ATT&CK® 技术与应用论坛

ThreatBook 微步在线

ATT&CK：从威胁框架到攻击链路

基于ATT&CK的入侵检测体系

微步在线 – 陈杰

威胁发现与响应专家

THREAT DETECTION AND RESPONSE EXPERT

ThreatBook
微步在线

陈 杰

微步在线 OneEDR 业务负责人

微步在线技术运营合伙人

华盛顿大学人工智能博士

微软 Exchange 邮箱服务器安全

微软 Azure 公有云基础安全

目 录

CONTENTS

01 ATT&CK威胁框架

威胁模型

高抽象模型

Lockheed Martin的Cyber Kill Chain 模型、 Microsoft 的 STRIDE 模型等

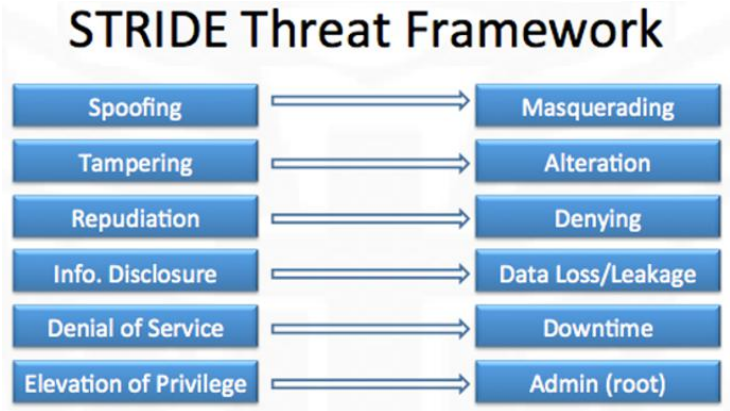
中抽象模型

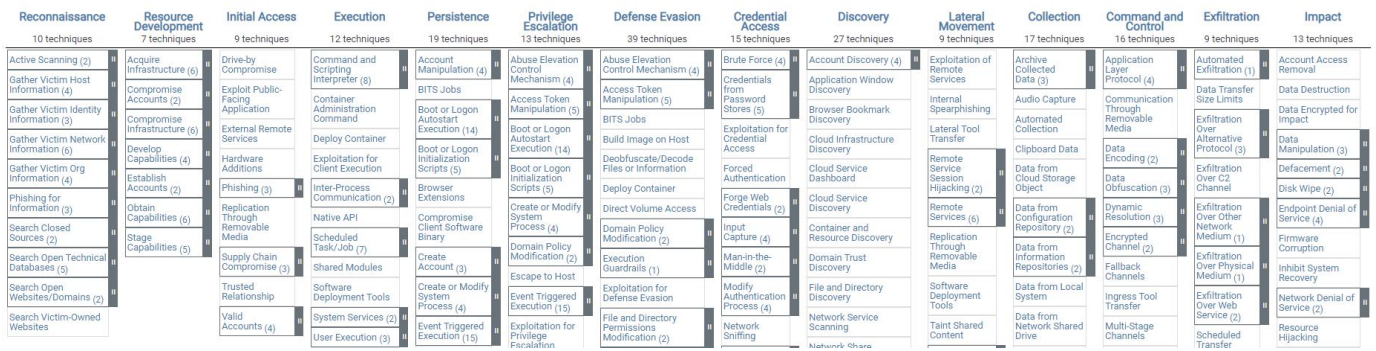
MITRE的 ATT&CK 模型

低抽象模型

漏洞库、恶意软件库等

Cyber Kill Chain

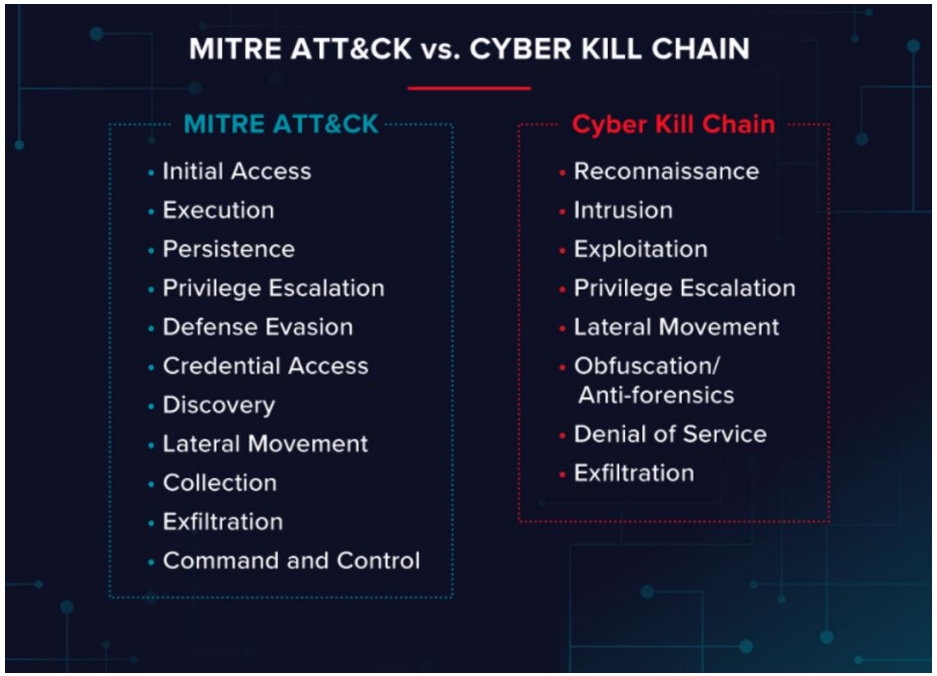




ATT&CK 威胁模型

- 攻击战术 Tactic：14个
- 攻击技术 Technique：215个

- Windows 攻击技术130+
- Linux攻击技术70+



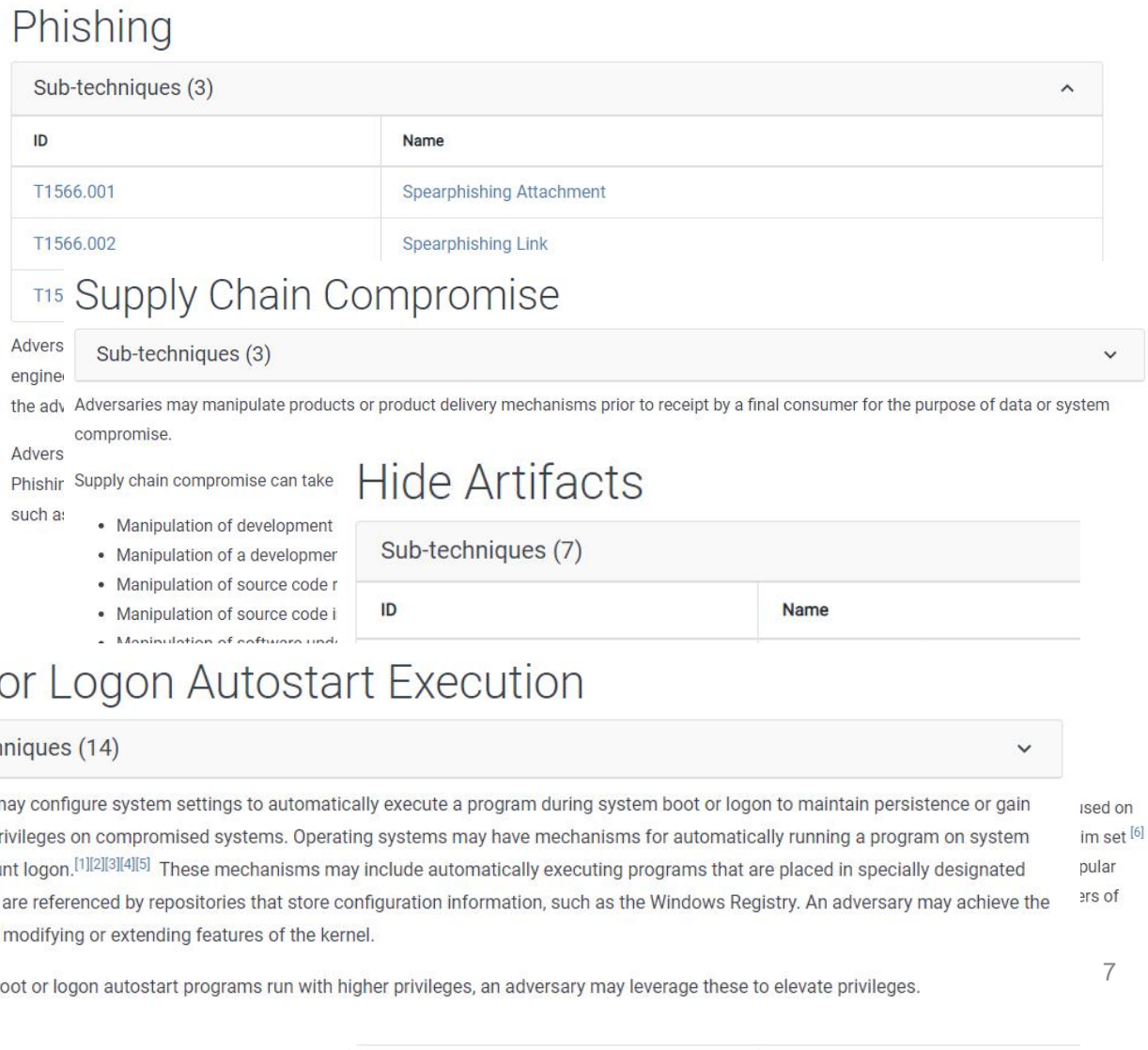
资产侦察	开发工具	初始入侵	恶意执行	巩固阵地	主机提权	躲避检测	权限窃取	资产发现	横向移动	数据收集	命令控制	数据外泄	破坏影响
10	7	9	12	19	13	39	15	27	9	17	17	9	13

攻击视角梳理攻击技术

系统化整理：TTP的战术、技术框架

统计全面：从攻击视角充分覆盖已知威胁

行业标准：威胁技术和入侵检测的行业标准

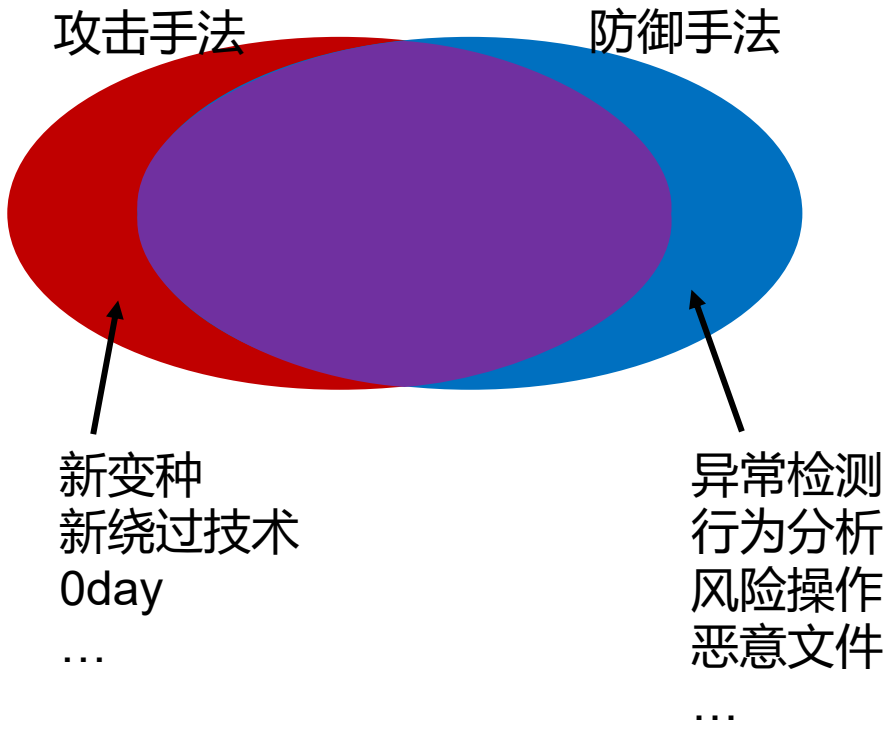


照搬ATT&CK框架
能不能构建实战化的威胁检测体系?

照搬ATT&CK框架构建的威胁检测体系的问题

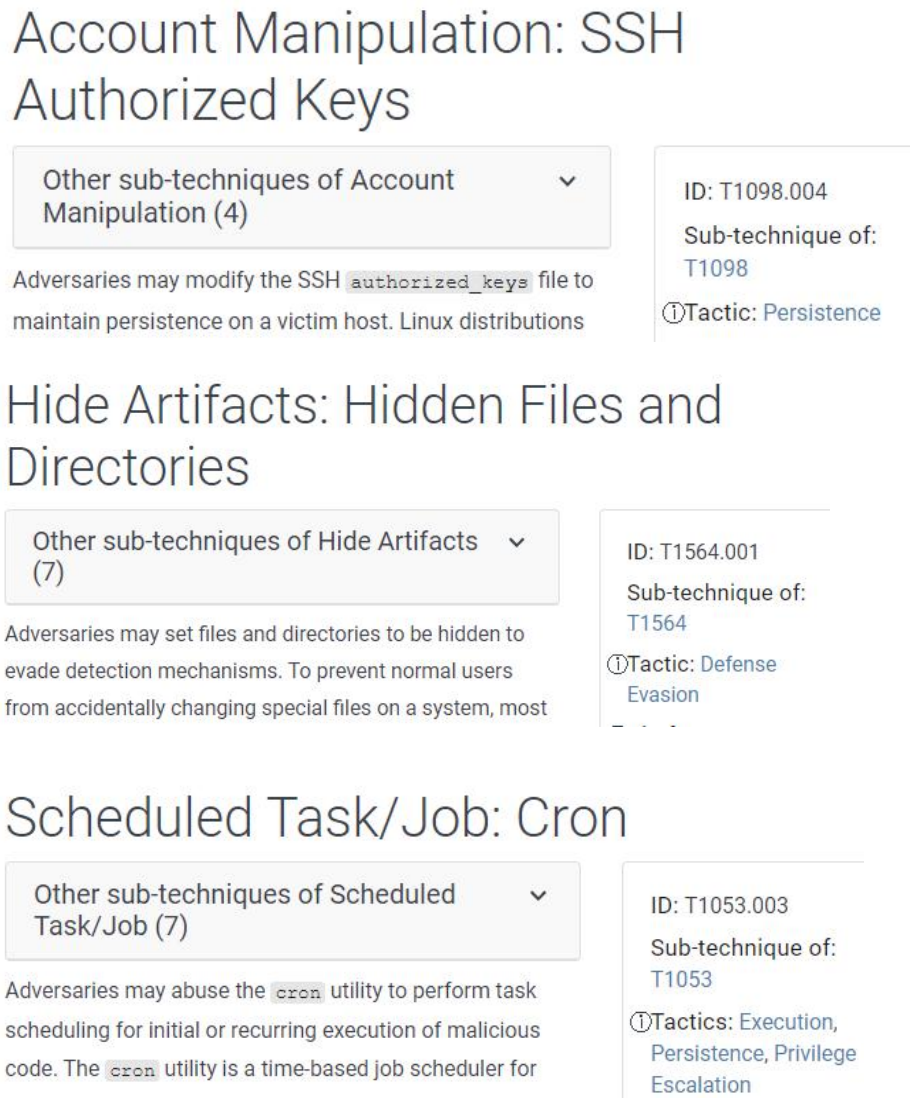
攻击视角 vs 防守视角

相交，但不重合



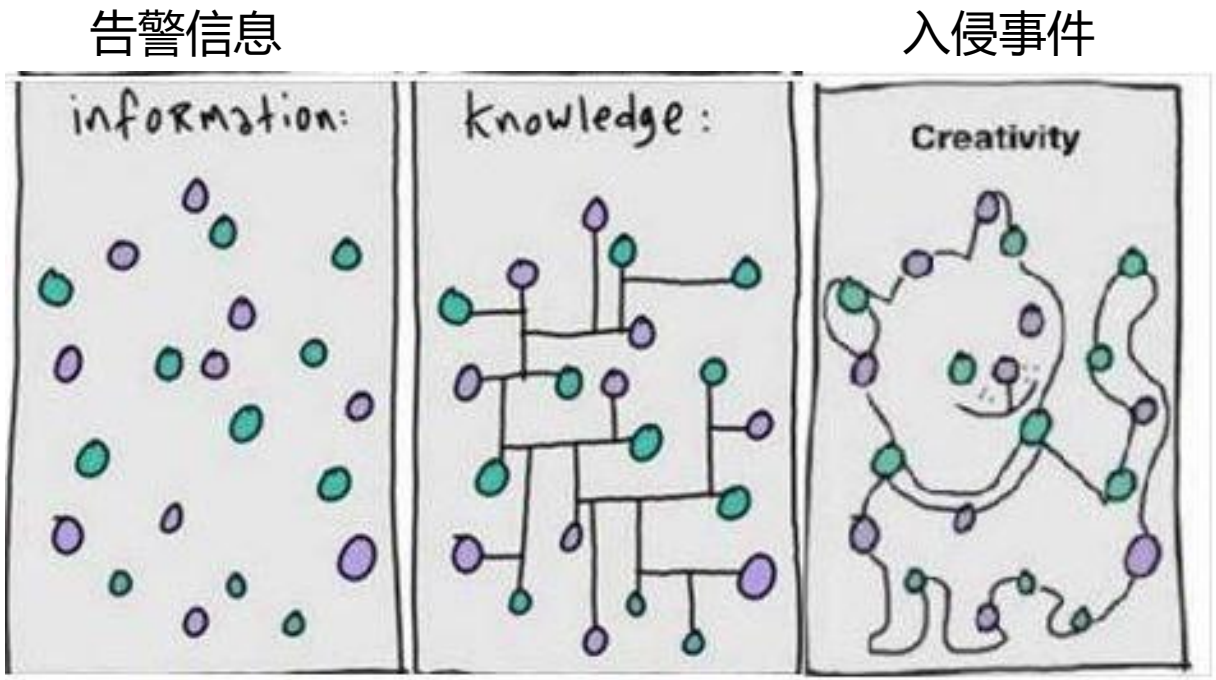
照搬ATT&CK框架构建的威胁检测体系的问题

单个行为的告警不准



照搬ATT&CK框架构建的威胁检测体系的问题

单个行为的告警
溯源困难



如何基于ATT&CK框架
构建实战化的威胁检测体系？

多级入侵检测体系

单点检测

- 攻击视角-ATT&CK
- 防守视角-风险异常
- 恶意文件-杀毒、云沙箱、Webshell

组合检测

- 行为组合提高准确率

攻击链路检测

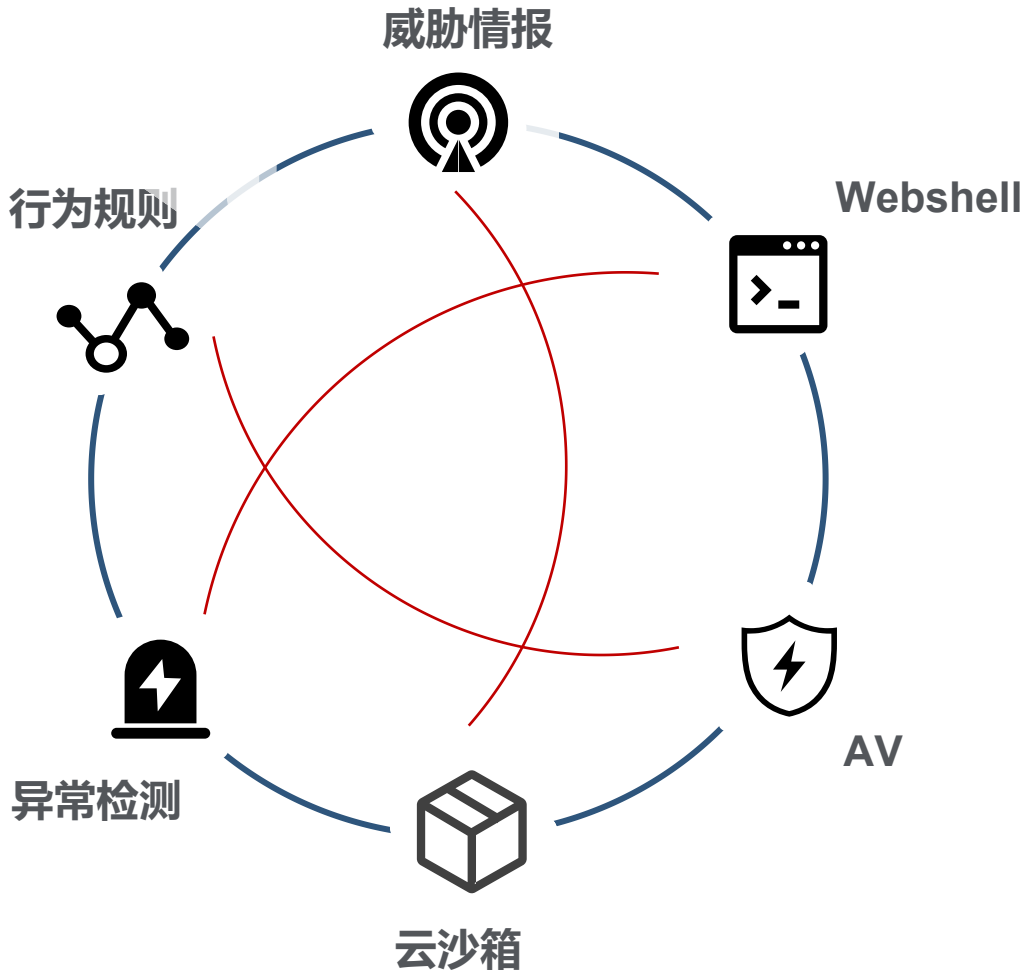
- 事件聚合
- 场景检测
- 准确+可视化溯源

02 单点检测

单点检查：防守视角

- **防守总纲：ATT&CK框架**

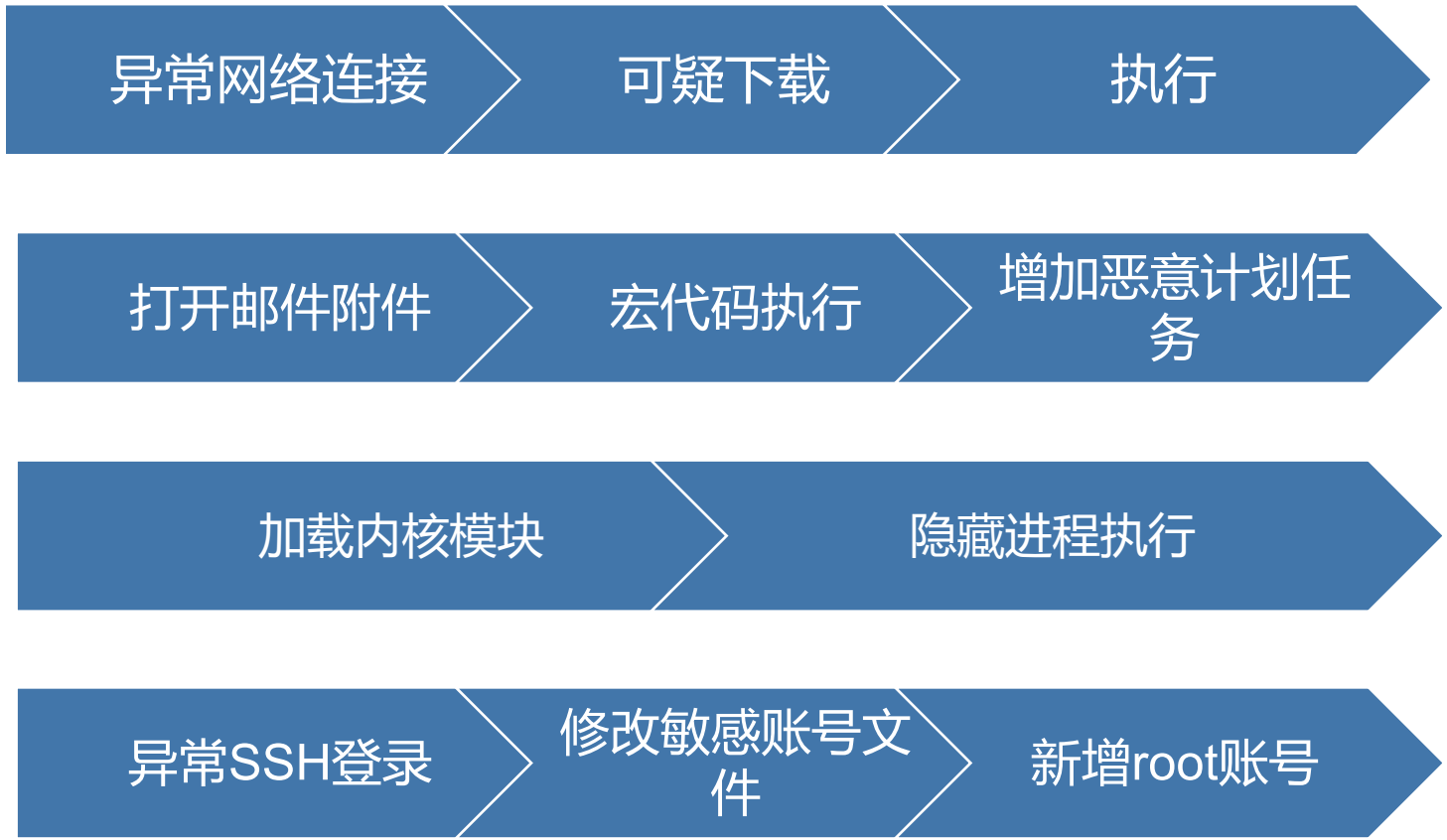
- **情报引擎**
  - 失陷外连、恶意外接
- **风险行为特征**
  - 主机提权、漏洞利用、可疑下载、修改权限等
- **异常检测**
  - 登录，进程，网络，文件，资源利用等
- **恶意文件**
  - Webshell、木马、病毒



03 行为组合检测

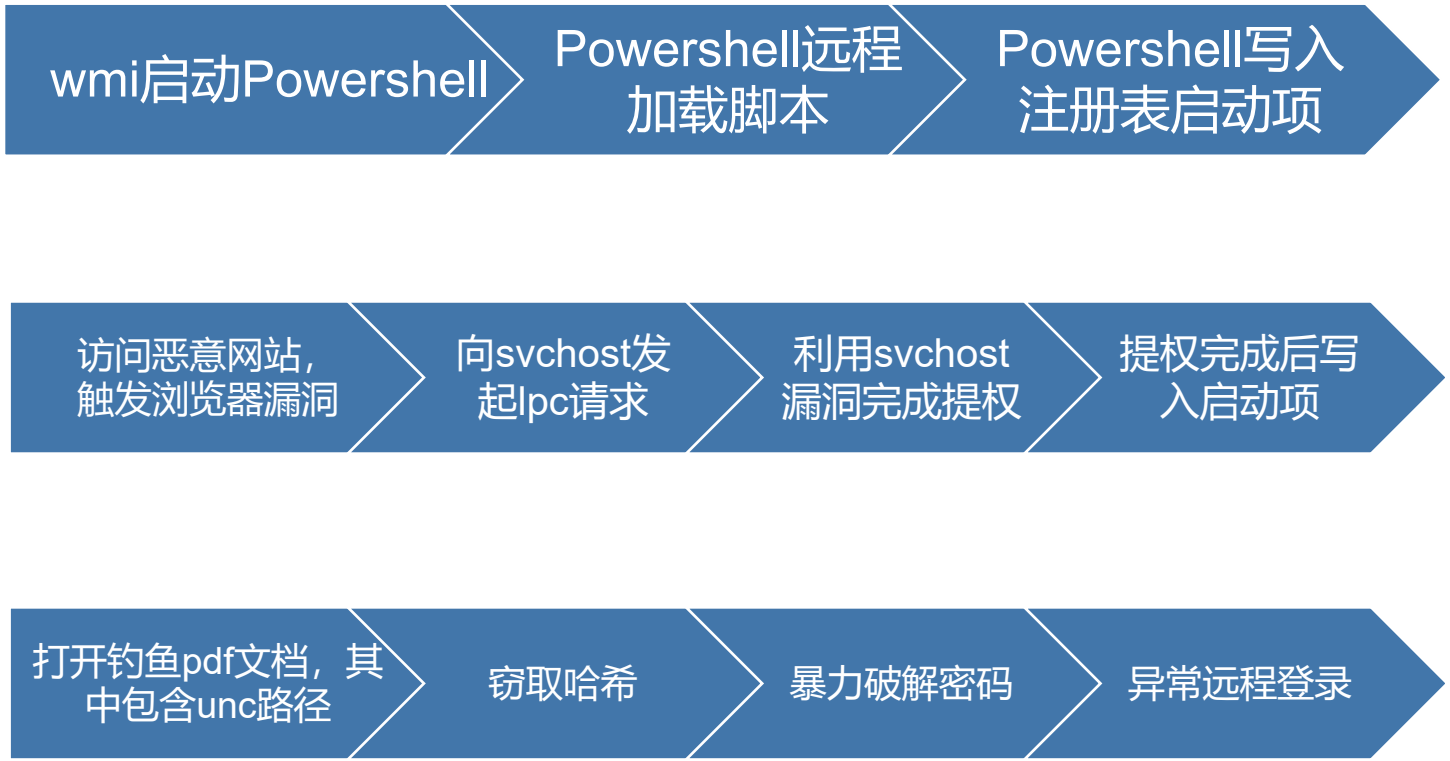
风险行为组合

- 组合行为检测提高准确率



风险行为组合

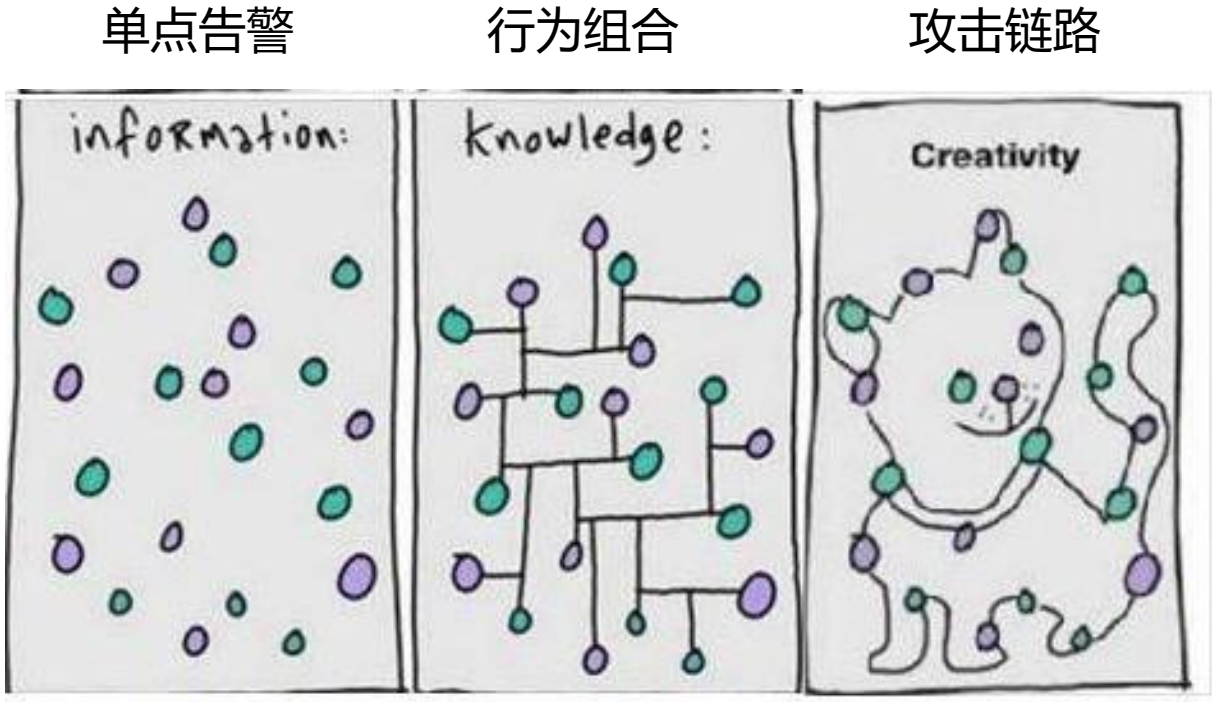
- 组合行为检测提高准确率



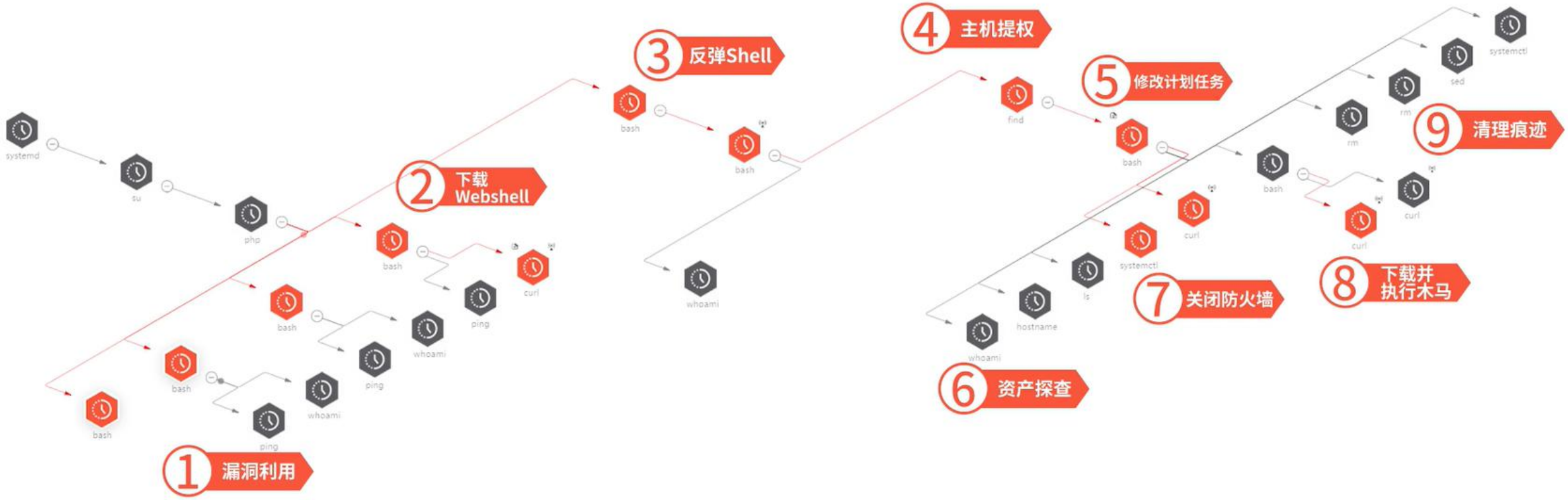
04 攻击链路检测与事件聚合

攻击链路：事件聚合

一次完整的APT攻击过程往往使用多种攻击战术与技术，并呈现一定的攻击流程。在ATT&CK框架的基础上，将攻击行为关联，并形成攻击链路用于告警研判，将极大地提升检测的准确率，并提供丰富的溯源依据。

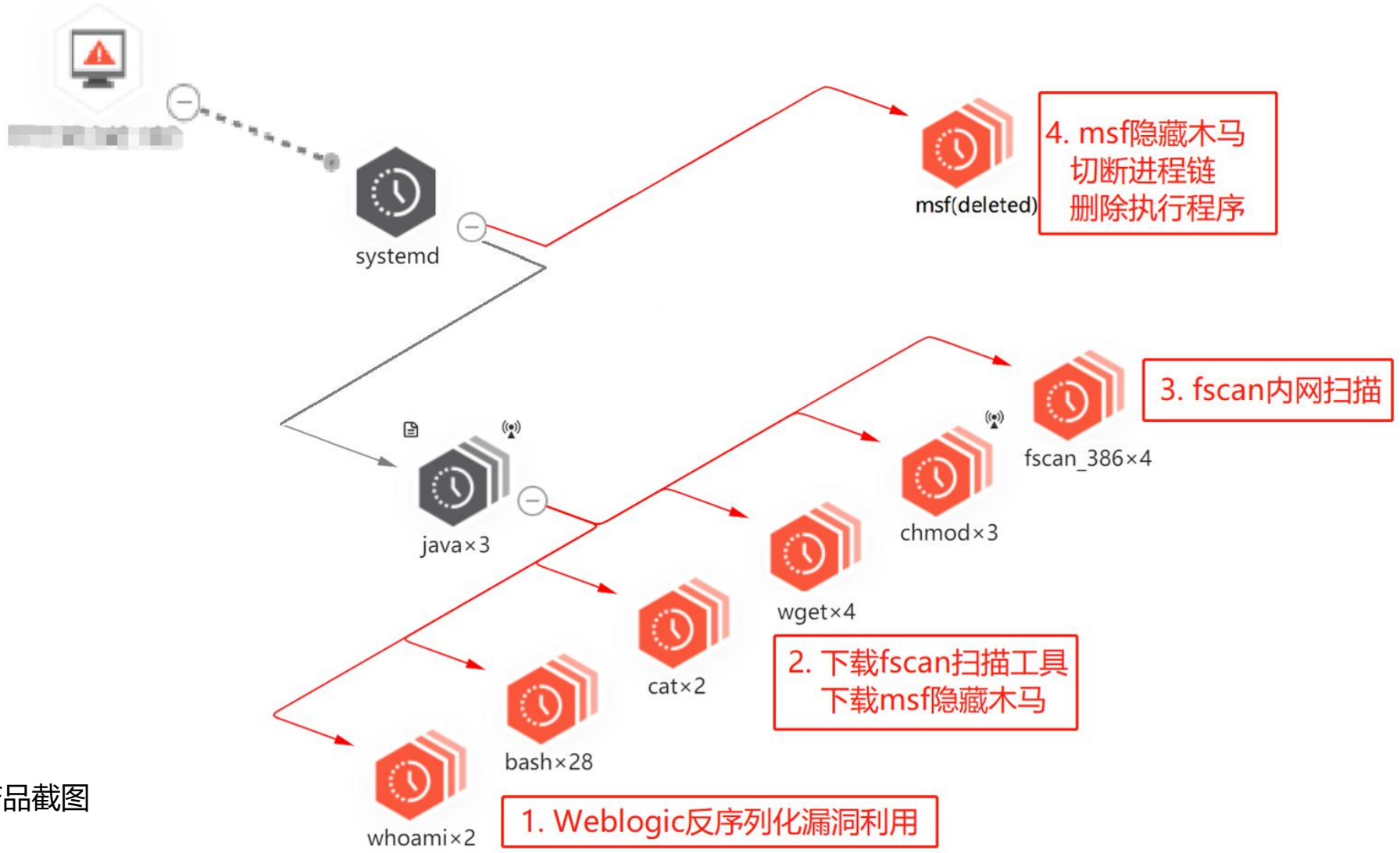


Web攻击场景



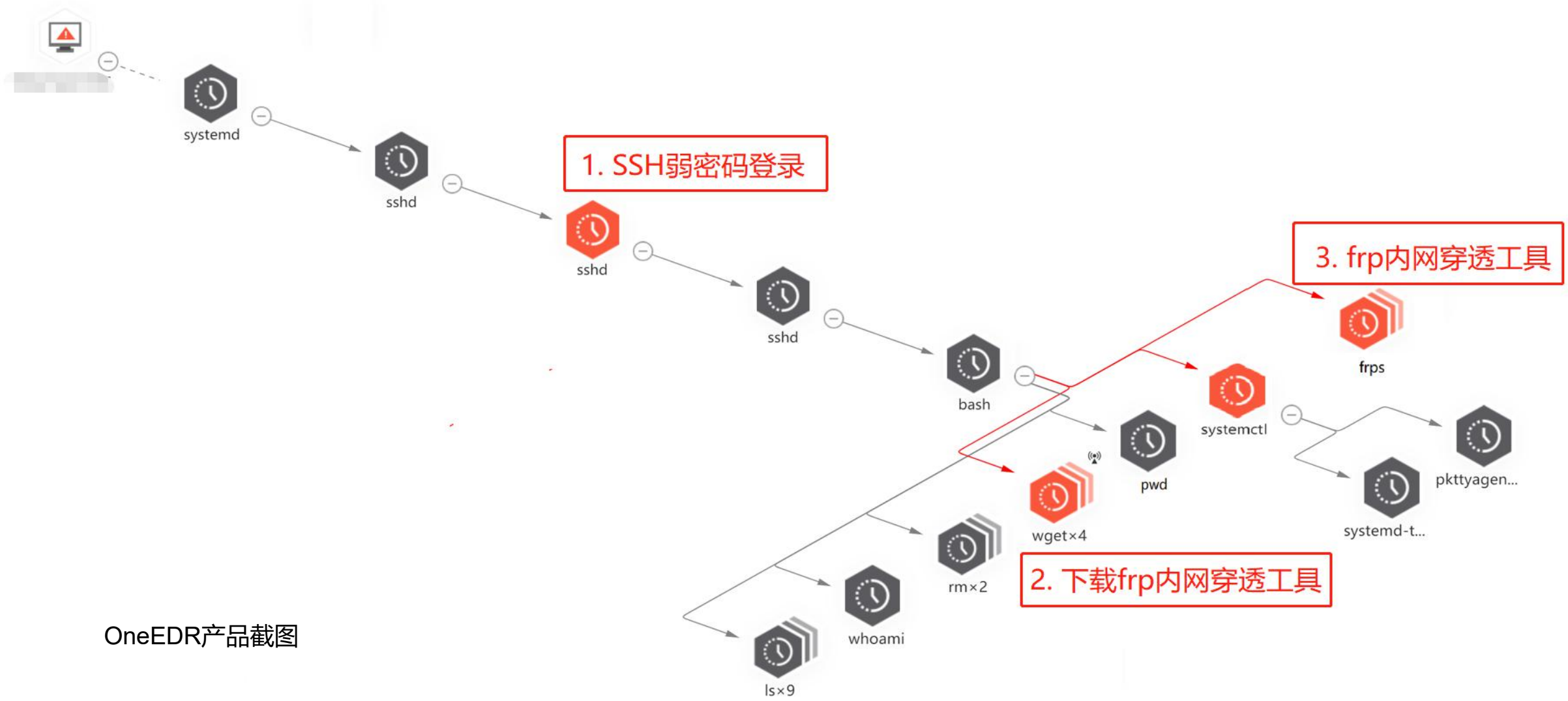
OneEDR产品截图

木马投递场景



OneEDR产品截图

建立远控通道场景



OneEDR产品截图

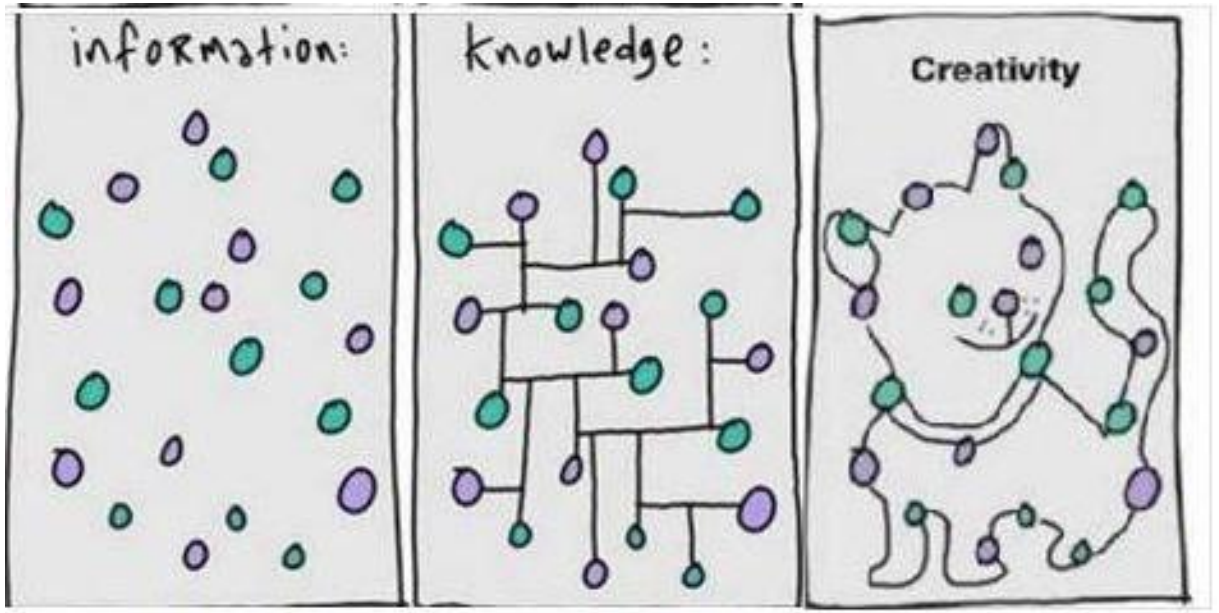
关联恶意行为上下文，**精准告警**

聚合相关告警，**还原攻击链路**

威胁链路可视化，**加快溯源**

从威胁框架到攻击链路

单点告警　　行为组合　　攻击链路



ATT&CK® 技术与应用论坛

威胁发现与响应专家

LEADER IN THREAT DETECTION AND RESPONSE

ThreatBook 微步在线

电话：400-030-1051

网址：www.threatbook.cn