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

态势感知中的威胁情报

韩志立
zenmind
360威胁情报中心

ISC 2017 中国互联网安全大会

360互联网安全中心

目录

态势感知

- 概述
- 关键因素
- 关键技术

态势感知历史发展

20世纪80年代 美国空军

分析空战环境信息，快速判断当前及未来形势并做出正确反应开始态势感知的研究

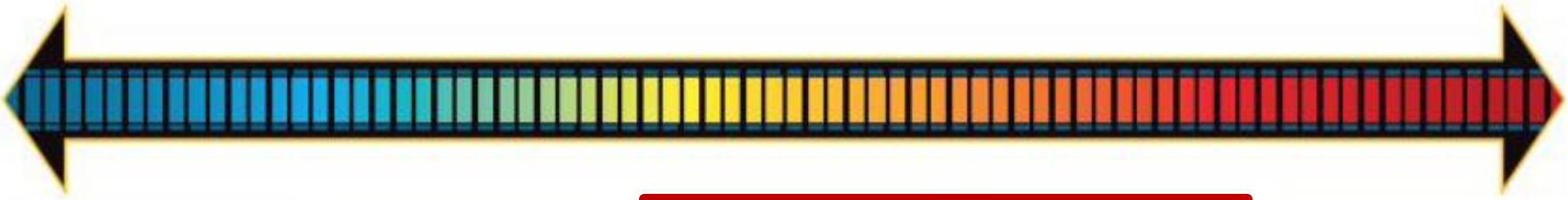
20世纪90年代 进入信息安全领域

在一定的时间和空间范围内，对组织的安全态势及其威胁环境的***感知***。***理解***这两者的含义以及意味的风险，并对他们未来的状态进行***预测***。

2016.4.19

全天候全方位感知网络安全态势。。。感知网络安全态势是最基本最基础的工作···要建立统一高效的网络安全***风险报告机制***、***情报共享机制***、***研判处置机制***，准确把握网络安全风险发生的规律、动向、趋势

态势感知兴起时建设阶段的必然

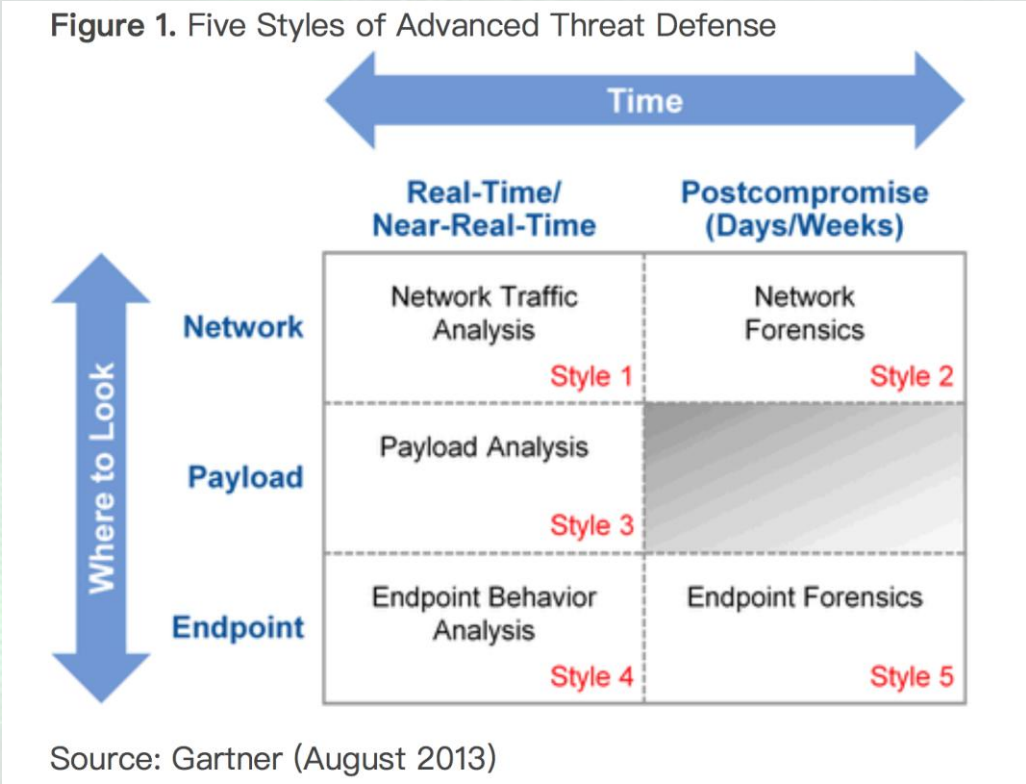


架构安全	被动防御	积极防御	情　报	进　攻
在系统规划、建设和维护的过程中充分考虑安全防护	在无人介入情况下，附加在系统架构上可提供持续威胁防御或威胁洞察的系统	分析人员对处于防御网络中的威胁进行监控、响应、学习和应用知识的过程	收集数据，将数据利用转化为情报，并将信息生产加工	对抗攻击者进行法律反制措施、自卫反击行为
自身足够强壮	提高攻击门槛，将大多数攻击拒之门外	发现有针对性攻击或者未知的攻击面、防御弱点	对对手有足够的了解，产生针对性的情报	威慑与反制

安全态势感知

关键要素——全天候、全方位

1. 基于流量特征的实时检测；（WAF、IPS、NGFW等）
2. 基于流量日志的异常分析机制；（流量传感器、Hunting、UEBA）
3. 针对内容的静态、动态分析机制；（沙箱）
4. 基于终端行为特征的实时检测；（ESP）
5. 基于终端行为日志的异常分析机制；（EDR、Hunting、UEBA）



关键要素：态

态

全局角度看到的现状

1. 是真实的攻击吗，是否可能误报，是否把扫描识别为真实攻击？
2. 是什么性质的攻击，定向或者随机？
3. 可能的影响范围和危害？
4. 缓解或者清除的方法及难度？
5. 重要的事件都体现出来了吗？

关键要素：势

势

未来可能的事件或状态

基于情报分享和情报分析

1. 是新的攻击团队还是已知团伙；
2. 攻击者的意图；
3. 攻击者的技战术水平及特点；
4. 是否属于一次大型战役的一部分；

关键技术分析

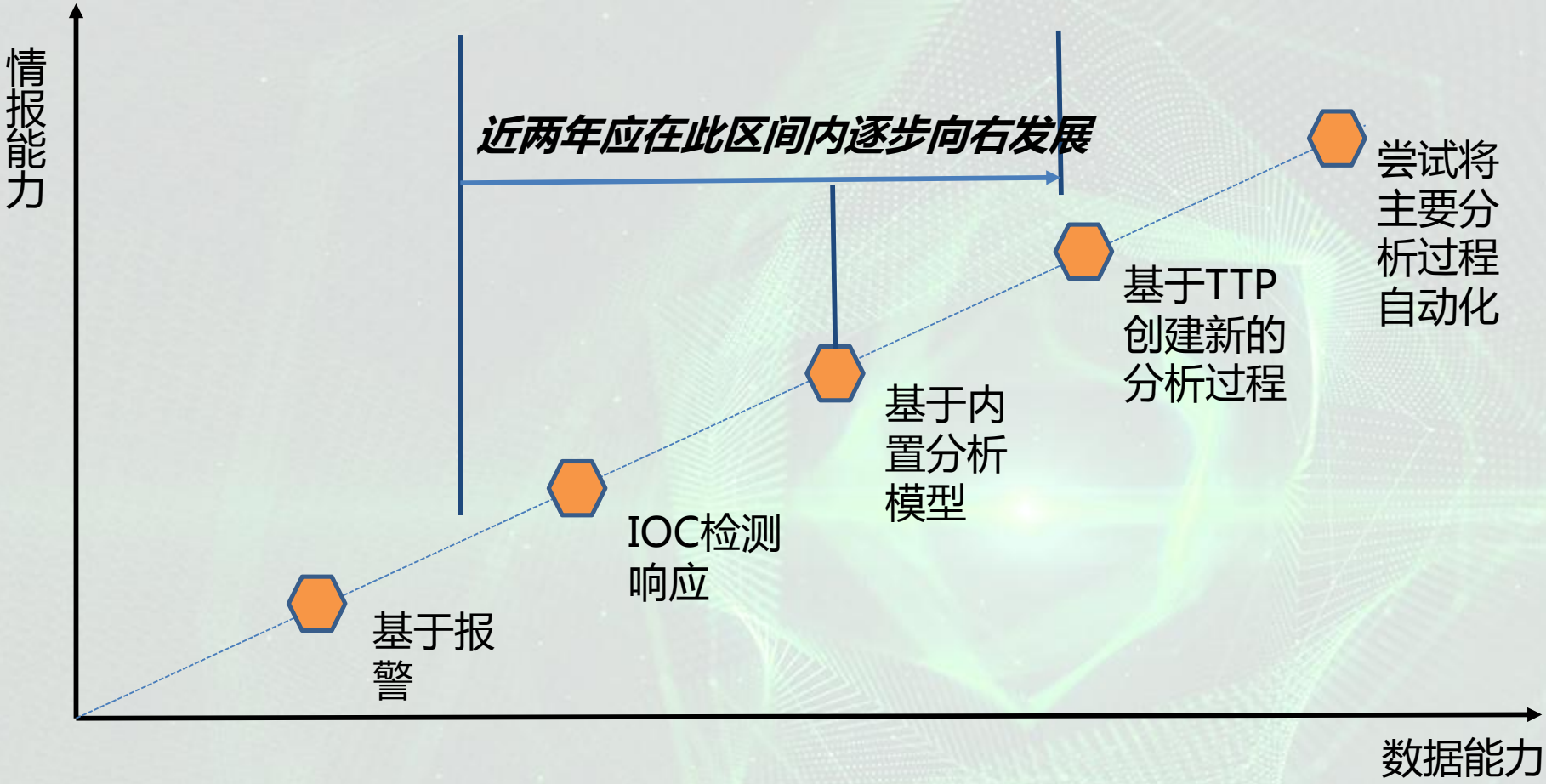
PALANTIR 的观点

1. THE DATA COMES FROM MANY DISPARATE SOURCES
2. THE DATA IS INCOMPLETE AND INCONSISTENT
3. YOU’RE LOOKING FOR SOMEONE OR SOMETHING THAT DOESN’T WANT TO BE FOUND, AND THAT CAN ADAPT TO AVOID DETECTION.

误判与机器学习

- **传统侦测误判率**
  - 1/10,000,00
- **机器学习误判率**
  - 1/1,000 ~ 1/10,000
- **扫描计算机里的所有档案?**
  - 1只恶意软件VS 20,000个良性软件➔ **1正判/2~20误判**
- **扫描所有的下载文件?**
  - 1只恶意软件VS 100个良性软件➔ **1正判/0.1~0.01误判**

关键技术分析


情报能力
近两年应在此区间内逐步向右发展
基于报警
IOC检测响应
基于内置分析模型
基于TTP创建新的分析过程
尝试将主要分析过程自动化
数据能力

ISC 2017 中国互联网安全大会

360互联网安全中心

目录

威胁情报

- 检测中的作用
- 事件响应中的作用
- 预警、预防

检测环节的威胁情报——MRTI

- **失陷检测情报**

有关APT事件、木马后门、僵尸网络、黑客工具使用的远控服务器信息

- **文件信誉**

利用云端更多检测机制对文件的综合判定信息，包括是否恶意、恶意类型、家族信息、C2地址等

- **IP信誉**

已知恶意IP（扫描、撞库等）、IP白名单（不同类型的网关）、IP的上下文（事件历史、开发端口、OS、应用、基本属性等）

响应环节的威胁情报——威胁分析平台

报警研判

360威胁情报中心 web.thoitietvietnam.org 简体中文

web.thoitietvietnam.org

APT CVE-2012-0158 RTF

流行度	☆ ☆ ☆ ☆ ★
动态域名	否
隐私保护	是
白名单	否
创建时间	2016/07/25
更新时间	2017/03/14
过期时间	2019/07/25
最近看到	2017/09/01

相关安全报告：

没有数据

高级可视化分析

威胁情报 3 | 域名解析 6 | 注册信息 2 | 关联域名 4 | 定制搜索

开源情报

情报源	最近看到	威胁类型
OSINT	2017/08/29	MALWARE SITE
SKYEYELABS	2017/06/09	C2

相关样本

样本HASH	最早看到	最近看到	恶意类型	家族信息
FD95AC4545273B0AA1D87EDFB9251B2C	2017/08/22	2017/08/23	黑市工具	RTF-OBFSSTRM

关联URL 没有数据

可视化分析

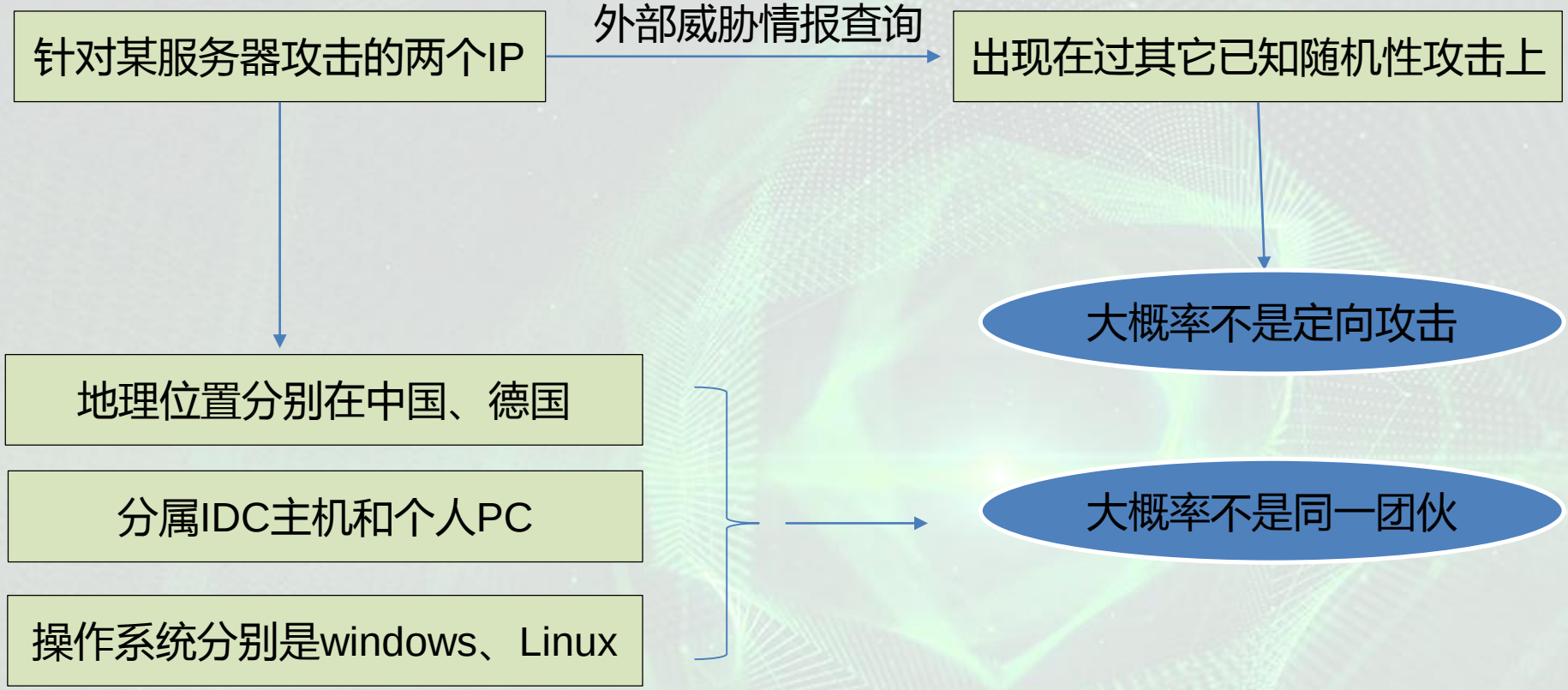
域名：web.thoitietvietnam.org

响应环节的威胁情报——威胁分析平台

攻击定性

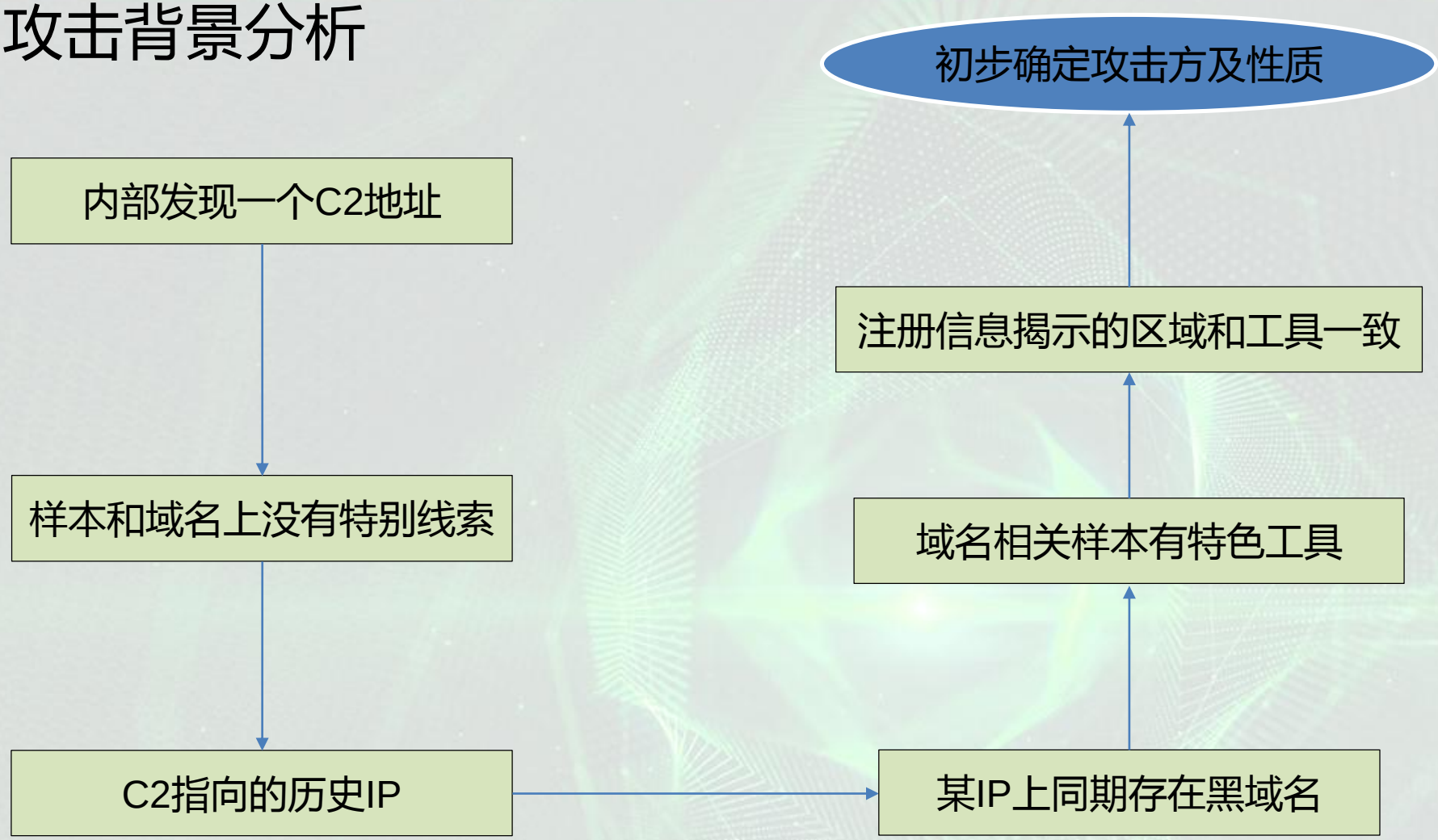
响应环节的威胁情报——威胁分析平台

攻击优先级分析



响应环节的威胁情报——威胁分析平台

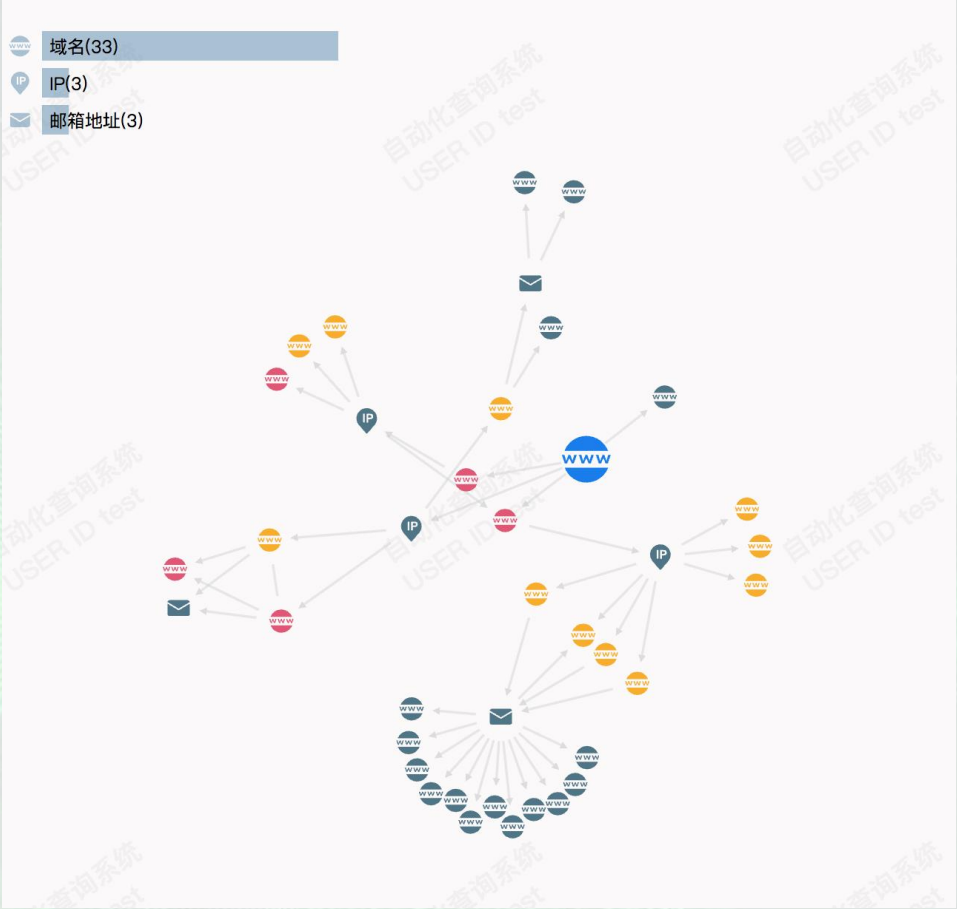
攻击背景分析



响应环节的威胁情报——威胁分析平台

自动化关联分析演示

https://ti.360.net/analyse?type=domain&value=web.thoitietvietnam.org



预警预防——TTP情报

- 攻击事件分析 / 预警
- 恶意样本分析 / 预警
- 漏洞分析建议 / 预警
- 关键性内容：

1. 危害
1. 影响范围
2. 机制
3. 检查和防范措施

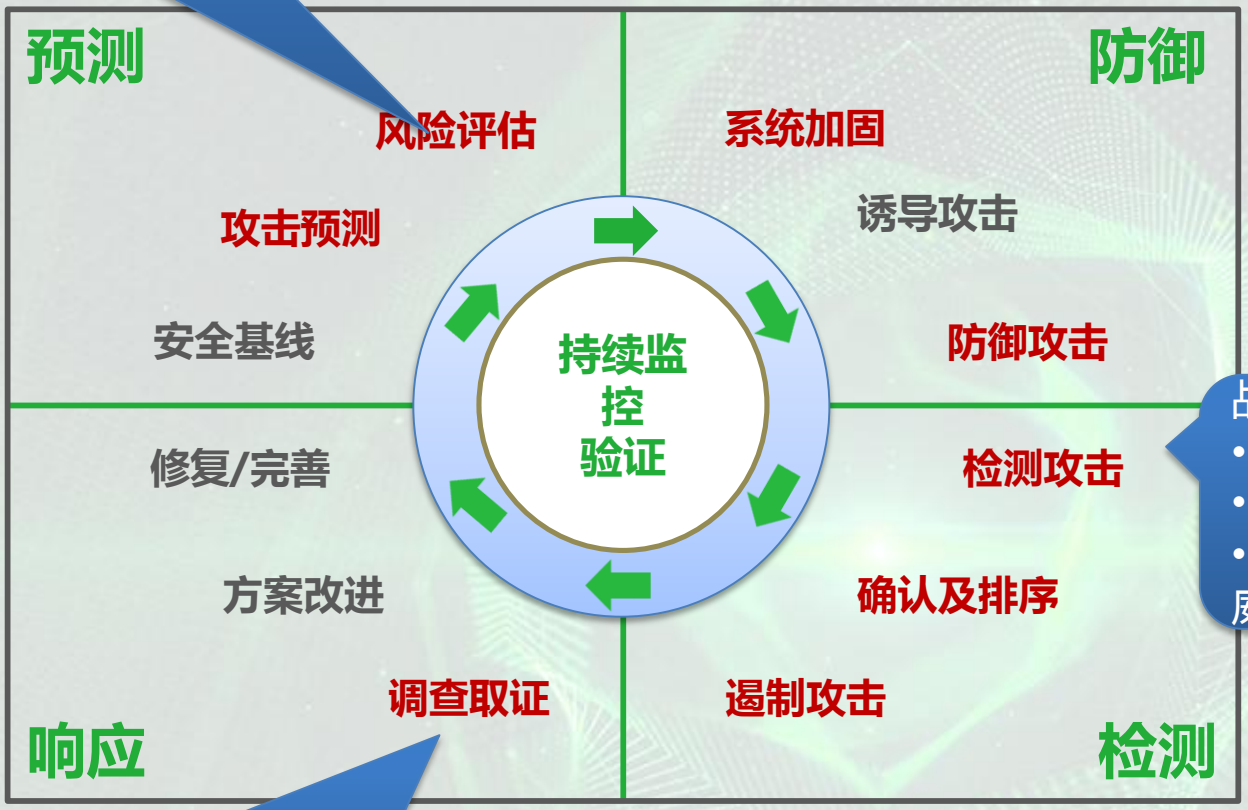
Xshell事件

FireBall 事件

供应链安全分析报告

威胁情报全景

运营情报TTP
- 攻击事件分析 / 预警
- 恶意样本分析 / 预警
- 漏洞分析建议 / 预警



战术情报
- IOC
- IP信誉
- 文件信誉

威胁分析平台

- 威胁分析平台

小结

威胁情报是现阶段保障态势感知项目实效，最有力的工具

多种类型的威胁情报保障安全生命周期全过程

关联分析平台的作用不仅是攻击溯源，可以通过多种方式对攻击进行定性分析

360威胁情报中心

研究类网站： HTTPS://TI.360.NET/BLOG/

分析平台: HTTPS://TI.360.NET

微信公众号:360威胁情报中心

谢　谢