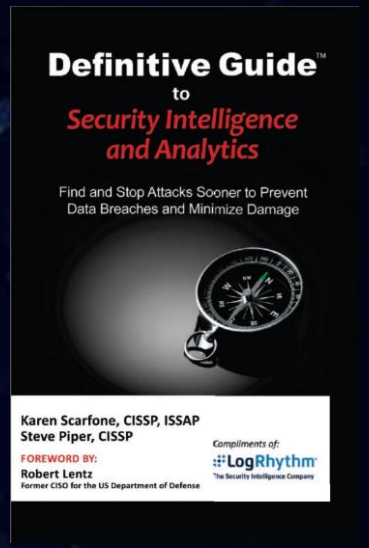
威胁情报--从IOC命中到安全分析的“催化剂”

张嵩

华泰证券 安全总监

一路走过来的威胁情报“玩法”

- **始于**：AWS大会的一次演讲，金融行业最早的一批玩家
- **1.5年+**：从使用盒子内置TI，一路到自主搭建、研发安全分析“产品”
- **一路上**：实践了一年LogRhythm Matrix Security Intelligence Maturity Model—MTTD/MTTR



1.0 盒子告警的被动阶段

NGFW内置的IOC告警：如C家的Anti-bot，P家的spyware威胁分类

网络审计盒子内置的IOC告警：如盒子厂家们纷纷宣称可以检测高级威胁

2.0 熟悉第三方IOC、信誉和PDNS查询的懵懂阶段

手工信誉查询：x.threatbook, deepsight, senderbase， 360TI… …

IOC下载到网络监控分析平台，识别出站流量中的攻陷主机，然而… …

3.0 对Security Analytics的持续探索阶段

RSA2017上关键字，Gartner TI报告，书，国外厂商白皮书，Google it

Gartner：Demystifying Security Analytics; SANS：Security Analytics Survey

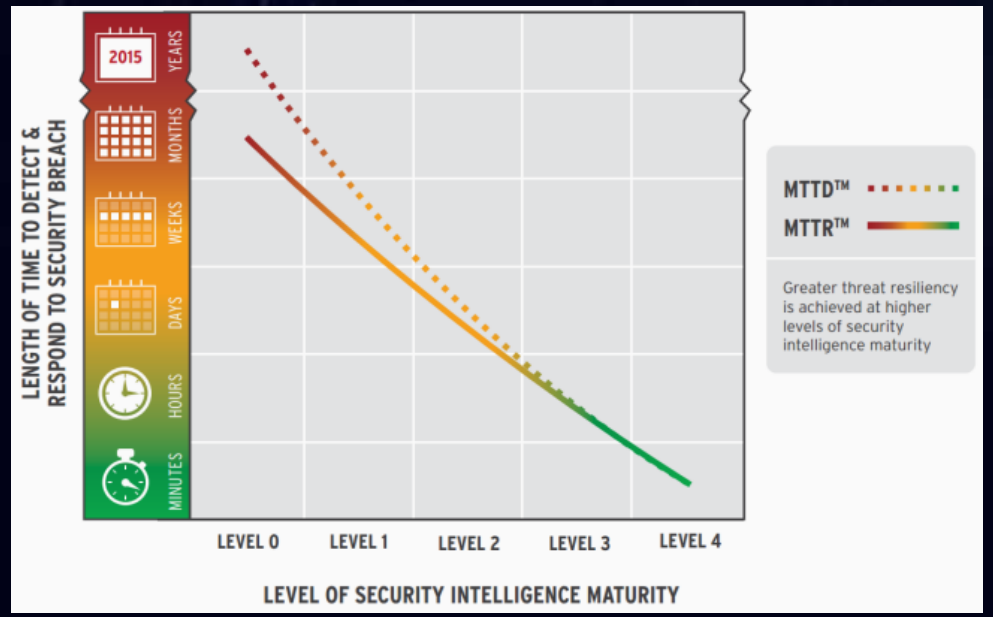
红蓝对抗演习中：和老司机们现场证明，“多家盒子的IOC也会侧漏”

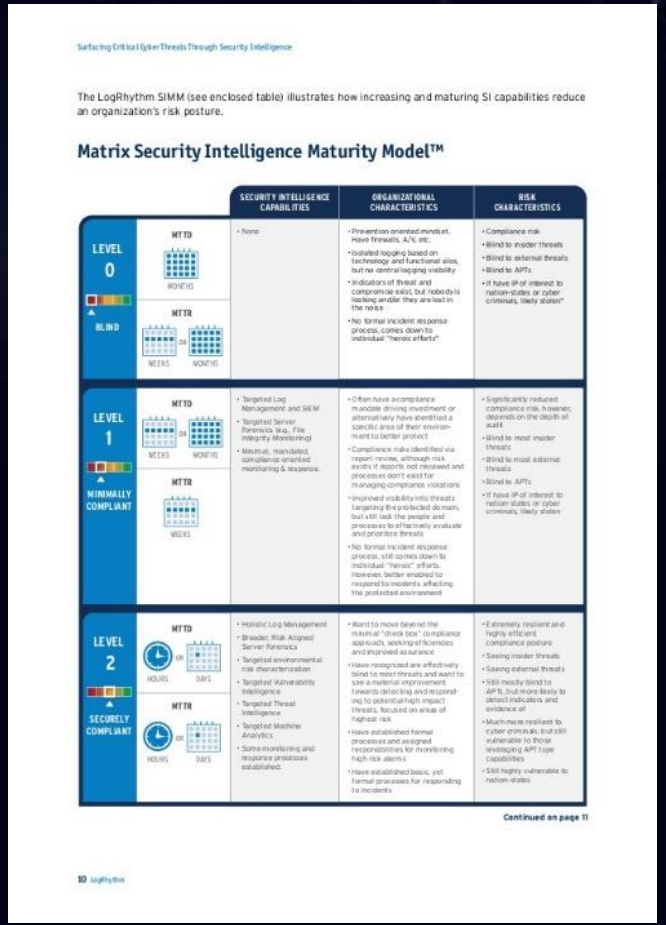
现在：多源威胁情报API

- 基于开源项目，自主搭建、研发**安全分析产品**
- 从依赖IOC作为告警指标，演变为TI是提升分析效率**催化剂**
- 开始使用ML等**AI**技术
- 从比对DNS到分析**EDR**数据
- **黑白灰分**级所有出站目标
- 积累**企业情报库**

安全分析—请不要上来就谈APT

- 终极目标：不是不出事儿，而是能力提升、MTTD，MTTR持续降低





Surfacing Critical Cyber Threats Through Security Intelligence

The LogRhythm SIMM (see enclosed table) illustrates how increasing and maturing SI capabilities reduce an organization's risk posture.

Matrix Security Intelligence Maturity Model™

		SECURITY INTELLIGENCE CAPABILITIES	ORGANIZATIONAL CHARACTERISTICS	RISK CHARACTERISTICS
LEVEL 0 — BLIND	MTTD: MONTHS; MTTR: WEEKS OR MONTHS	• None	• Prevention oriented mindset. Have firewalls, A/V, etc. • Isolated logging based on technology and functional silos, but no central logging visibility • Indicators of threat and compromise exist, but nobody is looking and/or they are lost in the noise • No formal incident response process, comes down to individual "heroic efforts"	• Compliance risk • Blind to insider threats • Blind to external threats • Blind to APTs • If have IP of interest to nation-states or cyber criminals, likely stolen
LEVEL 1 — MINIMALLY COMPLIANT	MTTD: WEEKS OR MONTHS; MTTR: WEEKS	• Targeted Log Management and SIEM • Targeted Server Forensics (e.g., File Integrity Monitoring) • Minimal, mandated, compliance oriented monitoring & response.	• Often have a compliance mandate driving investment or alternatively have identified a specific area of their environment to better protect • Compliance risks identified via report review, although risk exists it reports not reviewed and processes don't exist for managing compliance violations • Improved visibility into threats targeting the protected domain, but still lack the people and processes to effectively evaluate and prioritize threats • No formal incident response process, still comes down to individual "heroic" efforts. However, better enabled to respond to incidents affecting the protected environment	• Significantly reduced compliance risk, however, depends on the depth of audit • Blind to most insider threats • Blind to most external threats • Blind to APTs • If have IP of interest to nation-states or cyber criminals, likely stolen
LEVEL 2 — SECURELY COMPLIANT	MTTD: HOURS OR DAYS; MTTR: HOURS OR DAYS	• Holistic Log Management • Broader, Risk Aligned Server Forensics • Targeted environmental risk characterization • Targeted Vulnerability Intelligence • Targeted Threat Intelligence • Targeted Machine Analytics • Some monitoring and response processes established.	• Want to move beyond the minimal "check box" compliance approach, seeking efficiencies and improved assurance • Have recognized are effectively blind to most threats and want to see a material improvement towards detecting and responding to potential high impact threats, focused on areas of highest risk • Have established formal processes and assigned responsibilities for monitoring high risk alerts • Have established basic, yet formal processes for responding to incidents	• Extremely resilient and highly efficient compliance posture • Seeing insider threats • Seeing external threats • Still mostly blind to APTs, but more likely to detect indicators and evidence of • Much more resilient to cyber criminals, but still vulnerable to those leveraging APT type capabilities • Still highly vulnerable to nation-states

Continued on page 11

10

图来源: LogRhythm

MTTD: Mean Time to Detect
MTTR: Mean Time to Respond

单一厂商IOC的局限性 与 API Economy

吐槽单一来源IOC的局限性：

假设手中有100W条IOC，需要思考：

1. 来源质量、生成能力、生成效率、相对有效性
   - 购买 —国外买的适合国内，质量，失效？
   - 交换 —交换联盟机制真的运转有效？
   - 开源 —如何维护？失效率？质量？
   - 自主生成 —样本捕捉能力，生产效率？
   - 相对有效性 —外来IOC多大比例中国解析量很低？
2. IOC的存活期和失效率
   - IOC中有多大比例是DGA，多少是“未来”的IOC？
   - Sinkhole的IOC比例有多大？
   - 黑客继续使用静态IOC的方式会持续多久？
   - 一个（高级恶意程序）IOC域名的存活期？
   - 高级恶意程序会不会使用偏灰或背景干净的C2？
   - 厂商会清理T-N个月以前IOC？删掉的真的无效？

IOC动态有效率？

VS

设备的承载力？

畅想TI应用趋势：

自主，开放，解耦，混搭，API

- API化
- 多源化
- Auto-C2与云端能力
- 实时检测当下 + 追溯过去发生
- 从域名IOC为主的应用到综合使用各种情报元素以适应细分场景：
  IP的历史行为情报应用于入站
  终端与网络采集的样本Hash
- 建立针对企业特征的内部情报库
- 基于特征比对的传统TI形态降低
- 基于AI的分析能力替代静态域名

“后”IOC玩法：多源信誉情报API Vs 出站流量

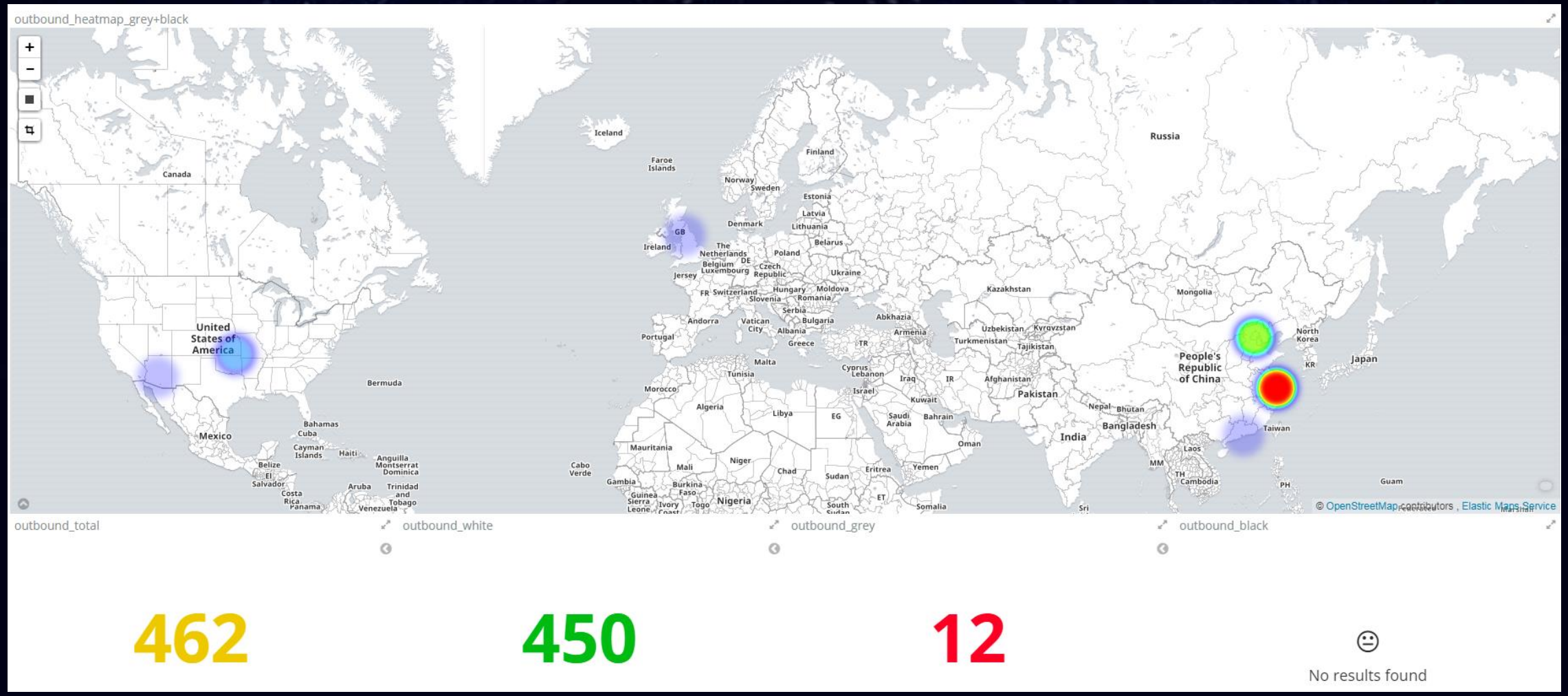
目标

1. 日内分析所有出站访问目的地的恶意度（黑灰白）
2. 动态分配有限资源的响应优先级
3. 应急恶意访问后，治理“随意”出站访问—白名单机制
4. 周期性根据最新的情报分析过去的出站访问历史
5. 企业深入理解和积累每一个独特的出站访问目的地

应用

1. 根据流量或者FW日志，获取每日实际出站连接的sip，dip，sport，dport，协议和服务，具体事件，数字证书等信息
2. Stack后，顺序调用一系列的“情报库”：1）企业必要的业务出站访问白名单；2）企业内部积累的情报库；3）2-3个优质情报源的信誉情报API
3. 协同N源API：1）N源都判定为白名单，即为白；2）任意源判定为黑（IOC），即为黑；3）其他的为灰；4）根据目的地恶意行为次数，累加恶意度，对灰进一步区分为偏白，纯灰，偏黑
4. 新增出站目的入库，连同情报信息
5. 定期将过去的访问stack后调用最新的情报后刷新企业情报库，并保存历史版本

“后”IOC玩法：多源信誉情报API Vs 出站流量



“后”IOC玩法：多源信誉情报API Vs 入站流量

几个可以优先关注的应用场景：

- 邮件的低频撞库—特征是一个僵尸网络源IP只撞1-2次
- 特权、业务后台的互联网访问入口
- 互联网认证页面
- 客户访问来源画像和风险提示
- 防御措施验证（扫描tag的IP校验in-line IPS有效性）
- WAF或WAF后攻击流量的攻击者画像

入站情报需结合应用日志，判断是否撞进门

“后”IOC玩法：企业的情报库

1. 理解企业所有的出、入站以及网络传输和主机新建进程等“背后的故事”
2. 入库保存每一次外部API调用后的结果，以便日后分析平台机器调用、人工查询
3. 企业对第三方多源情报数据的最终（针对性）判定
4. 行业威胁情报库和分享机制的基础

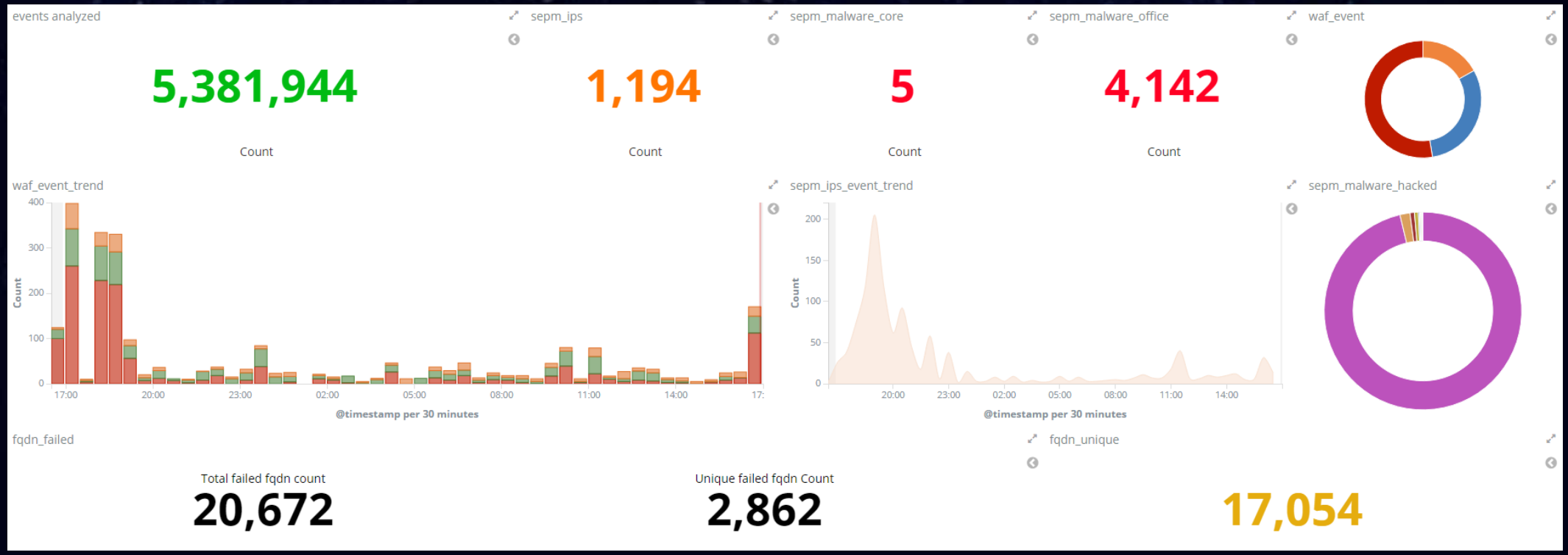
自主研发实现态势感知的产品—“泰坦”

安全可视化

攻陷前

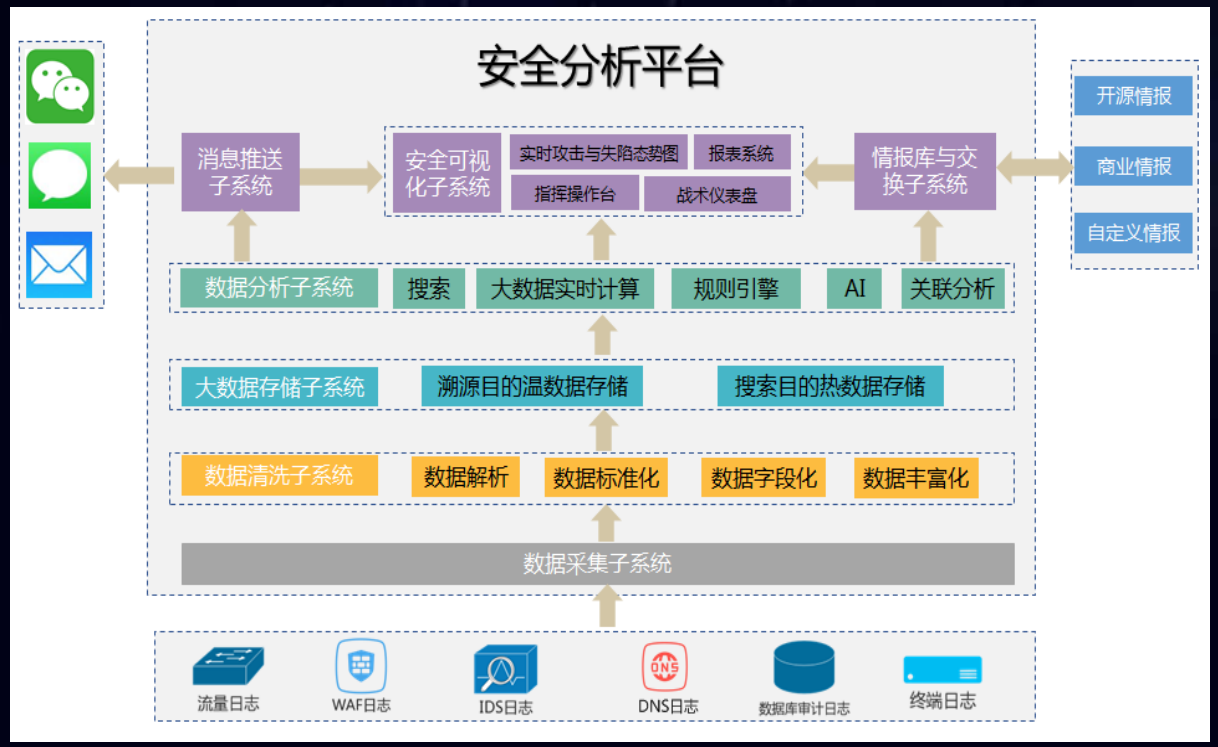
攻陷中

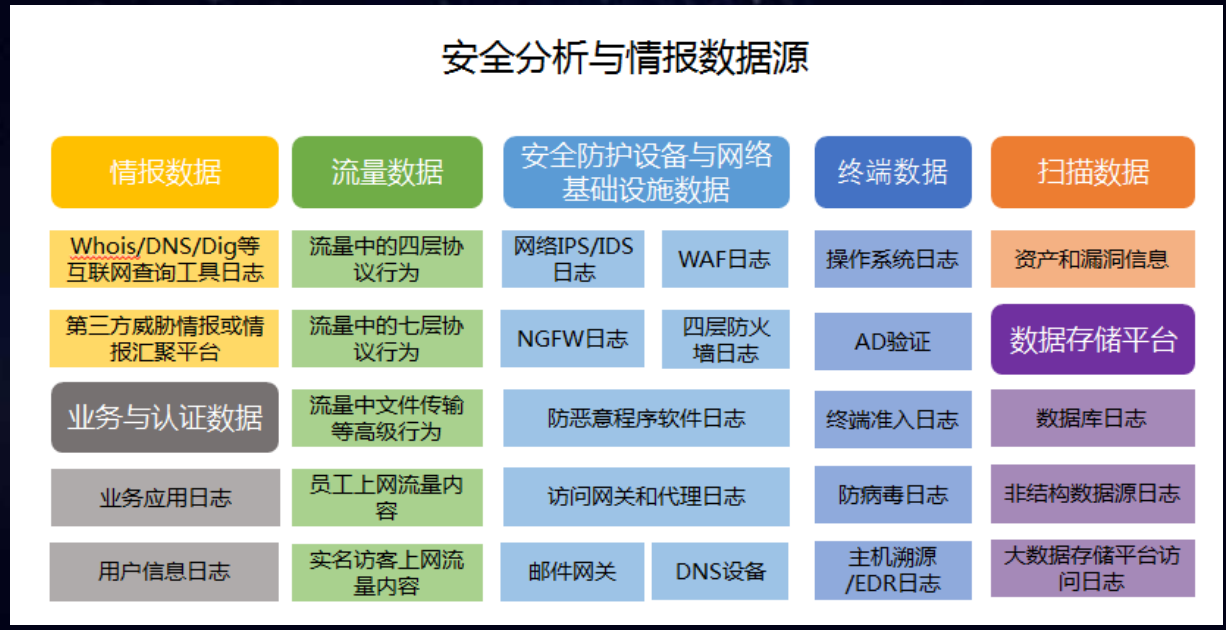
攻陷后



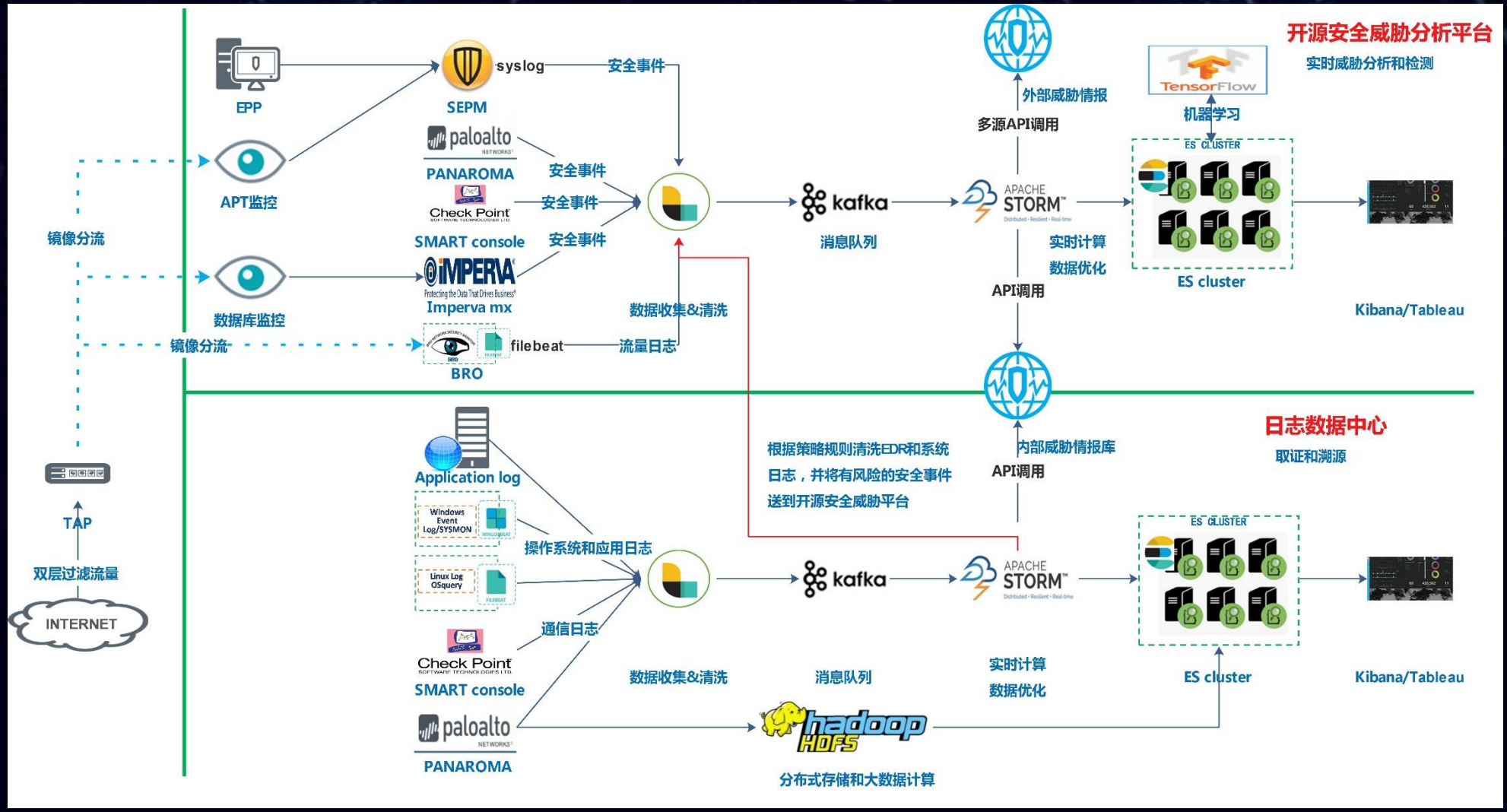
Sysmon采集Hash送多源API
实现基础EDR能力

安全分析平台功能架构与数据





演讲解耦题开放、混搭的安全分析“能力”



10个可实践的分析场景

攻陷前的“攻击态势”

1. 网络攻击的趋势分析与关联告警
2. 高风险应用的异常访问检测
3. 识别恶意程序的投递
4. 识别恶意程序的安装植入
5. “近地”高危攻击检测

攻陷中的“失陷态势”

1. 基于IOC比对和机器学习DGA识别的攻陷检测
2. 基于出站流量黑白灰化的攻陷检测

攻陷后的“响应态势”

1. 内部威胁检测与反欺诈
2. 横向Sysmon等EDR日志识别横向移动、内部渗透
3. 基于流量识别横向移动、内部渗透


谢谢！