

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



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

02 单点检测

03 行为组合检测

04 攻击链路检测

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

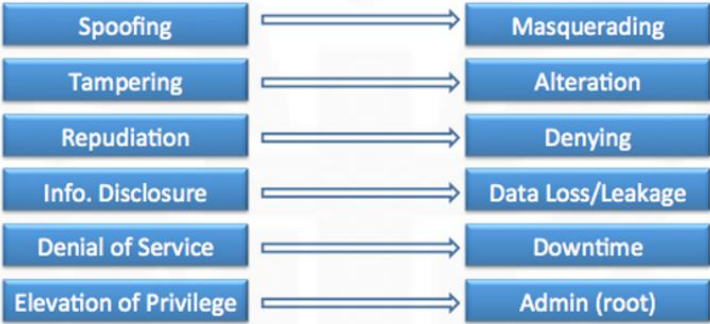
低抽象模型

漏洞库、恶意软件库等



Cyber Kill Chain

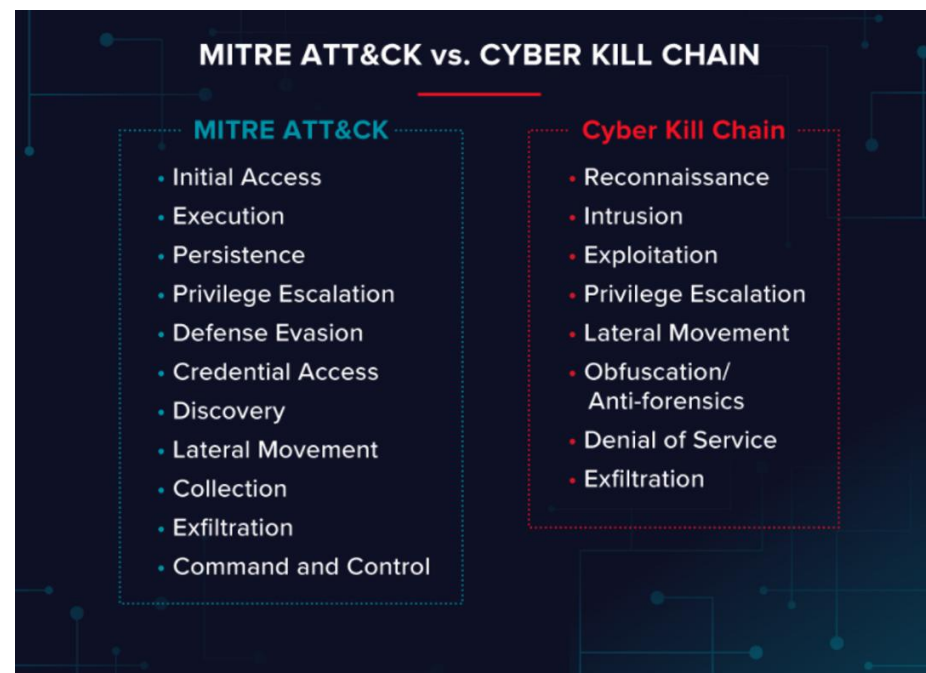
STRIDE Threat Framework



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	39 techniques	15 techniques	27 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (3) Search Closed Sources (2) Search Open Technical Databases (5) Search Open Websites/Domains (2) Search Victim-Owned Websites	Acquire Infrastructure (6) Compromise Accounts (2) Compromise Infrastructure (6) Develop Capabilities (4) Establish Accounts (2) Obtain Capabilities (6) Stage Capabilities (5) Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (3) Replication Through Removable Media Scheduled Task/Job (7) Shared Modules Software Deployment Tools System Services (2) User Execution (3)	Command and Scripting Interpreter (8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (2) Native API Scheduled Task/Job (7) Shared Modules Software Deployment Tools System Services (2) User Execution (3)	Account Manipulation (4) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Browser Extensions Compromise Client Software Binary Create Account (3) Create or Modify System Process (4) Domain Policy Modification (2) Event Triggered Execution (15) Exploitation for Privilege Escalation	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Create or Modify System Process (4) Domain Policy Modification (2) Execution Guardrails (11) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Input Capture (4) Man-in-the-Middle (2) Modify Authentication Process (4) Network Sniffing	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) BITS Jobs Build Image on Host Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (11) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Input Capture (4) Man-in-the-Middle (2) Modify Authentication Process (4) Network Sniffing	Brute Force (4) Credentials from Password Stores (5) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Man-in-the-Middle (2) Modify Authentication Process (4) Network Sniffing	Account Discovery (4) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Container and Resource Discovery Domain Trust Discovery File and Directory Discovery Network Scanning	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (6) Replication Through Removable Media Software Deployment Tools Taint Shared Content	Archive Collected Data (3) Audio Capture Automated Collection Clipboard Data Data from Cloud Storage Object Data from Configuration Repository (2) Data from Information Repositories (2) Data from Local System Data from Network Shared Drive	Application Layer Protocol (4) Communication Through Removable Media Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels	Automated Exfiltration (1) Data Transfer Size Limits Exfiltration Over Alternative Protocol (3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (2) Scheduled Transfer	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (3) Data Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking

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

Phishing

Sub-techniques (3)	
ID	Name
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link

T15 Supply Chain Compromise

Advers engine: the adv

Advers Phishir such a:

Sub-techniques (3)

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.

Supply chain compromise can take

- Manipulation of development
- Manipulation of a developer
- Manipulation of source code r
- Manipulation of source code i
- Manipulation of software und

Hide Artifacts

Sub-techniques (7)

ID	Name
----	------

Boot or Logon Autostart Execution

Sub-techniques (14)

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.^{[1][2][3][4][5]} These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel.

Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

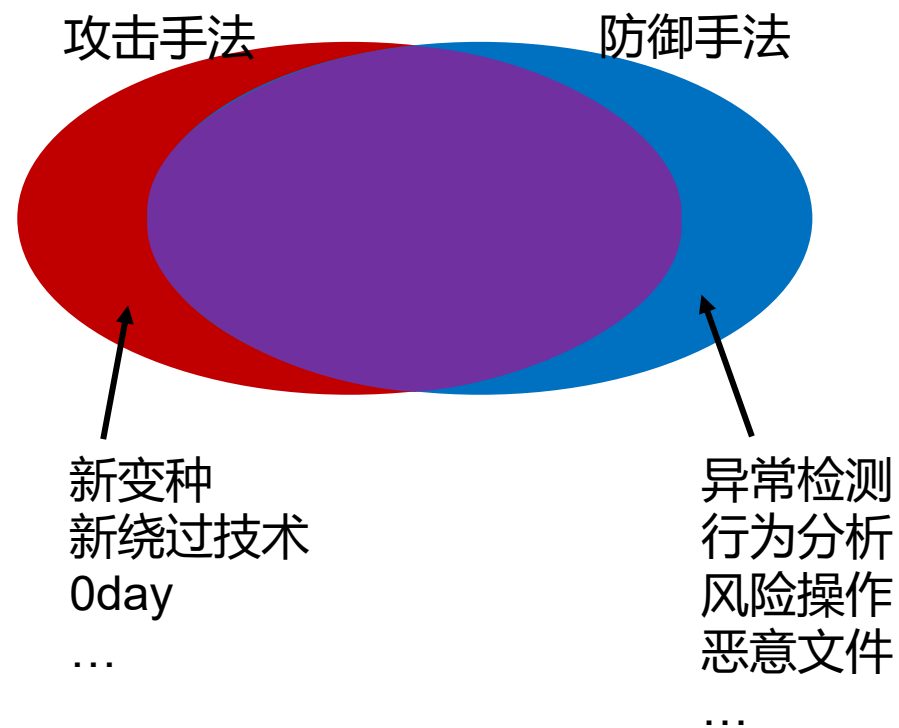
ised on
im set ^[6]
pular
ars of

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

Account Manipulation: SSH Authorized Keys

Other sub-techniques of Account Manipulation (4)

Adversaries may modify the SSH `authorized_keys` file to maintain persistence on a victim host. Linux distributions

ID: T1098.004

Sub-technique of: T1098

①Tactic: Persistence

Hide Artifacts: Hidden Files and Directories

Other sub-techniques of Hide Artifacts (7)

Adversaries may set files and directories to be hidden to evade detection mechanisms. To prevent normal users from accidentally changing special files on a system, most

ID: T1564.001

Sub-technique of: T1564

①Tactic: Defense Evasion

Scheduled Task/Job: Cron

Other sub-techniques of Scheduled Task/Job (7)

Adversaries may abuse the `cron` utility to perform task scheduling for initial or recurring execution of malicious code. The `cron` utility is a time-based job scheduler for

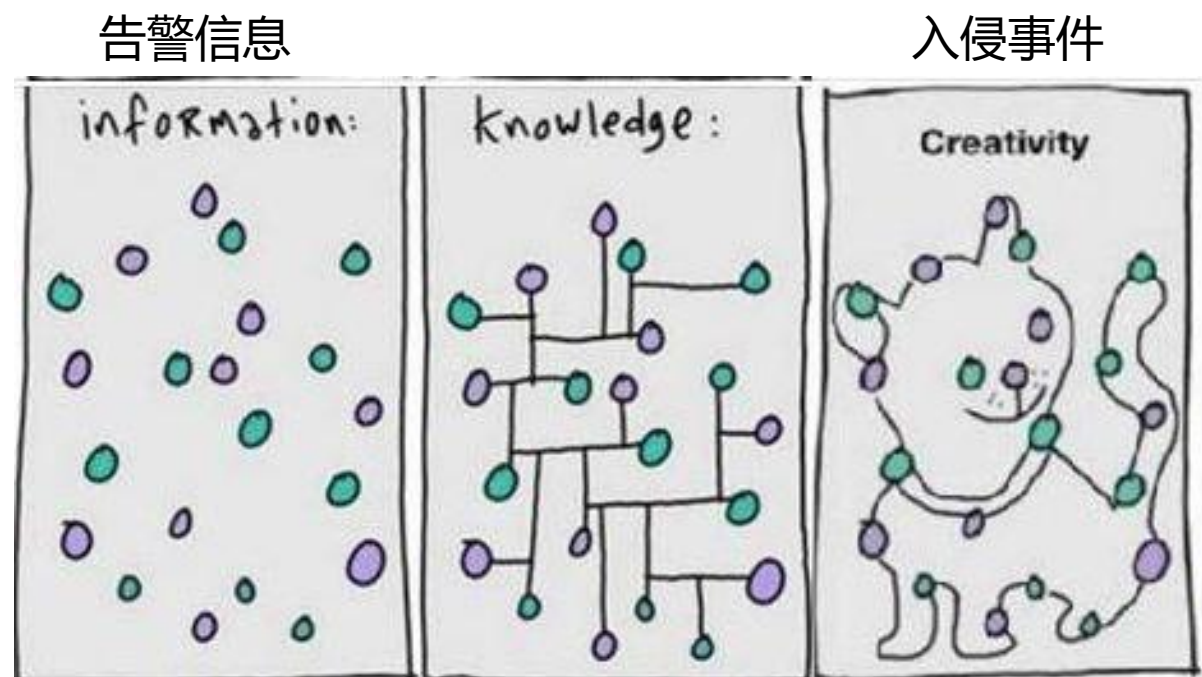
ID: T1053.003

Sub-technique of: T1053

①Tactics: Execution, Persistence, Privilege Escalation

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

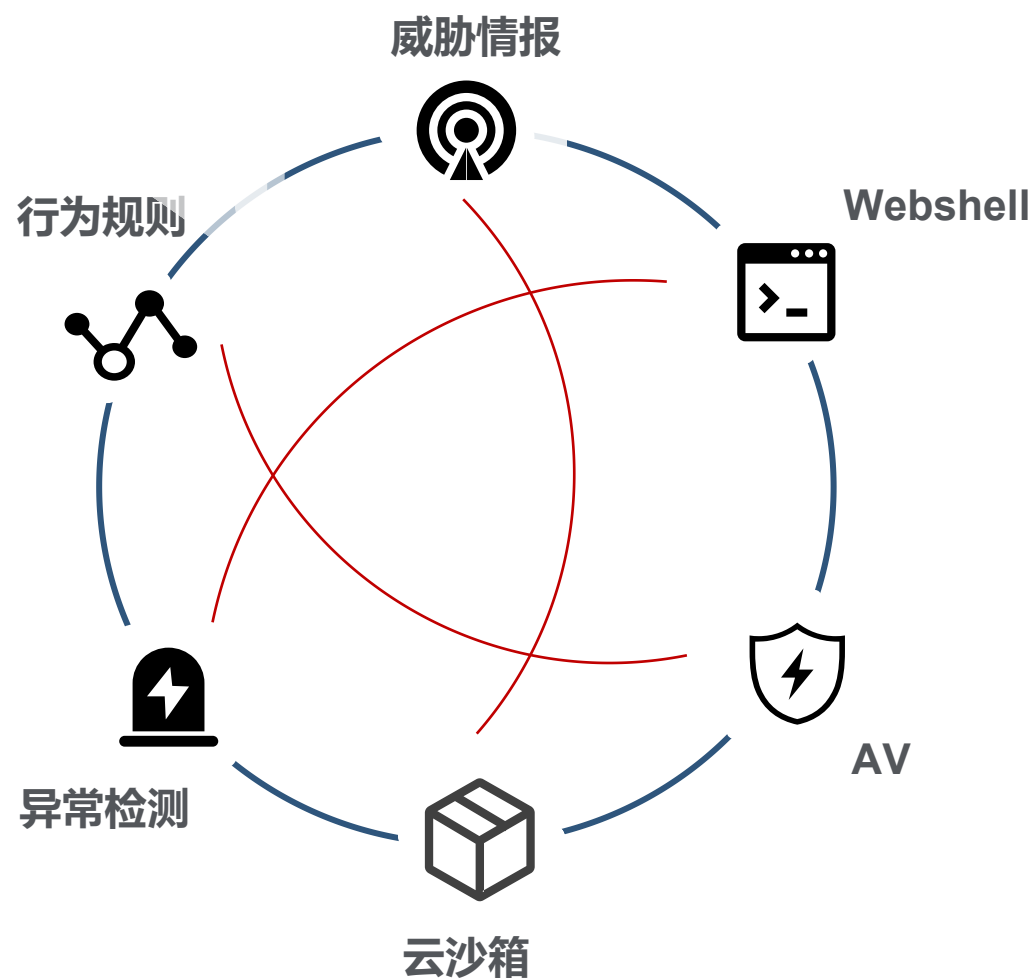
攻击链路检测

- 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

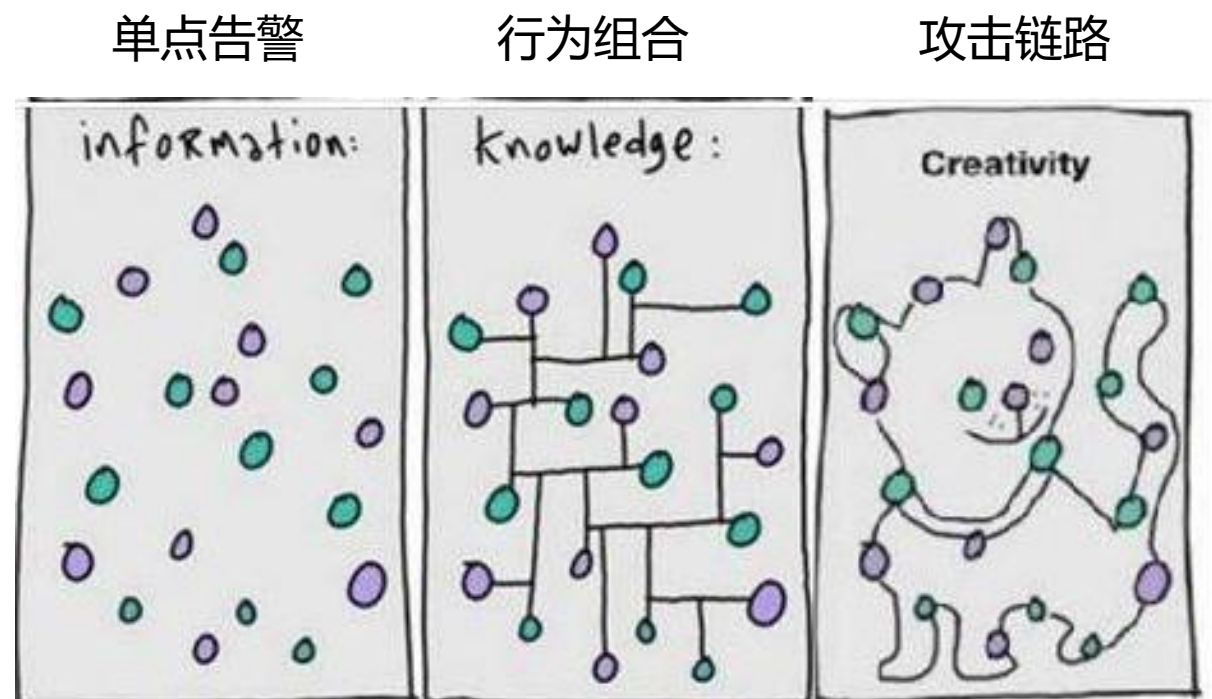


04

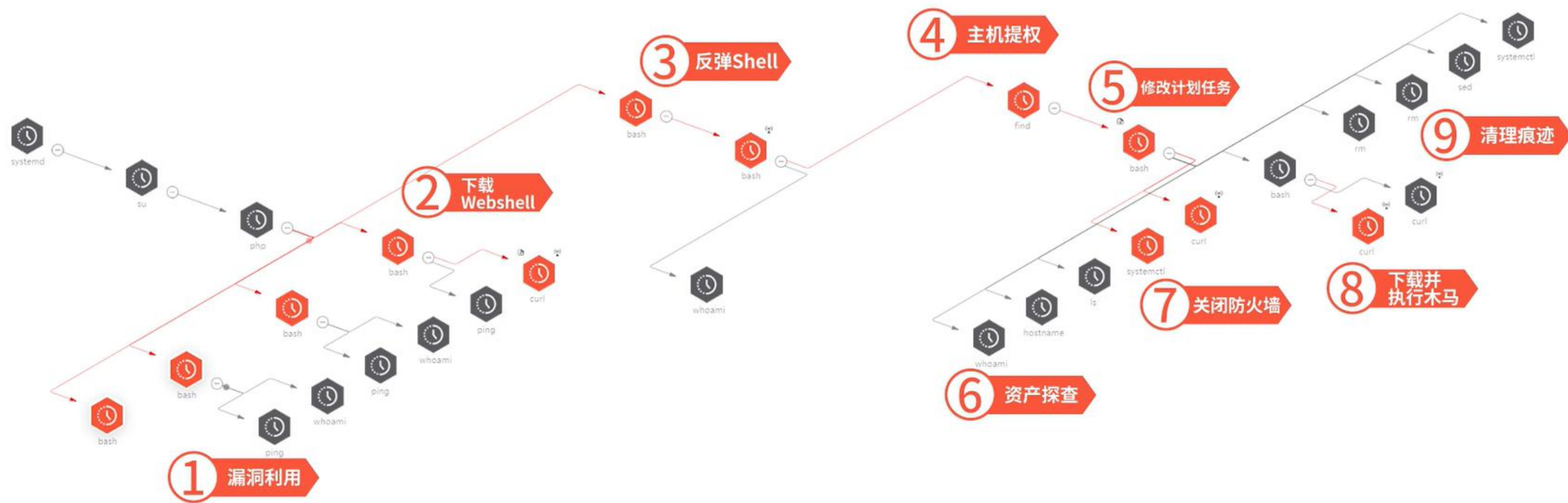
攻击链路检测与事件聚合

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。

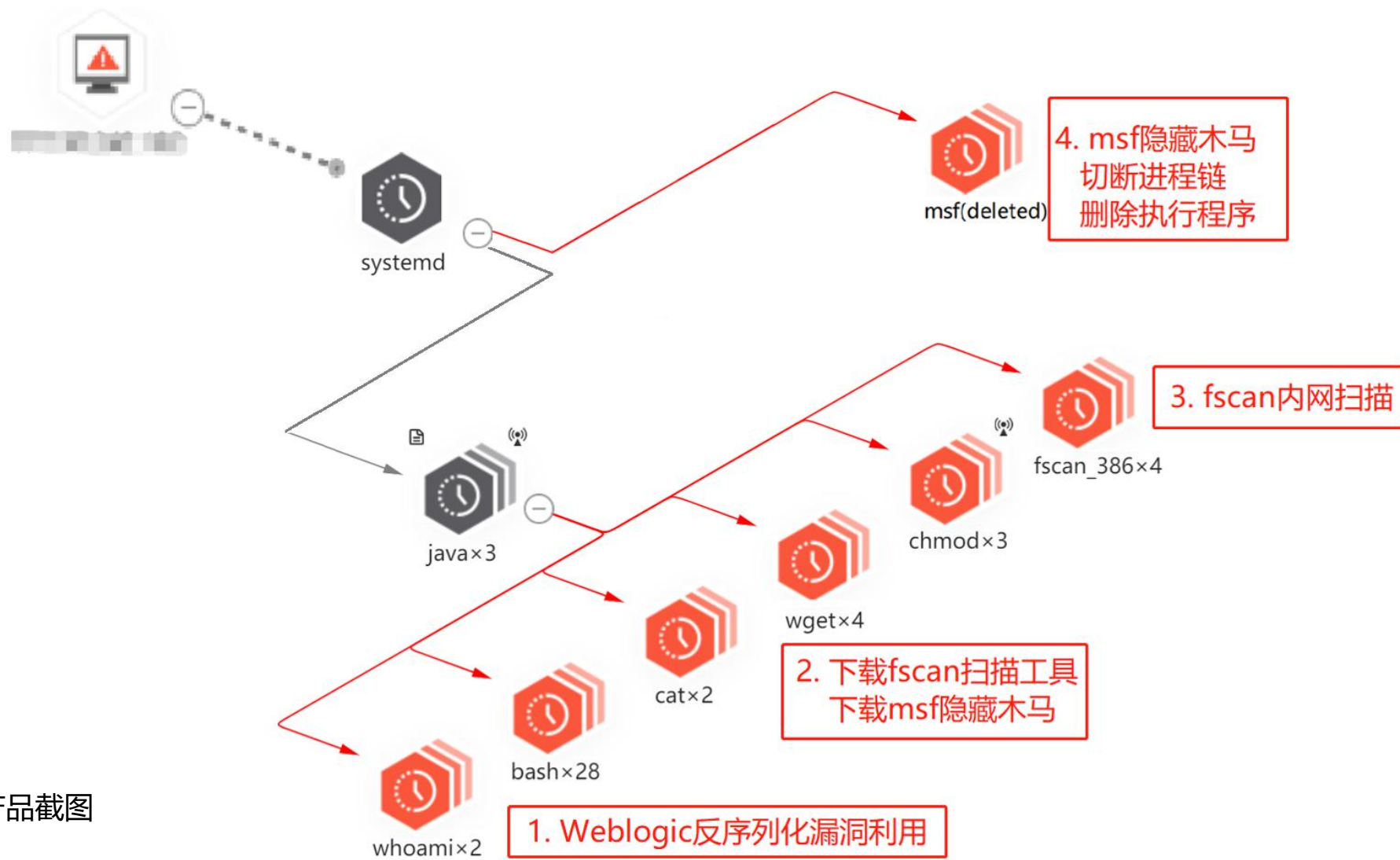


Web攻击场景



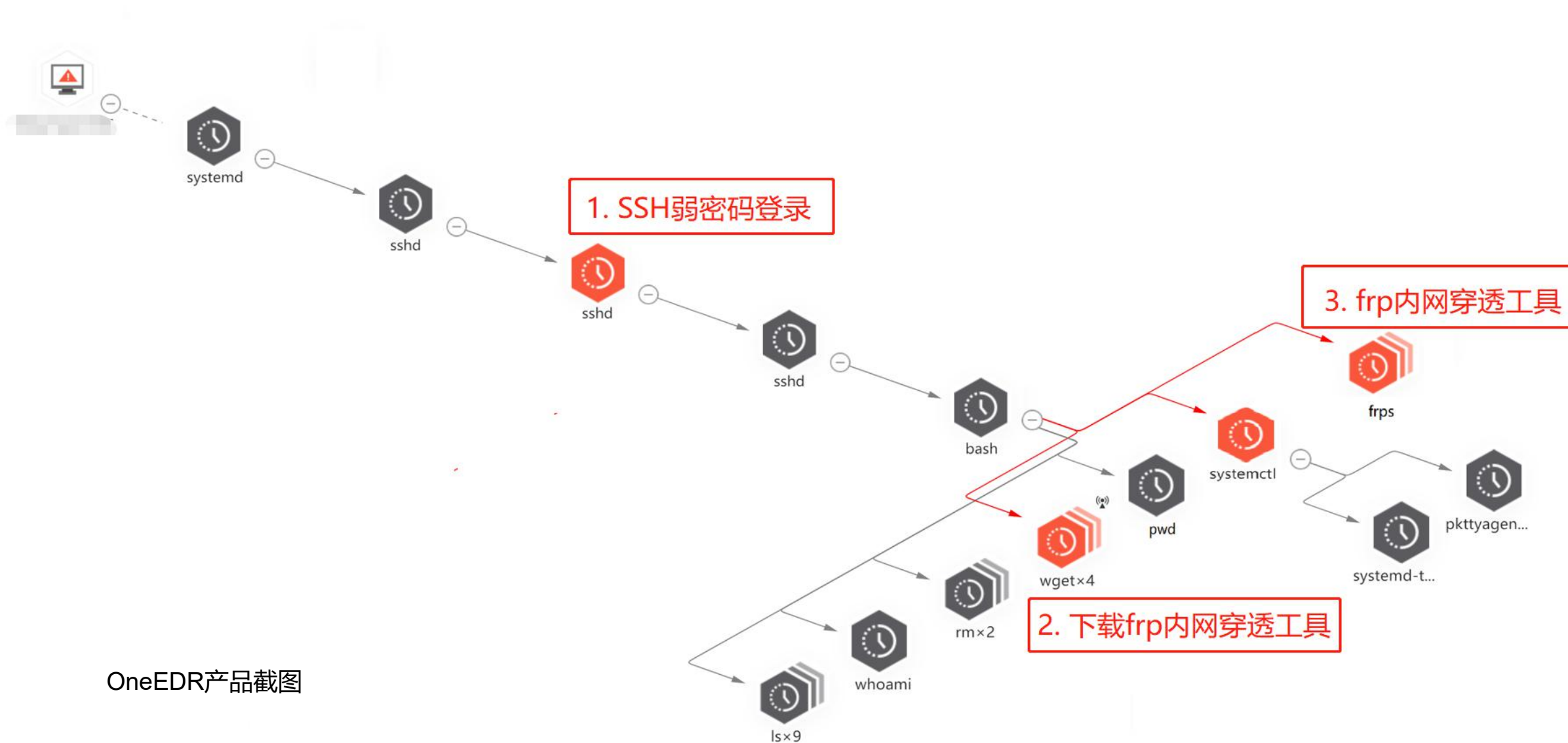
OneEDR产品截图

木马投递场景



OneEDR产品截图

建立远控通道场景



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**

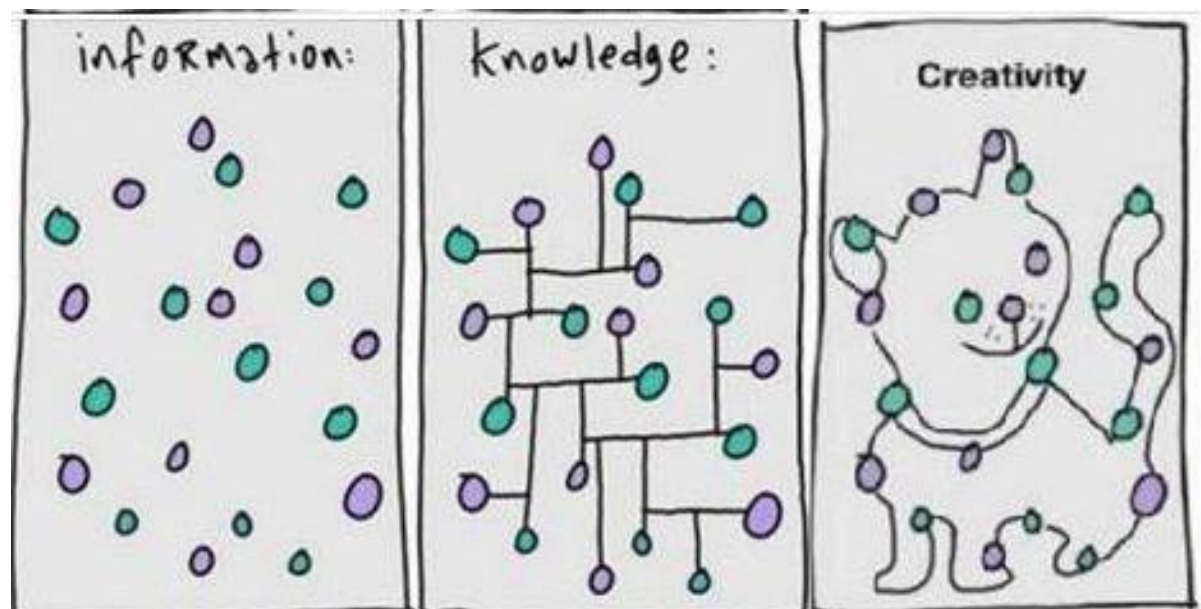
威胁链路可视化，**加快溯源**

从威胁框架到攻击链路

单点告警

行为组合

攻击链路





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