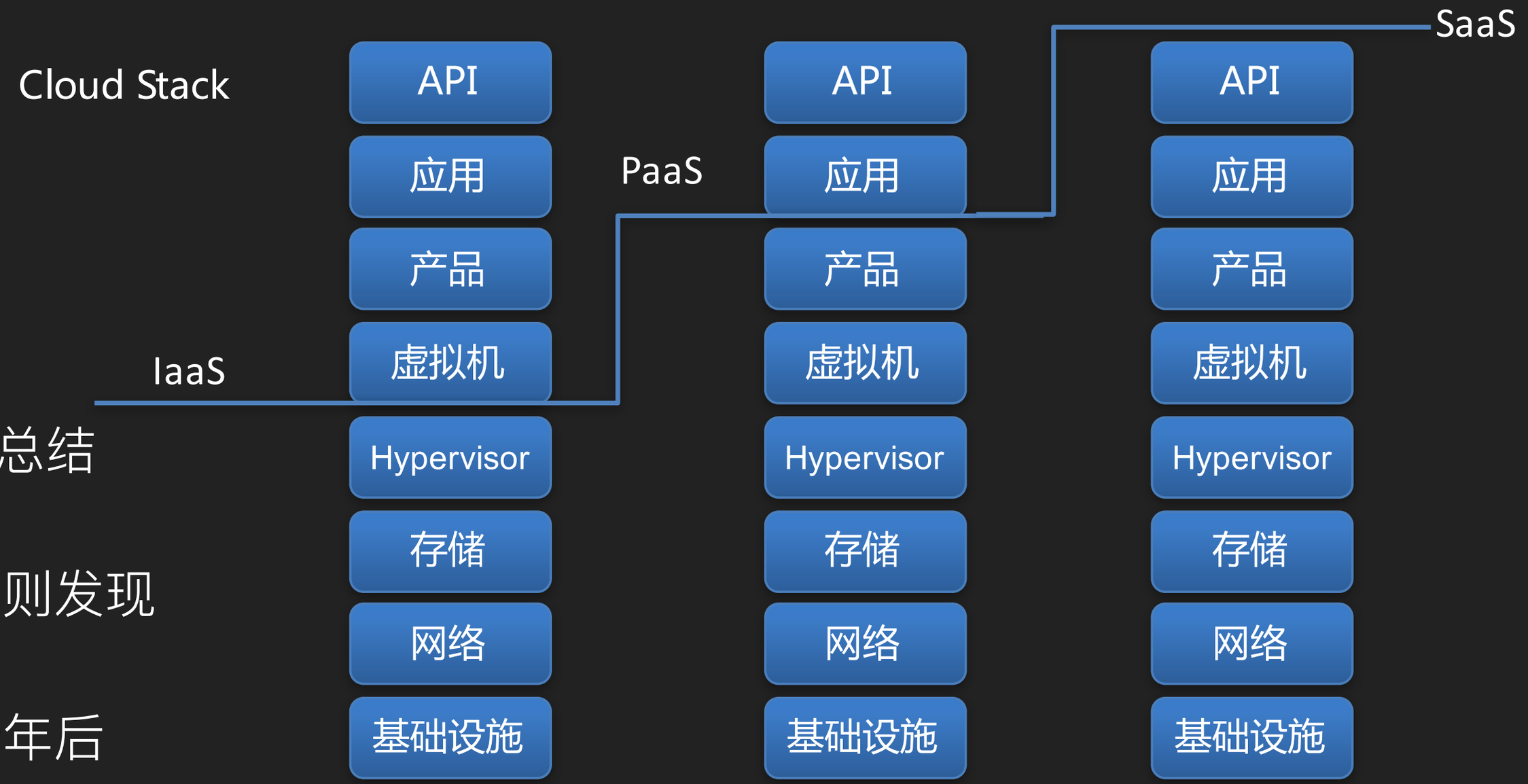
安全趋势和技术落地

ThreatSource

面临的威胁-云平台+传统企业



- 思路总结
  - 动则发现
  - 十年后
  - 提前做安全架构设计，产品体系

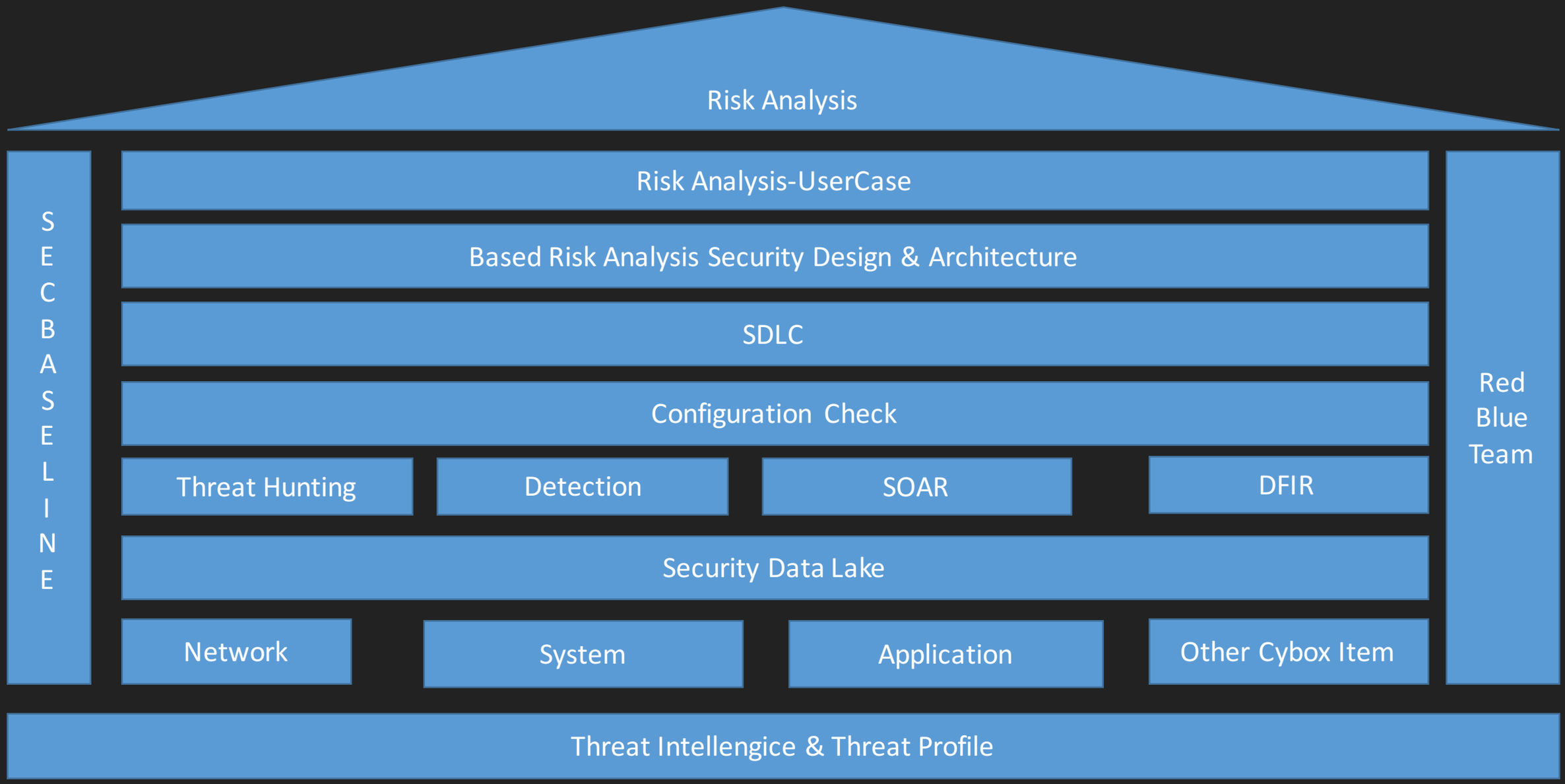
面临的威胁

应用层代码漏洞	OWASP TOP 10、越权	WEB SERVICE	代码执行、SSRF XXE、越权
配置	JDWP、JBoss	语言层漏洞	反序列化
框架漏洞	Struts、Spring	WEB SERVER	Tomcat+Tengine
框架依赖的开源组件	Json、Hession	系统库	LibXML2、FFMpeg
供应链	Python、JAVA、NPM	业务风险	薅羊毛、0元购、业务 逻辑漏洞

防御思维的转变

- 被动->主动
- 纵深防御->纵深检测
- 分散->打通
- 修漏洞->根源分析
- 人工响应->自动化处置
- 挖漏洞->模拟TTPs
- 剔除->监控
- 黑->白
- 混乱->统一
- 中心->边缘
- 封闭->开放
- 小众->标准

安全架构


Risk Analysis
SECBASELINE
Risk Analysis-UserCase
Based Risk Analysis Security Design & Architecture
SDLC
Configuration Check
Threat Hunting
Detection
SOAR
DFIR
Security Data Lake
Network
System
Application
Other Cybox Item
Red Blue Team
Threat Intellengice & Threat Profile

检测体系-检测体系标准化（CYBOX）

- Detection AAS
- 全面提升可见性
- 某个时间点的状态值
- 传统检测转移实体关系检测
  - Killed
  - Connected_to
  - Read_from
  - Downloaded_from
  - Parent_of
  - Child_of
  - Copied_from

- 采集
  - EDR
  - HIDS
  - IAC
- 关联+检测
  - STIX
  - CAPEC
  - 安全大脑
- 响应
  - SOAR

- Account
- Address
- API
- Code
- Device
- Disk
- Disk Partition
- DNS Cache
- DNS_Record
- Email Message
- File
- GUI
- GUI Dialog Box
- GUI Window
- Library
- Linux Package
- Memory
- Mutex
- Network Flow
- Network Packet
- Network Route Entry
- Network Route
- Network Subnet
- Pipe
- Port
- Process
- Product
- Semaphore
- Socket
- System
- Unix File
- Unix Network Route Entry
- Unix Pipe
- Unix Process
- Unix User Account
- Unix Volume
- URI
- User Account
- User Session
- Volume
- Win Computer Account
- Win Critical Section
- Win Driver
- Win Event
- Win Event Log
- Win Executable File
- Win File
- Win Kernel
- Win Kernel Hook
- Win Handle
- Win Mailslot
- Win Mutex
- Win Pipe
- Win Network Route Entry
- Win Network Share
- Win Pipe
- Win Prefetch
- Win Process
- Win Registry Key
- Win Semaphore
- Win Service
- Win System
- Win System Restore
- Win Task
- Win Thread
- Win User Account
- Win Volume
- Win Waitable Timer
- X509 Certificate

…

(more on the way)

检测体系-Threat Hunting

黑客组织

国家级黑客

主动TH

+

异常检测　安全防御　主机安全　反入侵　…

被动检测

黑产

Threat Actor Profile

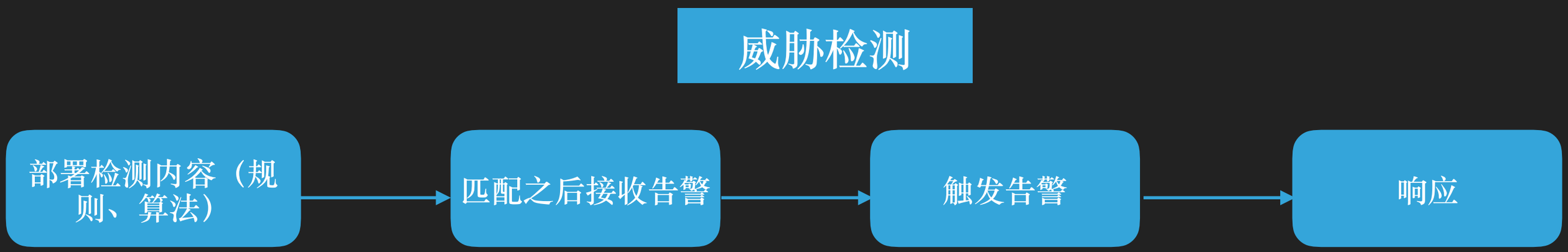
竞争对手

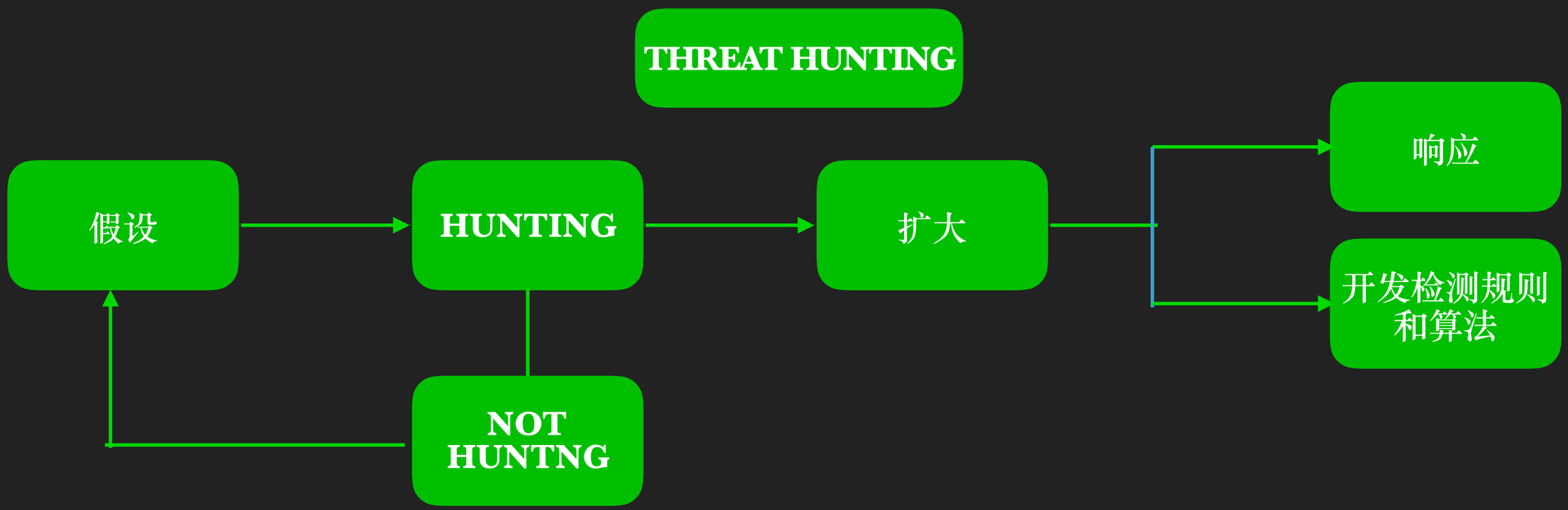
检测体系-Threat Hunting

- 主动
- 分析为中心
- 假设被入侵
- 补充检测能力
- 分析为中心
- 关注线索

- 基于威胁情报
- IoC
- Do More With More
- One clue All Trail

检测体系-Threat Hunting

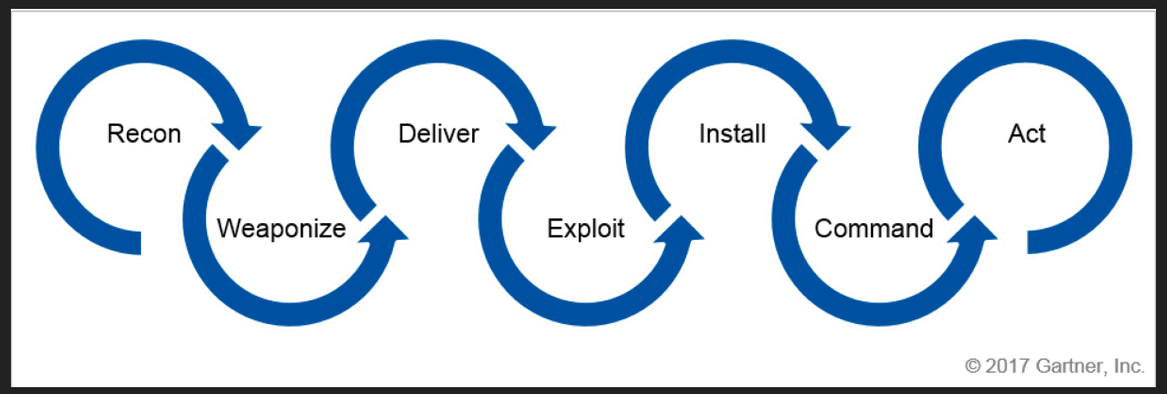




检测体系-Threat Hunting

工具分类	厂商	作用	场景
EDR	Carbon Black,CrowdStrike,FireEye	1、收集终端数据 2、搜索终端数据	所有机器进程中svchost.exe运行的路径不在c:\windows\system32
NTA	RSA NetWitness、BlueCoat Security Analysis、ProtectWise	收集和搜索网络流量	所有内部系统中的HTTP通信请求头中包含特定User-Agent的字符串
UEBA	Splunk、Securonix、Exabeam	利用用户活动数据分析异常行为	查看在身份认证行为异常的用户列表
Host FS	EnCase、AccessData、Forensic Toolkit、X-Ways、F-Response	内存和文件系统的深度分析取证	所有机器进程内存中的指定恶意特征匹配
TI	FireEye iSIGHT、Flashpoint、Digital Shadow	TTPs	查找所有黑客组织的通用后门技术
SIEM	Splunk、IBM QRadar、LogRhythm、Elastic Stack	日志和上下文分析	分析日志中的异常例如异常登录、HTTP恶意攻击

检测体系-Threat Hunting

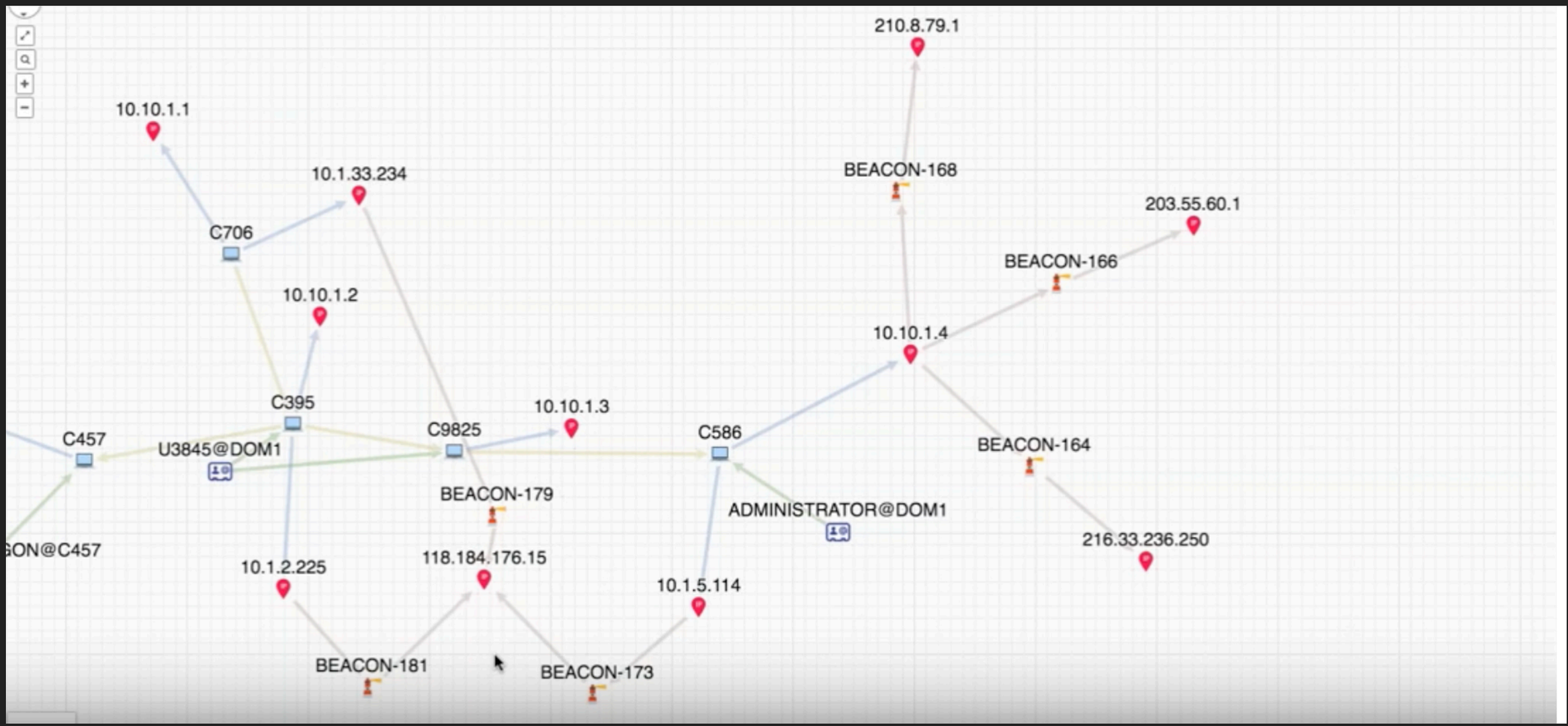


+

- Exploit：钓鱼邮件、异常流量、异常行为
- C&C：DNS日志匹配恶意后门
- 驻留：注册表、Crontab、Schedule
- 横向移动：PTH、PTT、内网扫描
- 数据提取：加密流量、数据加密、数据压缩
- 溯源和反制：主动收集黑客情报和攻击手法

检测体系-Threat Hunting

- Sqrrl DEMO（CYBOX落地最佳实践）
- 主机->账号->IP->Beacon->恶意域名



攻击体系-BAS

- 测试防御手段有效性（RASP）
- 模拟后攻击阶段（HIDS）
- 测试检测手段有效性（EDR、HIDS、系统调用、文件监控、WebSHELL检测、DLP）
- 测试蜜罐有效性（蜜罐）
- 数据库拖库演练（DAM、点滴数据泄露测试）
- 验证网络隔离效果有效性（网络微隔离策略）
- 蓝军TTPs模拟

攻击体系-BAS

ATT&CK™ Adversarial Tactics, Techniques & Common Knowledge

\+ 蓝军 TTPS \+ 生态合作伙伴 \+ 产品加运营体系

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-Stage Channels
	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	Launchctl	Component Object	Hooking	DLL Search Order	Kerberoasting	Remote System	SSH Hijacking	Screen Capture		Multiband

攻击体系-BAS

- 渗透测试
  - 寻找一个入侵点
- BAS
  - 安全能力在RUN
  - 安全能力RUN的正常
- 蓝军
  - 模拟APT
  - 模拟高级威胁源
  - 模拟最新TTPs
- 生态
  - 社会化力量
  - 白帽子
  - 安全公司
  - 民间隐藏高手
  - 国家队等
- 沉淀
  - 攻防数据沉淀

攻击体系-BAS

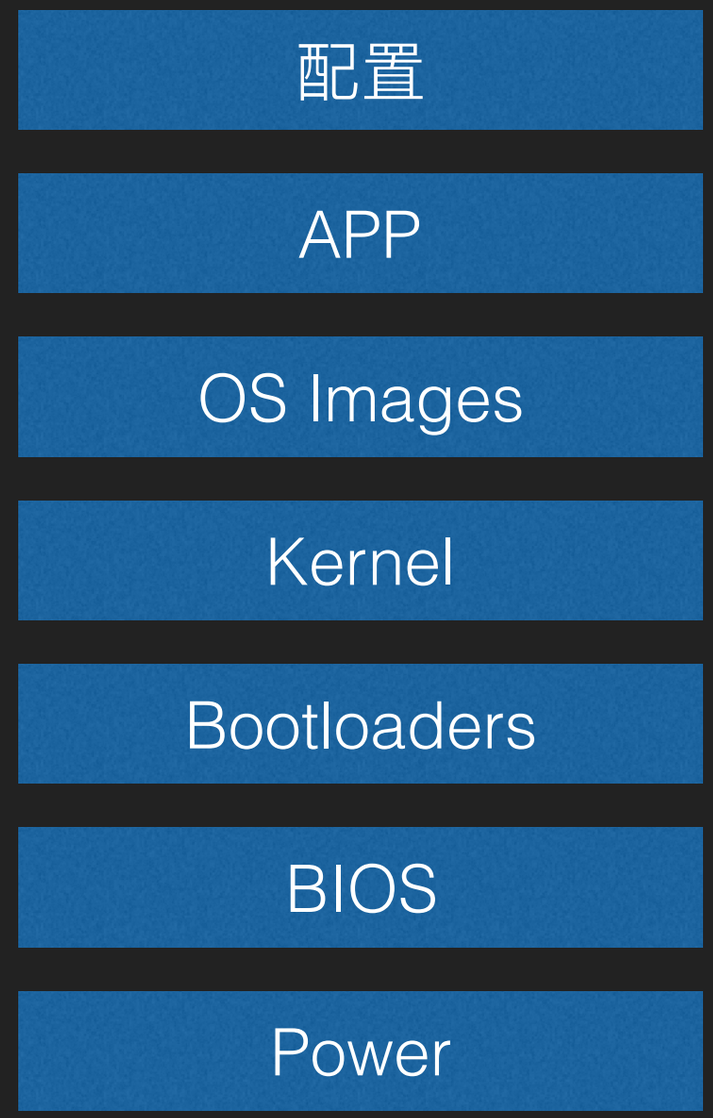
模拟动作	模拟方式	解释
威胁	模拟	模拟各种Threat Actor手法，从CIA、NSA、TAO
数据窃取	模拟	梳理路径，通过路径才进行真实模拟检测效果
恶意软件	模拟、真实	内存后门、Fileless、固件后门、硬件后门（从NSA泄露文档、HackingTeam、CIA、外部采购木马等手段）
攻击	模拟、真实	整合现有蓝军平台攻击武器库
后攻击阶段	真实	TTPs，模拟APT组织的各种驻留、隐藏痕迹等手法

攻击体系-BAS

控制和流程	解决的问题
攻击预测	攻击者会从哪里发起攻击? 哪个攻击点会比较容易? 需要多少步骤能达到窃取数据的目标?
防御控制	攻击者攻击会不会达到目标资产前被阻断? 恶意外链和C&C是否成功阻断? 安全基线是否被更改? 安全防御措施是否被改动、调整和关闭?
检测控制	攻击者行为是否被记录? 是否触发了告警? SIEM或者其他安全检测是否工作?
监控流程	是否可以和Threat Hunting进行结合来进行模拟发现?
响应流程	SOAR应急响应流程是否触发?

可信体系=可信+强制访问控制+自动化检测及响应

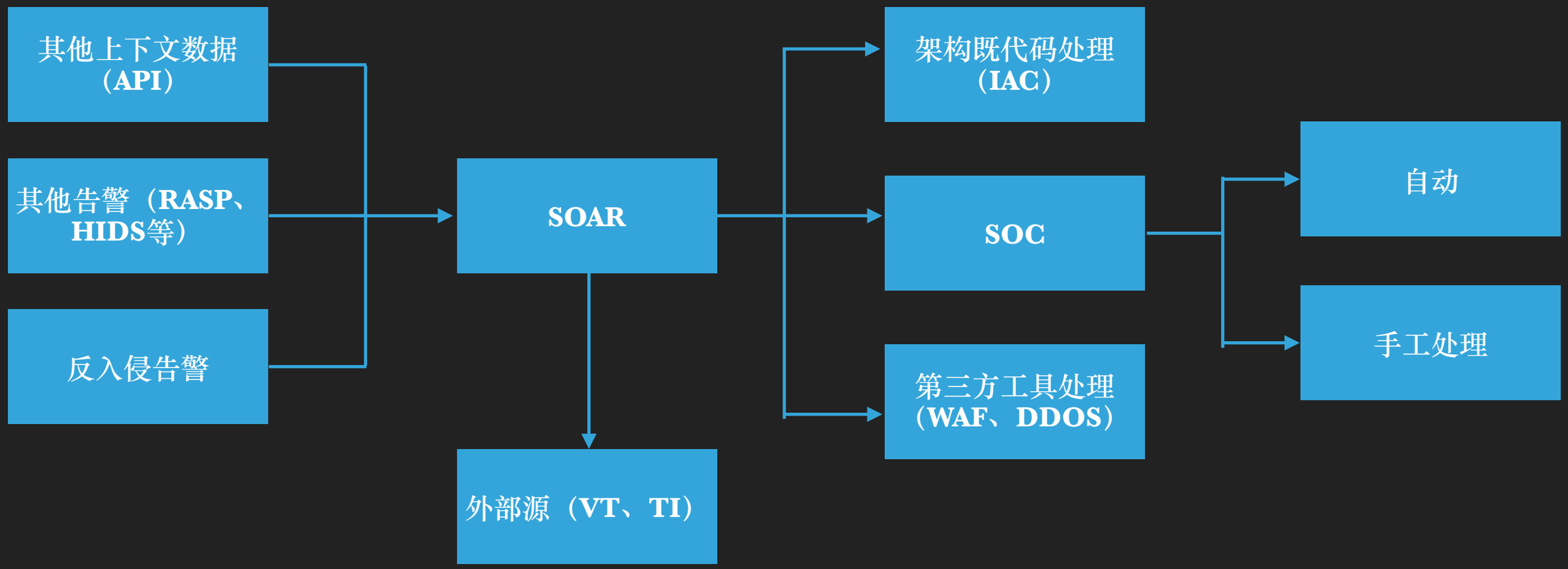
- 风险
  - 固件后门
  - Bootkit
  - Rooktit
  - 内核Module后门
  - 内存后门
  - Fileless后门



自动化响应体系-SOAR

- SOAR定义
  - Security Orchestration Automation and Response（安全编排自动化和响应）
- SOAR发展
  - 初级响应+大量人工决策->高级自动化响应+极少人工决策发展
  - 同样事件处理两次以上就要SOAR自动化处理
- SOAR依赖
  - 充分依赖基础平台API能力（系统、网络、应用、OpenIPMI、发布、VIP管理），需要推动基础设施进行架构升级
  - 需要封装IAC为代码既架构的能力
  - 整合现有代码发布平台、漏洞扫描平台、WAF、DDoS、HIDS等能力

自动化响应体系-SOAR



自动化响应体系-SOAR

- IP深度调查User-Case
  - IP信誉、Whois、Hunt IP、匹配后发送邮件

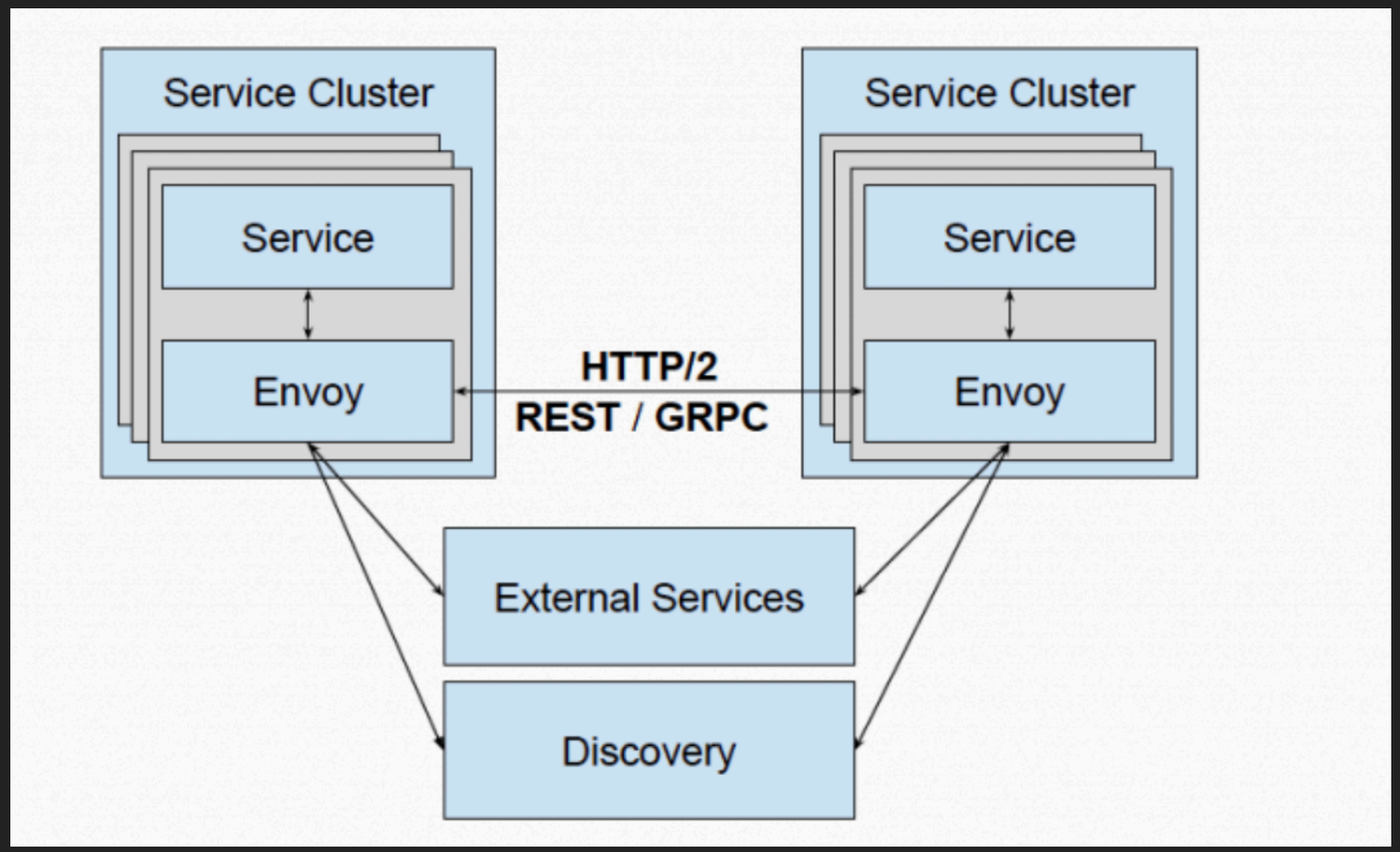
自动化响应体系-SOAR

基础设施安全-新形态网络安全

- 风险
  - 企业内部应用无认证、鉴权、链路无加密来进行细粒度控制

基础设施安全-网络安全

- 解决方案
  - Envoy来针对内部基础设施的通信、认证能力进行封装，打造链路加密、认证授权、协议控制能力；



基础设施安全-系统安全+网络安全+应用安全

- 用户：终端安全（可信+生物识别），证明设备可信，证明你是你；
- 身份生命周期（IDaaS）：你知道你知道的，你拥有的独一无二的、权限、审计；
- 数据环境安全及可信：云+平台安全、流程、人员管理、系统可信、强制访问控制；
- 接入网络可信：802.1X+PKI+NAC体系认证可信网络；
- 行为管理：点滴数据泄露，异常行为监控；
- 应用安全：微服务级细粒度访问控制、强制访问控制、密钥中心统一管理；
- 数据安全生命周期管理：其他通道封闭，只留数据流出域做严格限制；
- 全网无死角：SDWAN；
- 运营：响应、处置、溯源；

新形态的安全体系

- 每个客户都是一个探针，最终决策在安全中心大脑中心，大脑配合客户探针完成闭环体系；
- 客户内部形成自动化响应流程，每个客户间形成响应情报共享，完成企业内部+跨企业的闭环体系；
- 客户内部完成可信体系、爱因斯坦（NTA+IDS+IPS）、HBSS（主机安全体系）、情报共享体系（STIX+OpenIOC）、检测体系（ATT&CK+Cybox）、内部安全产品集成（OpenAPI）、内部自动化响应体系（OpenC2）、内部基础设施体系打通（IAC）、内部统一认证体系（IDaaS）