2017 中国互联网安全大会
China Internet Security Conference

大数据在应急响应中的应用

龚玉山

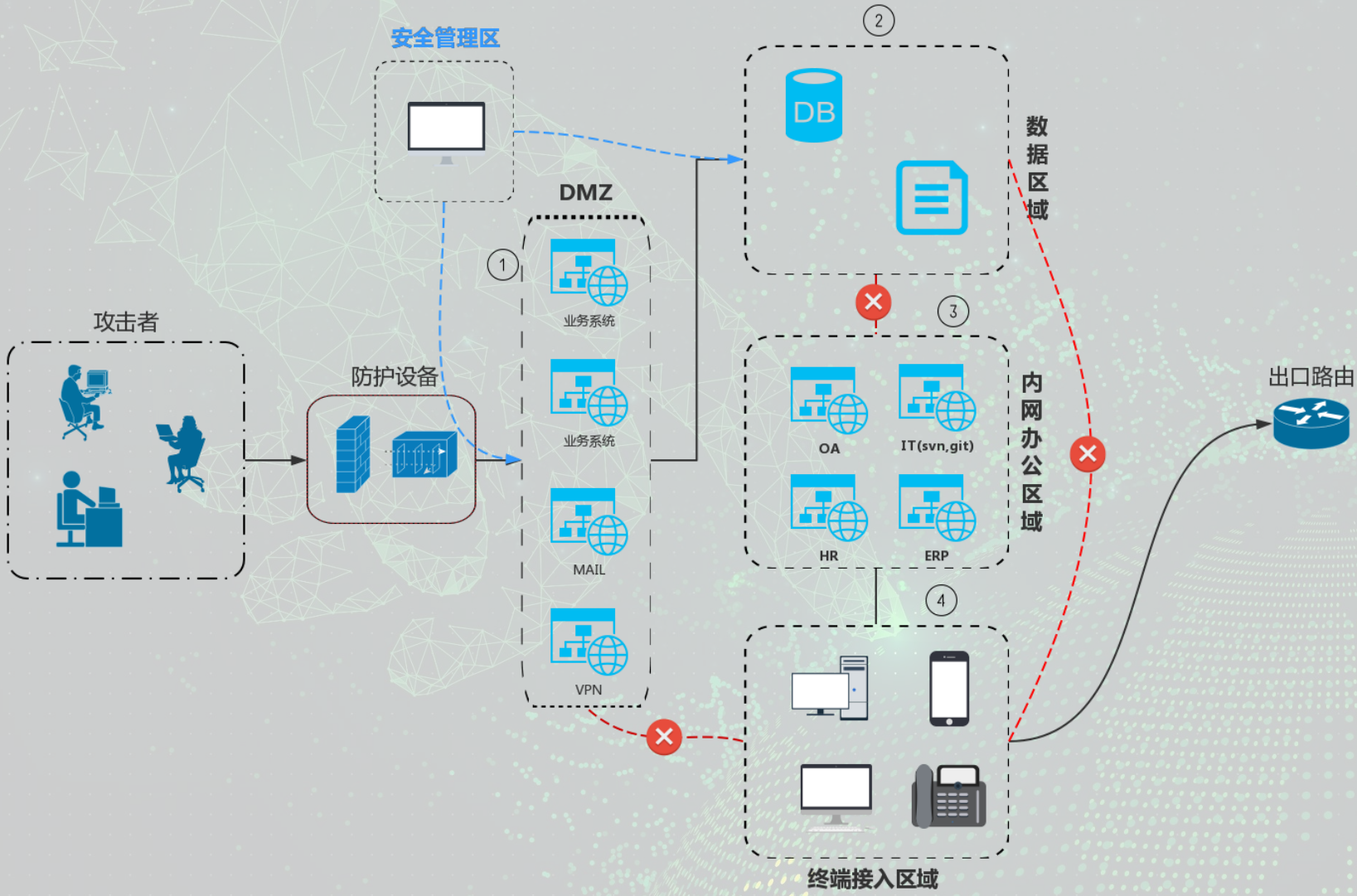
360企业安全高级安全研究员
360观星实验室总监

ISC 2017 中国互联网安全大会 | 360互联网安全中心

目录

企业在应急响应中的痛点

企业在应急响应中的痛点-复杂的网络结构



企业在应急响应中的痛点-外部威胁

已有的应急响应体系是否可以应对新形式下的挑战？

新的威胁环境

- APT攻击
- 0-day
- Web Shell
- “免杀”型木马
- ……

对立面的信息

- 攻击者是谁？（Who）
- 采用什么攻击手段？（How）
- 什么时间攻击？（When）
- 攻击的目的是什么？（What）
- 攻击者的位置？（Where）
- 攻击目标？（Target）
- 攻击进展？（Progress）

企业对外部对立方的信息一无所知，无法做到知彼知己，在攻防过程中处于被动局面。是否可以扭转被动挨打的局面？

企业在应急响应中的痛点-内部威胁

内部失陷

通过持续监控与分析组织的终端行为数据，并结合外部威胁情报的数据，可以找出组织内部已经被攻陷的终端。主要包括：

➢失陷主机：Web Shell、反弹shell、远控木马、Tunnel、潜伏后门、数据泄露l等。

内部威胁

通过持续监控与分析组织的内部安全大数据，并结合云端安全情报，发现客户内部的攻击面、漏洞信息、内部攻击和违规操作等威胁，主要包括：

➢资产管理

➢内部攻击：非法扫描、恶意探测、暴力破解等

➢违规操作：越权访问、非法业务数据查询

企业在应急响应中的痛点-致命点

资产管理混乱

管理制度问题（特权账号问题）

没有日志（或者没有开启日志）

弱口令问题

安全设备当摆设（缺少安全运营人员）

溯源困难

历史遗留问题

无法还原事件现场（无备份机制）

乌龙事件

缺少日常安全巡检

企业在应急响应中的痛点

数据驱动的应急响应理念

数据驱动的应急响应理念

数据驱动的应急响应一定是具备大数据能力的安全厂商和企业私有安全大数据的结合

安全大数据在应急响应中的场景

安全大数据在应急响应中的应用场景

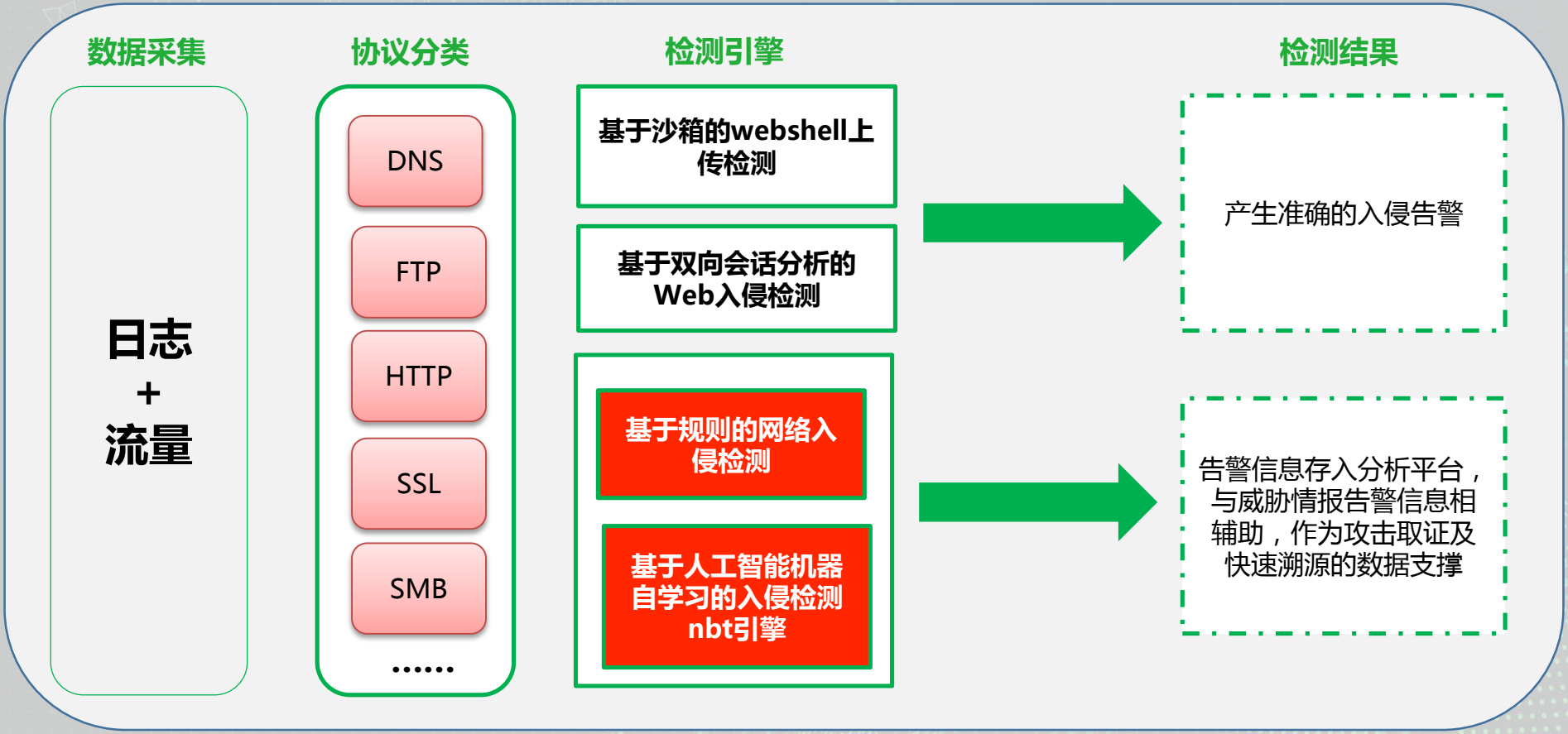
应急响应事件处理流程

准备阶段	检测阶段	分析阶段	处置阶段	总结阶段
• 应急预案 • 备份机制 • 应急演练	• 安全设备告警 • 设备日志 • 应急工具箱	• 事件告警分析 • 设备日志分析 • 事件关联分析	• 确定影响范围 • 定位受影响机器 • 清除\取证	• 事件复盘 • 完善监测策略 • 归纳不足

安全大数据发挥的作用取决于在各个阶段做的工作是否到位，只有在各个环节上充分准备，才能支撑整个事件的处置。

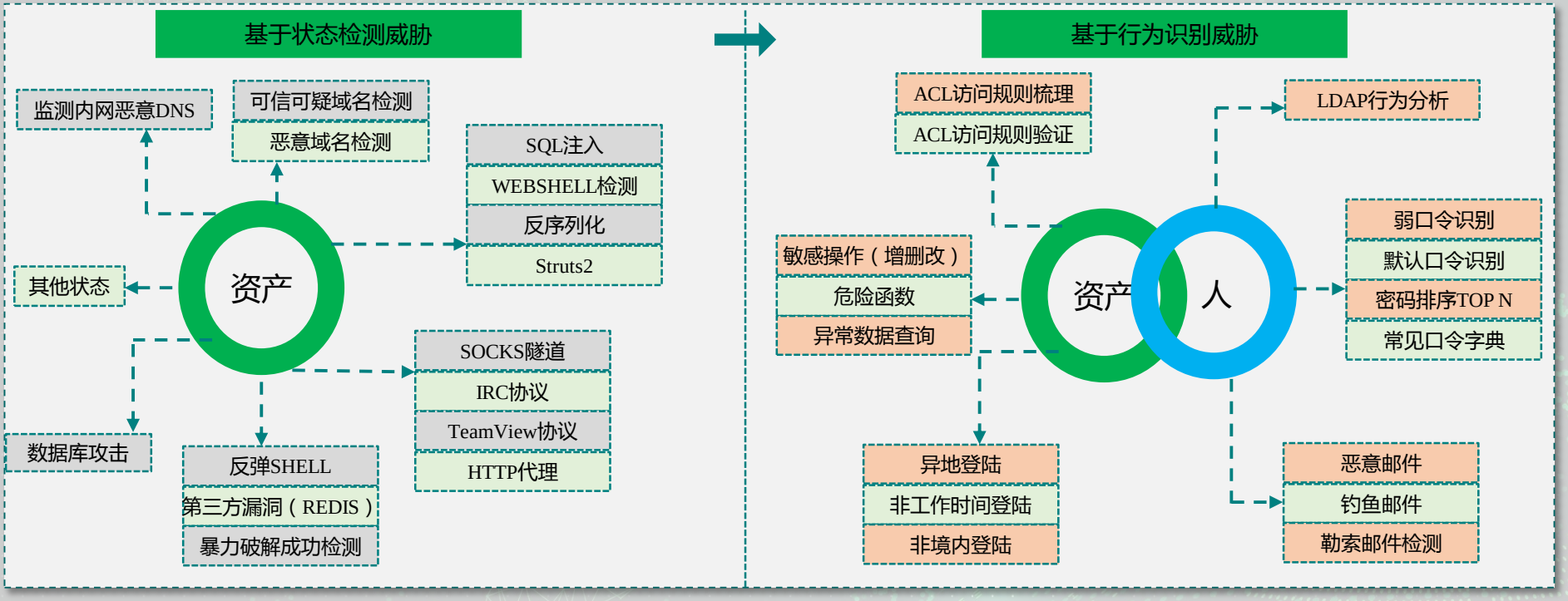
安全大数据在应急响应中的应用场景

场景一： 检测阶段



安全大数据在应急响应中的应用场景

场景二： 分析阶段



持续检测能力

通过工具，协助客户缩短内部安全检测发现的周期，提升客户安全事件的持续检测能力。

分析研判能力

采用攻击专家模型对流量深度分析，提升客户对安全事件的分析和研判能力

可监控能力

通过工具的自动化和可视化，提升客户对安全事件监控能力。

安全大数据在应急响应中的应用场景

场景三： 处置阶段

影响范围

- 除了告警发现的机器之外，还有哪些机器可能中招的？
- 当前发现的线索是否可以拓展，从而发现其它的潜在威胁？

终端定位

- 如果客户端没有装终端管控之类的软件，那么怎么找到受害者机器的所属人员信息？

处置措施

- 针对发现的问题，采用哪种方式的处置措施？这样的处置是否会对系统带来其它影响？

安全大数据在应急响应中的实践

安全大数据在应急响应中的实践-WannaCry

“永恒之蓝”勒索病毒事件

蠕虫不但破坏大量高价值数据，而且直接导致很多公共服务、重要业务无法正常开展。

高校、加油站、火车站、自助终端、邮政、医院、出入境签证、交通管理、政府办事等多机构瘫痪。

安全大数据在应急响应中的实践-WannaCry

安全大数据在应急响应中的实践-WannaCry

72小时会战

- **1500+安全应急响应人员**
  - 安全工程师上门紧急响应
- **1700+客户机构的现场支持**
  - 现场支持，重点是监管机构、一级部位、大型央企、大型金融机构客户
- **2000+客户机构的电话支持**
- **5000+工具U盘或光盘**
- **9个版本安全预警通告**
- **7个安全修复指南文档**
  - 操作指南、事件百问、开机手册等
- **6个安全软件修补工具**
  - 涵盖补丁、扫描、修复、解密多类别工具
- **人均睡眠时间<4小时**

永恒之蓝勒索蠕虫响应时间线

2017年3月15日	360针对旧操作系统（XP/2003/Win8）开始推送补丁。
2017年4月14日	黑客组织“影子经纪人”公开放出“永恒之蓝”攻击程序。
2017年4月15日—19日	360发布漏洞预警、蠕虫预警和独家免疫工具。
2017年4月27日	360首次监测到“永恒之蓝”用于传播勒索病毒“洋葱“。
2017年5月12日 13:00	360首次监测到勒索病毒wannacry1.0大规模爆发。
2017年5月13日 15:00	360开始推送针对“永恒之蓝”的修复补丁。
2017年5月14日 02:00	360全球首发勒索病毒恢复工具和自救教程。
2017年5月14日 14:39	360发布《周一安全开机保障指南》。
2017年5月14日 17:00	360首发离线救灾包一键解决勒索病毒感染和免疫问题。
2017年5月14日 20:00	360监测到勒索蠕虫病毒wannacry2.0版本开始传播。
2017年5月15日 13:00	360全球首发“永恒之蓝”热补丁。
2017年5月18日 11:54	360发布“勒索病毒文件恢复工具2.0”。
2017年5月19日 16:12	360发布“勒索病毒解密工具”。

安全大数据在应急响应中的实践-WannaCry

时间轴

早期感染阶段

5月12日 15:20，我们看到了首个访问开关域名的DNS请求。此时的域名解析是不成功的，自然无法访问到目标网页，机器一旦感染蠕虫，就会发作。

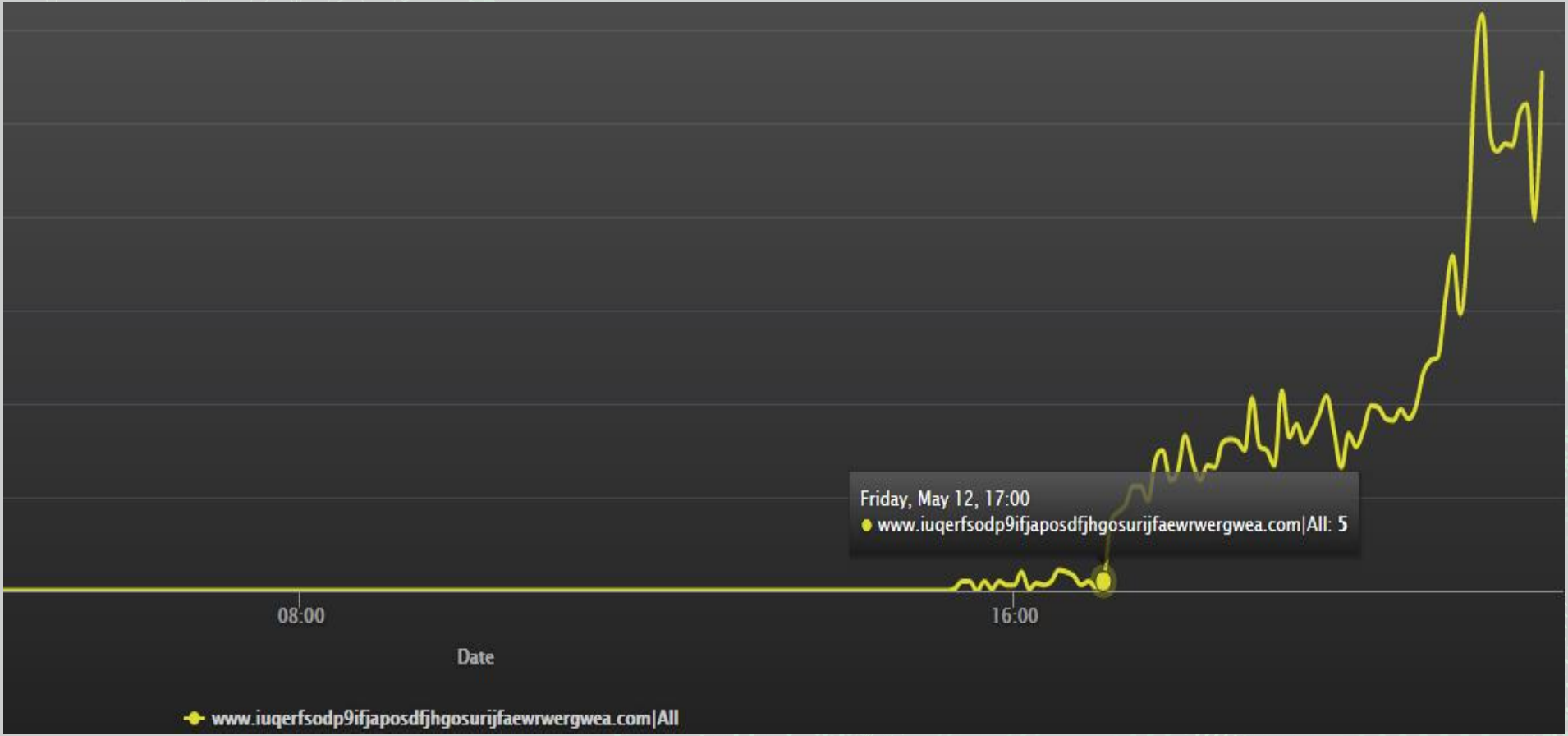
域名压制阶段

开关域名于周五23:30左右上线，开始了对WannaCry的压制，压制域名虽然最早于23:30左右上线，但是这个案例中还需要大约30分钟才能让全网所有节点都能感知到。

平稳控制阶段

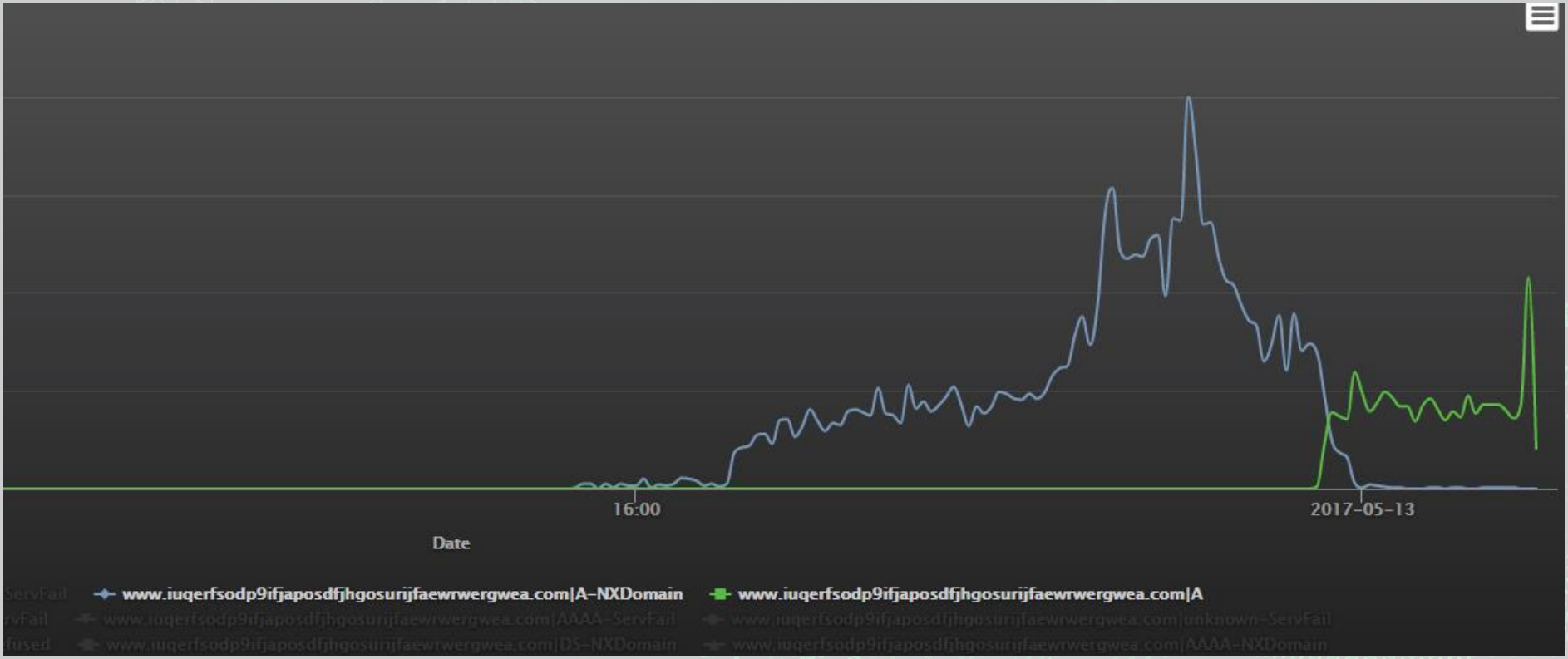
NXDOMAIN被压制以后，过度到了平稳控制阶段。在这个阶段，一方面，微软补丁更新和安全社区的共同努力减少了感染机器的数量；另一方面，总有机器因为各种原因被新增感染。总体而言，总感染量处于动态平衡状态，并且会随着时间推移最终平稳下降。

安全大数据在应急响应中的实践-WannaCry



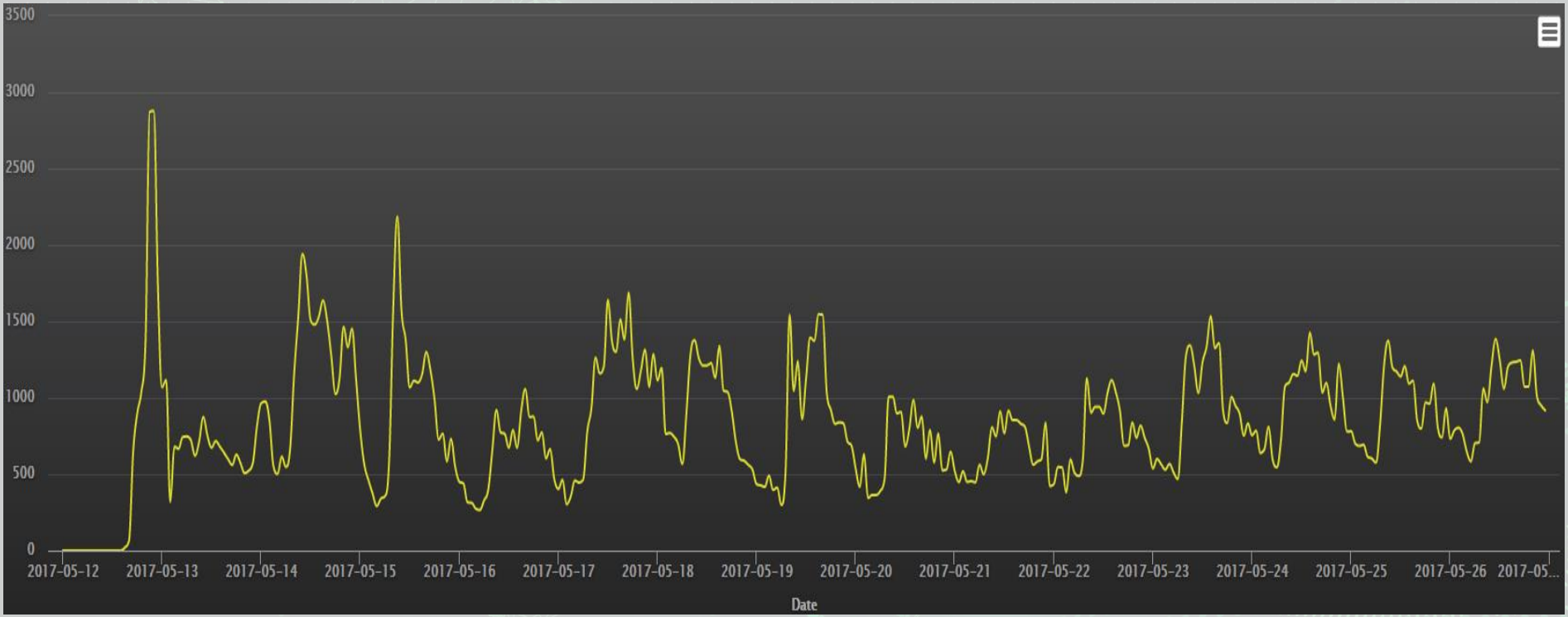
早期感染阶段

安全大数据在应急响应中的实践-WannaCry



域名压制阶段

安全大数据在应急响应中的实践-WannaCry

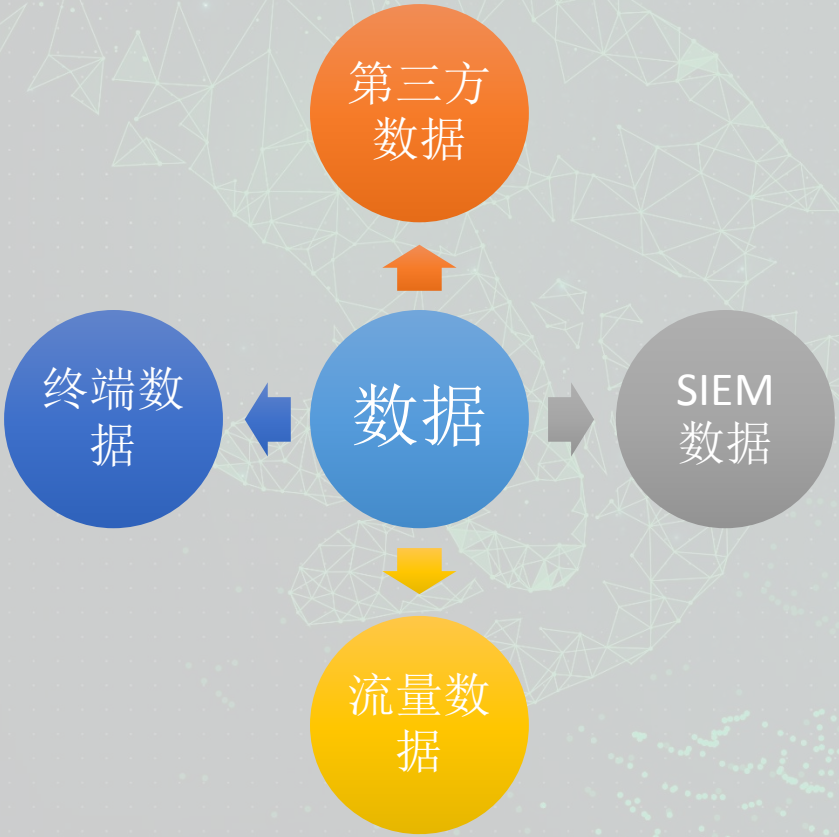


平稳控制阶段

企业如何提升应急响应能力

企业如何提升应急响应能力

应急响应到底需要哪些数据？



流量数据

- DNS
- HTTP/WEBMAIL、FTP
- SMTP/POP3/IMAP
- SMB
- ORACLE/MYSQL/SQLSERVER
- LDAP/SSL

终端数据

- 进程日志
- 杀毒日志

SIEM数据

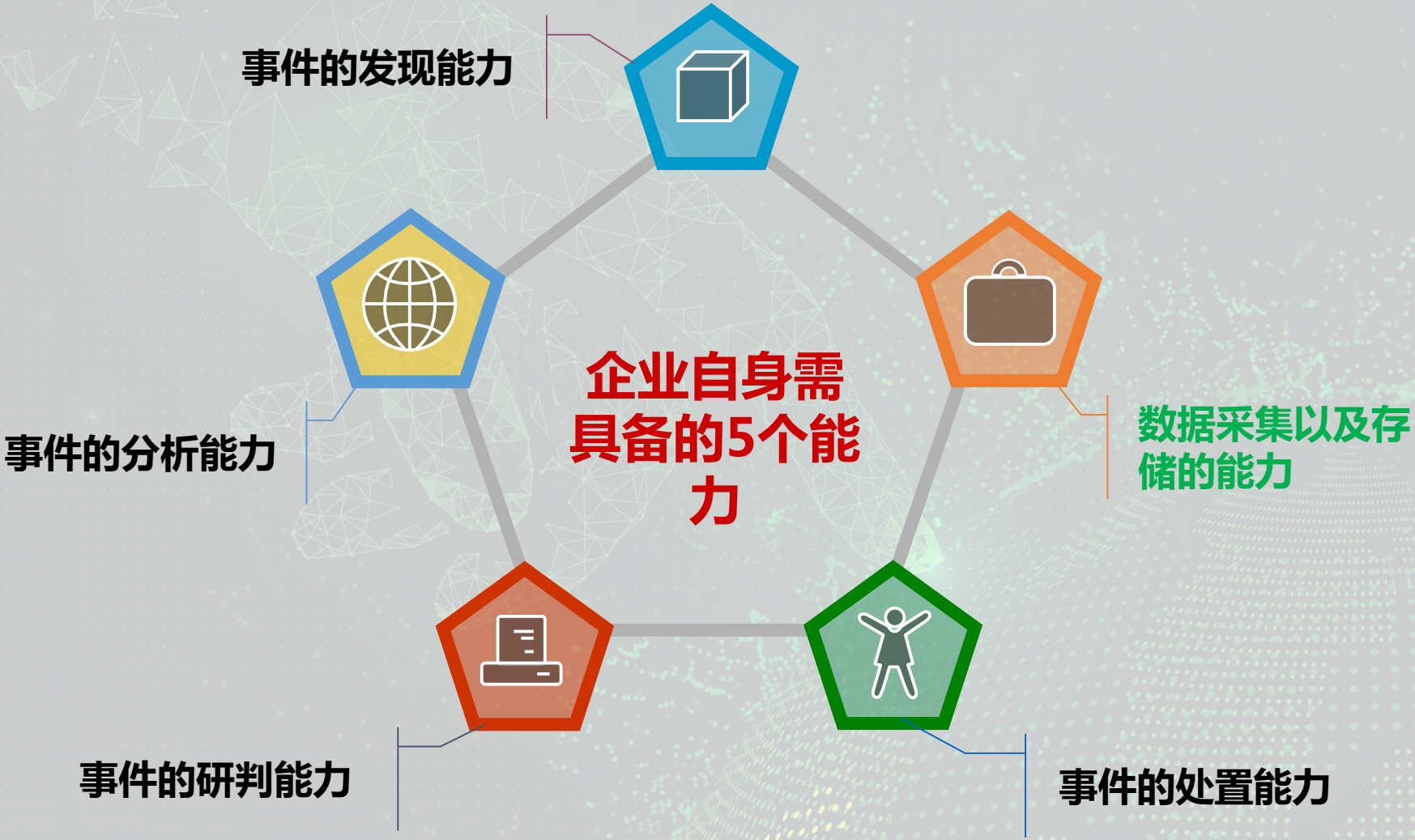
- 网络设备日志
- 主机日志
- WEB应用日志

第三方数据

- 威胁情报数据

企业如何提升应急响应能力

企业需具备的能力



企业如何提升应急响应能力

谢　谢

中国互联网安全大会

360互联网安全中心