WebRAY™

风声与暗算

如何在网络安全管理实践中利用威胁情报

远江盛邦（北京）网络安全科技股份有限公司

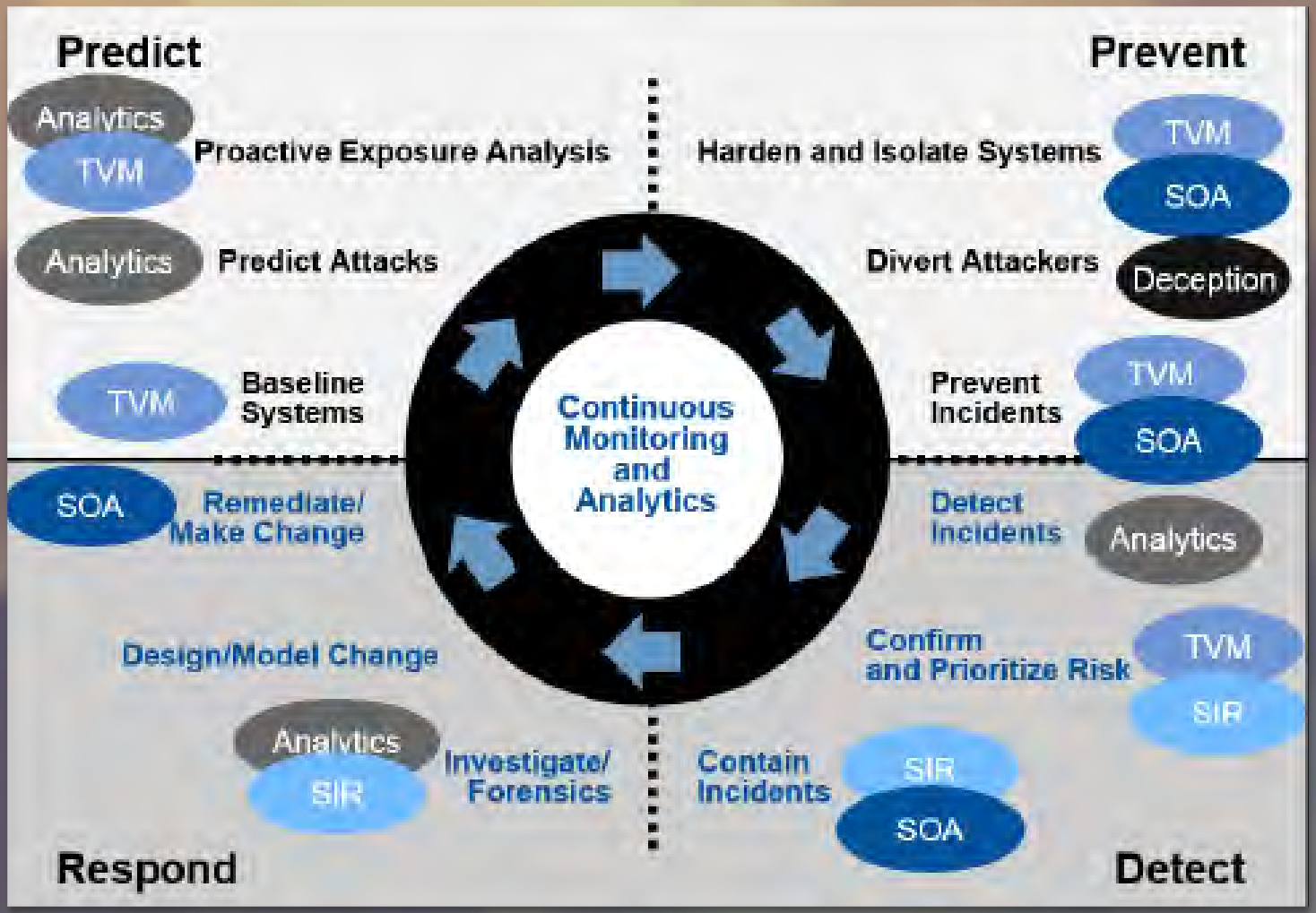
一个外国公司，一篇报告，把威胁情报带入前台

KEY FINDINGS

APT1 is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (总参三部二局), which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 (61398部队).

- The nature of "Unit 61398's" work is considered by China to be a state secret; however, we believe it engages in harmful "Computer Network Operations."
- Unit 61398 is partially situated on Datong Road (大同路) in Gaoqiaozhen (高桥镇), which is located in the Pudong New Area (浦东新区) of Shanghai (上海). The central building in this compound is a 130,663 square foot facility that is 12 stories high and was built in early 2007.
- We estimate that Unit 61398 is staffed by hundreds, and perhaps thousands of people based on the size of Unit 61398's physical infrastructure.
- China Telecom provided special fiber optic communications infrastructure for the unit in the name of national defense.
- Unit 61398 requires its personnel to be trained in computer security and computer network operations and also requires its personnel to be proficient in the English language.
- Mandiant has traced APT1's activity to four large networks in Shanghai, two of which serve the Pudong New Area where Unit 61398 is based.

预测--新一代安全防御体系



双轮驱动的威胁预警体系

威胁：
基本无法控制，只能尽量去了解，并做好防御准备。

漏洞：
基本属于可控制领域，没有漏洞就没有攻击。

威胁情报的正式的定义与预测

- "Threat intelligence" (TI) is evidence-based **knowledge** — including context, mechanisms, indicators, implications and actionable advice — about an existing or emerging menace or hazard to IT or information assets. It can be used to **inform decisions** regarding the subject's response to that menace or hazard.

- By 2018, **60%** of enterprises will utilize commercial threat intelligence services to help inform their security strategies.

• From GARTNER

威胁情报不是什么都能干

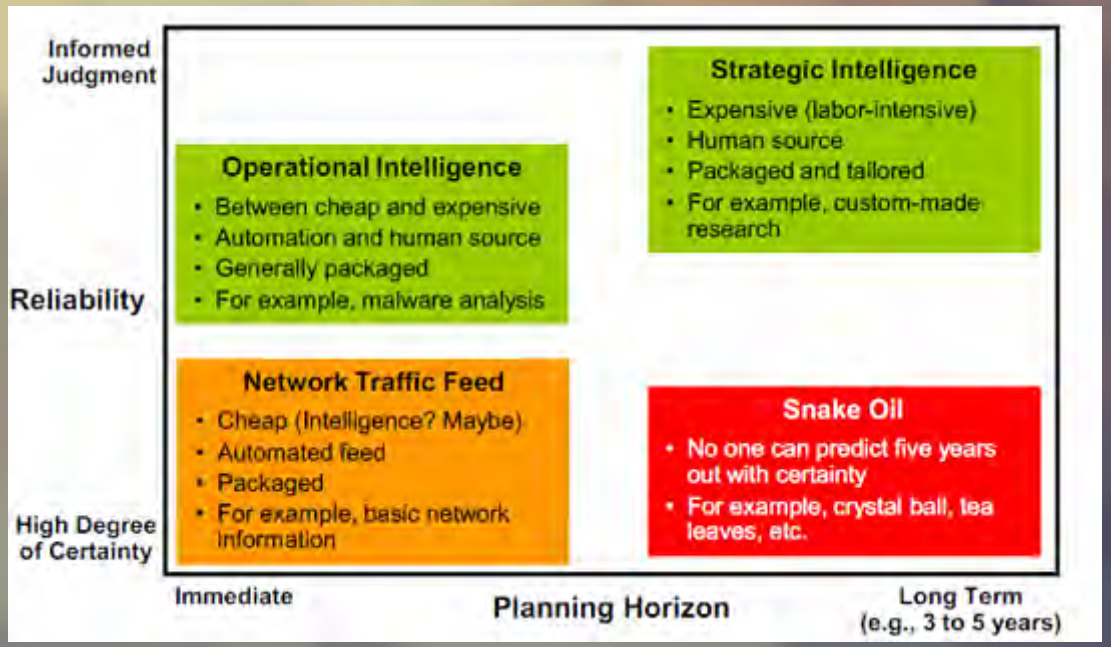
威胁情报给予了人们很多的想像空间，不过许多设想都过于飘渺。经过一段时期的验证，下面四个价值还是比较靠谱的：

1. 更加快速有效地发现和防御攻击（protection,detection）
2. 对可能发生的攻击进行提前预警（prediction）
3. 为安全管理和风险评估提供依据
4. 为安全架构的调整与设计提供依据

两大类威胁情报

- **战略型情报**
  - 人写的
  - 很贵
  - 回答一些较长期的，比较深刻的问题
  - 不确定性较高
  - 生产周期较长

- **战术型情报**
  - 机器生成，人工优化
  - 比较便宜
  - 回答眼下的一些技术性问题
  - 确定性很高
  - 生产周期很短



首先聚焦于可机读威胁情报（MRTI）

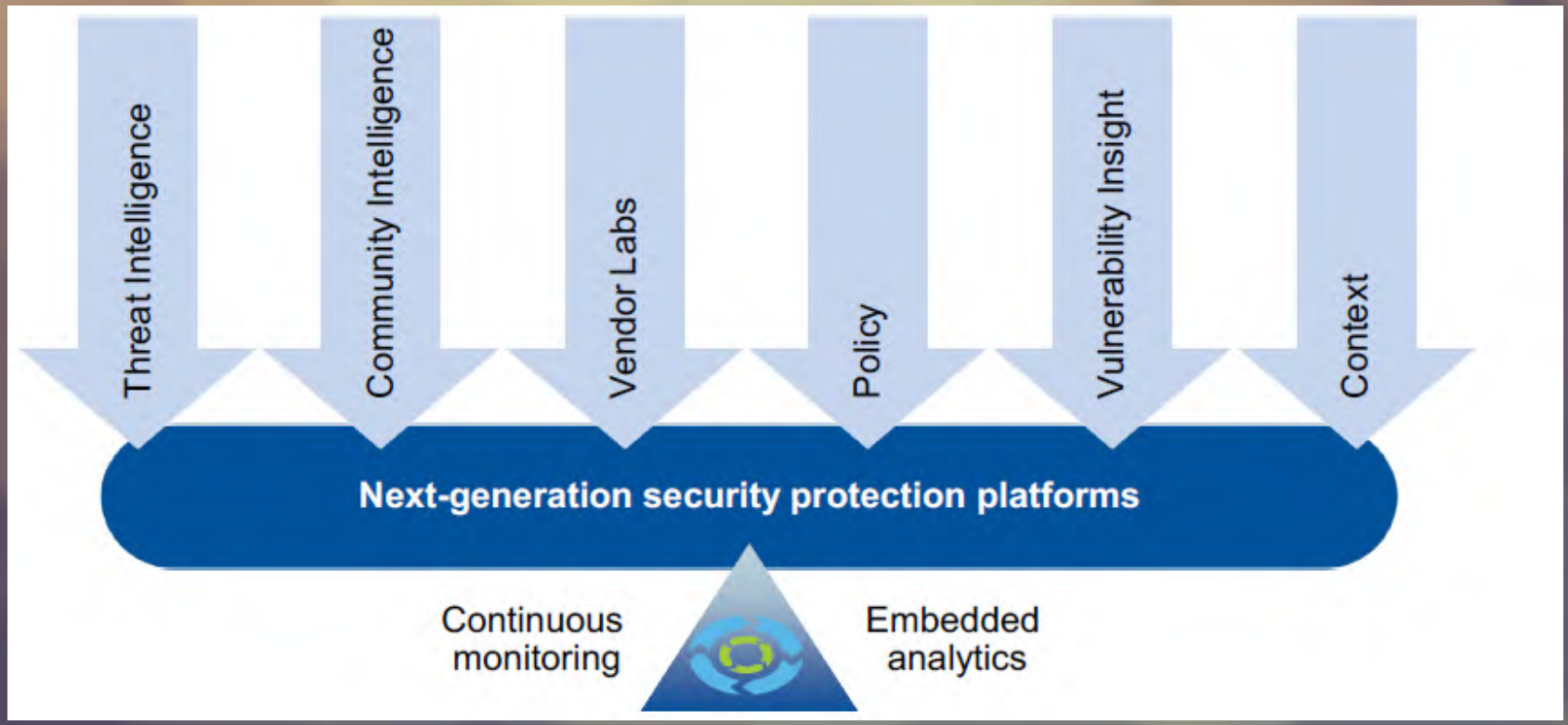
- 按标准格式进行描述的威胁情报
- 可以被安全设备读取
- 为现有安全策略提供“context”
- 可以有政府，第三方组织，行业协会，商业机构发布
- 是在安全防御体系中落地威胁情报的技术途径
- 在国外已经成为主流产品的必备能力

威胁情报标准

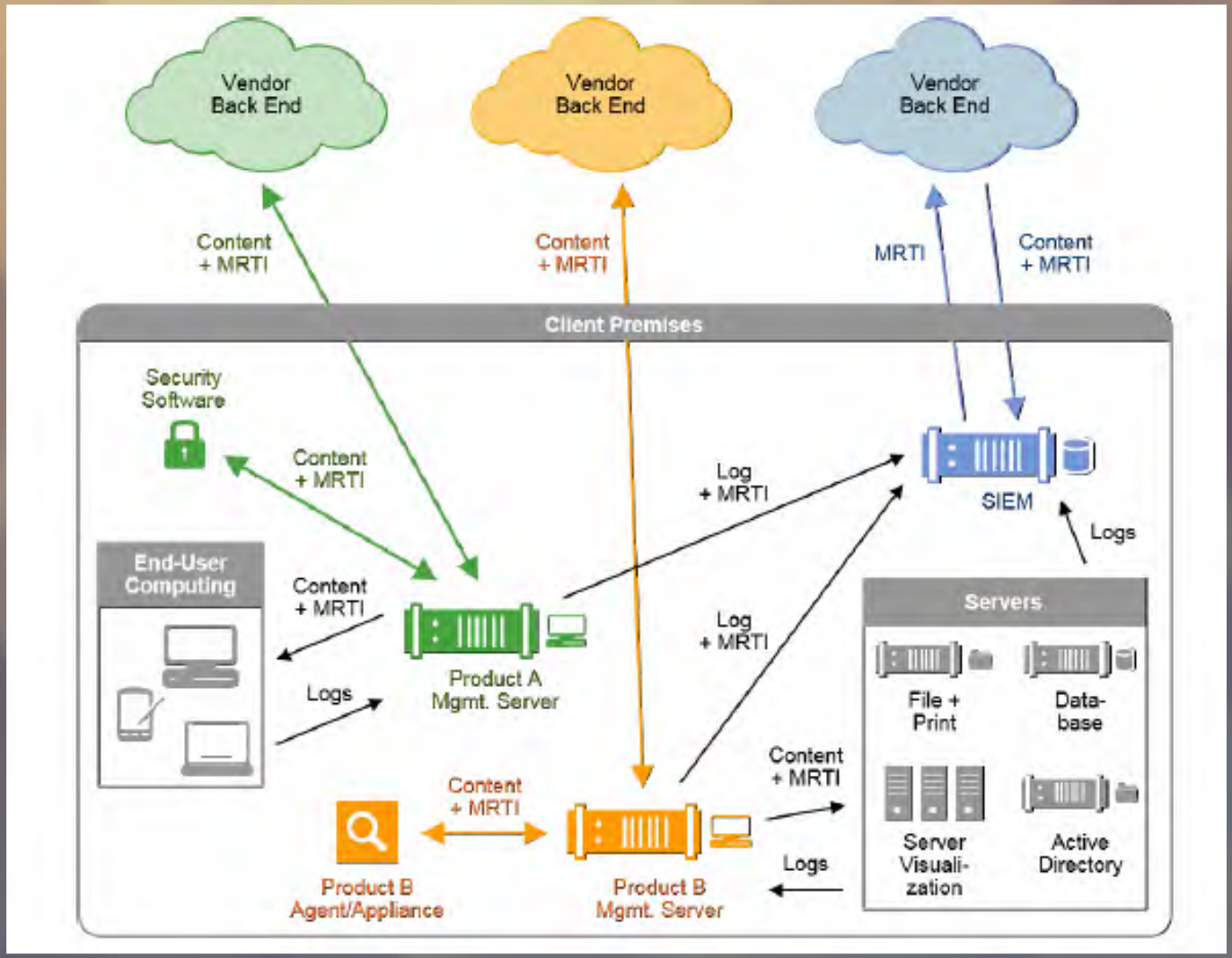
- STIX/TAXII:事实上的行业标准
  - STIX（Structured Threat Information eXpression）
    - 用于描述威胁信息
    - 现行标准1.2，2.0版本正在起草
  - TAXII(Trusted Automated eXchange of Indicator Information)
    - 用于交换威胁信息

- 国标正在起草中

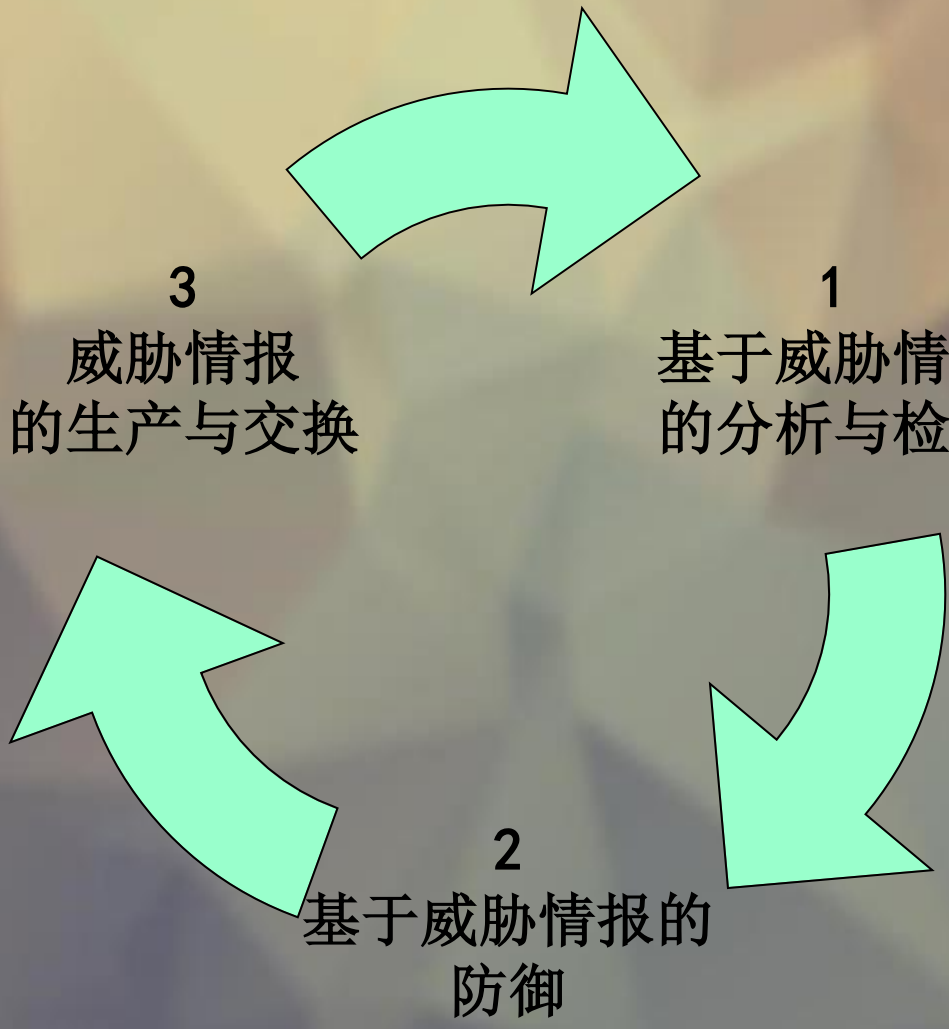
下一代安全平台的七种武器



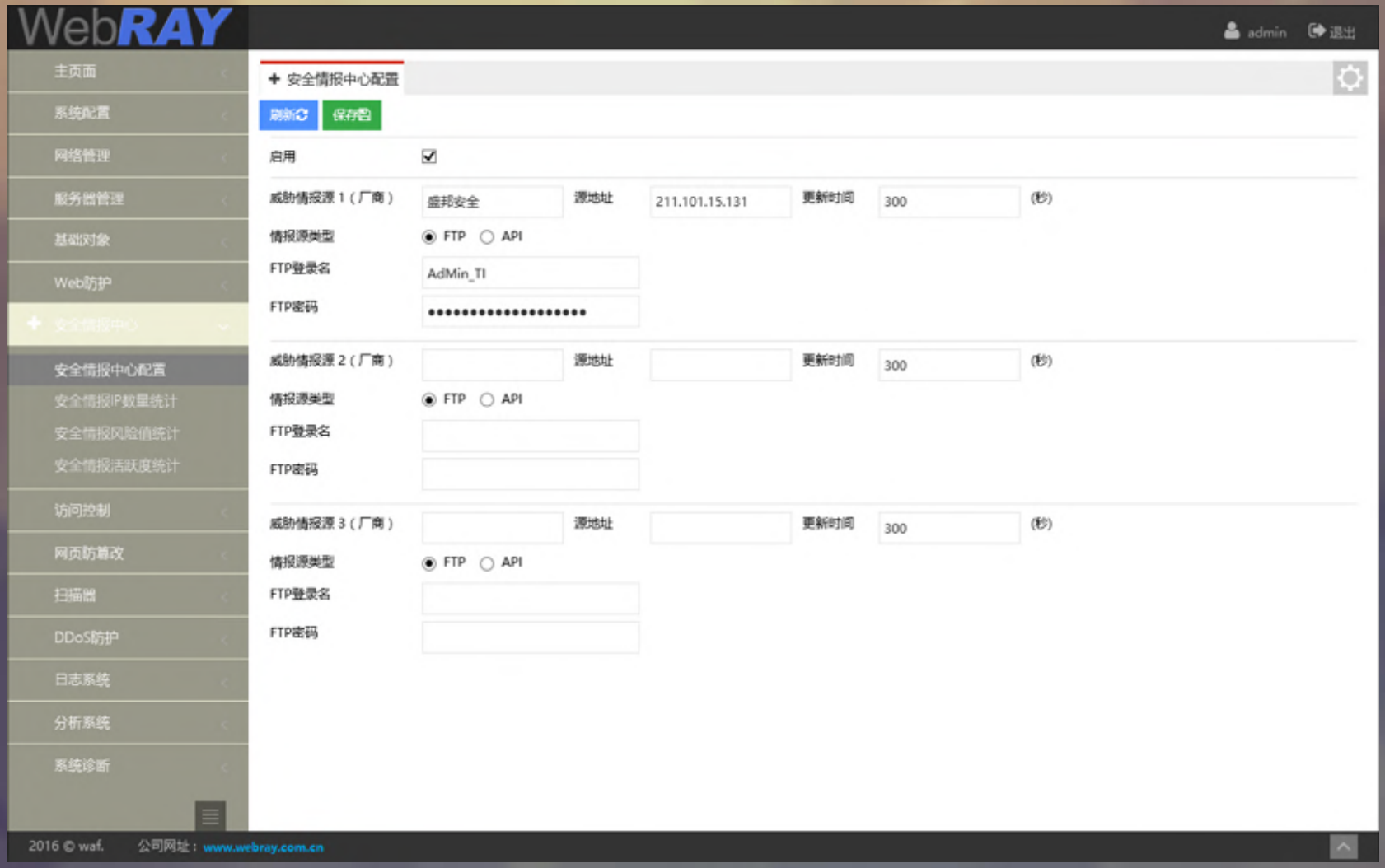
体系结构


Vendor Back End
Vendor Back End
Vendor Back End
Content + MRTI
Content + MRTI
MRTI
Content + MRTI
Client Premises
Security Software
Content + MRTI
Log + MRTI
SIEM
Logs
End-User Computing
Content + MRTI
Log + MRTI
Servers
Product A Mgmt. Server
Logs
File + Print
Data-base
Content + MRTI
Content + MRTI
Server Visuali-zation
Active Directory
Product B Agent/Appliance
Product B Mgmt. Server
Logs

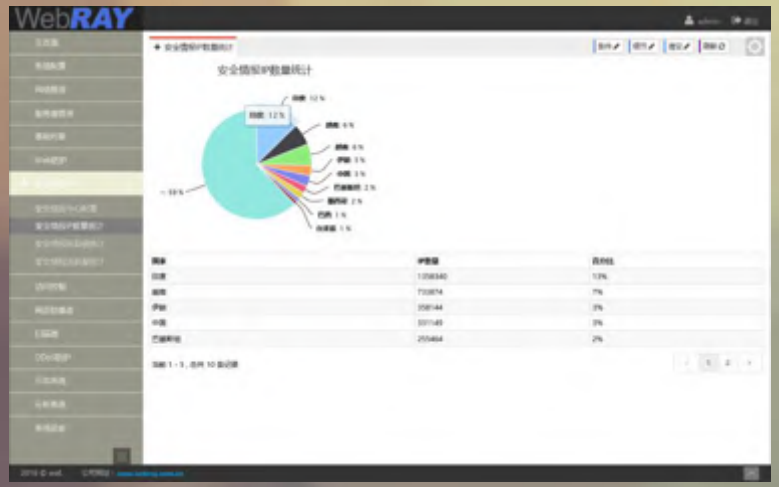
三步走威胁情报落地

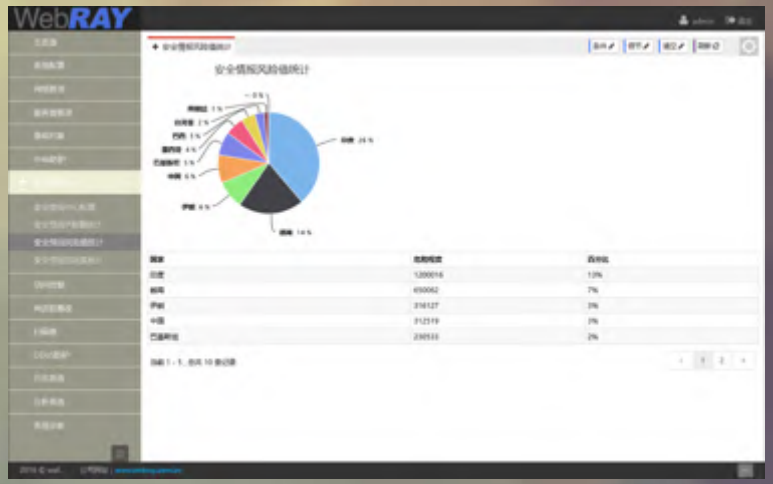


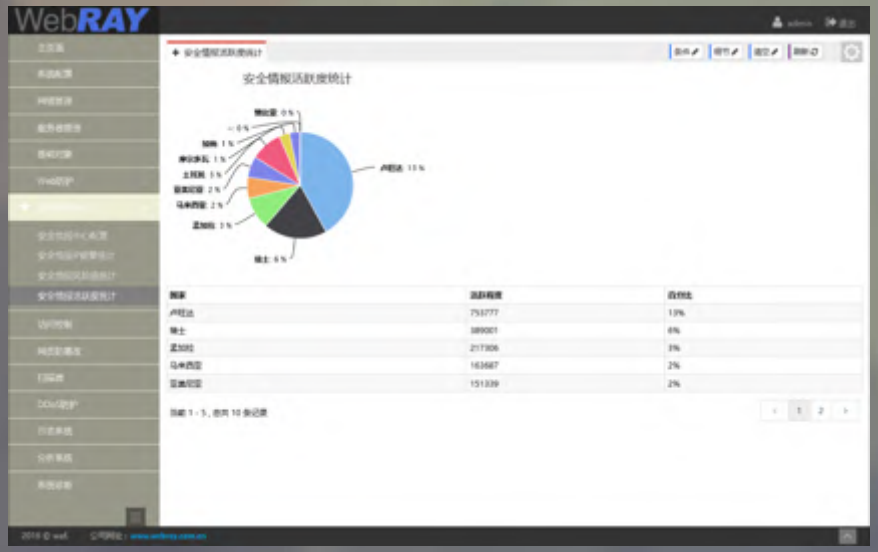
在安全产品上配置情报源



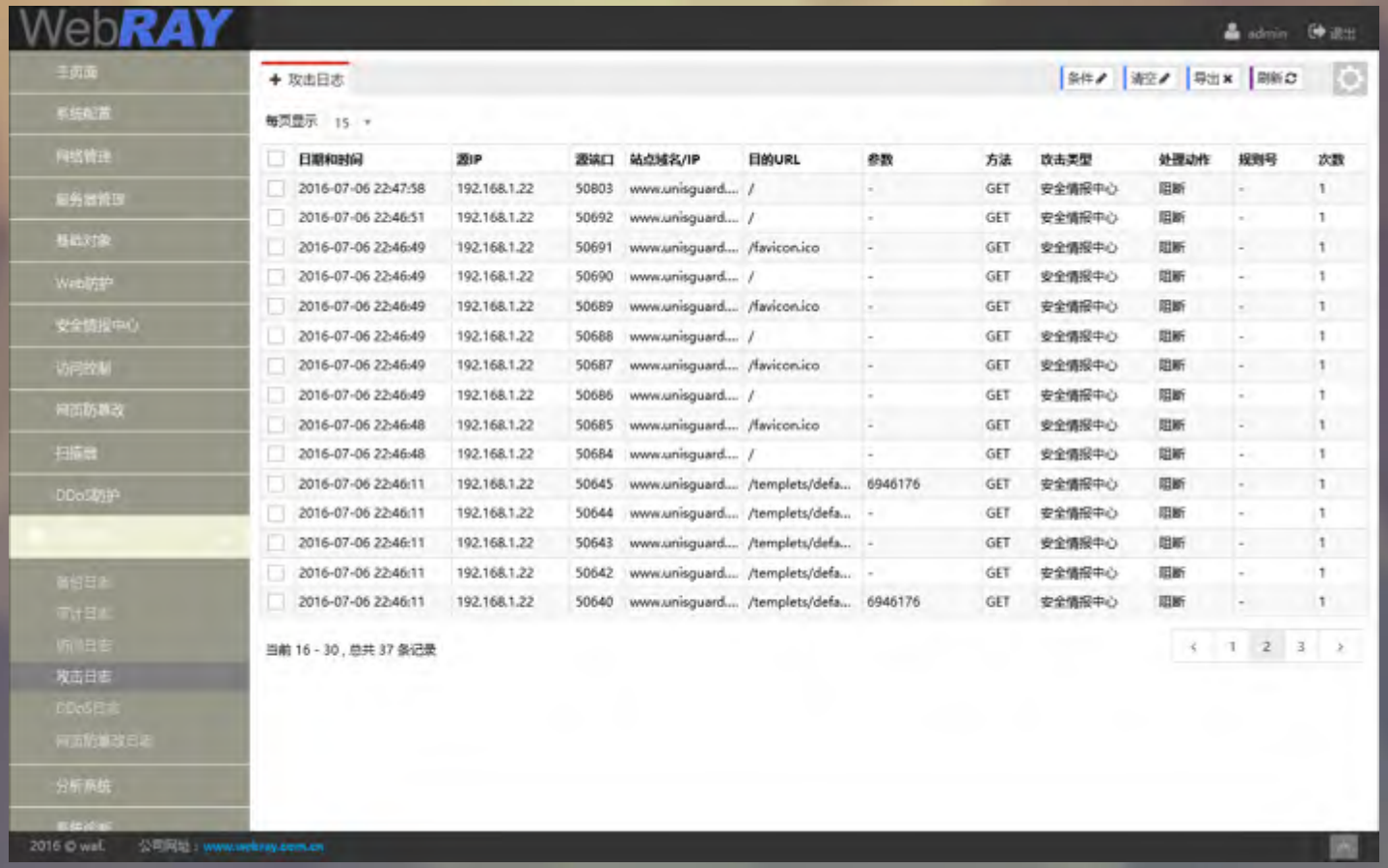
情报概况分析





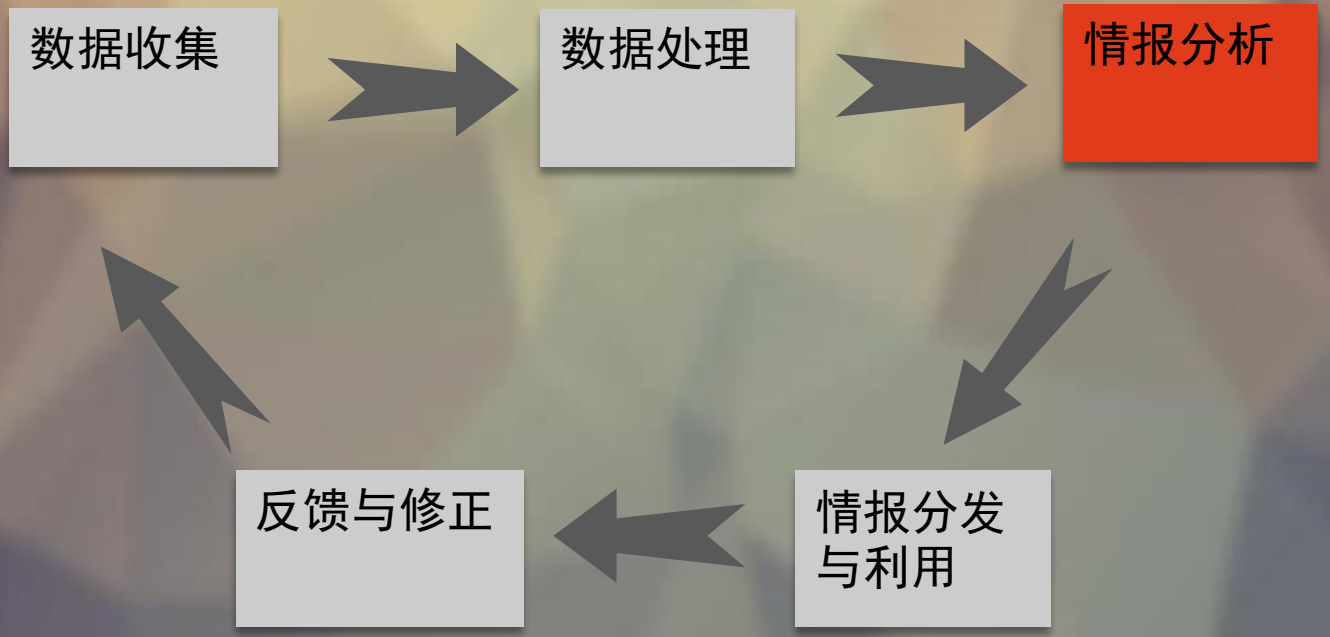


基于威胁情报的攻击侦测

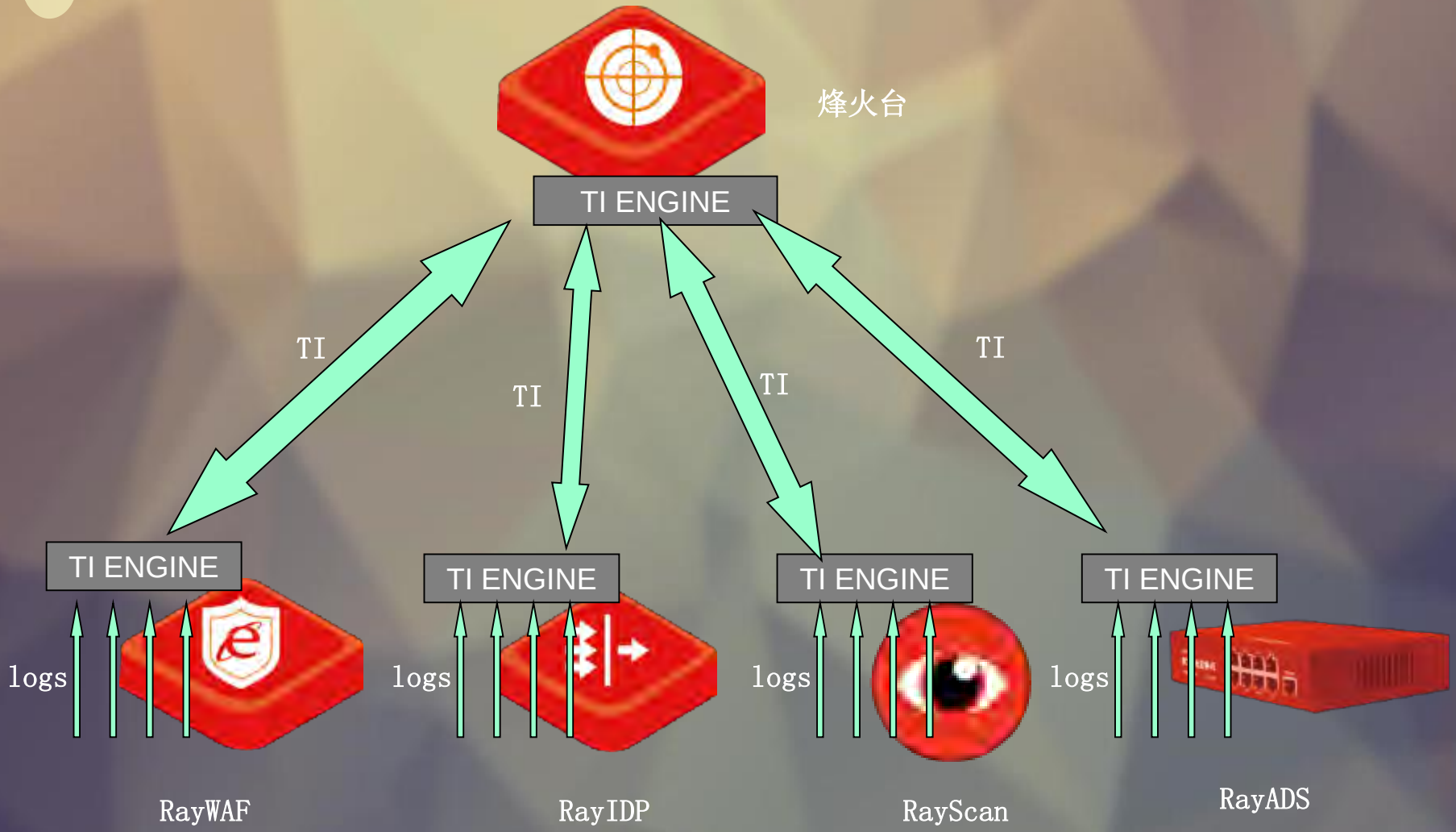


基于威胁情报的防御策略

威胁情报的一般生产过程



威胁情报治理模型


烽火台
TI ENGINE
TI
TI
TI
TI
TI ENGINE
TI ENGINE
TI ENGINE
TI ENGINE
logs
logs
logs
logs
RayWAF
RayIDP
RayScan
RayADS

WebRAY™

专业、专心、专注，安全就在你身边

Thanks

远江盛邦（北京）网络安全科技股份有限公司