资源代价与安全算力

安天安全方法框架

安天 | 研究院

安天的价值主张

- 依托**端到端的安全能力**和**供应链关口前移**的优势，实现全场景的有效防御覆盖与可信场景构造。并依托强大的**威胁对抗体系**，实现深度客户赋能，驱动客户完成从威胁情报消费，到自主安全能力生产的智能化安全运营变革。
- 我们支撑战略客户达成威胁对抗+安全防护+数字化的大闭环愿景，我们以价值创新体系驱动产业的价值提升。
- 我们的能力是国家网空防御能力的基石，是中国网络空间良赢治理的支点，是维护网络空间人类命运共同体安全的支撑力量。

CONTENTS

目 录

01 安全规划与建设的起点
——威胁想定框架

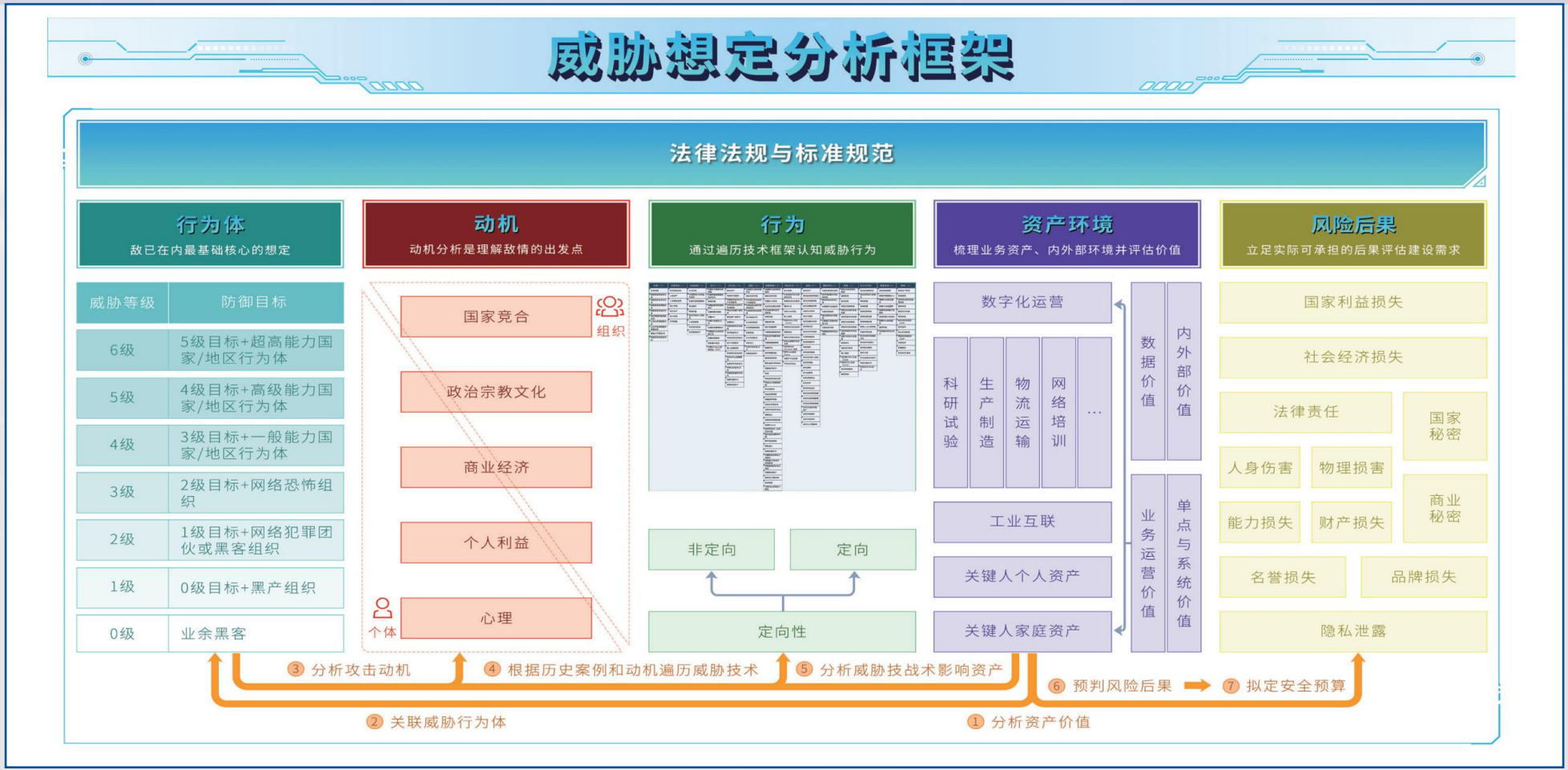
02 迅速建立威胁认知的能力
——杀伤链与威胁技术框架

03 从威胁框架落地到承载的产品
——能力型产品技术框架

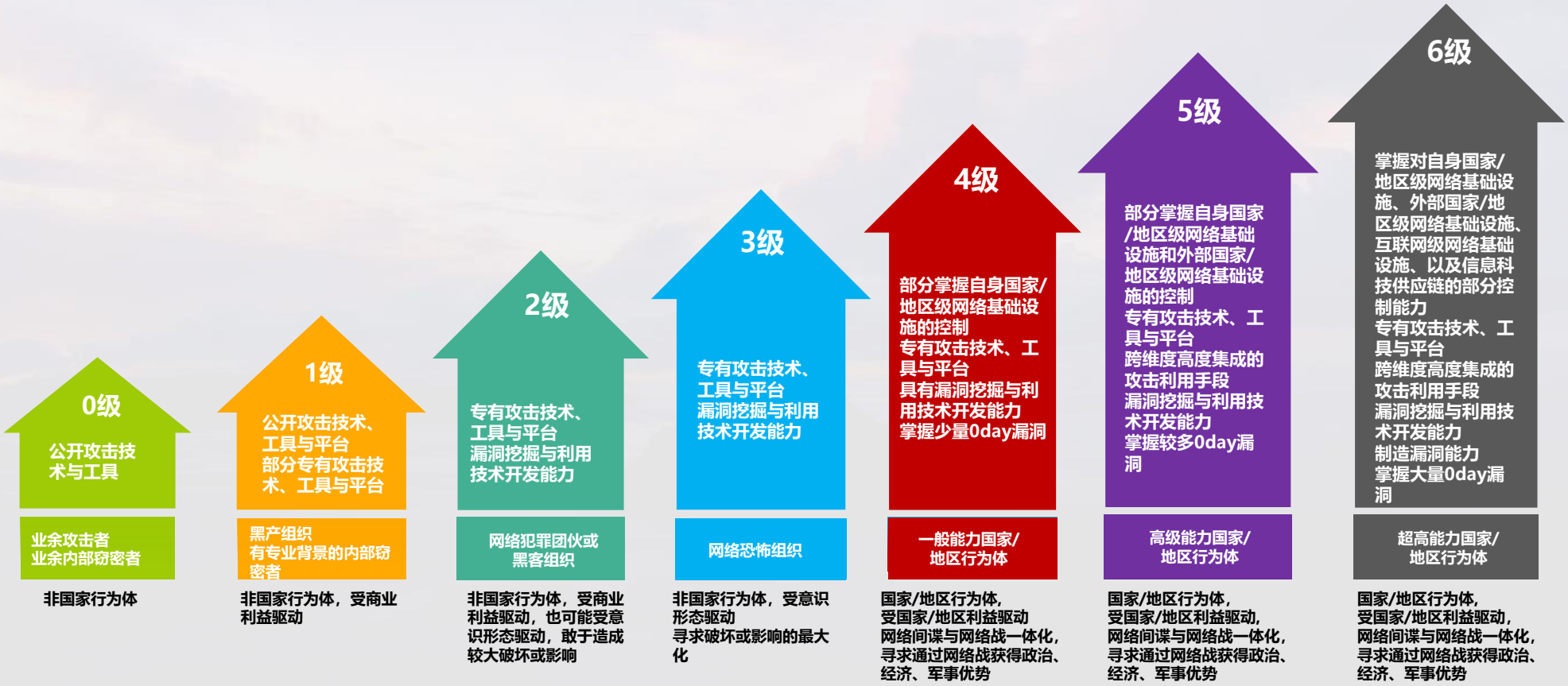
04 衔接规划（采购）与日常运营
——双环驱动与威胁猎杀

01 安全规划与建设的起点——威胁想定框架

威胁想定分析框架


威胁想定分析框架
法律法规与标准规范
行为体
敌已在内最基础核心的想定
动机
动机分析是理解敌情的出发点
行为
通过遍历技术框架认知威胁行为
资产环境
梳理业务资产、内外部环境并评估价值
风险后果
立足实际可承担的后果评估建设需求
威胁等级
防御目标
6级
5级目标+超高能力国家/地区行为体
5级
4级目标+高级能力国家/地区行为体
4级
3级目标+一般能力国家/地区行为体
3级
2级目标+网络恐怖组织
2级
1级目标+网络犯罪团伙或黑客组织
1级
0级目标+黑产组织
0级
业余黑客
国家竞合
组织
政治宗教文化
商业经济
个人利益
心理
个体
非定向
定向
定向性
数字化运营
科研试验
生产制造
物流运输
网络培训
…
工业互联
关键人个人资产
关键人家庭资产
数据价值
内外部价值
业务运营价值
单点与系统价值
国家利益损失
社会经济损失
法律责任
国家秘密
人身伤害
物理损害
商业秘密
能力损失
财产损失
名誉损失
品牌损失
隐私泄露
③ 分析攻击动机
④ 根据历史案例和动机遍历威胁技术
⑤ 分析威胁技战术影响资产
⑥ 预判风险后果
⑦ 拟定安全预算
② 关联威胁行为体
① 分析资产价值

威胁行为体评估体系


0级
公开攻击技术与工具
业余攻击者
业余内部窃密者
非国家行为体
1级
公开攻击技术、工具与平台
部分专有攻击技术、工具与平台
黑产组织
有专业背景的内部窃密者
非国家行为体，受商业利益驱动
2级
专有攻击技术、工具与平台
漏洞挖掘与利用技术开发能力
网络犯罪团伙或黑客组织
非国家行为体，受商业利益驱动，也可能受意识形态驱动，敢于造成较大破坏或影响
3级
专有攻击技术、工具与平台
漏洞挖掘与利用技术开发能力
网络恐怖组织
非国家行为体，受意识形态驱动
寻求破坏或影响的最大化
4级
部分掌握自身国家/地区级网络基础设施的控制
专有攻击技术、工具与平台
具有漏洞挖掘与利用技术开发能力
掌握少量0day漏洞
一般能力国家/地区行为体
国家/地区行为体，
受国家/地区利益驱动
网络间谍与网络战一体化，
寻求通过网络战获得政治、经济、军事优势
5级
部分掌握自身国家/地区级网络基础设施和外部国家/地区级网络基础设施的控制
专有攻击技术、工具与平台
跨维度高度集成的攻击利用手段
漏洞挖掘与利用技术开发能力
掌握较多0day漏洞
高级能力国家/地区行为体
国家/地区行为体，
受国家/地区利益驱动，
网络间谍与网络战一体化，
寻求通过网络战获得政治、经济、军事优势
6级
掌握对自身国家/地区级网络基础设施、外部国家/地区级网络基础设施、互联网级网络基础设施、以及信息科技供应链的部分控制能力
专有攻击技术、工具与平台
跨维度高度集成的攻击利用手段
漏洞挖掘与利用技术开发能力
制造漏洞能力
掌握大量0day漏洞
超高能力国家/地区行为体
国家/地区行为体，
受国家/地区利益驱动，
网络间谍与网络战一体化，
寻求通过网络战获得政治、经济、军事优势

威胁想定分析方法与现有方法相比的进步和差异

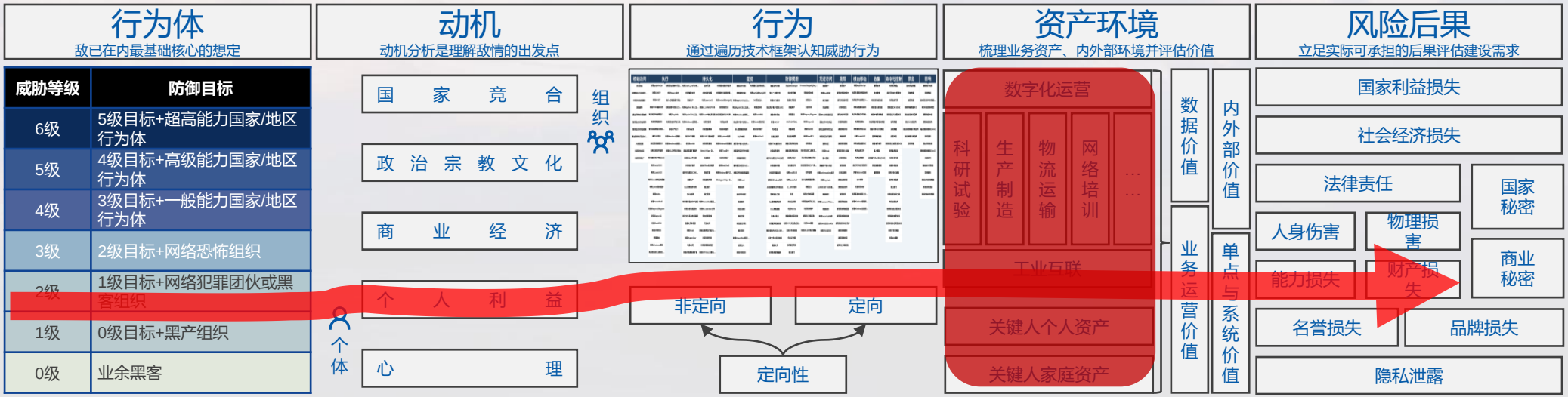
- 威胁想定分析框架与传统的等保评估、风险评估是由较大不同，等保评估是一个类似合规点清单的方法，用来评价防御手段建设是否覆盖了等级保护要求。风险评估是基于暴露面和脆弱性的分析，分析。

- 安天威胁想定分析方法，是以客户资产（IT设施）价值与威胁活动和行为体的相关性来入手展开的，其重点分析客户可能遭到何种层级，甚至哪一个具体的威胁行为体、以何种动机遭到的攻击。同时从国家安全、社会安全、政企机构安全和个人安全四个层次，来分析不同攻击的后果和影响。

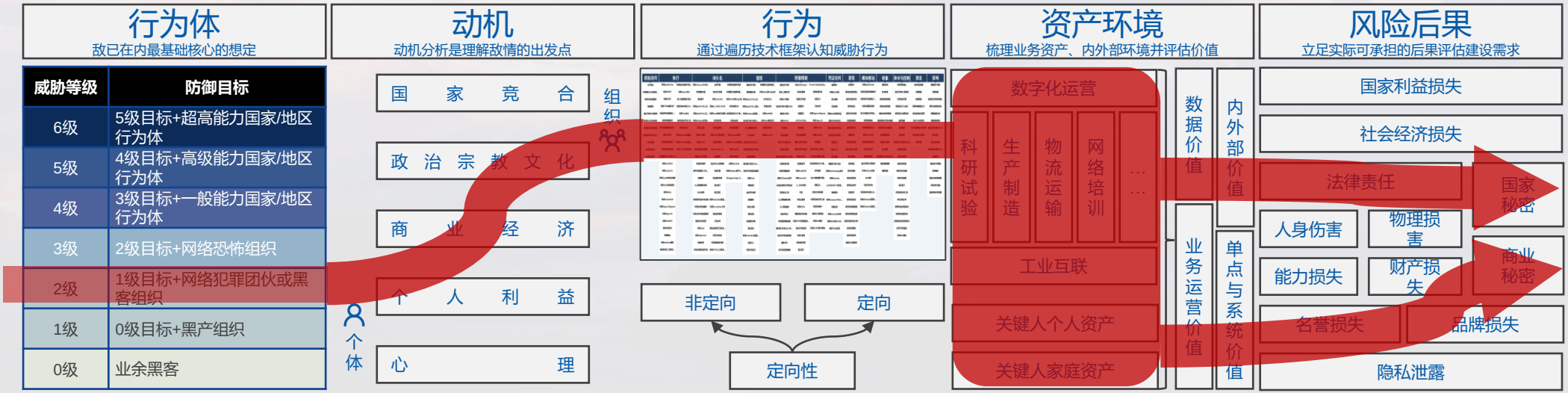
- 进一步从后果和影响来反过来测算安全预算和资源的规模

- 在预算丰富的情况下，帮助客户建构与业务高度融合的一体化运营体系，在预算不充足的情况下帮助客户优先完成端点统管、情报驱动等关键环节建设。

框架推演1：勒索软件威胁数字转型企业，造成直接经济损失



框架推演2： 对手以商业竞争为目的购买黑产服务、投递窃密木马



02 迅速建立威胁认知的能力

——OODA循环、杀伤链与威胁技术框架

OODA循环、网空杀伤链与威胁框架

- OODA循环：闭环是一切持续对抗性活动的本质特性。
- 网空杀伤链：杀伤链是OODA循环拆解为向前连续支撑动作阶段的线性映射。
- 网空威胁框架：网空威胁框架是网空杀伤链按照攻击技术/子技术遍历进行的矩阵化拆解。

OODA循环

展开

侦查 → 定制 → 投放 → 利用 → 安装 → 控制 → 行动

分析攻击目标及攻击面

准备后门和渗入途径

发起攻击并注入后门

触发后门或漏洞利用

实现在受害机器的长期隐蔽

建立远程控制机制

执行预定行动，达成目标

技战术遍历

TA0043 侦察 (10)	TA0042 资源开发(7)	TA0001 初始访问 (9)	TA0002 执行 (12)	TA0003 持久化 (19)	TA0004 提权 (13)	TA0005 防御规避 (40)	TA0006 凭证访问 (15)	TA0007 发现 (29)	TA0008 横向移动 (9)	TA0009 收集 (17)	TA0011 命令与控制 (16)	TA0010 数据渗出 (9)	TA0040 影响 (13)
T1595 主动扫描	T1583 获取基础设施	T1189 水坑攻击	T1059 利用命令和脚本解释器	T1098 操纵账户	T1548 滥用操作控制机制机制	T1548 滥用操作控制机制机制	T1557 利用中间人攻击 (MITM)	T1087 发现账户	T1210 利用远程服务漏洞	T1557 利用中间人攻击 (MITM)	T1071 使用应用层协议	T1020 自动渗出数据	T1531 删除账户和数据
T1592 搜集受害者主机信息	T1586 入侵帐户	T1190 利用面向公众的应用程序	T1609 利用容器管理服务执行命令	T1197 利用BITS服务	T1134 操纵访问令牌	T1134 操纵访问令牌	T1110 暴力破解	T1010 发现应用程序窗口	T1534 执行内部鱼叉式钓鱼攻击	T1560 压缩/加密收集的数据	T1092 通过可移动介质通信	T1029 定时传输	T1485 损坏数据
T1589 搜集受害者身份信息	T1584 入侵基础设施	T1133 利用外部远程服务	T1610 部署容器	T1547 利用自动启动执行的引导或登录	T1547 利用自动启动执行的引导或登录	T1197 利用BITS服务	T1542 在操作系统前启动	T1217 发现浏览器书签	T1570 横向传输文件或工具	T1123 捕获音频	T1132 编码数据	T1048 使用非C2协议外传	T1486 造成企业所依赖服务不可用
T1590 搜集受害者网络信息	T1587 能力开发	T1200 添加硬件	T1203 利用主机软件漏洞执行	T1037 利用启动或登录初始化脚本引导或登录	T1037 利用启动或登录初始化脚本引导或登录	T1612 在主机上建立映像	T1055 进程注入	T1580 发现云基础架构	T1563 远程服务会话劫持	T1119 自动收集	T1001 混淆数据	T1041 使用C2信道外传	T1565 操纵数据
T1591 搜集受害者组织信息	T1585 建立账户	T1566 网络钓鱼	T1559 利用容器编排部署	T1176 浏览器扩展/插件	T1543 创建或修改系统进程	T1140 反混淆/解码文件或信息	T1212 利用凭证访问漏洞	T1538 云服务仪表板	T1021 远程服务	T1185 浏览器中间人攻击 (MitB)	T1568 使用动态解析	T1011 使用其他网络介质传输	T1491 篡改可访问性
T1598 通过网络钓鱼搜集信息	T1588 能力获取	T1091 通过可移动介质复制	T1106 利用API	T1554 修改客户端软件	T1546 事件触发执行	T1610 部署容器	T1606 伪造Web凭证	T1526 发现云服务	T1091 通过可移动介质复制	T1115 收集剪贴板数据	T1573 使用加密信道	T1052 使用物理介质传输	T1561 擦除磁盘
T1597 从非公开源搜集信息	T1608 传播服务	T1195 入侵供应链	T1053 利用计划任务/工作	T1136 创建账户	T1068 利用漏洞提权	T1006 直接卷访问	T1207 注册获取域控制器	T1619 发现云存储对象	T1072 利用第三方软件部署工具	T1530 收集云存储对象的数据	T1008 使用备用信道	T1567 使用Web服务回传	T1499 端点拒绝服务 (DoS)
T1596 从公开技术数据库搜集信息		T1199 利用受信关系	T1129 利用共享模块执行	T1543 创建或修改系统进程	T1484 利用域策略修改	T1480 执行区域检验	T1014 使用Rootkit	T1613 发现容器和资源	T1080 污染共享介质	T1602 收集配置库的数据	T1105 使用入口工具传输	T1029 定时传输	T1495 固件损坏
T1593 搜索公开网站/域		T1078 利用有效账户	T1072 利用第三方软件部署工具	T1546 事件触发执行	T1611 容器逃逸	T1222 修改文件和目录权限	T1218 执行签名的二进制文件代理	T1614 发现系统地理位置		T1213 收集信息库数据	T1104 创建多级信道	T1011 使用其他网络介质传输	T1490 禁止恢复系统
T1594 搜索受害者自有网站			T1569 利用系统服务	T1574 执行劫持流程	T1574 执行劫持流程	T1484 利用域策略修改	T1218 执行签名的脚本代理	T1016 发现系统网络配置		T1005 收集本地系统数据	T1095 使用标准应用层协议		网络拒绝服务 (DoS)
			T1204 诱导用户执行	T1525 植入容器映像	T1055 进程注入	T1564 隐藏行为	T1553 篡改信任控制	T1083 发现文件和目录	T1049 发现系统网络连接	T1039 收集网络共享数据	T1571 使用非标准端口		T1496 资源劫持
			T1047 利用Windows管理规范 (WMI)	T1053 利用计划任务/工作	T1053 利用计划任务/工作	T1574 执行劫持流程	T1221 模板注入	T1615 发现组策略	T1033 发现系统所有者/用户	T1025 收集可移动介质数据	T1572 使用协议隧道		T1489 服务停止
				T1556 修改身份验证过程	T1078 利用有效账户	T1562 削弱防御机制	T1205 使用流量信令	T1046 扫描网络服务	T1007 发现系统服务	T1074 数据暂存	T1090 使用代理		T1529 系统关机/重启
				T1137 启动Office 应用程序	T1127 利用受信任的二进制文件执行	T1070 删除主机中的信息	T1111 双因子认证拦截	T1135 发现网络共享	T1124 发现系统时间	T1114 收集电子邮件	T1219 远程访问软件		
				T1542 在操作系统前启动	T1535 未使用/不受支持的云区域	T1202 间接执行命令	T1552 不安全的凭证	T1040 网络嗅探	T1497 虚拟化/沙箱规避	T1056 输入捕获	T1205 使用流量信令		
				T1053 利用计划任务/工作	T1550 使用备用身份验证材料	T1036 伪装		T1201 发现密码策略		T1113 获取屏幕截图	T1102 利用合法Web服务		
				T1505 利用服务器软件组件		T1556 修改身份验证过程				T1125 捕获视频			
				T1205 使用流量信令		T1578 修改云计算基础架构							
				T1078 利用有效账户		T1112 修改注册表							
						T1601 修改系统映像							

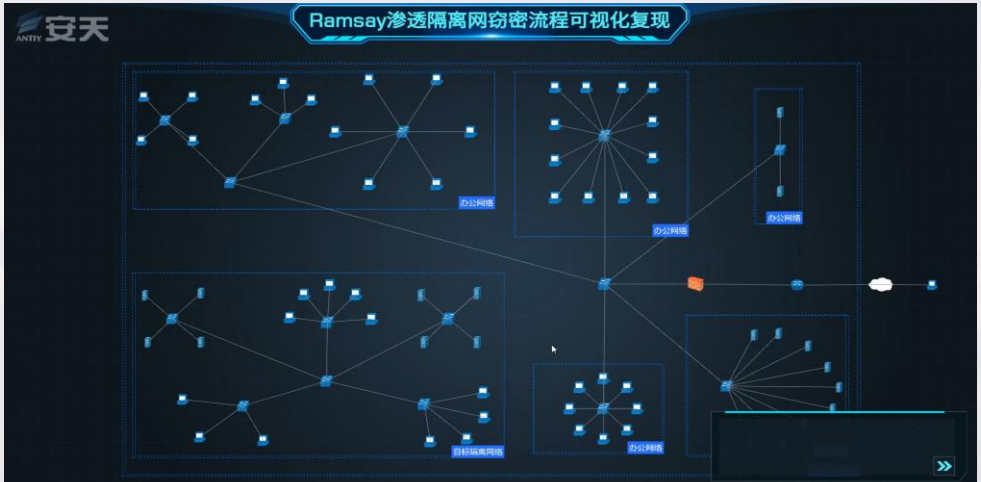
威胁框架是基于攻击技术枚举的完成的杀伤链技战术拆解

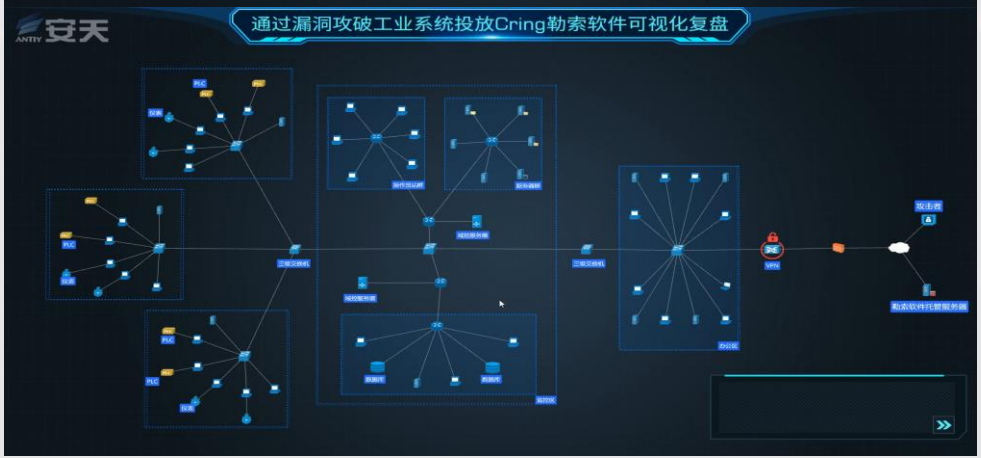
TA0043 侦察（10）	TA0042 资源开发(7)	TA0001 初始访问（9）	TA0002 执行（12）	TA0003 持久化（19）	TA0004 提权（13）	TA0005 防御规避（40）		TA0006 凭证访问（15）	TA0007 发现（29）		TA0008 横向移动（9）	TA0009 收集（17）	TA0011 命令与控制（16）	TA0010 数据渗出（9）	TA0040 影响（13）
T1595 主动扫描	T1583 获取基础设施	T1189 水坑攻击	T1059 利用命令和脚本解释器	T1098 操纵账户	T1548 滥用提升控制权限机制	T1548 滥用提升控制权限机制	T1599 网络边界桥接	T1557 利用中间人攻击（MITM）	T1087 发现账户	T1120 发现主机接入设备	T1210 利用远程服务漏洞	T1557 利用中间人攻击（MITM）	T1071 使用应用层协议	T1020 自动渗出数据	T1531 删除账户权限
T1592 搜集受害者主机信息	T1586 入侵账户	T1190 利用面向公众的应用程序	T1609 利用容器管理服务执行命令	T1197 利用BITS服务	T1134 操纵访问令牌	T1134 操纵访问令牌	T1027 混淆文件或信息	T1110 暴力破解	T1010 发现应用程序窗口	T1069 发现权限组	T1534 执行内部鱼叉式钓鱼攻击	T1560 压缩/加密收集的数据	T1092 通过可移动介质通信	T1030 限制传输数据大小	T1485 损毁数据
T1589 搜集受害者身份信息	T1584 入侵基础设施	T1133 利用外部远程服务	T1610 部署容器	T1547 利用自动启动执行引导或登录	T1547 利用自动启动执行引导或登录	T1197 利用BITS服务	T1542 在操作系统前启动	T1555 从存储密码的位置获取凭证	T1217 发现浏览器书签	T1057 发现进程	T1570 横向传输文件或工具	T1123 捕获音频	T1132 编码数据	T1048 使用非C2协议回传	T1486 造成恶劣影响的数据加密
T1590 搜集受害者网络信息	T1587 能力开发	T1200 添加硬件	T1203 利用主机软件漏洞执行	T1037 利用初始化脚本引导或登录	T1037 利用初始化脚本引导或登录	T1612 在主机上建立映像	T1055 进程注入	T1212 利用凭证访问漏洞	T1580 发现云基础架构	T1012 查询注册表	T1563 远程服务会话劫持	T1119 自动收集	T1001 混淆数据	T1041 使用C2信道回传	T1565 操纵数据
T1591 搜集受害者组织信息	T1585 建立账户	T1566 网络钓鱼	T1559 利用进程间通信	T1176 添加浏览器扩展插件	T1543 创建或修改系统进程	T1140 反混淆/解码文件或信息	T1211 利用漏洞规避防御	T1187 强制认证	T1538 云服务仪表板	T1018 发现远程系统	T1021 利用远程服务	T1185 浏览器中间人攻击（MitB）	T1568 使用动态参数	T1011 使用其他网络介质回传	T1491 篡改可见内容
T1598 通过网络钓鱼搜集信息	T1588 能力获取	T1091 通过可移动介质复制	T1106 利用API	T1554 篡改客户端软件	T1546 事件触发执行	T1610 部署容器	T1620 利用反射代码加载	T1606 伪造Web凭证	T1526 发现云服务	T1518 发现软件	T1091 通过可移动介质复制	T1115 收集剪贴板数据	T1573 使用加密信道	T1052 使用物理介质回传	T1561 擦除磁盘
T1597 从非公开源搜集信息	T1608 环境整备	T1195 入侵供应链	T1053 利用计划任务/工作	T1136 创建账户	T1068 利用漏洞提权	T1006 直接访问卷	T1207 注册恶意域控制器	T1056 输入捕捉	T1619 发现云存储对象	T1082 发现系统信息	T1072 利用第三方软件部署工具	T1530 收集云存储对象的数据	T1008 使用备用信道	T1567 使用Web服务回传	T1499 端点侧拒绝服务（DoS）
T1596 从公开技术数据库搜集信息		T1199 利用受信关系	T1129 利用共享模块执行	T1543 创建或修改系统进程	T1484 利用域策略修改	T1480 执行范围保护	T1014 使用Rootkit	T1556 修改身份验证过程	T1613 发现容器和资源	T1614 发现系统地理位置	T1080 污染共享内容	T1602 收集配置库的数据	T1105 使用入口工具传输	T1029 定时传输	T1495 损坏固件
T1593 搜索公开网站/域		T1078 利用有效账户	T1072 利用第三方软件部署工具	T1546 事件触发执行	T1611 容器逃逸	T1222 修改文件和目录权限	T1218 执行签名的二进制文件代理	T1040 网络嗅探	T1482 发现域信任	T1016 发现系统网络配置	T1550 使用备用身份验证材料	T1213 收集信息库数据	T1104 创建多级信道	T1537 将数据转移到云账户	T1490 禁止系统恢复
T1594 搜索受害者自有网站			T1569 利用系统服务	T1133 利用外部远程服务	T1574 执行流程劫持	T1484 利用域策略修改	T1216 执行签名的脚本代理	T1003 操作系统凭证转储	T1083 发现文件和目录	T1049 发现系统网络连接		T1005 收集本地系统数据	T1095 使用标准非应用层协议		T1498 网络侧拒绝服务（DoS）
			T1204 诱导用户执行	T1574 执行流程劫持	T1055 进程注入	T1564 隐藏行为	T1553 损坏信任控制	T1528 窃取应用程序访问令牌	T1615 发现组策略	T1033 发现系统所有者/用户		T1039 收集网络共享驱动数据	T1571 使用非标准端口		T1496 资源劫持
			T1047 利用Windows管理规范（WMI）	T1525 植入容器映像	T1053 利用计划任务/工作	T1574 执行流程劫持	T1221 模板注入	T1558 窃取或伪造Kerberos 凭证	T1046 扫描网络服务	T1007 发现系统服务		T1025 收集可移动介质数据	T1572 使用协议隧道		T1489 禁用服务
				T1556 修改身份验证过程	T1078 利用有效账户	T1562 削弱防御机制	T1205 使用流量信令	T1539 窃取Web会话Cookie	T1135 发现网络共享	T1124 发现系统时间		T1074 数据暂存	T1090 使用代理		T1529 系统关机/重启
				T1137 启动Office应用程序		T1070 删除主机中的信标	T1127 利用受信的开发工具执行	T1111 双因子认证拦截	T1040 网络嗅探	T1497 虚拟化/沙箱逃逸		T1114 收集电子邮件	T1219 利用远程访问软件		
				T1542 在操作系统前启动		T1202 间接执行命令	T1535 未使用/不受支持的云区域	T1552 不安全的凭证	T1201 发现密码策略			T1056 输入捕捉	T1205 使用流量信令		
				T1053 利用计划任务/工作		T1036 伪装	T1550 使用备用身份验证材料					T1113 获取屏幕截图	T1102 利用合法Web服务		
				T1505 利用服务器软件组件		T1556 修改身份验证过程	T1078 利用有效账户					T1125 捕获视频			
				T1205 使用流量信令		T1578 修改云计算基础构架	T1497 虚拟化/沙箱逃逸								
				T1078 利用有效账户		T1112 修改注册表	T1600 削弱加密								
						T1601 修改系统映像	T1220 利用XSL文件执行脚本								

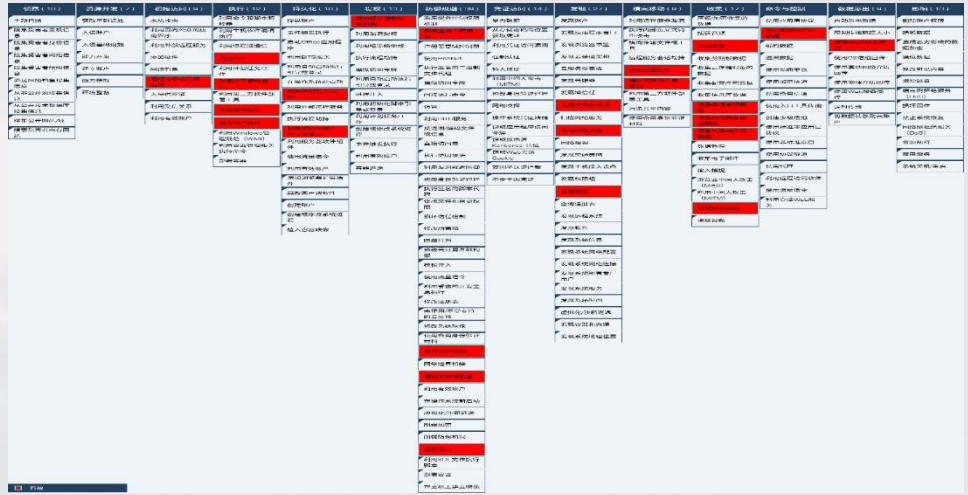
MITRE ATT&CK威胁框架
安天中译版

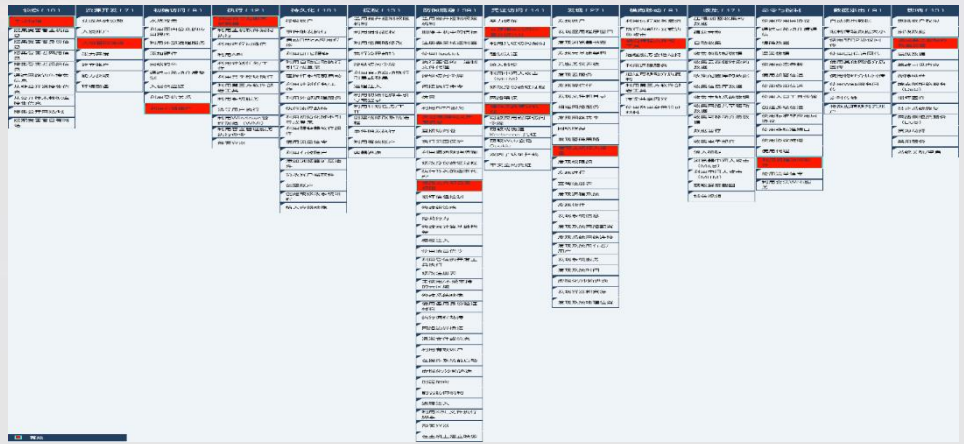
威胁框架是一个丰富的（多维）知识框架

威胁框架能有效用于认知威胁，进行技术和战术的分析

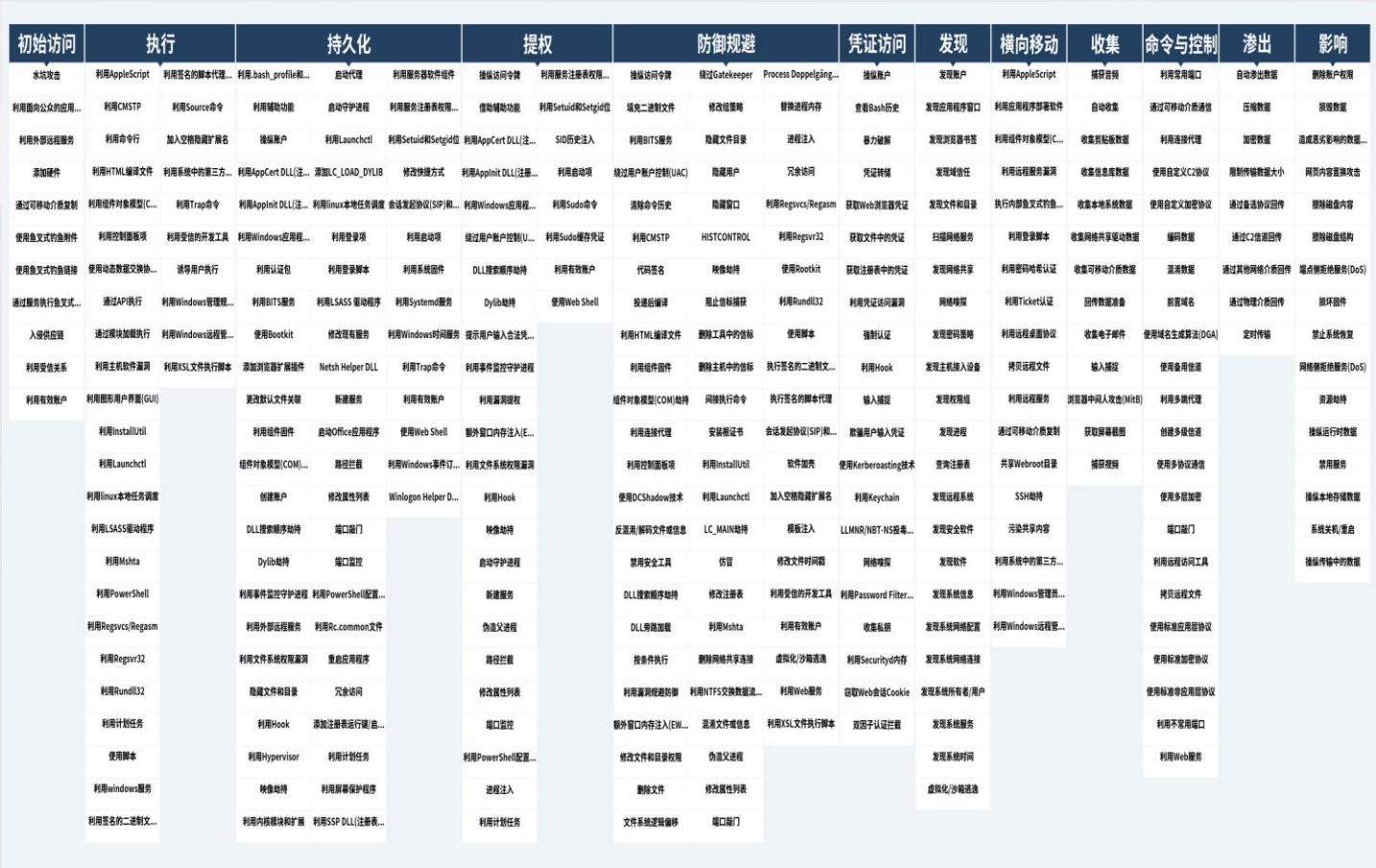






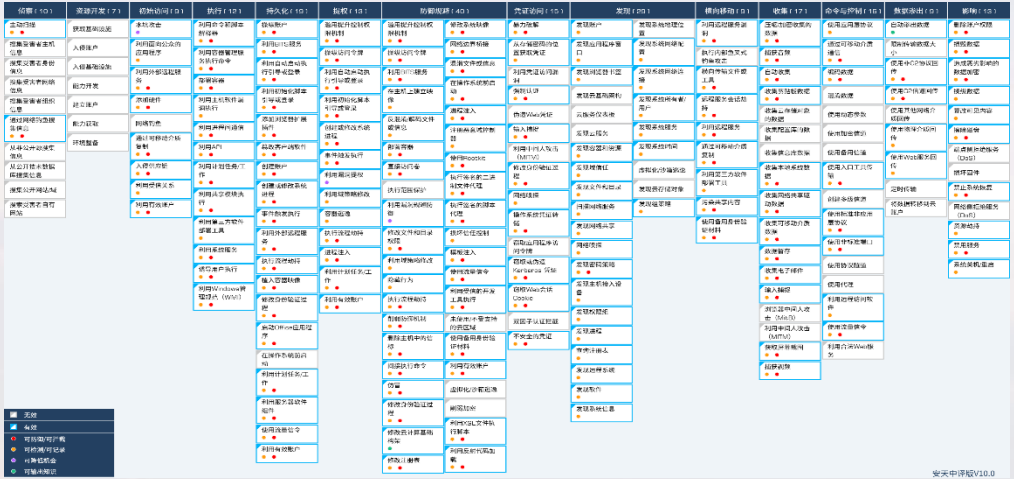


将威胁框架映射到产品能力环节



- 相关/无关
- 降低动作成功率（降低机会）
- 记录/告警
- 拦截
- 能力揭示

通过威胁框架可以分析产品的布防与互补价值



基于端点侧部署的安天智甲终端防御系统的检测和拦截点

- 通过两者的对比，可见大部分攻击动作是基于系统实施和完成的。
- 同时各种安全能力环节有不同的价值和互补作用。

基于流量侧部署的安天探海威胁监测系统的可输出的攻击动作标签

对抗效果评价定义：感知、干扰、阻断和呈现网空杀伤链

产品	与杀伤链、威胁框架之间的关系
探海	在网络流量中检测威胁技术、呈现对应的杀伤链并干扰（RST包）威胁行为体的初始访问、收集、获取、命令控制等各种战术动作。
智甲	利用防御技术措施在主机干扰、阻断威胁行为体初始访问、执行、持久化、提权、访问屏障、获取数据、横向移动、命令控制等各种战术动作，并对单机和多主机构成的网络中的杀伤链进行呈现。
追影	通过对威胁载荷的行为体补全各杀伤链环节间的缺失环节和线索，提升检测杀伤链的能力，供给载荷相关情报用以支撑猎杀活动中对杀伤链的干扰和阻断，呈现载荷具备的威胁技术。
拓痕	检测威胁的持久化，呈现其他环节留存的痕迹，辅助分析响应人员及时阻断杀伤链，固化威胁行为证据。
捕风	借助合理塑造的欺骗环境，增大侦查难度、消耗横向移动所需的时间，记录执行、持久化、防御规避、凭证访问、收集、命令控制、影响等其他环节的战术动作和技术细节，实现对杀伤链的干扰。
铸岳	通过清晰测绘网空资产、统一管理访问策略将暴露面呈现出来，并通过合理的塑造建立防御者的先发优势，限制威胁技术可攻击的范围和路径，使得检测杀伤链各环节变得更容易。
智信	管理身份、凭证、访问可达性，检测初始访问、凭证访问、收集、数据渗出等相关的战术动作，限制威胁的活动路径范围，呈现多地域环境下的杀伤链。

03 从威胁框架落地到承载的产品——能力型产品技术框架

目前的几个防御矩阵

	网络安全框架（CSF）	Shield积极防御框架	D3FEND知识图谱	安天ISPDR 防御技术框架
发布机构	NIST	MITRE	MITRE	安天
首次发布	2014年	2020年	2021年	2020年
发布背景	CSF由NIST与私营和公共部门密切合作开发，是美国各组织**自愿**采用的**基于风险的方法。**	SHIELD是MITRE在攻击建模分析取得良好成功后，对防御建模进行的有益尝试 。	D3FEND 最初版本的主要目标是促进防御性网络安全技术功能词汇的标准化。	融合相关经验，特别是威胁对抗与安全规划的整合。
主要特色	使用易于理解的通用语言提供一系列所需的网络安全活动和结果，指导企业管理和降低其网络安全风险。	SHIELD的表现形式有利于组织进行网络防御基础设施的部署决策过程。	细化网络安全防御对策功能、技术，使网络安全从业人员能针对特定网络威胁制定防御措施，缩窄防御系统潜在攻击面。	基于防御关键动作的概念，面对杀伤链形成响应过程。
当前版本	V1.1	V9.0	0.9.2-BETA3	V0.2

安天安全能力框架——关键防御动作战术环节

塑造是建立防御主动性的前提。塑造是对IT场景的构建、重构和调整过程，通过对IT规划和场景的干预，形成环境、场景、拓扑路径、配置和安全策略的优化，并结合欺骗布防，使攻击者处于不利位置。

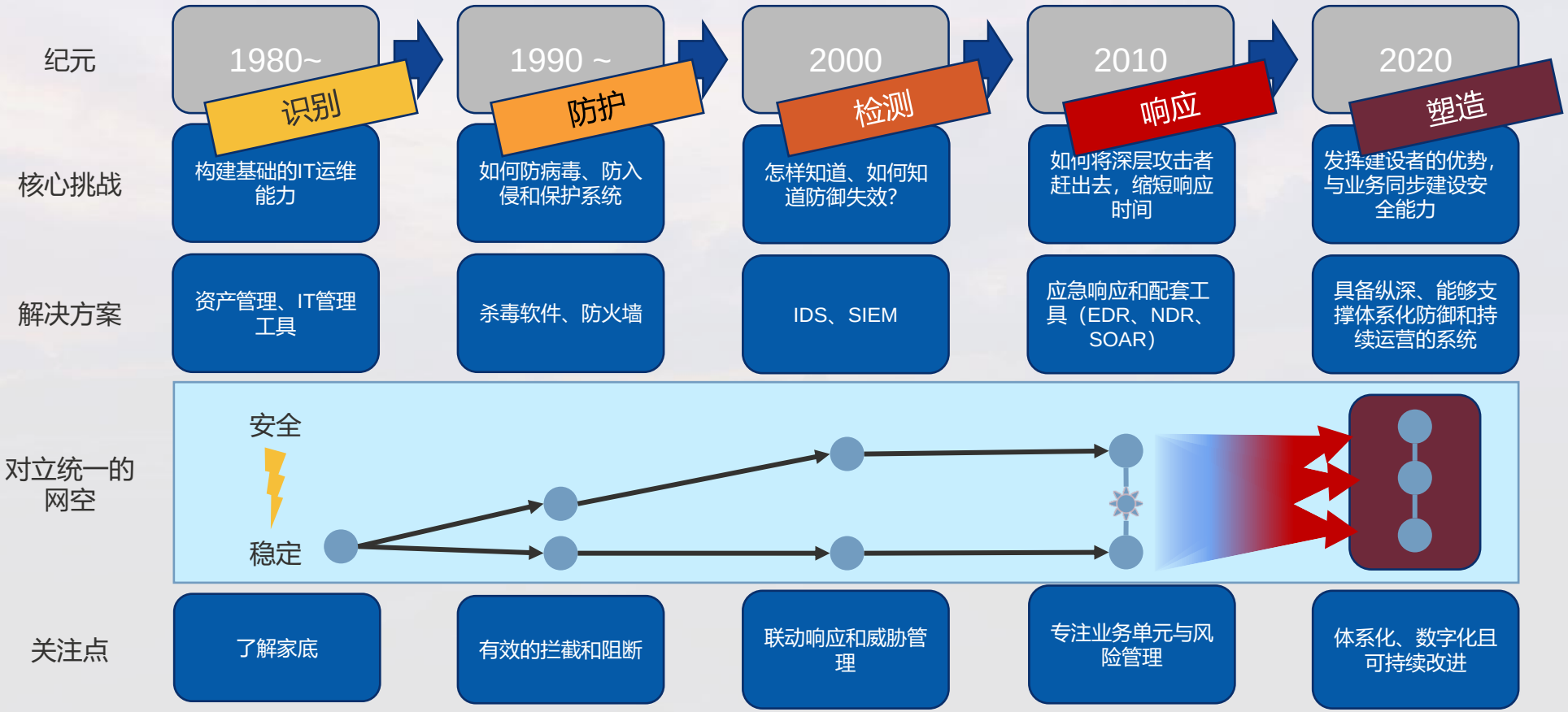
检测是发现、定位和定性网络安全威胁的方法统称。本质上是在数据对象和行为对象、实体对象中发现、标定和量化风险实体、风险活动的过程。

识别是网络安全管理的基础。识别是是一个自我了解和认知过程，基于采集和探测枚举，形成对资产、人员、业务、暴露面、脆弱性等完整认识，构筑起网空防御地形认知基础。

防护是系统对威胁做出的行为反应。防护是避免威胁行为达成预期后果的交互过程。其核心是对威胁活动和违规行为的拒止动作。

响应是处理、管理风险和威胁事件的过程。通过制定并执行适当的行动，利用组织所具备的控制潜在网络安全事件影响的能力，对检测到的网络安全事件采取处置措施，旨在清除网络安全事件影响。

关键防御动作的成型历史



核心要素——作用对象集合

网络类对象

- 地址、端口、通联、协议、拓扑

信息类对象

- 配置、脆弱点、补丁、……

用户类对象

- 用户、帐户、身份、权限

作用承载类对象

- 文件、载荷、进程、内存、服务……

应用类对象

- 基础类：DNS、TLS、VPN、RDP……
- 业务类：邮件、WEB、FTP、网盘、视频会议……

作用位置属性类对象

- 主机、边界、流量、应用系统、供应链……

安全的可运营基础来自持续的对象数据采集和元数据化

安天产品防御矩阵

指挥、决策与控制

汇聚、关联、统计、分析模型与呈现

关键防御动作矩阵

识别	塑造	防护	检测	响应
系统环境识别	系统环境策略塑造	资源访问拒止	系统环境检测	缓解
网络环境识别	网络管控策略塑造	连接拒止	流量环境检测	固证
业务识别	配置加固	创建拒止	应用环境检测	主机环境处置
用户识别	加密环境塑造	写入拒止	数据体检测	网络侧处置
配置识别	欺骗环境构造	执行拒止	用户行为检测	环境与数据恢复
暴露面/脆弱性识别		加载拒止		策略调整
活动识别		……		

作用对象

网络类	用户类	应用类	信息类	执行体类
内容	用户	DNS	配置	载荷
地址	帐户	TLS	补丁	进程
协议	身份	VPN	脆弱点	内存
端口	权限	邮件	……	服务
……		WEB		……
		……		

作用位置

主机 | 边界 | 流量 | 应用 | 流程

部署方式：与被保护对象原生融合or安装 | 基于载体设备部署 | 基于虚拟化资源部署

管理模式：单点管控/集中管控 | 无管控

认知威胁	攻击者	意图	装备	载荷	行为	被攻击者	脆弱性	检测结果	后果

保护目标	硬件资产	软件资产	外设资产	数据资产	仿真资产

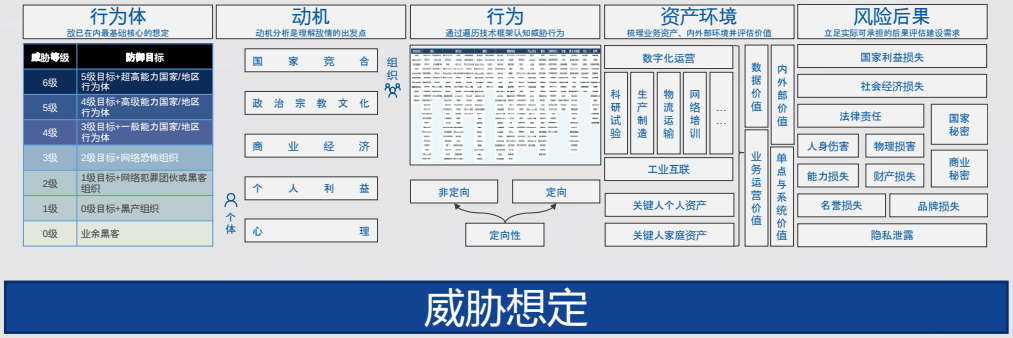
防御框架关键防御动作映射威胁框架，实现向防御体系的能力组装

体系对抗威胁

威胁场景化想定

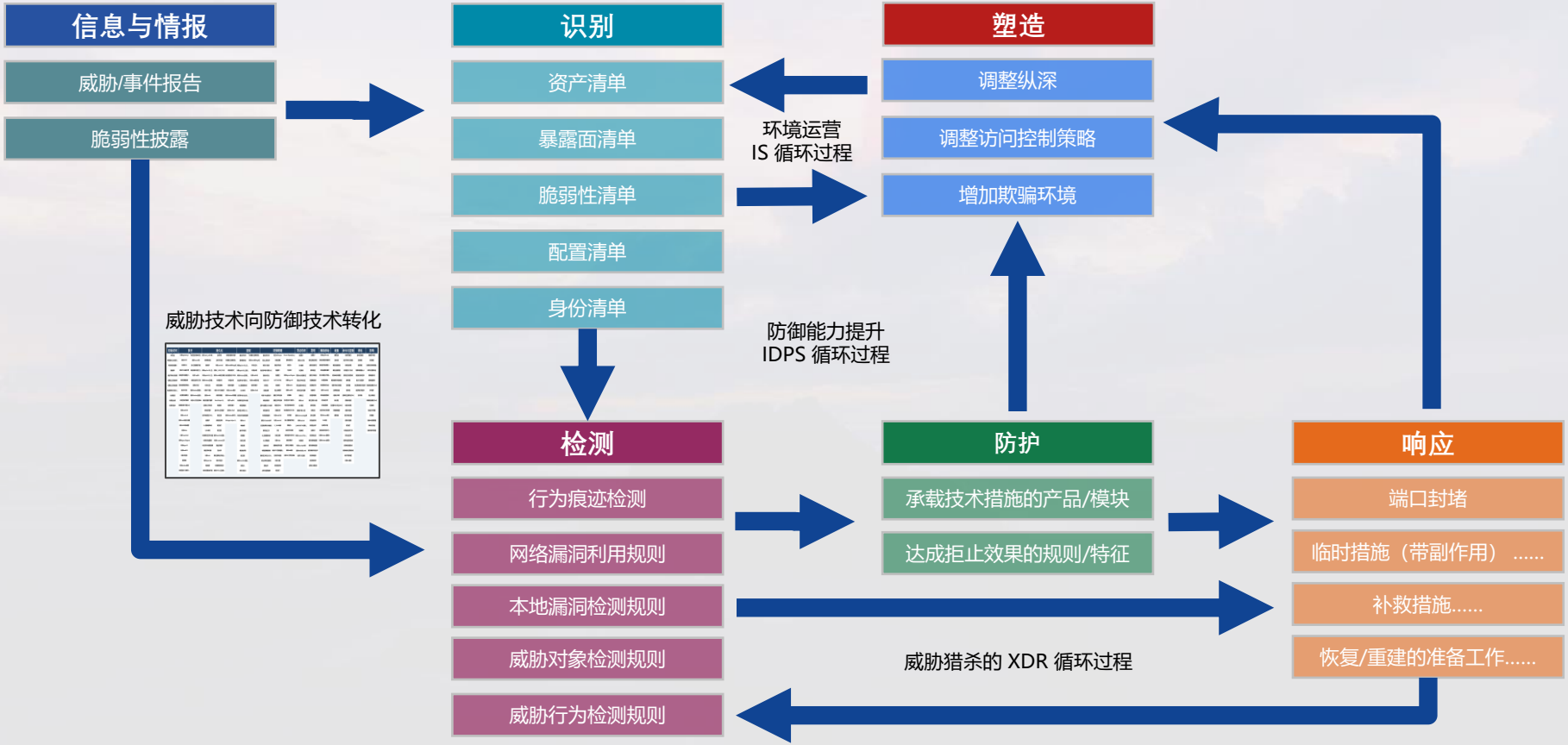
检验防御充分性

能力组装



关键防御动作

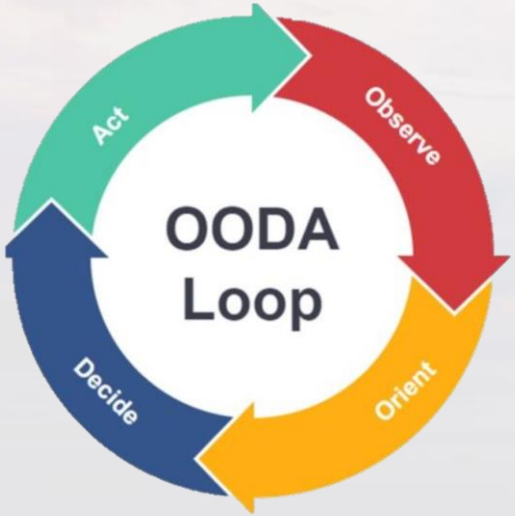
威胁对抗驱动防御能力提升



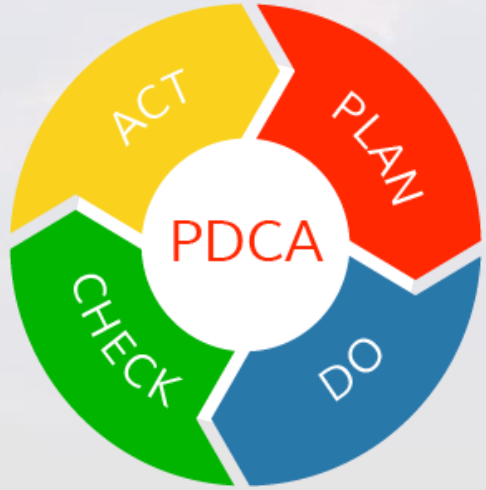
04 衔接规划（采购）与日常运营——双环驱动与威胁猎杀

数字化企业安全运营两类工作闭环

在数字化企业网络安全运营工作业务流程支持上，构建面向日常安全运营工作的OODA循环和面向安全治理、策略调整的PDCA循环的双业务流程引擎。

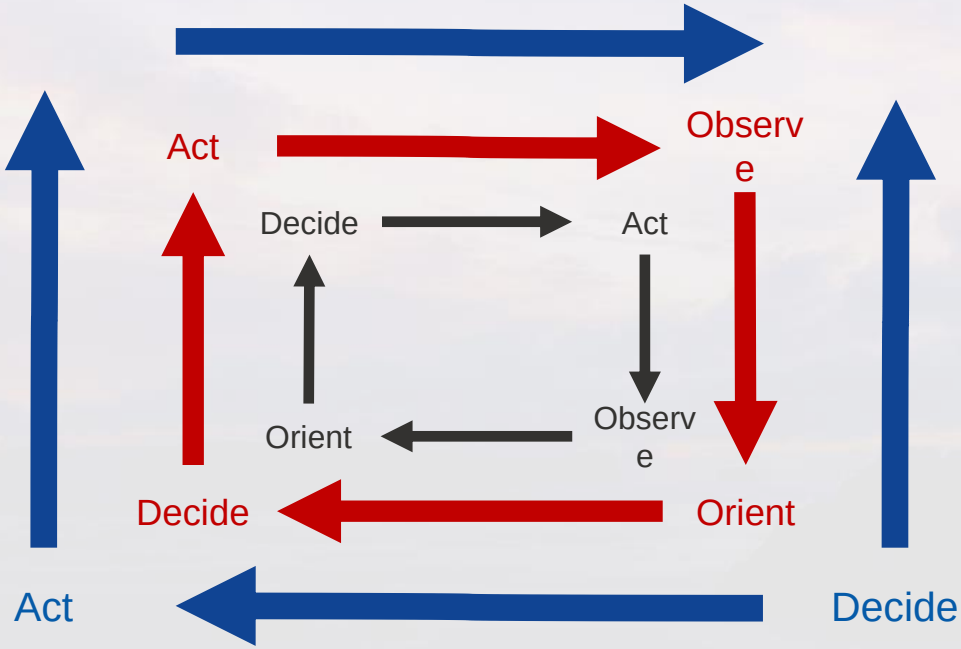


针对日常安全运营工作，实现支撑“观察-研判-决策-执行”的“OODA” 型业务闭环，达成比威胁方更快的OODA循环。



针对监管政策要求、企业安全治理需求，实现支撑“策划-实施-检查-调整”的“PDCA”型业务闭环。

威胁对抗的数字化运营与 OODA 循环



防御方 OODA 循环

威胁方 OODA 循环

业务循环受到传统安全设计的限制

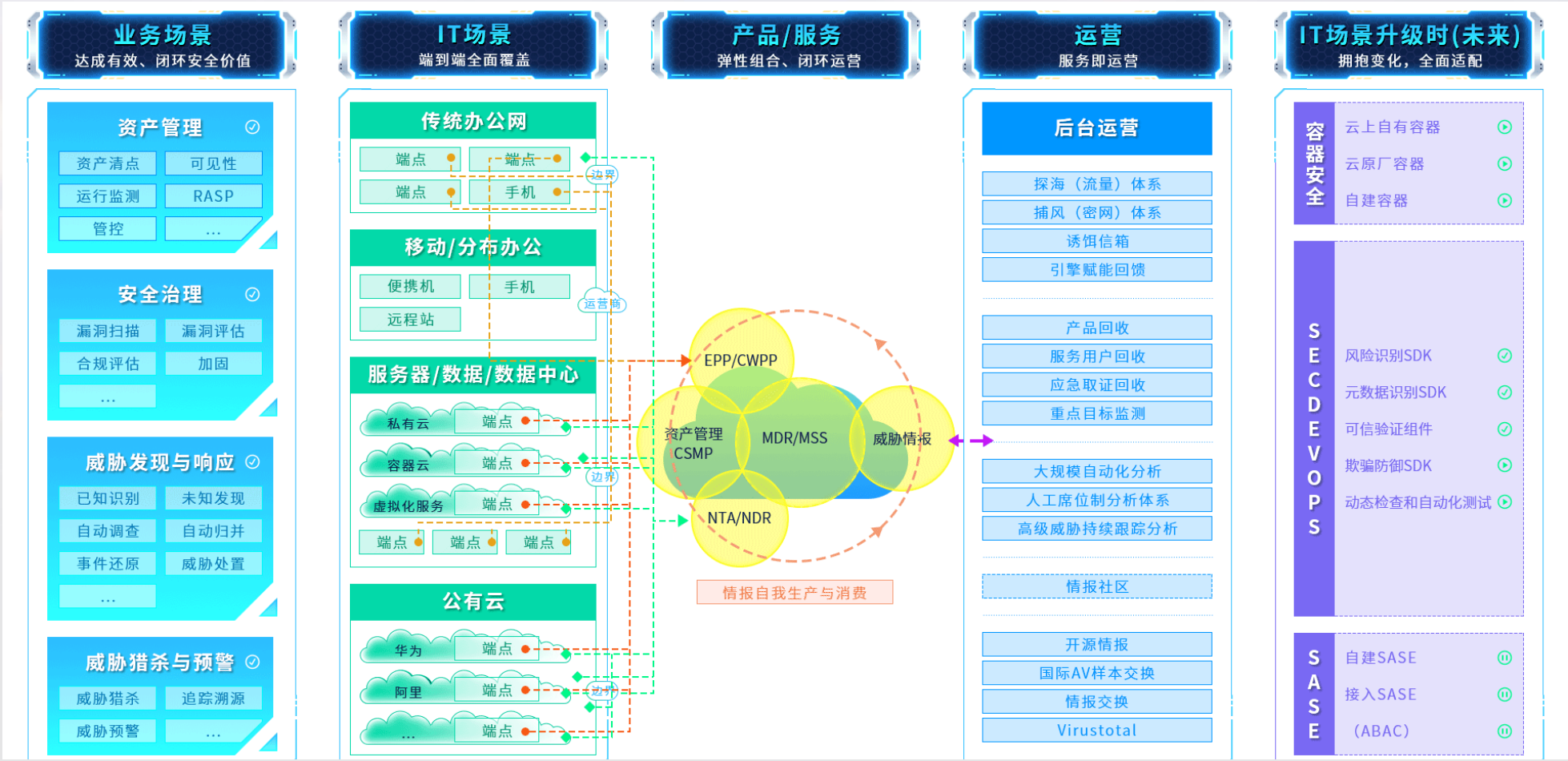
持续运营业务循环

基于威胁假定的合理设计可以大幅提升数字化业务安全响应速度

$(OODA_{业务} - OODA_{CIO+CISO})$ = 滞后的响应时间

新企业在早期能够更早更迅速收敛更大的攻击敞口，往往不是因为安全是目标。（而是因为更快的响应速度）—— 美国国防部 引自 Ryan McGeehan

安全运营体系示例

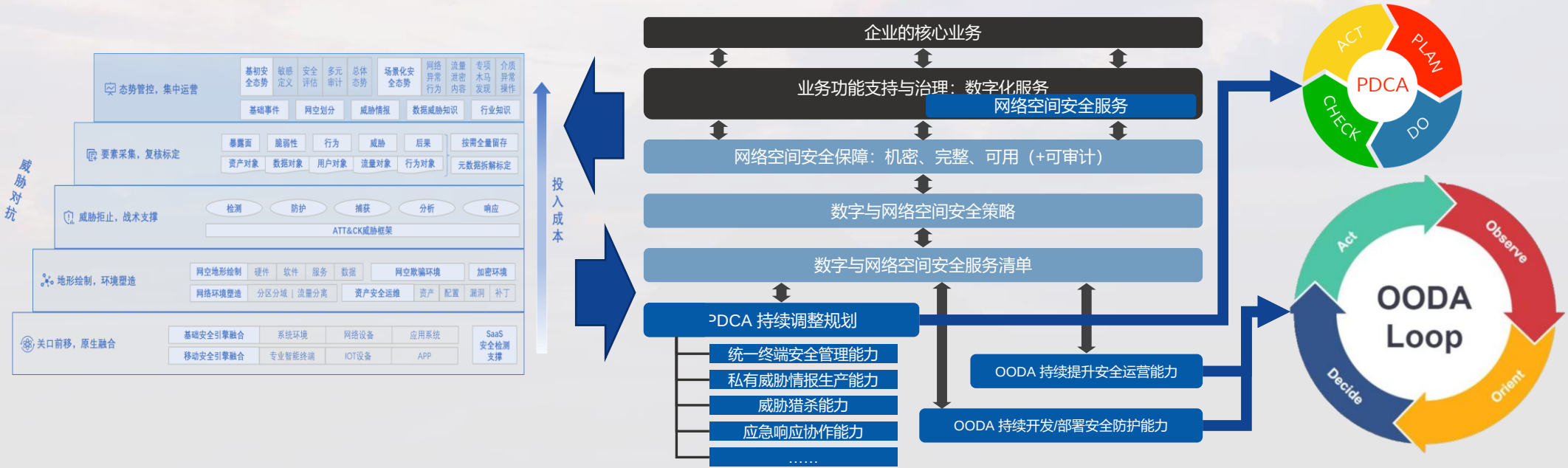

业务场景
达成有效、闭环安全价值
资产管理
资产清点
可见性
运行监测
RASP
管控
...
安全治理
漏洞扫描
漏洞评估
合规评估
加固
...
威胁发现与响应
已知识别
未知发现
自动调查
自动归并
事件还原
威胁处置
...
威胁猎杀与预警
威胁猎杀
追踪溯源
威胁预警
...
IT场景
端到端全面覆盖
传统办公网
端点
端点
端点
手机
边界
移动/分布办公
便携机
手机
远程站
运营商
服务器/数据/数据中心
私有云
端点
容器云
端点
虚拟化服务
端点
端点
端点
端点
边界
公有云
华为
端点
阿里
端点
...
端点
边界
产品/服务
弹性组合、闭环运营
EPP/CWPP
资产管理
CSMP
MDR/MSS
威胁情报
NTA/NDR
情报自我生产与消费
运营
服务即运营
后台运营
探海（流量）体系
捕风（密网）体系
诱饵信箱
引擎赋能回馈
产品回收
服务用户回收
应急取证回收
重点目标监测
大规模自动化分析
人工席位制分析体系
高级威胁持续跟踪分析
情报社区
开源情报
国际AV样本交换
情报交换
Virustotal
IT场景升级时(未来)
拥抱变化，全面适配
容器安全
云上自有容器
云原厂容器
自建容器
SECDEVOPS
风险识别SDK
元数据识别SDK
可信验证组件
欺骗防御SDK
动态检查和自动化测试
SASE
自建SASE
接入SASE
（ABAC）

动态综合防御体系框架


威胁对抗
投入成本
态势管控，集中运营
基初安全态势
敏感定义
安全评估
多元审计
总体态势
场景化安全态势
网络异常行为
流量泄密内容
专项木马发现
介质异常操作
基础事件
网空划分
威胁情报
数据威胁知识
行业知识
要素采集，复核标定
暴露面
脆弱性
行为
威胁
后果
按需全量留存
资产对象
数据对象
用户对象
流量对象
行为对象
元数据拆解标定
威胁拒止，战术支撑
识别
塑造
检测
防护
响应
ATT&CK威胁框架
地形绘制，环境塑造
网空地形绘制
硬件
软件
服务
数据
网空欺骗环境
加密环境
网络环境塑造
分区分域 | 流量分离
资产安全运维
资产
配置
漏洞
补丁
关口前移，原生融合
基础安全引擎融合
系统环境
网络设备
应用系统
移动安全引擎融合
专业智能终端
IOT设备
APP
SaaS安全检测支撑

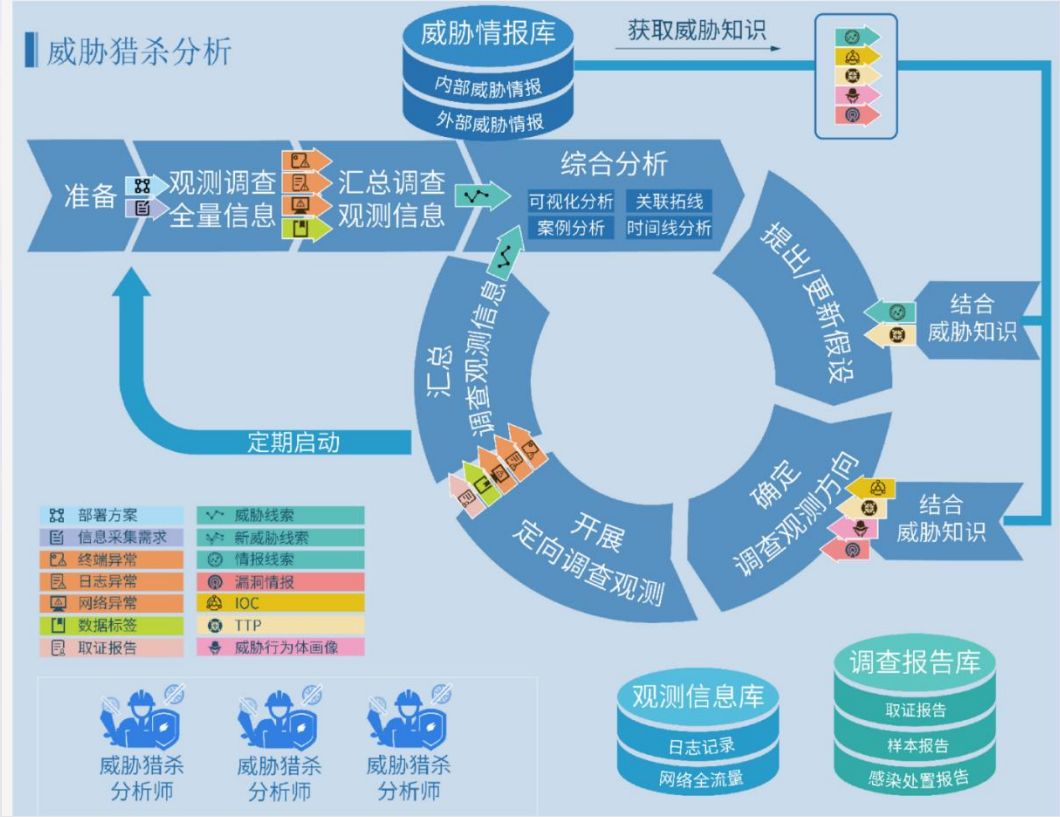
此消彼长，在数字化世界对抗威胁比拼的是速度

通过防御体系建设支撑数字化世界快速检测与响应威胁攻击，支撑企业安全数字化转型成功。



威胁猎杀分析

- 信息系统需具备全量信息采集能力
  - 如果没有可以临时部署探海
  - 终端亦可通过工具手工采集
- 全量观测、排查已知、分析异常
  - 不符合业务场景的“白流量”
  - P2P等隐蔽通讯的网络流量
  - 不常用的端口、字符、扩展名
  - 格式与扩展名不一致
  - 非系统目录下的系统程序
  - 快捷方式中调用系统命令或脚本
- 汇总调查、形成线索
- 综合分析
  - 可视化分析
  - 关联拓线分析
  - 案例分析
  - 时间线分析
- 提出假设、用事实验证或排除



谢谢大家

安天冬训营 wtc.antiy.cn