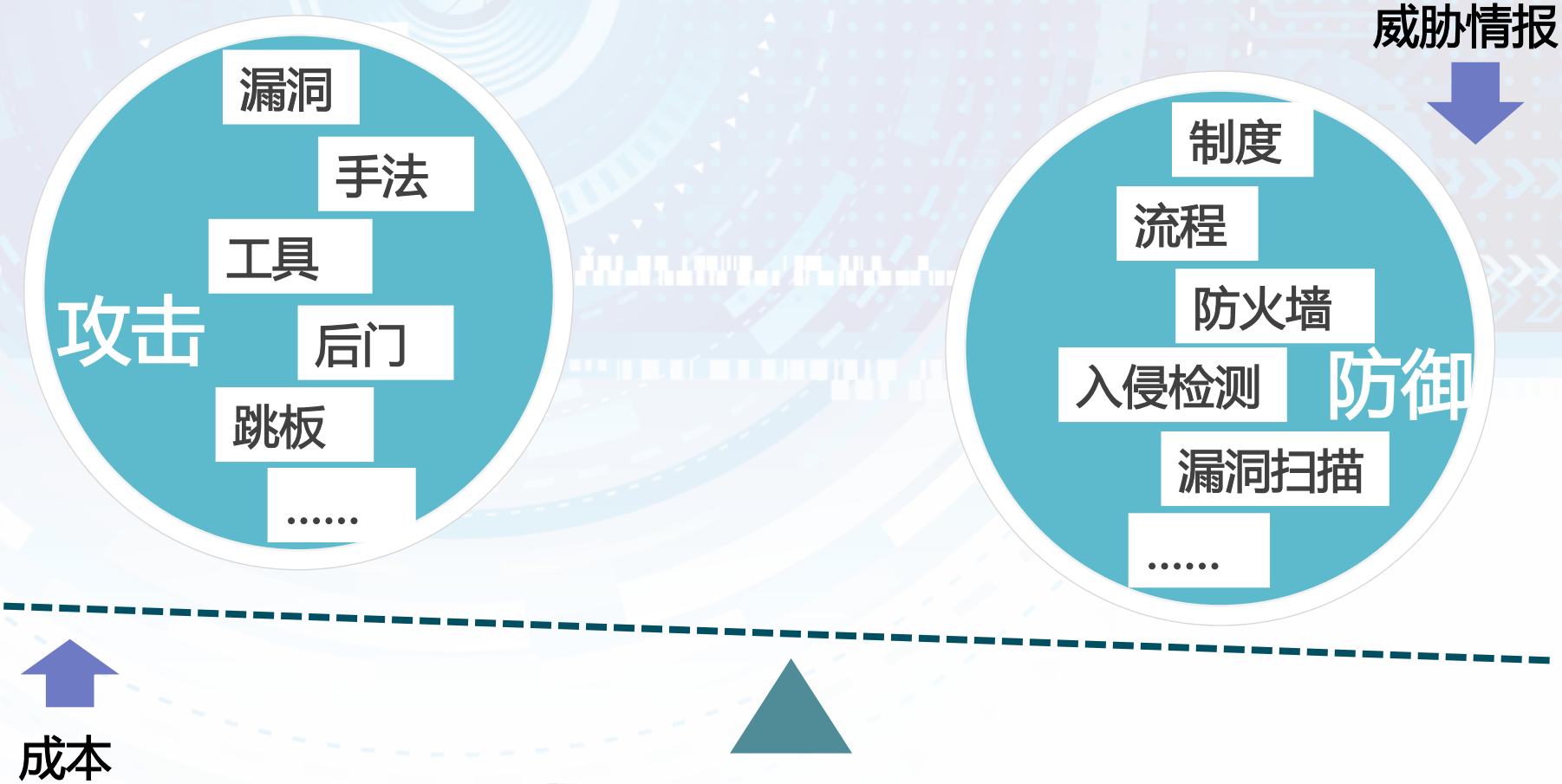
02 案例分析

03 攻防对抗技术民用化应用场景

04 反思总结

场景一：威胁情报民用化

帮助企业更好地了解针对其的威胁和风险，例如零日和APT等
分析和筛选数据，以管理报告和数据源的形式生成有用的信息用于自动化安全控制系统。
帮助企业保持IT基础设施的更新，让安全专业人员更好地阻止安全漏洞，防止数据丢失或系统故障
从而有效地抵御攻击者。



场景二：新形势下的刑侦取证技术运用

没有先进的手段和现代信息技术，就不可能有效地打击各种犯罪活动、维护经济秩序和国家利益
积极运用现代科技手段，是侦破工作发展的客观需要，也是科技发展和社会进步的必然趋势
广泛应用信息化技术，构建起以信息网络为基础、以信息应用为主导、以信息人才为依托、以信息
为保障的综合体系，实现了办案现代化、办公自动化。

犯罪手段向类型新型化、手段智能化、危害严重化等方向发展

计算机犯罪等利用专业技术和高科技犯罪作案的比例正在逐年上升

流窜犯罪、严重暴力犯罪、系列犯罪等群体性犯罪事件呈高发之势

刑侦取证面临严峻的新形势

解决策略

- 重视网络技术的运用
- 加大刑侦技术的应用
- 正确认识及推广科技
- 加大投入 提高刑侦工作技术含

用成效

现场破案率
连续9年
超过90%

1月至10月，全国共破获各类诈骗案件12万起，同比增长12.2%。

2014年，共破获“伪基站”犯罪案件3122起，捣毁生产窝点115个，缴获设备4172套，破获下游犯罪案件374起

2013较2004
命案件数下降
50.36%

科技、法治建设“双剑合璧”
提升刑事执法公信力

- 公安刑侦系统已建成全国在逃人员、犯指纹、失踪人员、DNA、现场勘查信息统等多个贯通全国、服务全警的信息系统。
- 利用社会信息化的海量资源已成为公安关的“撒手锏”。
- 公安机关利用信息化手段破获案件的数已达到破案总数的30%以上。

01 网络攻防形势分析

02 攻防对抗技术民用化应用场景

03 案例分析

04 反思总结

状的总结与反思

- 网络攻击技术和网络防御技术是一对“矛”和“盾”的关系。
- 如今，网络攻击技术越来越复杂，而且常常超前于网络防御技术，传统的防御手段显然难以应付现存的网络安全环境。

防御能力是静止的

传统防御完全依靠网络管理员对设备的人工配置来实现，难以应对当前来越多的、技术手段越来越高的网络入侵事件

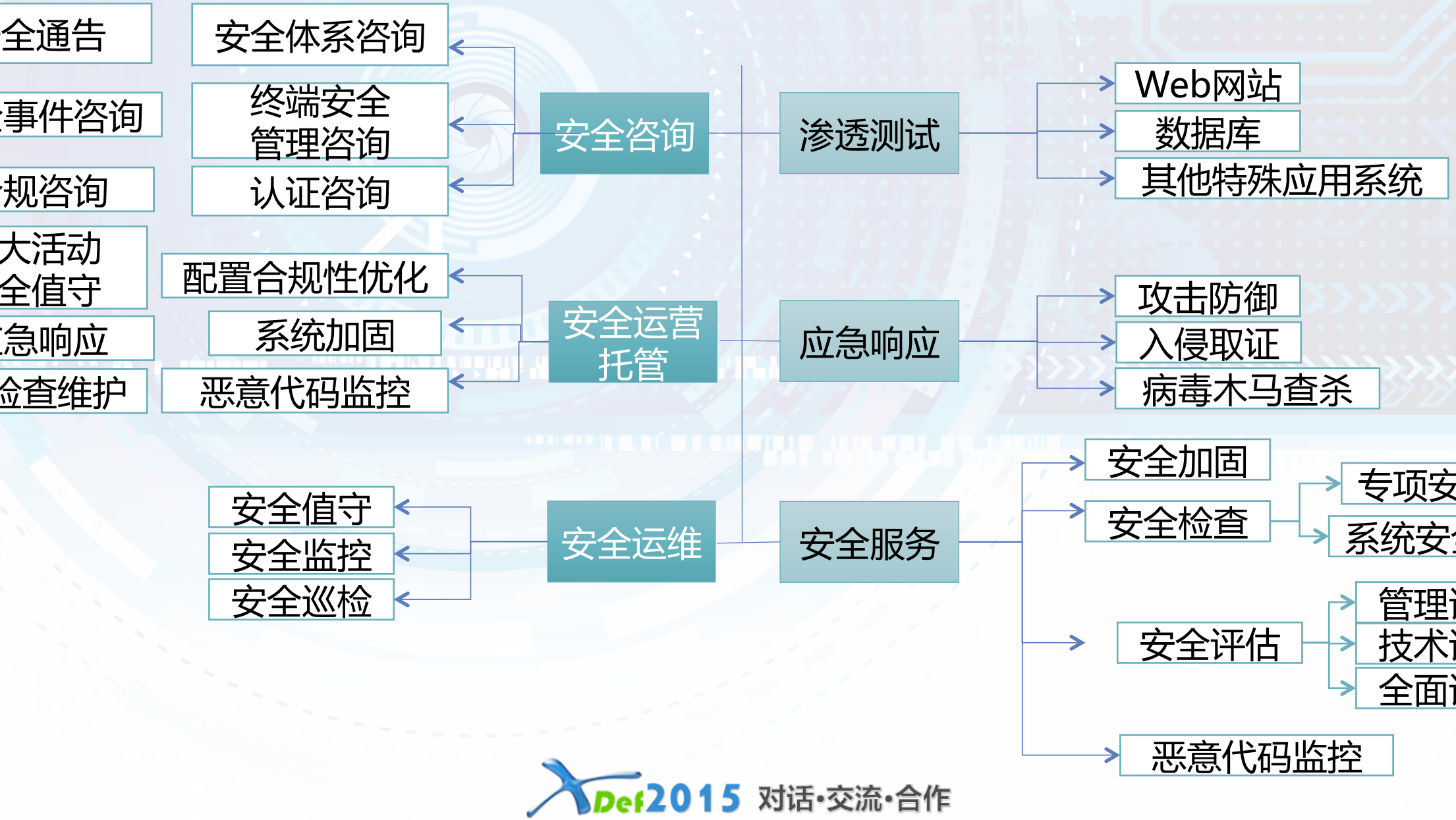
防御具有很大的被动性

采用传统的防御技术只能被动地接受入侵者的每一次攻击，而不能对入者实施任何影响

无法识别新的网络威胁

传统防御技术大多都依靠基于特征库的检测技术，这就使网络防御始终后于网络攻击，难以从根本上解决网络安全问题

全运营现状内容


全通告
事件咨询
规咨询
大活动
全值守
急响应
检查维护
安全体系咨询
终端安全
管理咨询
认证咨询
配置合规性优化
系统加固
恶意代码监控
安全值守
安全监控
安全巡检
安全咨询
安全运营
托管
安全运维
渗透测试
应急响应
安全服务
Web网站
数据库
其他特殊应用系统
攻击防御
入侵取证
病毒木马查杀
安全加固
安全检查
专项安全
系统安全
安全评估
管理评
技术评
全面评
恶意代码监控

全运营升级思考


国家机构
企业
协会、组织
安全行业
安全咨询
渗透测试
安全运营托管
应急响应
安全运维
安全服务
联动防御
业务风控
威胁情报
边界防控
云化管理
.....
安全运营拓展

感谢您的关注！

Thanks for your attention！