



网络空间威胁对抗与防御技术研讨会  
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

# 安天安全方法框架

安天 | 研究院

- 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



网络空间威胁对抗与防御技术研讨会  
暨 第九届安天网络安全冬训营

安天 | 智者安天下  
ANTIY

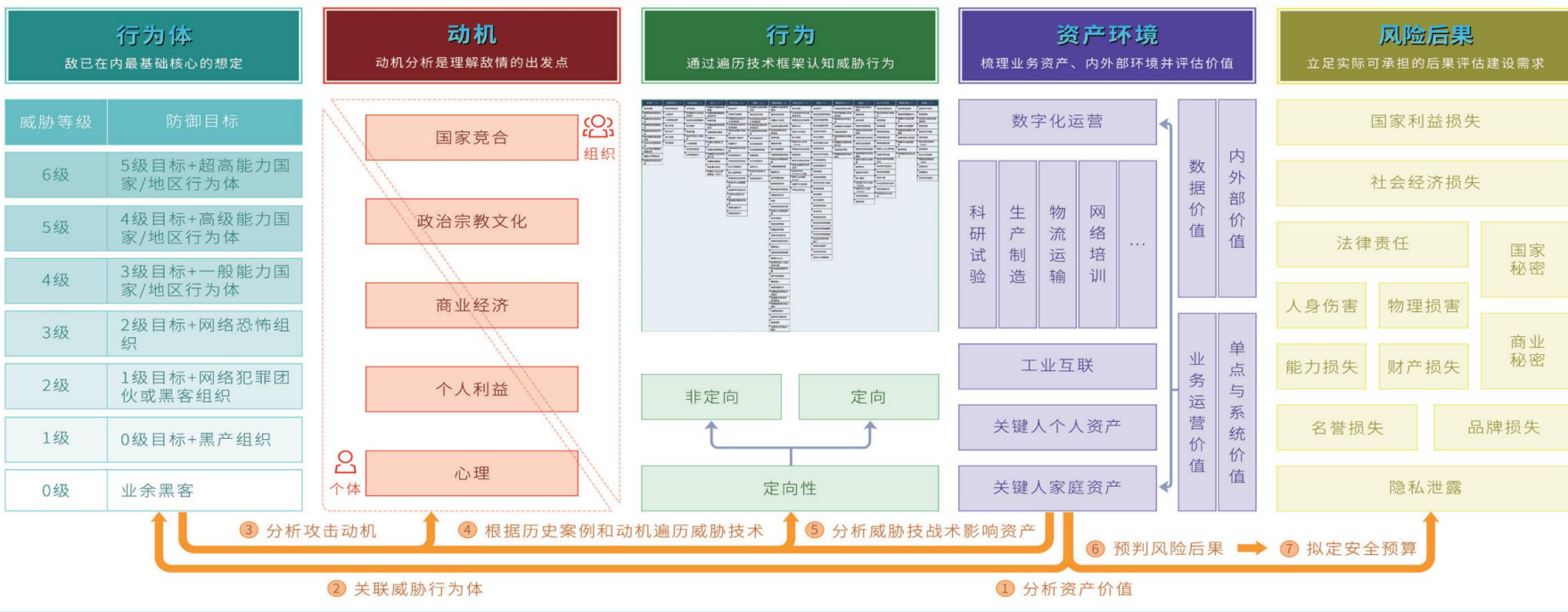
# 01

## 安全规划与建设的起点 ——威胁想定框架



## 威胁想定分析框架

### 法律法规与标准规范



# 威胁行为体评估体系



# 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





网络空间威胁对抗与防御技术研讨会  
暨 第九届安天网络安全冬训营

安天 | 智者安天下

# 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



# 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 漏洞开发(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 发现用户	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 自动导出数据	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 利用设备管理器执行命令	T1197 利用BITS服务	T1134 操纵访问令牌	T1134 操纵访问令牌	T1027 泄露文件或信息	T1110 暴力破解	T1010 发现收集器	T1069 发现收集器	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 窃取数据
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 从存储密钥的位置获取凭证	T1217 发现进程	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	T1140 在主机上建立映像	T1055 进程注入	T1212 利用凭证访问漏洞	T1580 发现云基础设施	T1012 查询注册表	T1563 远程服务会话劫持	T1119 自动收集	T1001 部署数据	T1041 使用C2协议回传	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 添加浏览器扩展控件	T1543 创建或修改系统进程	T1140 反弹壳/解密文件或信息	T1211 利用漏洞绕过防御	T1187 强制认证	T1538 云服务仪表盘	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 使用其他网络协议回传	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 利用反射代理加载	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 收集浏览器数据	T1573 使用加密信道	T1052 使用物理介质回传	T1561 删除磁盘
T1597 从非公开源搜集信息	T1608 环境部署	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 注册恶毒域控制器	T1056 输入凭证	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 端点制地址服务 (DoS)
T1596 从公开技术数据库搜集信息	T1199 利用信任关系	T1199 利用信任关系	T1543 利用共享模块执行	T1484 创建或修改系统进程	T1484 利用策略修改	T1140 执行漏洞保护	T1154 使用Rootkit	T1613 修改身份验证过程	T1602 发现密钥和资源	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 植入组件
T1593 搜集公开网站/论坛	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 发现可信性	T1016 发现系统网络配置	T1550 使用备用身份验证材料	T1213 收集信息数据库	T1104 创建可信信道	T1537 将数据转移到云账户	T1498 网络制地址服务 (DoS)	T1490 禁止系统恢复
T1594 搜集受害者自有网站	T1569 利用云服务	T1133 利用外部远程服务	T1574 执行流程劫持	T1484 利用策略修改	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	T1039 收集网络共享驱动数据	T1571 使用非标准端口	T1496 资源劫持	T1489 禁用服务	T1529 系统关机/重启
	T1204 诱导用户执行	T1574 执行流程劫持	T1055 进程注入	T1564 隐藏行为	T1528 窃取应用程序访问令牌	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	T1007 发现系统服务	T1124 发现系统时间	T1114 收集电子邮件	T1219 利用远程访问软件	T1205 使用流量指令		
	T1047 利用Windows管理规范 (WMI)	T1525 植入恶意软件	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	T1135 发现网络共享	T1124 发现系统时间	T1114 收集电子邮件	T1219 利用远程访问软件	T1205 使用流量指令		
	T1556 修改身份验证过程	T1078 利用有效账户	T1562 欺骗防御机制	T1205 使用流量指令	T1539 窃取Web会话Cookie	T1539 窃取Web会话Cookie	T1135 发现网络共享	T1124 发现系统时间	T1049 虚拟化/沙箱逃逸	T1056 输入凭证	T1113 获取屏幕截图	T1102 利用合法Web服务			
	T1137 启动Office应用程序	T1070 删除主机中的信标	T1127 利用受害者的开发工具执行	T1111 双因子认证拦截	T1552 不安全的凭证	T1552 不安全的凭证	T1040 网络嗅探	T1201 发现策略策略							
	T1542 在操作系统前启动	T1202 阅读执行命令	T1535 未使用/不受支持的云区域	T1036 伪装	T1550 使用备用身份验证材料	T1550 使用备用身份验证材料	T1078 利用有效账户								
	T1053 利用计划任务/工作	T1036 伪装	T1556 修改身份验证过程	T1078 利用有效账户	T1578 修改云计算基础设施	T1578 修改云计算基础设施	T1497 虚拟化/沙箱逃逸								
	T1505 利用服务器软件组件	T1112 修改注册表	T1600 数据加密	T1601 修改系统映像	T1220 利用XSL文件执行脚本	T1220 利用XSL文件执行脚本									
	T1205 使用流量指令	T1112 修改注册表	T1600 数据加密	T1601 修改系统映像	T1220 利用XSL文件执行脚本	T1220 利用XSL文件执行脚本									
	T1078 利用有效账户	T1112 修改注册表	T1600 数据加密	T1601 修改系统映像	T1220 利用XSL文件执行脚本	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

安天 ATT&CK威胁框架内部教学与演示系统

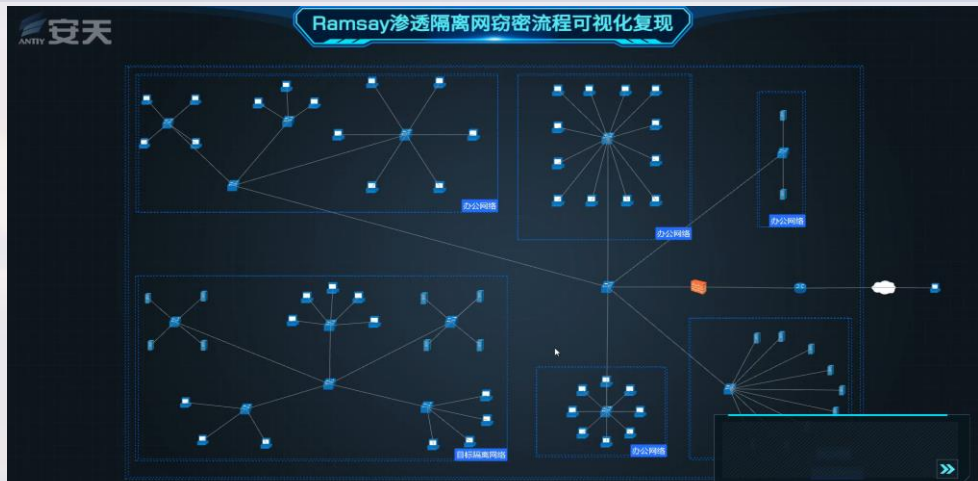
二维视图 三维视图

请输入子任务名称

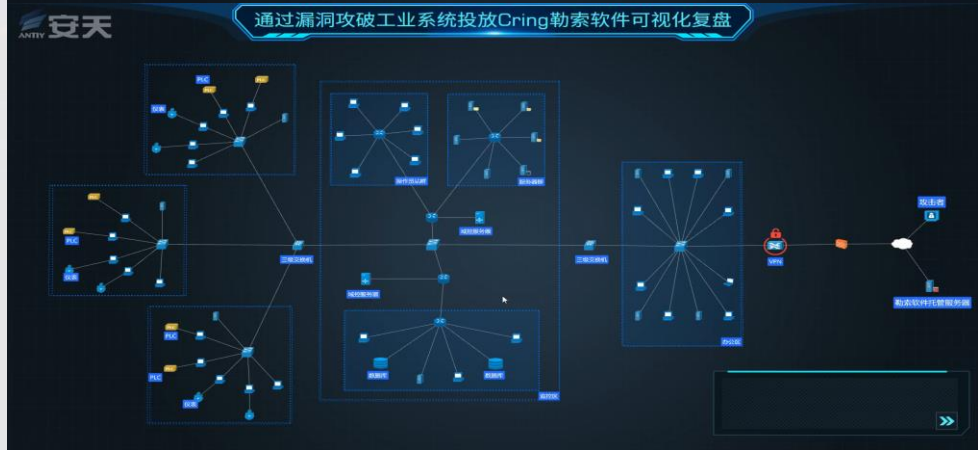
侦察 (10)	资源开发 (6)	初始访问 (9)	执行 (10)	持久化 (18)	提权 (12)	防御规避 (37)	凭证访问 (14)	发现 (25)	横向移动 (9)	收集 (17)	命令与控制 (16)	数据渗出 (9)	影响 (13)
主动扫描	获取基础设施	水坑攻击	利用命令和脚本解释器	挂载账户	禁用操作控制机制	禁用操作控制机制	暴力破解	发现用户	利用远程服务漏洞	恶意/可疑的进程	使用应用程序协议	导出数据	删除账户权限
搜集受害者主机信息	入侵程序	利用漏洞公众的应用程序	利用主机软件漏洞执行	利用ITX服务	提取访问令牌	提取访问令牌	获取应用程序中的凭证	发现应用程序窗口	执行网络攻击的恶意软件	捕获数据	通过可移动介质传播	限制传输数据大小	提取数据
搜集受害者身份信息	入侵基础设施	利用外部远程服务	利用进程间通信	利用动态链接库引导或劫持	利用ITX服务	利用ITX服务	利用凭证仿冒漏洞	发现进程窗口	纵向移动工具	自动收集	使用可移动介质传播	使用非C2协议传输	提取程序非预期的数据
搜集受害者网络信息	能力开发	添加条件	利用API	利用初始化工具引导或劫持	攻击漏洞/漏洞文件劫持	攻击漏洞/漏洞文件劫持	篡改认证	发现基础设施	远程服务会议劫持	收集网络数据	使用命令参数	使用C2通道传输	提取数据
搜集受害者网络信息	建立账户	网络钓鱼	利用计划任务/工作	添加注册扩展程序	创建/修改系统进程	创建/修改系统进程	输入凭证	云服务劫持	利用恶意软件	收集云存储的数据	使用命令参数	使用其他媒介传播	提取数据
通过网络钓鱼搜集信息	能力窃取	通过可移动介质传播	利用共享模块执行	篡改客户端软件	事件触发执行	事件触发执行	利用中间人攻击 (MITM)	云服务发现	凭证劫持	收集配置库的数据	使用加密信道	使用物理媒介传播	篡改数据
从非公开渠道搜集信息	入侵供应链	入侵供应链	利用第三方软件部署工具	创建账户	利用漏洞提权	利用漏洞提权	修改身份验证过程	发现信任链	使用可信中间件	收集信息库数据	使用可信信道	使用Web-服务传输	篡改数据
从公开渠道搜集信息	利用供应链	利用供应链	利用系统服务	创建账户	利用漏洞提权	利用漏洞提权	网络劫持	发现文件和目录	扫描网络服务	收集本地系统数据	使用入口工具传输	定时传输	篡改数据
搜集公开网站/域	利用有效用户	利用有效用户	诱导用户执行	事件触发执行	执行流程劫持	执行流程劫持	操作凭证互证	扫描网络服务	发现网络共享	收集可移动介质的数据	创建多级信道	和数据源转移到云用户	篡改数据
搜集受害者自有网站	利用有效用户	利用有效用户	利用Windows管理单元 (WMI)	利用外部远程服务	进程注入	进程注入	网络劫持	发现网络共享	网络劫持	收集可移动介质的数据	使用标准非可信信道	和数据源转移到云用户	篡改数据
				执行流程劫持	利用计划任务/工作	利用计划任务/工作	篡改数据	发现文件和目录	网络劫持	数据缓存	使用非可信信道	和数据源转移到云用户	篡改数据
			输入容器劫持	输入容器劫持	输入容器劫持	输入容器劫持	篡改数据	发现文件和目录	发现恶意软件	收集电子邮件	使用协议通道	和数据源转移到云用户	篡改数据
			启动Office应用程序	启动Office应用程序	启动Office应用程序	启动Office应用程序	篡改数据	发现文件和目录	发现恶意软件	收集电子邮件	使用协议通道	和数据源转移到云用户	篡改数据
			在操作系统启动	在操作系统启动	在操作系统启动	在操作系统启动	篡改数据	发现文件和目录	发现恶意软件	收集电子邮件	使用协议通道	和数据源转移到云用户	篡改数据
			利用计划任务/工作	利用计划任务/工作	利用计划任务/工作	利用计划任务/工作	篡改数据	发现文件和目录	发现恶意软件	收集电子邮件	使用协议通道	和数据源转移到云用户	篡改数据
			利用服务器软件组件	利用服务器软件组件	利用服务器软件组件	利用服务器软件组件	篡改数据	发现文件和目录	发现恶意软件	收集电子邮件	使用协议通道	和数据源转移到云用户	篡改数据
			使用流量命令	使用流量命令	使用流量命令	使用流量命令	篡改数据	发现文件和目录	发现恶意软件	收集电子邮件	使用协议通道	和数据源转移到云用户	篡改数据
			利用有效用户	利用有效用户	利用有效用户	利用有效用户	篡改数据	发现文件和目录	发现恶意软件	收集电子邮件	使用协议通道	和数据源转移到云用户	篡改数据



# 威胁框架能有效用于认知威胁，进行技术和战术的分析



阶段/步骤	工具/技术	攻击手法/原理	攻击结果/影响	防御/缓解措施
信息收集	搜索引擎、社工库	通过公开渠道获取目标IP、域名、员工信息等	获取目标网络架构、敏感信息	加强信息保护，限制搜索引擎索引
漏洞扫描	Nmap, Metasploit	扫描目标网络端口、漏洞	发现开放端口、漏洞	定期漏洞扫描，及时修补漏洞
漏洞利用	Metasploit, Exploit-DB	利用漏洞获取初始访问权限	成功获取初始访问权限	漏洞修复，入侵检测
权限提升	Powercat, Meterpreter	利用本地漏洞提升权限	获取系统管理员权限	权限最小化，定期审计
横向移动	Powercat, Meterpreter	在网内其他主机间移动	访问更多主机，扩大攻击范围	网络分段，访问控制
数据窃取	Powercat, Meterpreter	窃取敏感数据并上传	窃取大量敏感数据	数据加密，备份恢复
清除痕迹	Powercat, Meterpreter	删除日志、关闭端口	清除攻击痕迹	日志审计，端口管理



阶段/步骤	工具/技术	攻击手法/原理	攻击结果/影响	防御/缓解措施
信息收集	搜索引擎、社工库	获取目标工业系统信息	获取目标IP、域名	加强信息保护
漏洞扫描	Nmap, Metasploit	扫描工业系统漏洞	发现工业系统漏洞	定期漏洞扫描
漏洞利用	Metasploit, Exploit-DB	利用漏洞获取访问权限	成功获取访问权限	漏洞修复
权限提升	Powercat, Meterpreter	提升为系统管理员	获取系统管理员权限	权限最小化
勒索软件投放	Powercat, Meterpreter	部署Cring勒索软件	成功部署勒索软件	数据备份
勒索软件运行	Powercat, Meterpreter	加密数据、勒索赎金	数据被加密、勒索赎金	数据加密、备份恢复
清除痕迹	Powercat, Meterpreter	删除日志、关闭端口	清除攻击痕迹	日志审计、端口管理

# 将威胁框架映射到产品能力环节

初始访问	执行	持久化	提权	防御规避	凭证访问	发现	横向移动	收集	命令与控制	渗出	影响
水坑攻击	利用AppleScript 利用系统中的第三方...	利用bash_profile和... 启动守护	利用服务器软件组件 修改注册表数据...	修改注册表数据...	修改注册表数据...	扫描进程令牌 绕过GateKeeper Process Doppelg...	扫描账户 发现程序窗口	捕获视频 利用AppleScript	利用凭据窗口	自动渗出数据	删除账户权限
利用面向公众的应用...	利用CMSTP 利用Source命令	利用辅助功能 启动守护进程	利用服务器注册表数据...	修改注册表数据...	修改注册表数据...	绕过二进制文件 修改注册表	查看bash历史 发现应用程序窗口	自动收集 通过可移动介质通信	通过可移动介质通信	压缩数据	提取数据
利用外部远程服务	利用命令行 加入空格隐藏扩展名	隐藏账户 利用Launchctl	利用Setuid和Setgid位 利用AppCert.DLL(注...)	SID历史注入 利用BITS服务	隐藏文件目录 进程注入	暴力破解 发现浏览器书签	利用组件对象模型(C... 收集智能板数据	利用网络代理	加密数据	造成恶劣影响的数...	网页内容篡改攻击
添加硬件	利用HTML编译文件 利用系统中的第三方...	利用AppCert.DLL注... 添加C_LOAD_DYLIB	修改快捷方式 利用AppInit.DLL(注...)	利用自启动 绕过用户账户控制(UAC)	隐藏用户 冗余访问	凭证传播 发现域信任	利用远程服务漏洞 收集信息数据	使用自定义加密协议 限制传输数据大小	通过自定义加密协议	删除磁盘内容	
通过可移动介质复制	利用组件对象模型(C... 利用Trap命令	利用AppInit.DLL注... 利用linux本地任务调度	会话发起协议(SIP)和... 利用Windows应用程...	利用Windows应用程... 利用Sudo命令	清除命令历史 隐藏窗口	利用Regsvcs/Regasm 获取Web浏览器凭证	发现文件和目录 执行内部鱼叉攻击...	收集本地系统数据 使用自定义加密协议	通过自定义加密协议	删除磁盘内容	
使用鱼叉式钓鱼附件	利用远程控制板项 使用受信的工作工具	利用Windows应用程... 利用变量项	利用自启动 绕过用户账户控制(U...)	利用Sudo提权凭证 利用CMSTP	HISTCONTROL 利用Regsvr32	获取文件中的凭证 扫描网络服务	利用登录脚本 收集网络共享数据	编码数据 通过C2信道回传	删除磁盘内容		
使用鱼叉式钓鱼链接	使用动态数据交换... 诱导用户执行	利用证书包 利用登录脚本	利用系统组件 DLL搜索顺序劫持	利用有效账户 代码签名	映像劫持 使用rootkit	获取注册表中的凭证 发现网络共享	利用密码哈希验证 收集可移动介质数据	混淆数据 通过其他网络介绍回传	编写数据	编写数据	编写数据
通过服务执行鱼叉式...	通过API执行 利用Windows管理理...	利用BITS服务 利用SASS驱动程序	利用Systemd服务 Dylib劫持	使用Web Shell 发送后编译	阻止身份验证 利用Rundll32	利用凭证访问漏洞 网络嗅探	利用Ticket认证 回传数据准备	前置域名 通过物理介绍回传	损坏硬件		
入侵供应链	通过模块加载执行 利用Windows远程管...	使用Bootkit 修改现有服务	利用Windows时间服务 提示用户输入合法凭...		利用HTML编译文件 删除工具中的标识	使用脚本 强制认证	发现密码策略 利用远程桌面协议	收集电子邮件 使用生成或算法(DGA)	定时传输	禁止系统恢复	
利用有效账户	利用主机软件漏洞 利用XSL文件执行脚本	添加浏览器扩展项 Netch Helper DLL	利用Trap命令 利用事件监听守护进程		利用组件对象模型(COM)劫持 网络执行命令	执行签名的二进制文... 利用Hook	发现主机输入设备 浏览网页文件	输入捕捉 使用备用信道		网络断绝服务(DoS)	
	利用图形用户界面(GUI)	更改默认文件安装 新建服务	利用有效账户 利用漏洞提权		组件对象模型(COM)劫持 网络执行命令	执行签名的二进制文... 输入捕捉	发现数据流 利用远程服务	浏览器中间人攻击(MitB... 利用多跳代理		资源劫持	
	利用InstallUtil	利用组件对象模型(COM)...	启动Office应用程序 使用Web Shell	删除窗口内存注入(EW... 利用网络代理	安装数字证书 会话发起协议(SIP)和...	欺骗用户输入凭证 发现进程	通过可移动介质复制 获取屏幕数据	创建多跳信道 使用多协议通信		禁用服务	
	利用Launchctl	利用组件对象模型(COM)...	路径拦截 利用Windows事件订...	利用系统权限漏洞 利用网络代理	安装数字证书 会话发起协议(SIP)和...	欺骗用户输入凭证 发现进程	通过可移动介质复制 获取屏幕数据	创建多跳信道 使用多协议通信		禁用服务	
利用linux本地任务调度	创建账户 修改信任列表	Winlogon Helper D... 利用Hook		使用DCShadow技术 利用Launchctl	加入空格的隐藏扩展名 利用Keychain	发现远程系统 SSH劫持	使用多跳加密 删除本地存储数据				
利用SASS驱动程序	DLL搜索顺序劫持 端口监听		映像劫持	反向工程/解密文件信息 LC_MAIN劫持	硬注入 LLMNR/NBNS投毒...	发现安全软件 污染共享内容	端口监听 删除本地存储数据				
利用Mhta	Dylib劫持 端口监听		启动守护进程	禁用安全工具 仿冒	修改文件时间戳 网络嗅探	发现软件 利用系统中的第三...	利用网络访问工具 删除本地存储数据				
利用PowerShell	利用事件监听守护进程 利用PowerShell配置...		新建服务	DLL搜索顺序劫持 修改注册表	利用受信的开发工具 利用Password Filter...	发现系统信息 利用Windows管理理...	浏览网页文件 利用标准应用层协议				
利用Regsvcs/Regasm	利用外部远程服务 利用Rcommon文件		伪造父进程	DLL搜索顺序劫持 修改注册表	利用受信的开发工具 利用Password Filter...	发现系统信息 利用Windows管理理...	浏览网页文件 利用标准应用层协议				
利用Regsvr32	利用文件系统权限漏洞 重启应用程序		路径拦截	操作文件执行 删除网络共享连接	虚拟化/沙箱逃逸 利用Security的内存	发现系统网络连接 发现系统所有者/用户	使用标准应用层协议 利用Windows远程管...				
利用Rundll32	隐藏文件和目录 冗余访问		伪装属性列表	利用漏洞规避防御 利用NTFS交换数据流...	利用Web服务 窃取Web会话Cookie	发现系统所有者/用户 发现系统时间	利用Web服务 使用标准应用层协议				
利用计划任务	利用Hook 添加注册表运行项目...		端口监听	删除窗口内存注入(EW... 混淆文件信息	利用XSL文件执行脚本 双因子认证拦截	发现系统服务 发现系统时间	利用Web服务 使用标准应用层协议				
使用脚本	利用Hypervisor 利用计划任务		利用PowerShell配置...	修改文件和目录权限 伪造父进程			利用Web服务 使用标准应用层协议				
利用windows服务	映像劫持 利用屏幕保护程序		进程注入	删除文件 修改属性列表			利用Web服务 使用标准应用层协议				
利用签名的二进制文...	利用内核模块和扩展 利用SSP DLL(注...		利用计划任务	文件系统逻辑劫持 端口监听			利用Web服务 使用标准应用层协议				

- 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

	不相关
	无效 (未覆盖)
	有效
	可防御/可拦截
	可检测/可记录
	可降低机会
	可输出知识

# 通过威胁框架可以分析产品的布防与互补价值

侦察 (10)	资源开发 (7)	初始访问 (6)	执行 (13)	持久化 (10)	权限 (13)	初始权限 (40)	凭证访问 (15)	发现 (29)	横向移动 (9)	收集 (17)	命令与控制 (16)	数据渗出 (9)	影响 (13)
主动扫描	被动监听/嗅探	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备

- 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。

## 基于端点侧部署的安天智甲终端防御系统的检测和拦截点

侦察 (10)	资源开发 (7)	初始访问 (6)	执行 (13)	持久化 (10)	权限 (13)	初始权限 (40)	凭证访问 (15)	发现 (29)	横向移动 (9)	收集 (17)	命令与控制 (16)	数据渗出 (9)	影响 (13)
主动扫描	被动监听/嗅探	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备

侦察 (10)	资源开发 (7)	初始访问 (6)	执行 (13)	持久化 (10)	权限 (13)	初始权限 (40)	凭证访问 (15)	发现 (29)	横向移动 (9)	收集 (17)	命令与控制 (16)	数据渗出 (9)	影响 (13)
主动扫描	被动监听/嗅探	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备	利用合法身份/设备

## 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。





网络空间威胁对抗与防御技术研讨会  
暨 第九届安天网络安全冬训营

安天 | 智者安天下

# 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 <b>基于风险的方法</b> 。	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 (Identify)



塑造 (Shape)



防护 (Protect)



检测 (Detect)



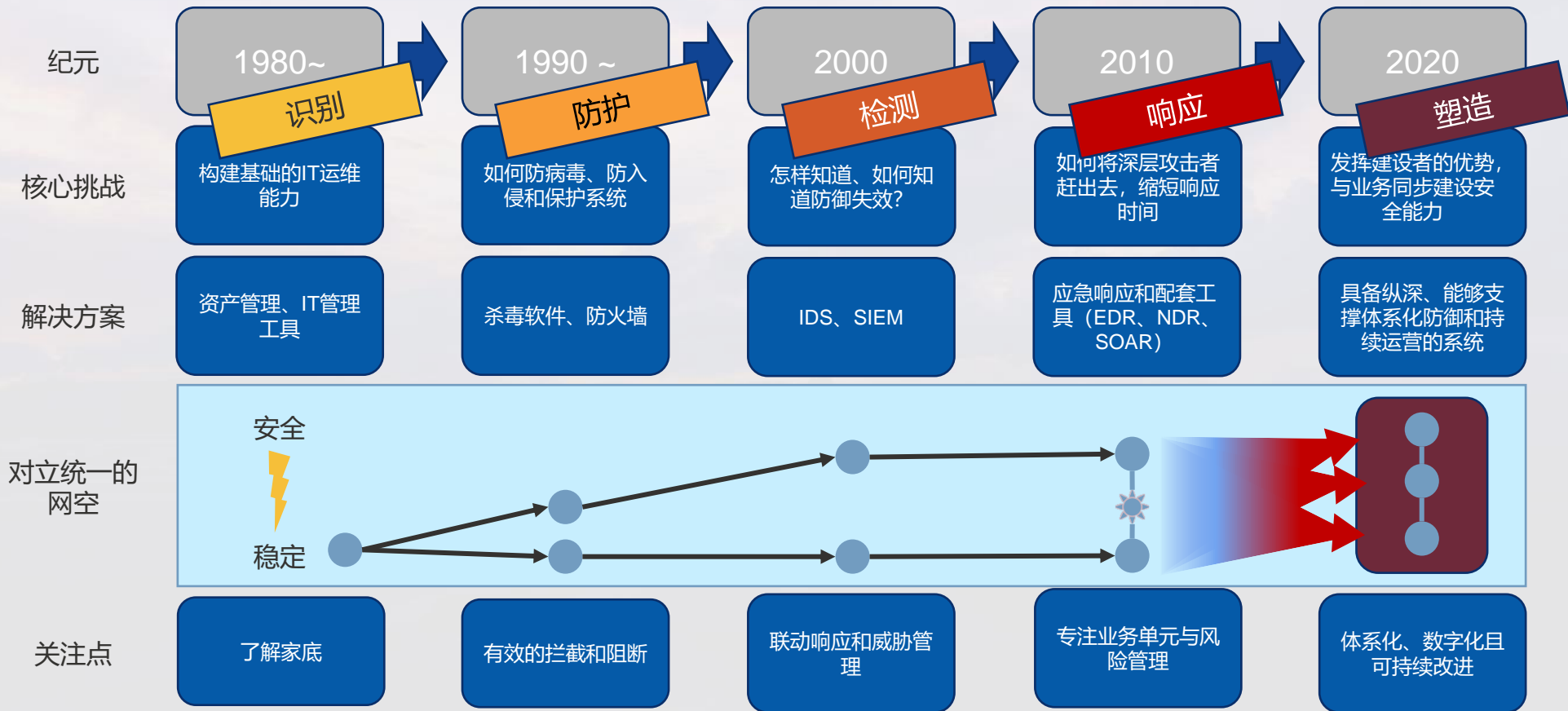
响应 (Respond)

识别是网络安全管理的基础。识别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。

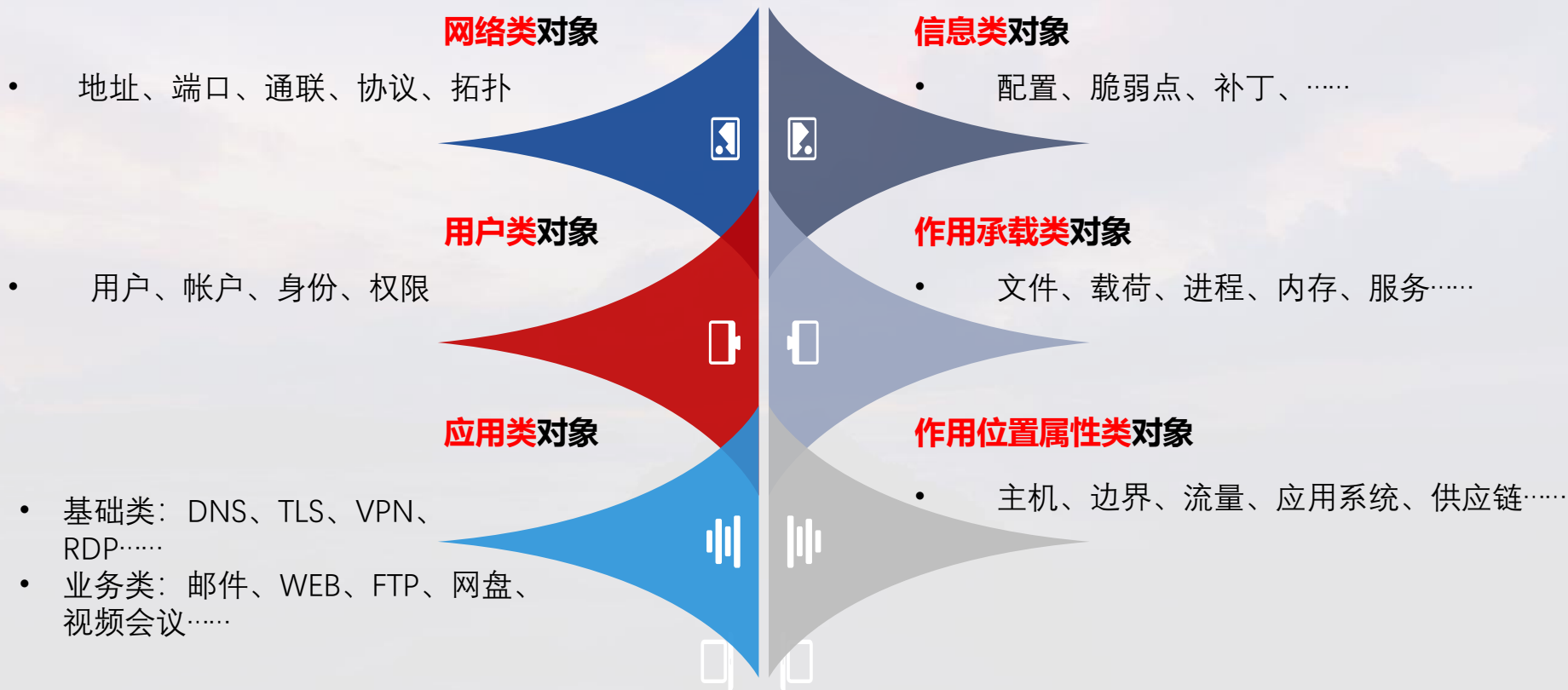
防护是系统对威胁做出的行为反应。防护是避免威胁行为达成预期后果的交互过程。其核心是对威胁活动和违规行为的拒止动作。

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



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	作用位置
	内容 地址 协议 端口 .....	用户 帐户 身份 权限	DNS TLS VPN 邮件 WEB .....	配置 补丁 脆弱点 .....	载荷 进程 内存 服务 .....	

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



威胁等级	威胁名称	威胁描述	威胁类型	威胁来源	威胁目标	威胁影响	威胁检测	威胁防御	威胁响应	威胁处置
6级	国家利益损失	窃取国家机密、破坏国家基础设施	网络攻击	境外敌对势力	国家利益	严重	入侵检测、流量分析	防火墙、入侵防御	应急响应、溯源	修复、加固
5级	国家秘密泄露	窃取国家秘密、破坏国家声誉	网络攻击	境外敌对势力	国家秘密	严重	入侵检测、流量分析	防火墙、入侵防御	应急响应、溯源	修复、加固
4级	国家经济受损	破坏国家经济、窃取国家财产	网络攻击	境外敌对势力	国家经济	严重	入侵检测、流量分析	防火墙、入侵防御	应急响应、溯源	修复、加固
3级	国家声誉受损	破坏国家声誉、窃取国家财产	网络攻击	境外敌对势力	国家声誉	严重	入侵检测、流量分析	防火墙、入侵防御	应急响应、溯源	修复、加固
2级	国家基础设施受损	破坏国家基础设施、窃取国家财产	网络攻击	境外敌对势力	国家基础设施	严重	入侵检测、流量分析	防火墙、入侵防御	应急响应、溯源	修复、加固
1级	国家财产受损	破坏国家财产、窃取国家财产	网络攻击	境外敌对势力	国家财产	严重	入侵检测、流量分析	防火墙、入侵防御	应急响应、溯源	修复、加固
0级	国家声誉受损	破坏国家声誉、窃取国家财产	网络攻击	境外敌对势力	国家声誉	严重	入侵检测、流量分析	防火墙、入侵防御	应急响应、溯源	修复、加固

威胁框架

威胁场景化想定



威胁想定

体系对抗威胁

检验防御充分性

关键防御动作



防御体系

能力组装

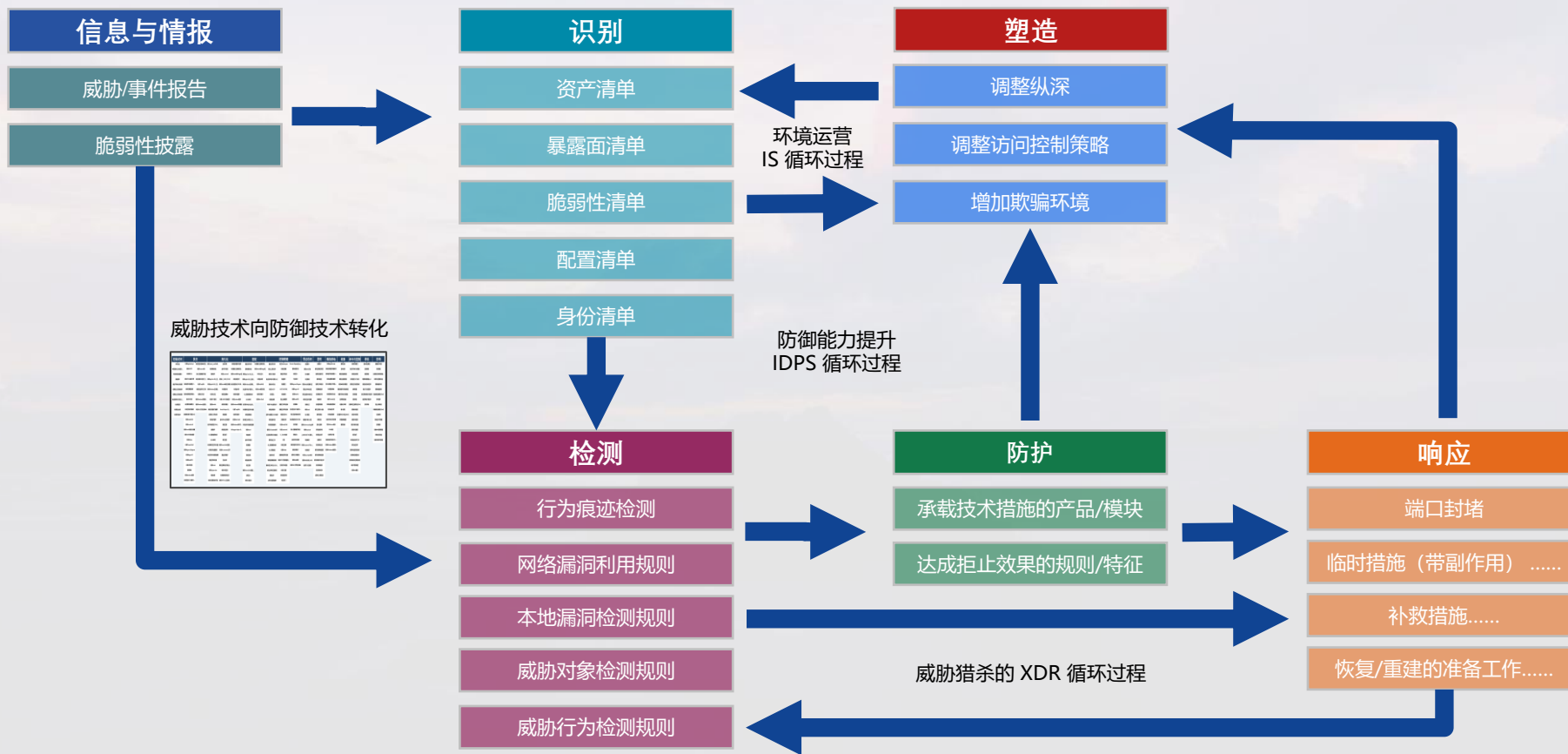
关键防御动作矩阵	识别	塑造	防护	检测	响应
	系统环境识别 网络环境识别 业务识别 用户识别 配置识别 暴露面/脆弱性识别 漏洞识别	系统环境策略塑造 网络管理策略塑造 配置加固 加密环境塑造 暴露面环境塑造	控制访问禁止 传输禁止 创建禁止 写入禁止 执行禁止 加载禁止 .....	系统环境检测 流量环境检测 应用环境检测 数据库检测 用户行为检测	阻断 修正 主机环境处置 网络侧位置 环境参数调整修复 策略调整
作用对象	网络类	用户类	应用类	信息类	执行类
部署方式	与被保护对象原生融合or安装   基于载体设备部署   基于虚拟化资源部署				
管理模式	单点管控/集中管控/无管控				

防御框架



智者安天下

# 威胁对抗驱动防御能力提升





网络空间威胁对抗与防御技术研讨会  
暨 第九届安天网络安全冬训营

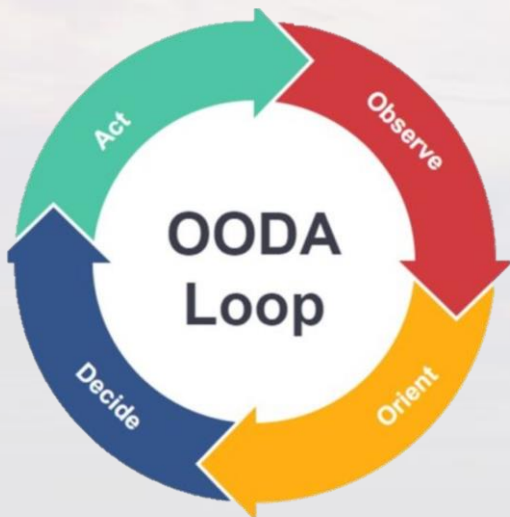


# 04

## 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。

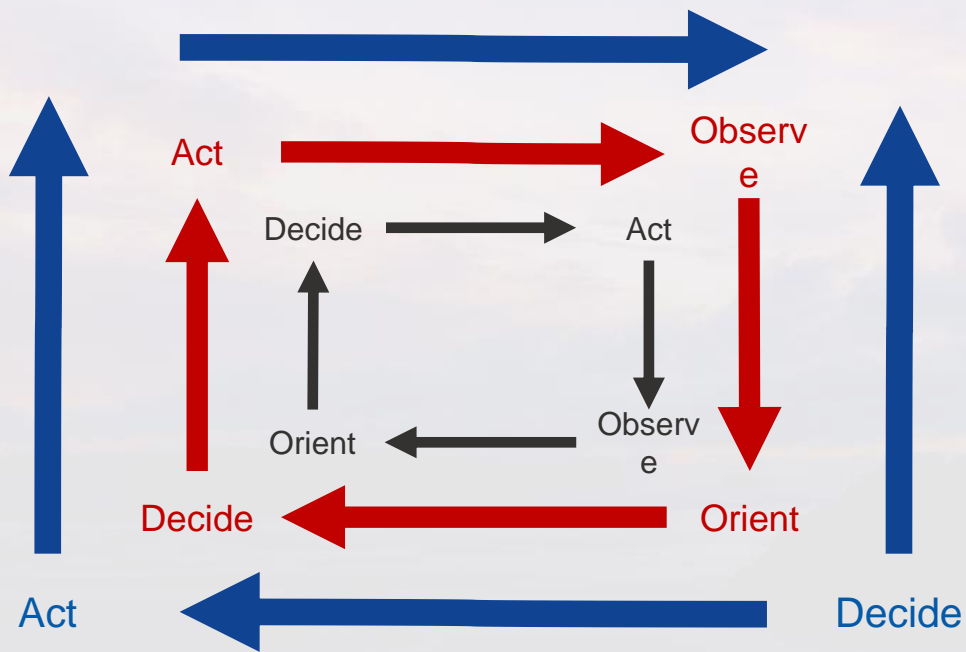


针对日常安全运营工作，实现支撑“观察-研判-决策-执行”的“OODA”型业务闭环，达成比威胁方更快的OODA循环。



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

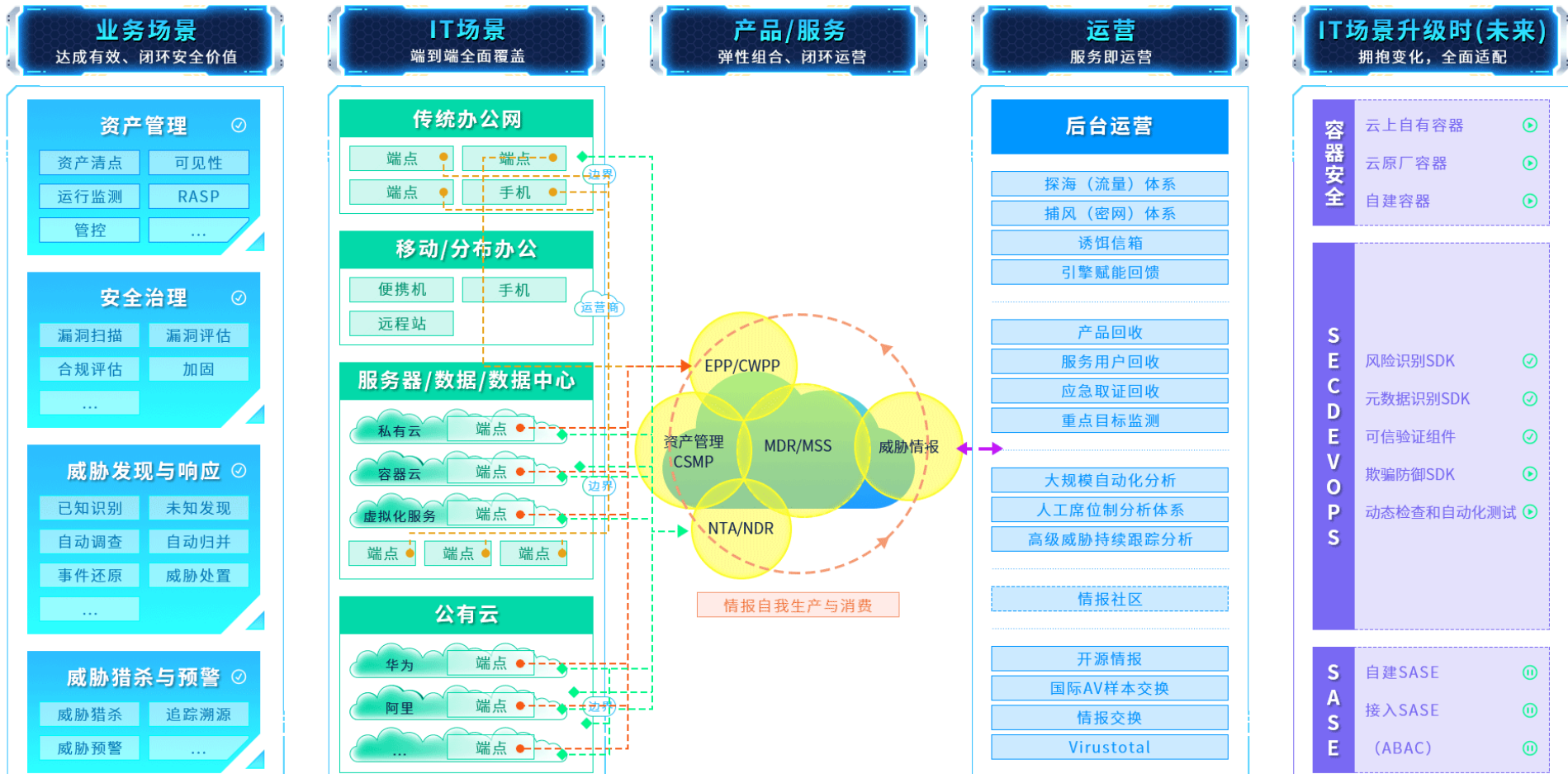
基于威胁假定的合理设计可以大幅提升数字化业务安全响应速度

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

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

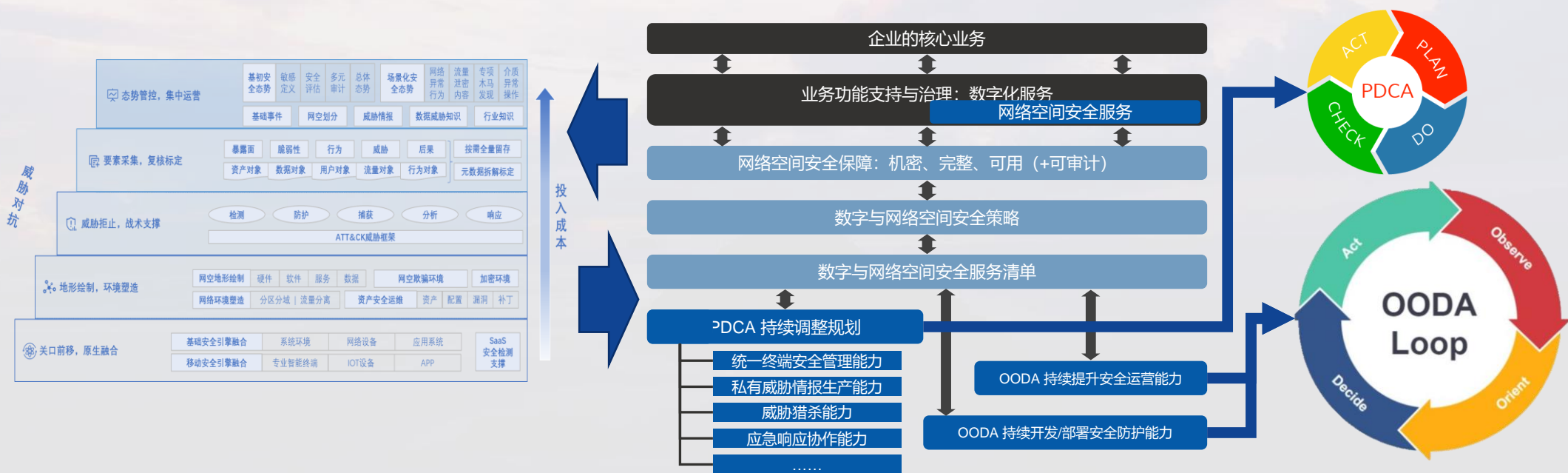


# 动态综合防御体系框架



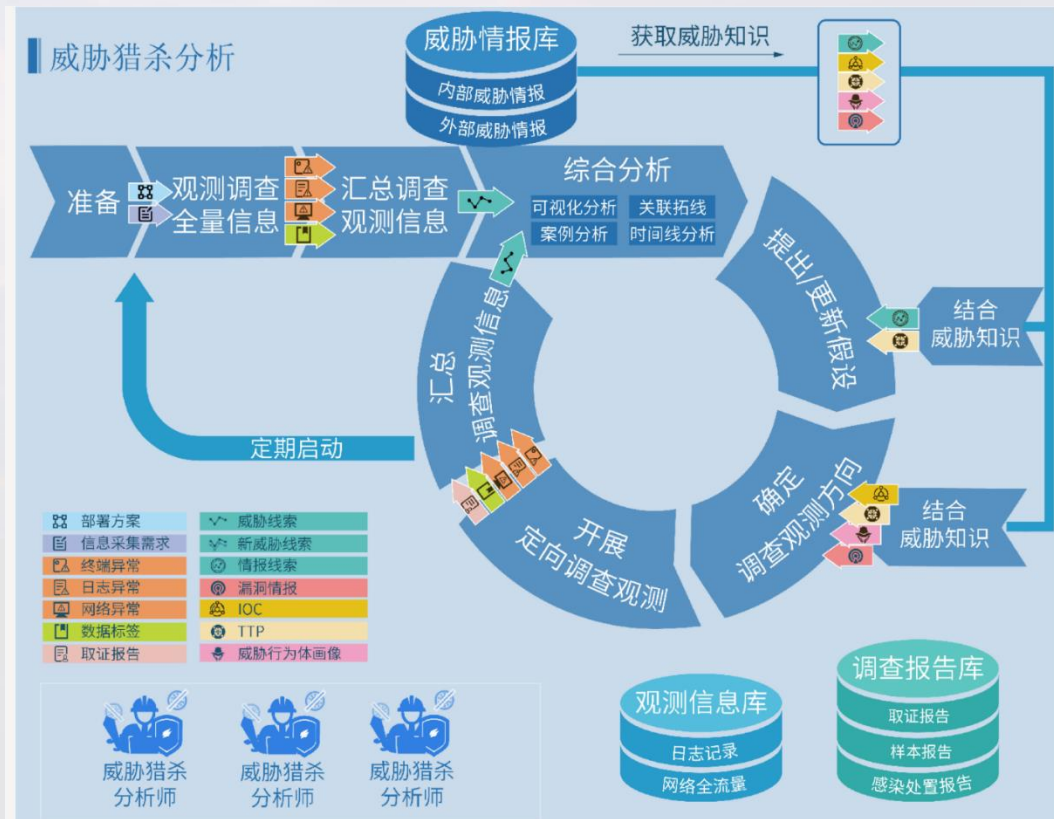
# 此消彼长，在数字化世界对抗威胁比拼的是速度

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







网络空间威胁对抗与防御技术研讨会  
暨 第九届安天网络安全冬训营

亂雲飛渡

# 谢谢大家



安天冬训营 [wtc.antiy.cn](http://wtc.antiy.cn)