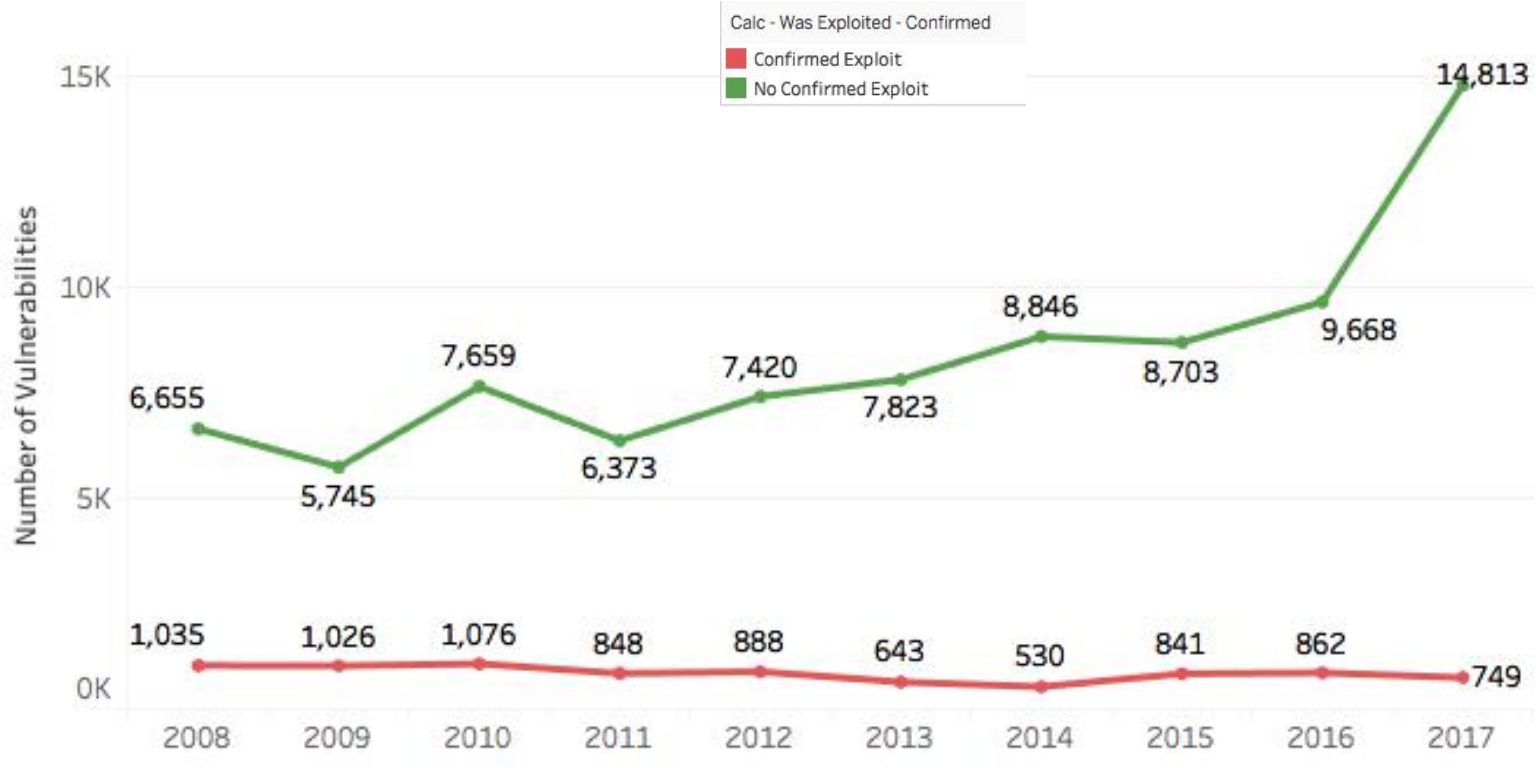
安全运营与应急发展趋势纵览

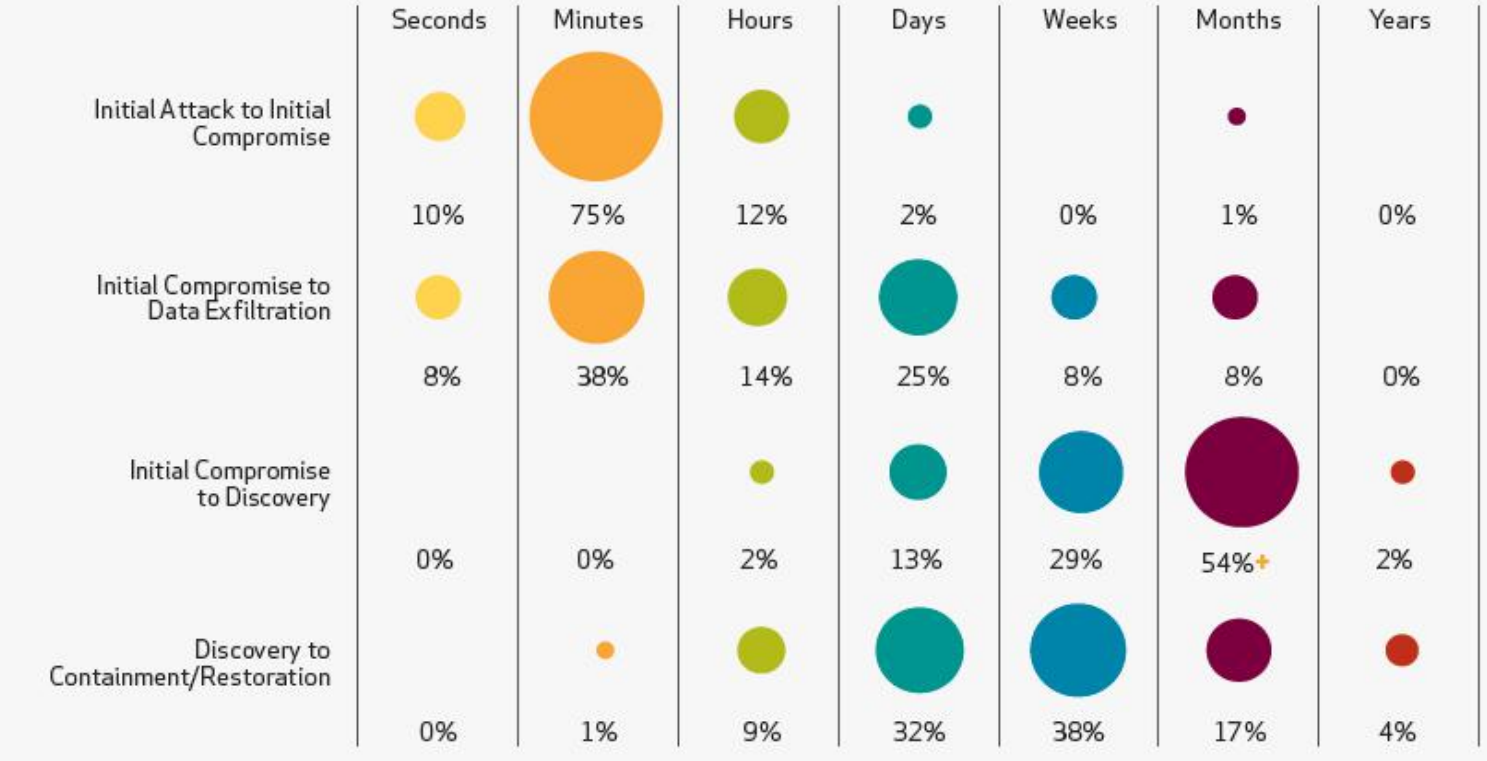
从黑产灰产到国家黑客
不断进击的网络安全威胁

漏洞永恒存在，攻击永不停歇

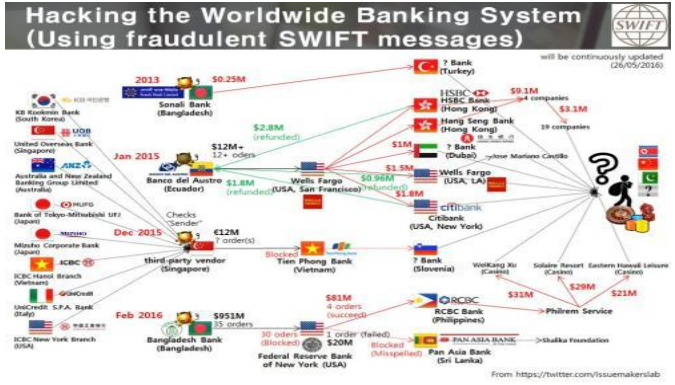


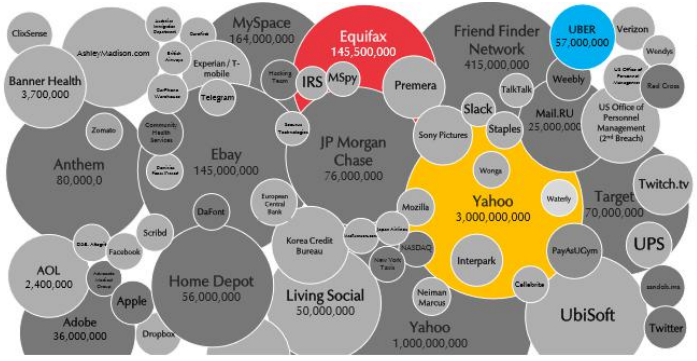
当前的网络安全防护体系已落后攻击技术发展

Figure 40. Timespan of events by percent of breaches



网络安全对抗进入新的时代





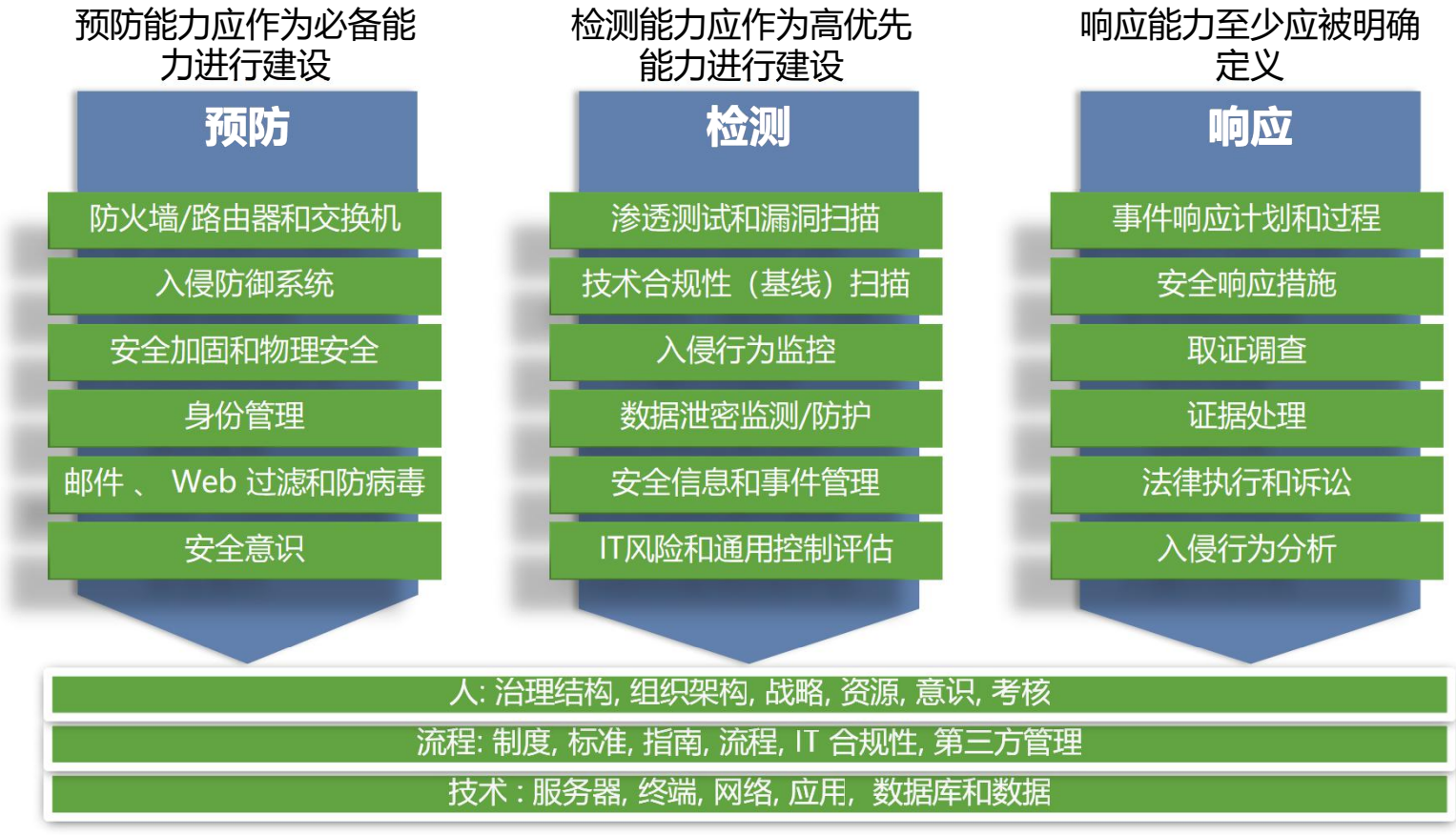
- 安全威胁极度爆发，从勒索软件到SWIFT系统攻击，国家黑客行为泛滥，对抗进入全新降维打击时代
- 黑产从窃取数据、到绑架数据、进而转向窃取企业计算能力，模式极度演进

GDPR、个人信息保护等合规性要求不断提升

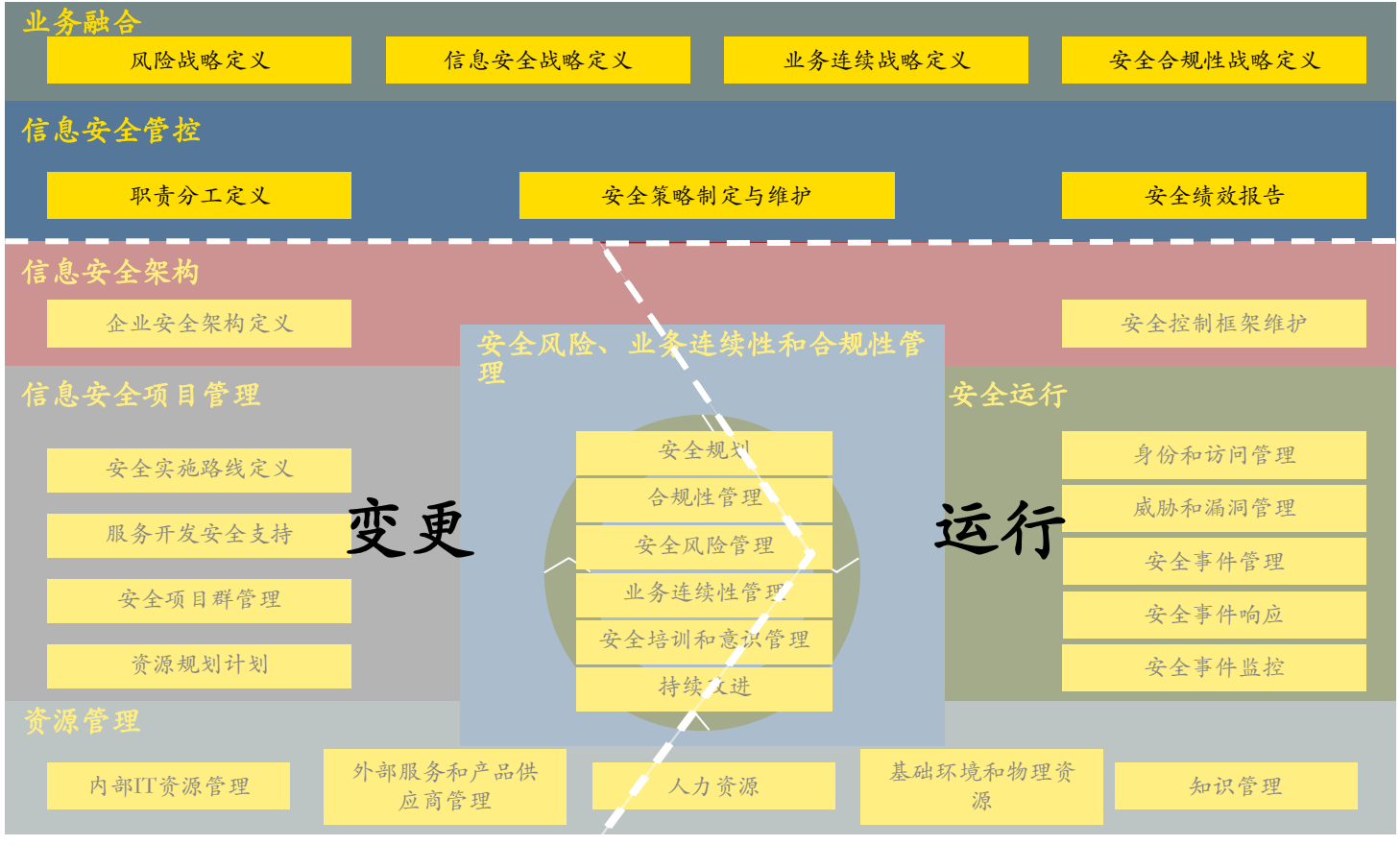
- 全球个人信息保护相关法律法规不断出台，合规性要求成为新的贸易战武器
- 数据保护、隐私保护挑战前所未有，企业必须进行重视和应对
- CDO-首席数据官应运而生，CISO的部分职责分离
- 数据保护预算大增（欧盟$1.4m/美国$1-10m），新的数据防护技术和产品需求猛增

从PDR到自适应
安全运营与应急体系不断进化

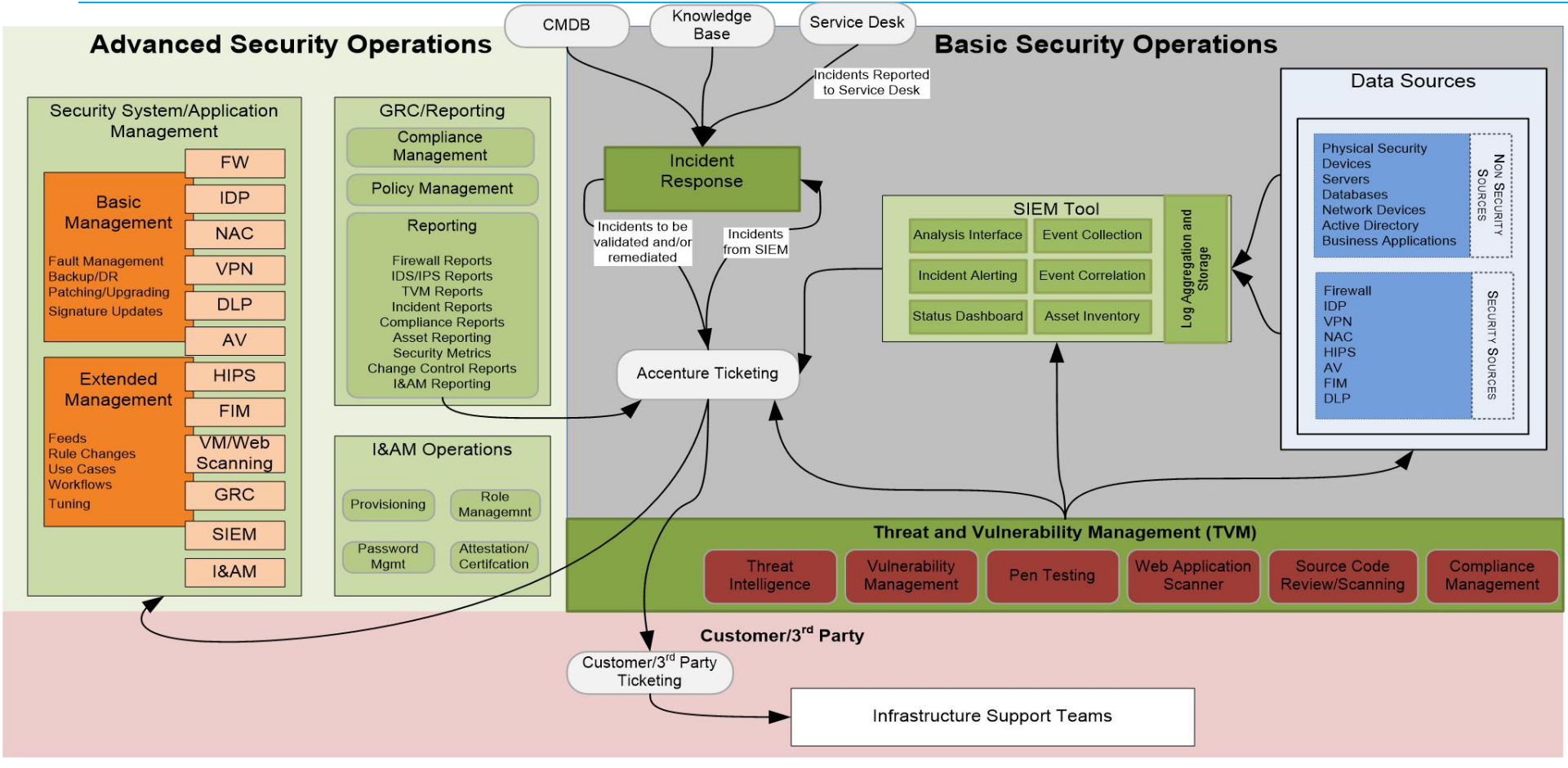
PDR+PPT


预防能力应作为必备能力进行建设
预防
防火墙/路由器和交换机
入侵防御系统
安全加固和物理安全
身份管理
邮件 、 Web 过滤和防病毒
安全意识
检测能力应作为高优先能力进行建设
检测
渗透测试和漏洞扫描
技术合规性（基线）扫描
入侵行为监控
数据泄密监测/防护
安全信息和事件管理
IT风险和通用控制评估
响应能力至少应被明确定义
响应
事件响应计划和过程
安全响应措施
取证调查
证据处理
法律执行和诉讼
入侵行为分析
人: 治理结构, 组织架构, 战略, 资源, 意识, 考核
流程: 制度, 标准, 指南, 流程, IT 合规性, 第三方管理
技术 : 服务器, 终端, 网络, 应用, 数据库和数据

以风险为核心的安全运营模型



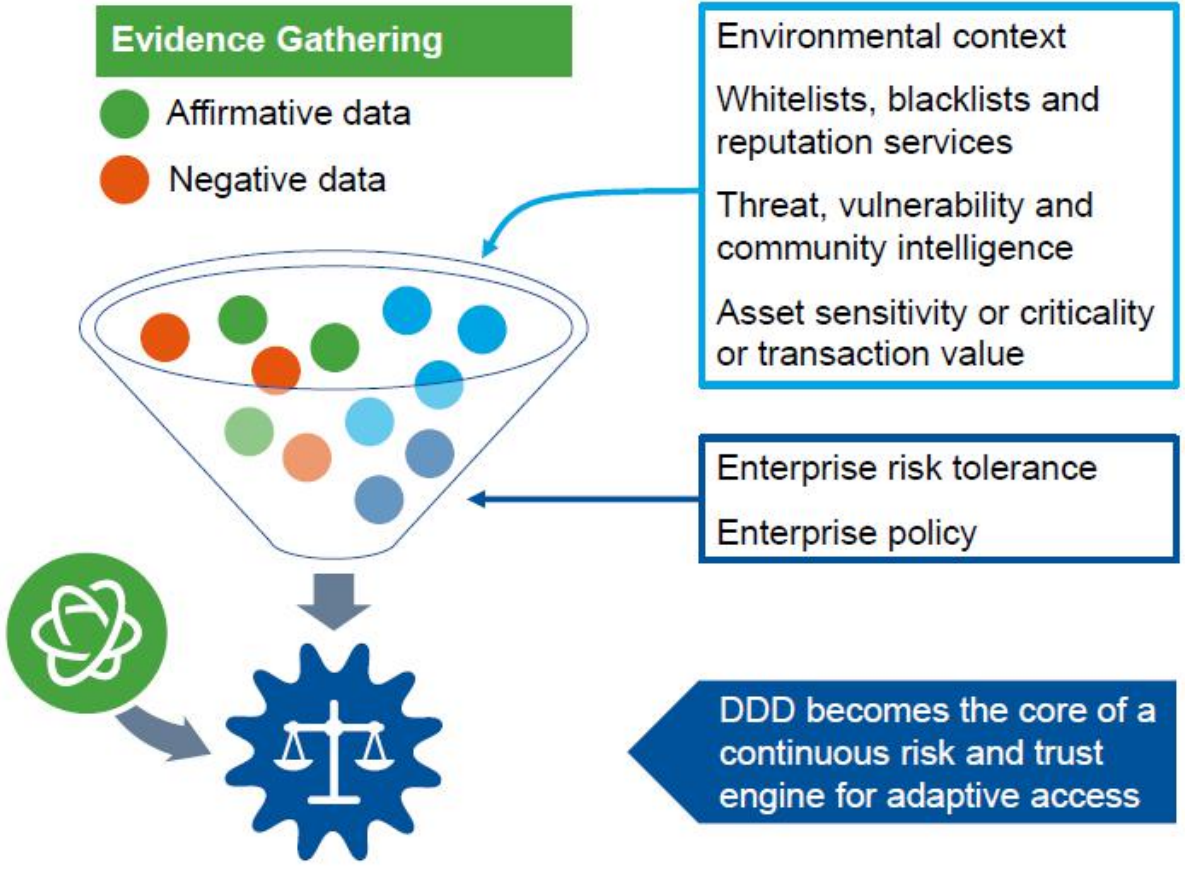
以SIEM为核心的安全架构



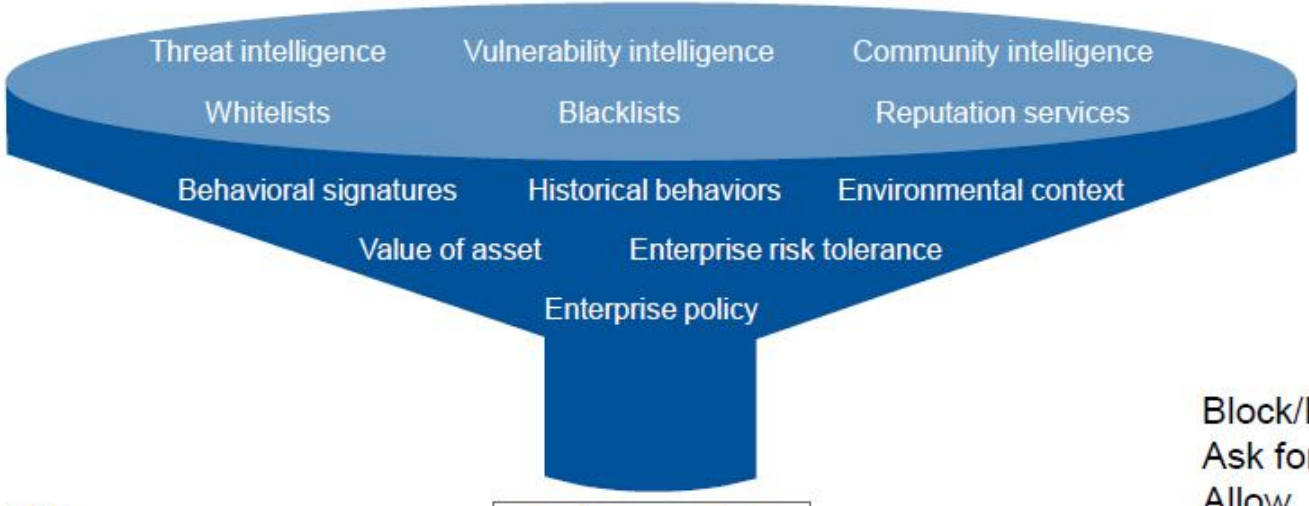
不断进化的安全模型

CARTA

Continuous Adaptive Risk and Trust Assessment



Continuous Adaptive Risk and Assessment (CARTA)

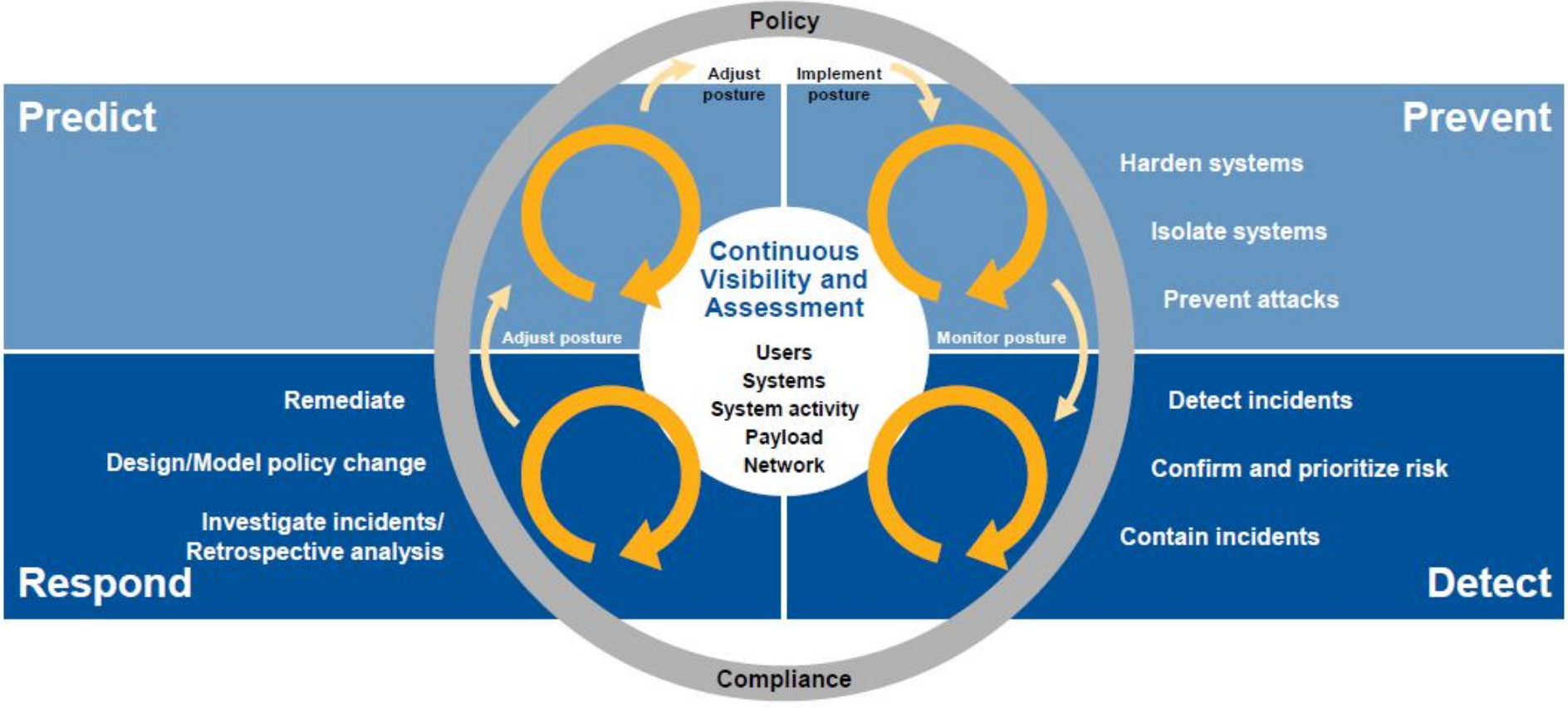


Should this entity take this requested action on this entity given the current context, my trust of the entity and my tolerance for risk?

Block/Prevent
Ask for more context
Allow
Allow and log
Allow and audit
Allow and isolate
Allow and throttle
Deceive

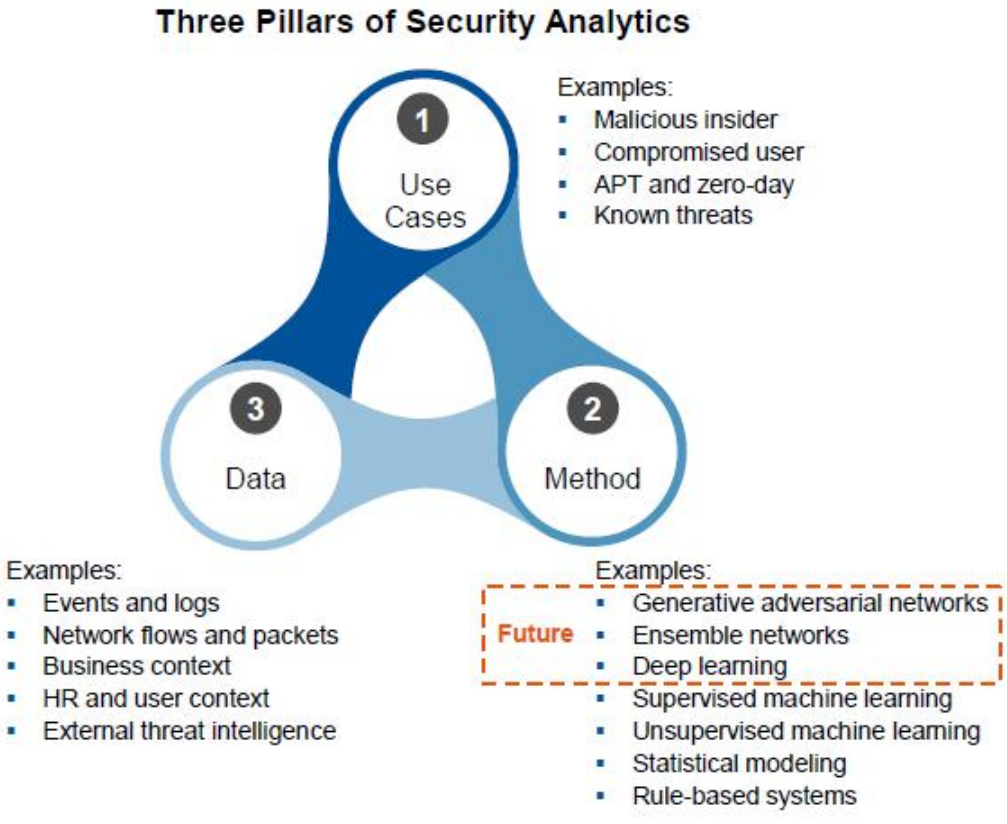
Continuous adaptive risk and trust assessment

CARTA与Gartner 自适应安全架构

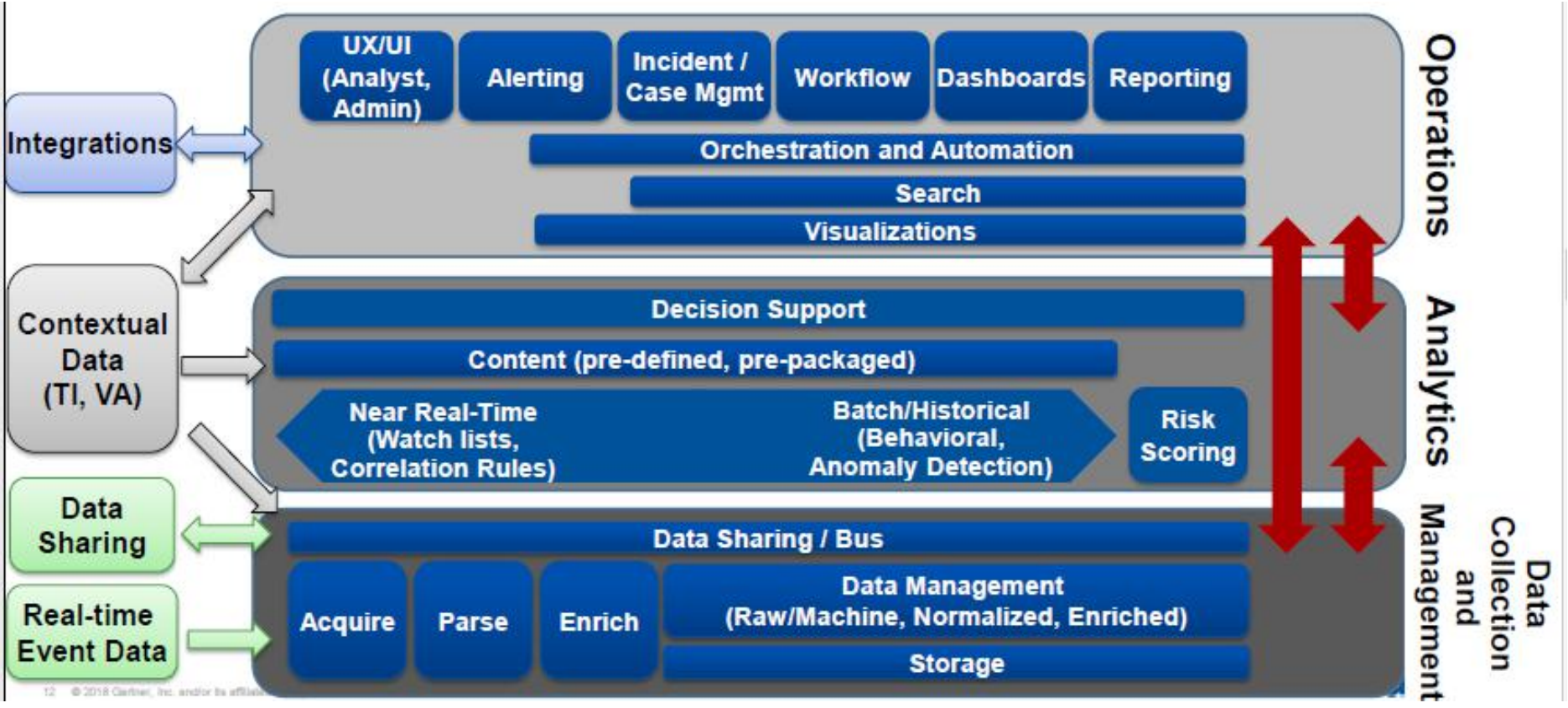


长江后浪推前浪，前浪倒在沙滩上
不断进化的安全运营与应急解决方案

安全分析简单框架


Three Pillars of Security Analytics
1
Use Cases
Examples:
Malicious insider
Compromised user
APT and zero-day
Known threats
3
Data
2
Method
Examples:
Events and logs
Network flows and packets
Business context
HR and user context
External threat intelligence
Examples:
Future
Generative adversarial networks
Ensemble networks
Deep learning
Supervised machine learning
Unsupervised machine learning
Statistical modeling
Rule-based systems

SIEM平台的进化


UX/UI (Analyst, Admin)
Alerting
Incident / Case Mgmt
Workflow
Dashboards
Reporting
Integrations
Orchestration and Automation
Search
Visualizations
Operations
Contextual Data (TI, VA)
Decision Support
Content (pre-defined, pre-packaged)
Near Real-Time (Watch lists, Correlation Rules)
Batch/Historical (Behavioral, Anomaly Detection)
Risk Scoring
Analytics
Data Sharing
Data Sharing / Bus
Real-time Event Data
Acquire
Parse
Enrich
Data Management (Raw/Machine, Normalized, Enriched)
Storage
Data Collection and Management

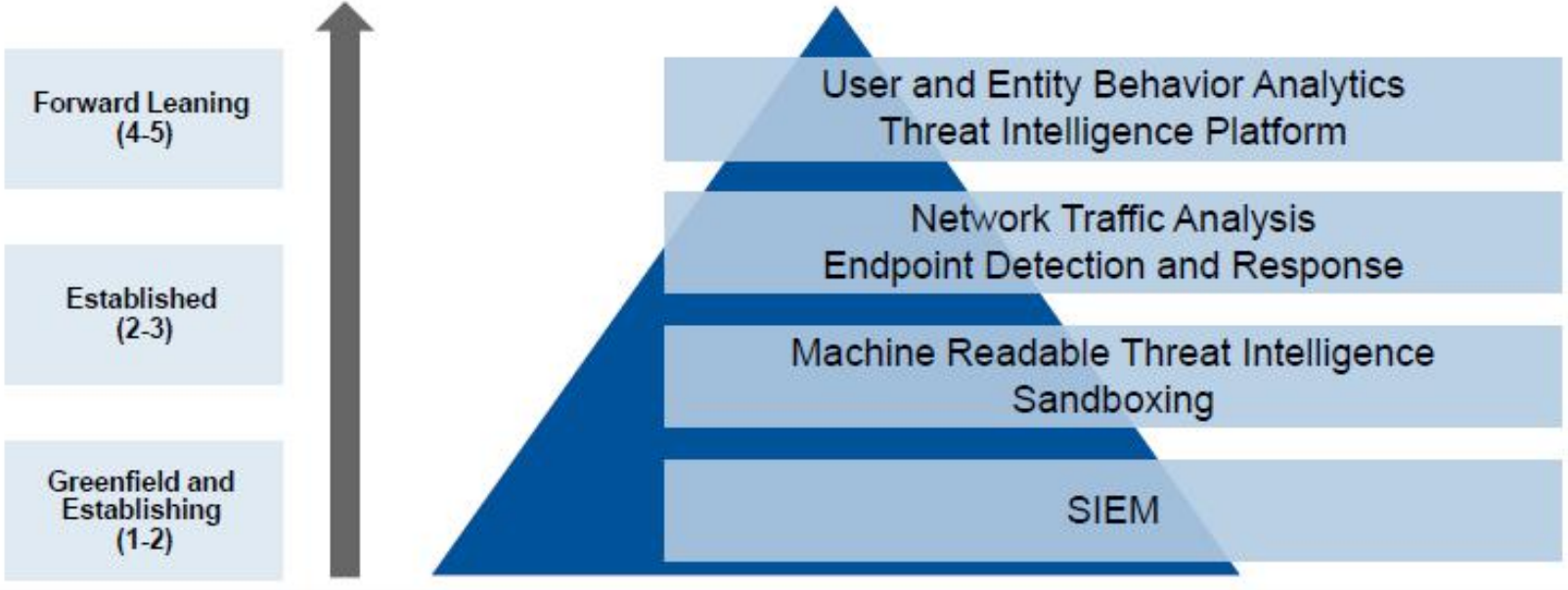
现代安全运营中心要素

- **Processes**:
  - Not just alert triage!
  - Hunting and proactive data exploration
  - Active and continuous content dev.
  - Wider integration of services
- **People**:
  - Expansion and evolution of the L1/L2/L3 model
  - Specialty skills grow: TI, malware reversing, data analysis, etc.
  - Services play many tactical roles (MDR)
- **Technology**:
  - Not just an SIEM! Endpoint and network visibility
  - A role for analytics tools (UEBA and other security analytics)
  - Broader use (and creation!) of threat intelligence (TI)
  - Orchestration and automation tools to streamline workflows

现代安全运营中心工具

- SOC "Nuclear Triad":
  - **LOGS:** Log analysis — **SIEM**
  - **NETWORK:** Network traffic analysis — **IDPS, NTA and/or NFT**
  - **ENDPOINT:** Endpoint activity analysis — **EDR**
- Analytics:
  - **UEBA** and other security analytics
- Threat intelligence — **TI**
- Workflow and orchestration — **SOAR**
- Exciting extras: Deception, cloud monitoring (CASB and CWPP), breach and attack simulation (BAS), etc.

现代安全运营中心工具的选择



Reminder #2: The maturity of the security analytics program does not correlate with the number of tools.

SOAR 成为安全运营新焦点

SOAR = (**Workflow** + **orchestration** + **automation** + **knowledge management**) for (security operations, incident response, threat intelligence)

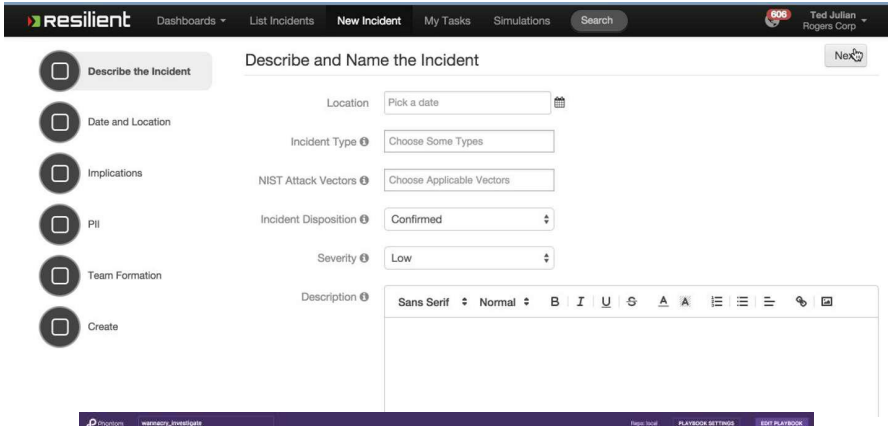
- **Workflow** = Controlling the execution of a process as a repeatable pattern of business activity (such as "triaging an alert")
- **Automation** = Machines do stuff on their own
- **Orchestration** = Coordinated workflow with manual and automated steps *involving many components*, done mostly to machines

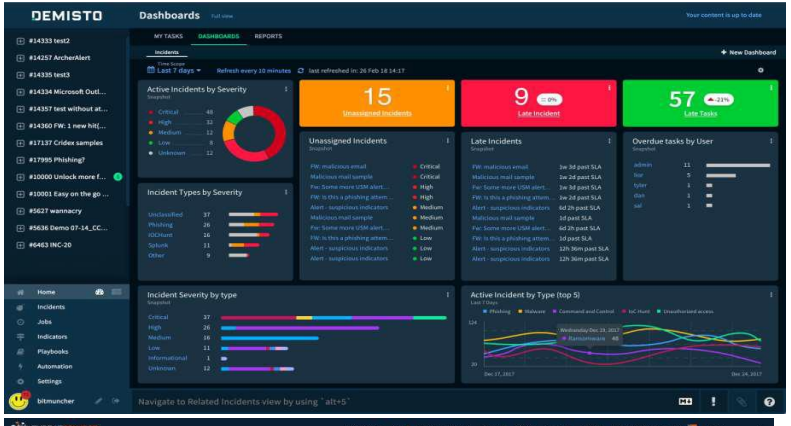
SOAR的来源

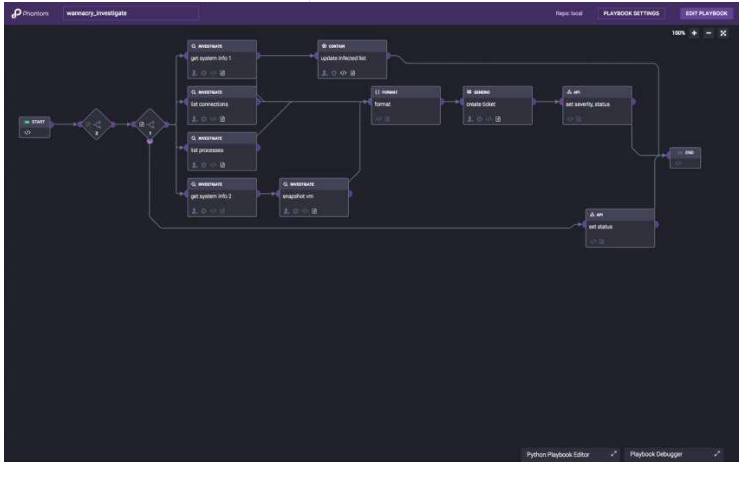

Security
Automation
and Orchestration
Security
Incident
Response
Platforms
SOAR
Threat
Intelligence
Platforms

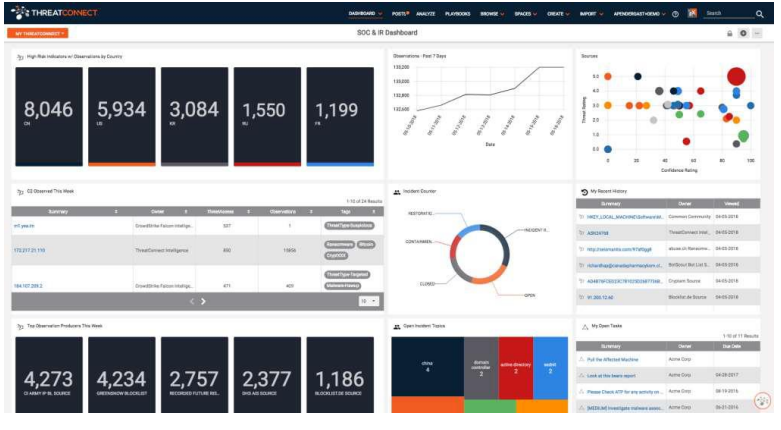

Orchestration
Prioritize
Detect
Respond
Triage
Business
intel
Collect
Risk
Decision
Making
Measure
SOAR
Threat
Hunting
Remediate
Investigation
Workflow
Human
Intervention
Threat Intelligence

SOAR示例


Resilient
Dashboards
List Incidents
New Incident
My Tasks
Simulations
Search
Describe the Incident
Date and Location
Implications
PII
Team Formation
Create
Describe and Name the Incident
Next
Location
Pick a date
Incident Type
Choose Some Types
NIST Attack Vectors
Choose Applicable Vectors
Incident Disposition
Confirmed
Severity
Low
Description
Sans Serif
Normal

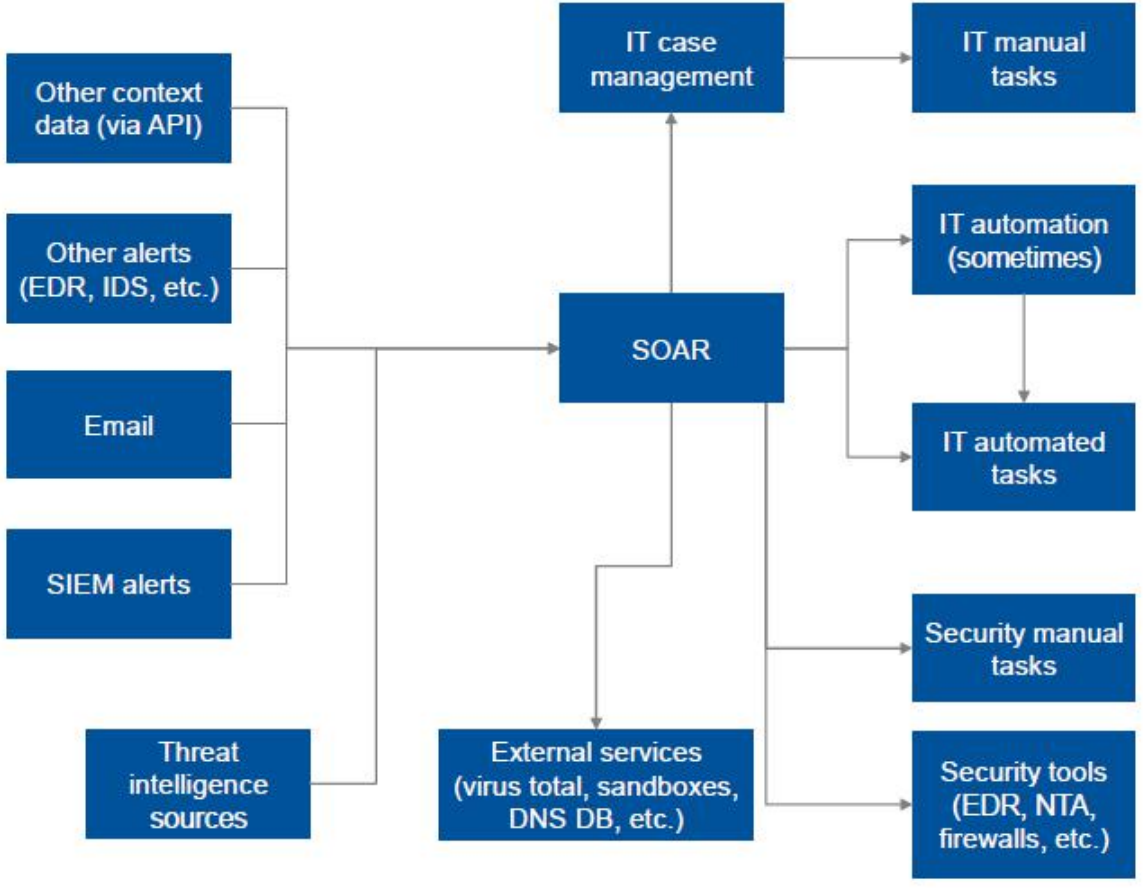

DEMISTO
Dashboards
15
9
57
Active Incidents by Severity
Unassigned Incidents
Late Incidents
Overdue tasks by User
Incident Types by Severity
Incident Severity by type
Active Incident by Type (top 5)
Navigate to Related Incidents view by using `alt+5`


Python Playbook Editor
Playbook Debugger


THREATCONNECT
SOC & IR Dashboard
8,046
5,934
3,084
1,550
1,199
4,273
4,234
2,757
2,377
1,186

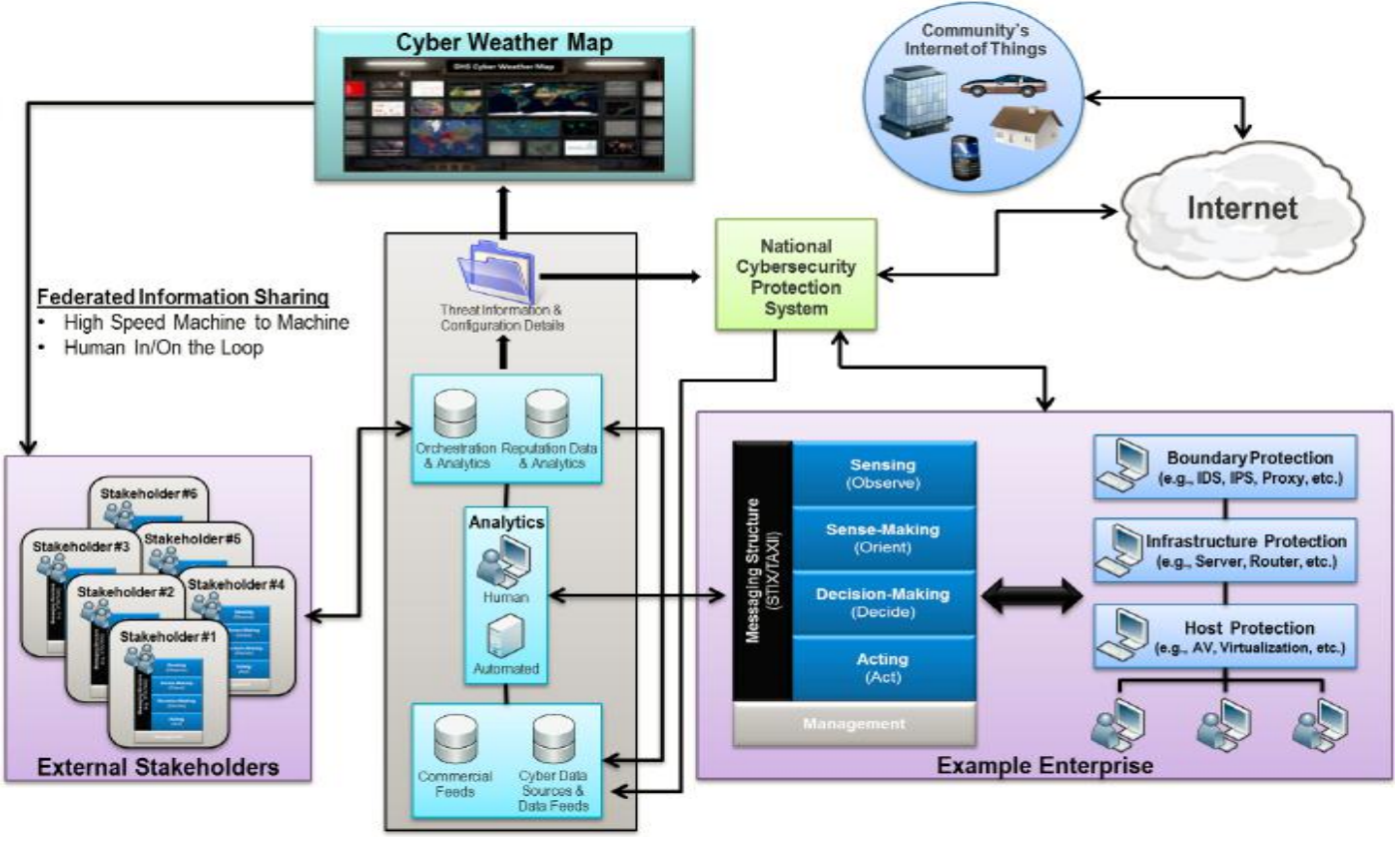
SOAR与安全集成

SOAR Integrations

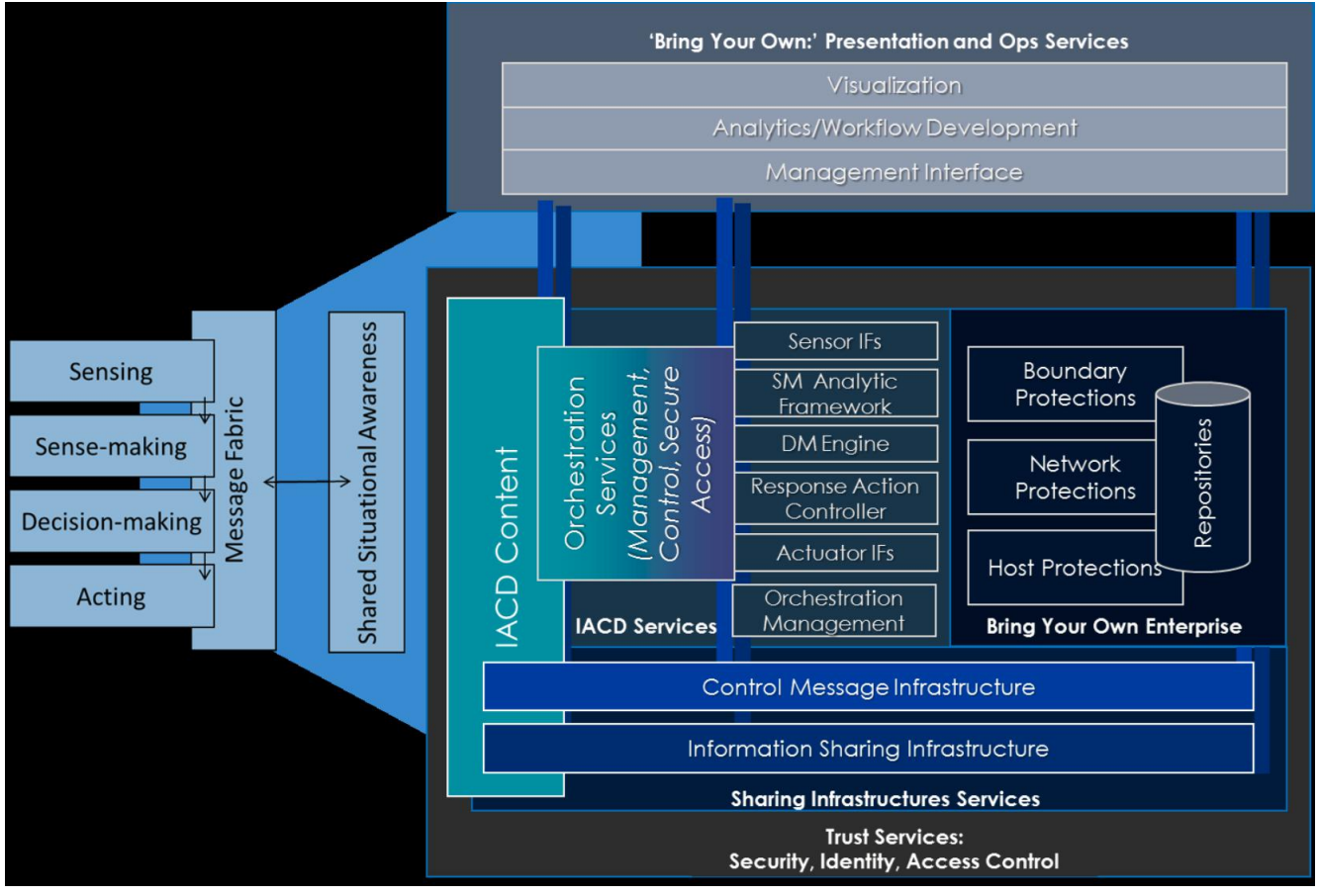


弹性、生态成为新的网络安全防护体系方向

DHS Secure and Resilient Cyber Ecosystem Example Architecture

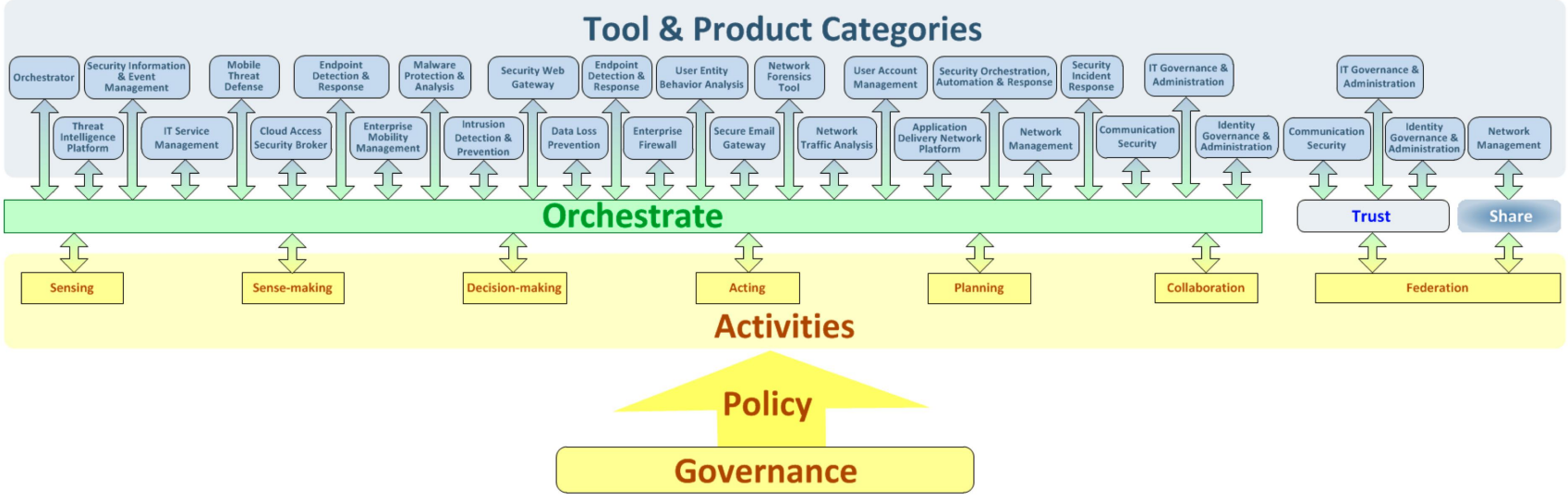


集成的自适应网络安全防护框架 IACD



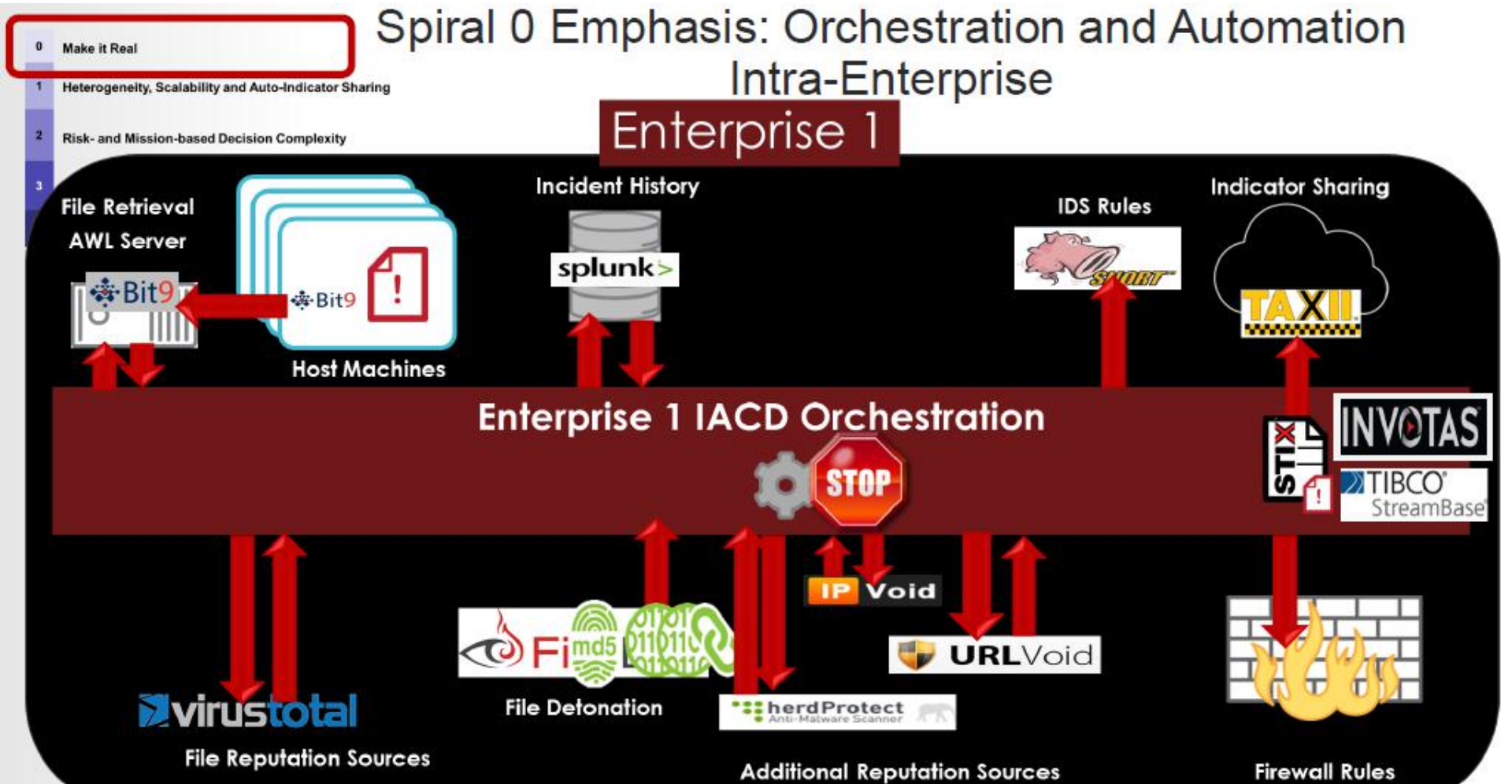
集成的自适应网络安全防护框架 IACD

Integrated Cyber Defense reference architecture - IACD

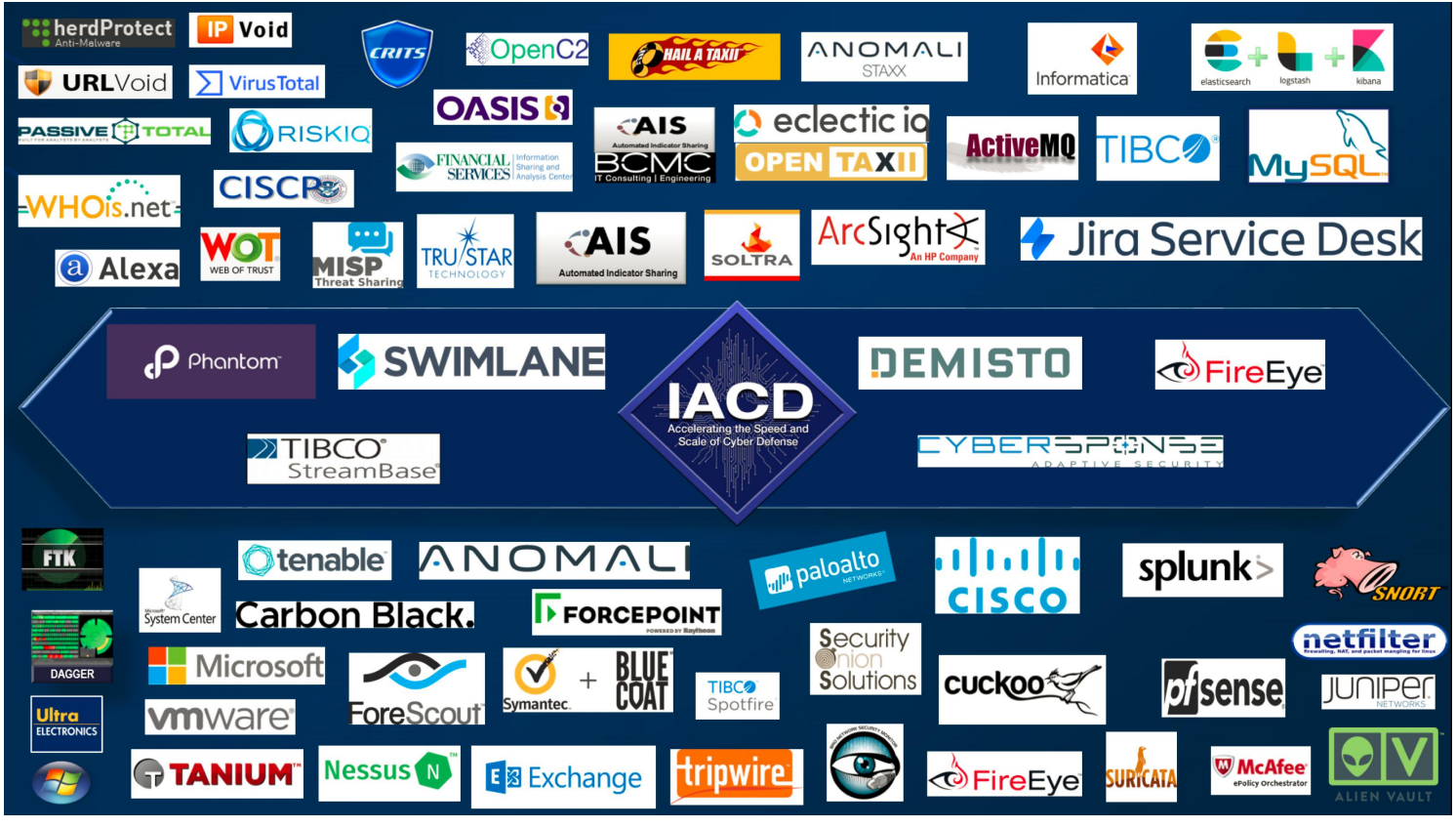


- 所有的安全防护组件能力化、标准化、API化
- 从STIX、TAXII到OpenC2，安全统一格式标准范围逐渐扩大
- 解耦、市场、生态

基于集成和自动化的新一代安全运营与应急响应解决方案



整个安全防护体系、产品即将全面升级



感谢聆听！