网络空间威胁对抗与防御技术研讨会
暨 第七届安天网络安全冬训营

从态势感知视角看方程式攻击中东SWIFT服务商事件

通过ATT&CK威胁框架技战术分析驱动防御改善

安天态势感知研发部

威胁框架：认知与实践

寒夜远征

寒夜远征

CONTENTS

目 录

01 SWIFT攻击事件回顾

由SWIFT攻击过程看防御体系

02 动态综合防御体系

面向失效建设高对抗能力的防御体系

寒夜速记

威胁框架：认知与实践

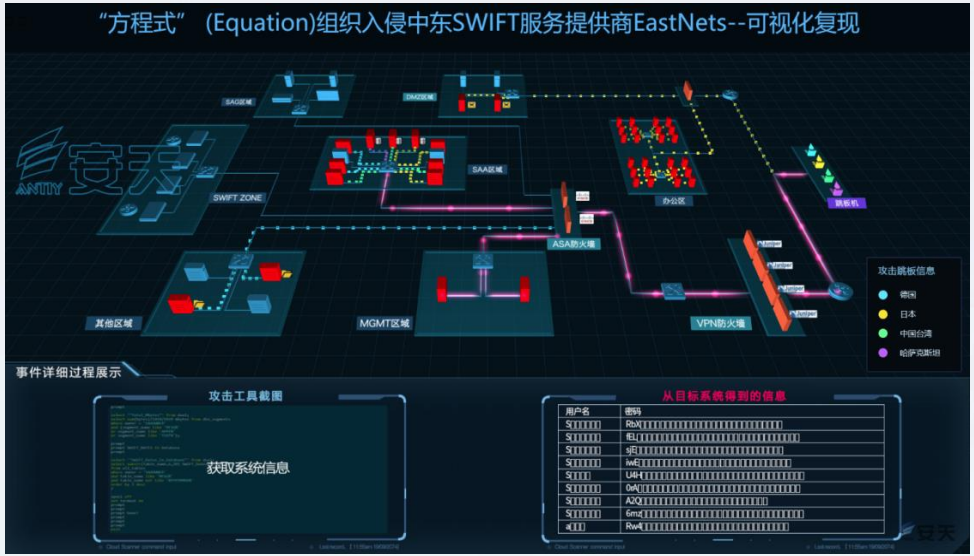
01 SWIFT攻击事件回顾

由SWIFT攻击过程看防御体系

安天完整复盘SWIFT攻击事件

金融、能源、电力、通信、交通等领域的关键信息基础设施，是经济社会运行的神经中枢，也是可能遭到重点攻击的目标。安天从2010年的震网事件开始，将应急分析工作的重心转入到**高级网空威胁行为体**所发动的定向化的高级威胁中，在高级威胁发现、分析、溯源方面取得了一系列进展。

在2019年6月1日，**安天发布《“方程式组织”攻击中东SWIFT服务商事件复盘分析报告》，完整复盘了超级大国网空威胁行为体攻击中东金融服务机构的全过程**，这一分析成果被新华社等权威媒体引用发布。



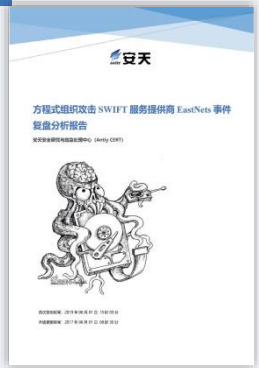
近日，安天实验室发布了对NSA下属的“方程式”组织攻击中东地区最大的SWIFT金融服务提供商EastNets事件的复盘分析，表明“方程式”组织利用国家级网络武器，层层渗透控制SWIFT这样的商业组织网络，以获取长久控制权，实现其长期潜伏、持续获取相关信息的战略目的。


署名文章：对美国网络攻击目标泛化的隐忧

新华社署名文章题为“对美国网络攻击目标泛化的隐忧”
http://www.xinhuanet.com/politics/2019-06/13/c_1124617833.htm

SWIFT攻击事件简介

扫码阅读安天原创报告



SWIFT介绍

SWIFT（Society for Worldwide Interbank Financial Telecommunications），中文名称为“环球银行金融电信协会”。

- 总部位于比利时，提供了一个计算机网络允许超过200个国家的金融机构相互收发金融交易信息。
- SWIFT的成员多数为银行和贸易机构。
- SWIFT网络不直接交易现金，而是在机构账户之间，使用SWIFT码，发送付款委托书。SWIFT码又称为银行识别码，在SWIFT网络中用于交易，例如英国的巴克莱银行的代码为BARCGB22。
- SWIFT服务机构提供了一种最划算的访问完整SWIFT服务的方式，不需要了解SWIFT的专业知识，它相当于银行的云服务供应商。
- 全世界范围内共有74家官方认可的SWIFT服务机构。SWIFT服务机构通过SWIFT软件和Oracle数据库来管理金融交易。

安天对网空威胁行为体的能力分级

威胁等级：6级

防御目标：5级目标+超高能力国家/地区行为体

特点：

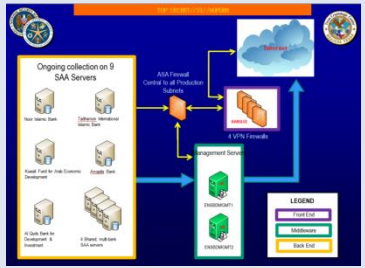
- 国家/地区行为体，
- 受国家/地区利益驱动，
- 网络网络与网络战一体化，
- 寻求通过网络战获得政治、经济、军事优势

攻击技术和工具：

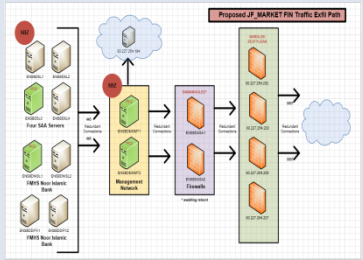
- 掌握对自身国家/地区级网络基础设施、外部国家/地区级网络基础设施、互联网级网络基础设施、以及信息科技供应链的部分控制能力
- 专有攻击技术、工具与平台
- 跨维度高度集成的攻击利用手段
- 漏洞挖掘与利用技术开发能力
- 制造漏洞能力
- 掌握大量0day漏洞

SWIFT攻击事件是一起由超高能力网空威胁行为体发起，以窃取关键金融基础设施数据为目标的高级持续性威胁攻击事件。2012年7月至2013年9月，“方程式组织”（Equation Group）采用全球多个区域的预设跳板机和复合手段，对EastNets（中东地区最大SWIFT服务提供商）发起了6次网络攻击，最终攻入数据库获取了大量关键数据信息。

攻陷了**4台**VPN防火墙设备、**2台**企业级防火墙、**2台**管理服务器，以及**9台**运行多国金融机构业务系统的SAA服务器和FTP服务器以及对外提供的邮件服务器。



攻击者的入侵路线



攻击者回传数据的路线

网络侧：主要利用Cisco和Juniper两种品牌防火墙的0day漏洞，完全获取了相关设备名称、软件版本、开放端口等信息。

主机侧：使用“永恒”系列0day漏洞突破内网Mgmt（管理服务器）、SAA业务服务器和应用服务器。

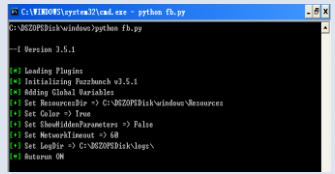
漏洞名称	漏洞介绍
ETERNALROMANCE	“永恒浪漫”漏洞，可用于远程提升用户权限，目标是开放445端口的Windows XP 至 Windows 2008 操作系统
ENTERNALCHAMPION	“永恒冠军”漏洞，针对Windows8和Windows2012操作系统的远程利用漏洞
ETERNALBLUE	“永恒之蓝”漏洞，攻击Windows XP至Windows 2012 操作系统SMB和NBT服务的远程利用漏洞
EXPLODINGCAN	“爆炸罐头”漏洞，是针对Windows 2003操作系统中IIS 6.0的远程利用漏洞
EWORKFRENZY	针对Lotus Domino 6.5.4 和7.0.2的漏洞
ETERNALSYNERGY	“永恒协作”漏洞，是Windows 8 和Windows Server 2012操作系统上的远程利用漏洞

主机侧利用“永恒”系列0Day漏洞

多种攻击装备覆盖全设备和系统，包括网络边界的VPN防火墙设备、企业级防火墙设备、管理服务器以及支撑SWIFT业务的SAA服务器等。

漏洞利用工具和攻击平台

主要使用FuzzBunch漏洞利用攻击平台，用于对目标主机进行探测和漏洞利用



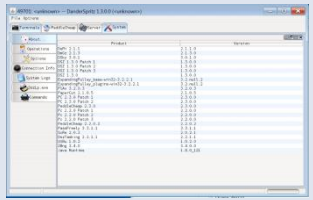
FuzzBunch攻击装备界面

持久化/植入攻击装备

获取内部网络拓扑、登录凭证后突破目标，形成可反复植入的作业目标窗口，实现持久化。

控制/后门类恶意代码

主要使用DanderSpritz远程控制程序，当植入目标主机的后门执行后，攻击者可以通过该平台对目标主机进行完整控制。



DanderSpritz远程控制装备界面

编写SQL脚本，从Oracle数据库中提取敏感信息

使用的两种SQL脚本

- initial_oracle_exploit.sql脚本获取系统信息
- swift_msg_queries_all.sql脚本获取金融机构交易信息

在SAA服务器上执行SQL脚本对本地Oracle数据库中存储的多家银行机构业务数据（账号名、账号状态、密码等）进行转储。还通过管理服务器对其它区域中的FTP服务器进行攻击。

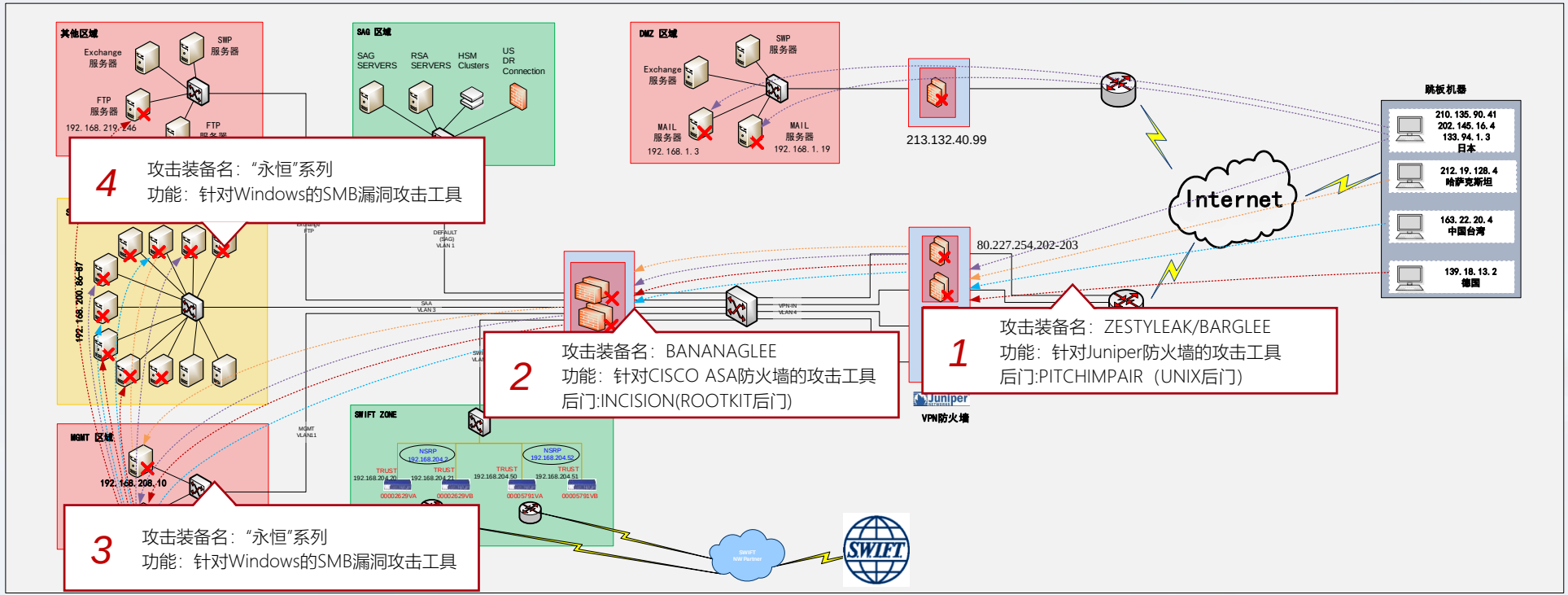
攻击过程简述

步骤1：
通过外网跳板机攻击
内网VPN防火墙

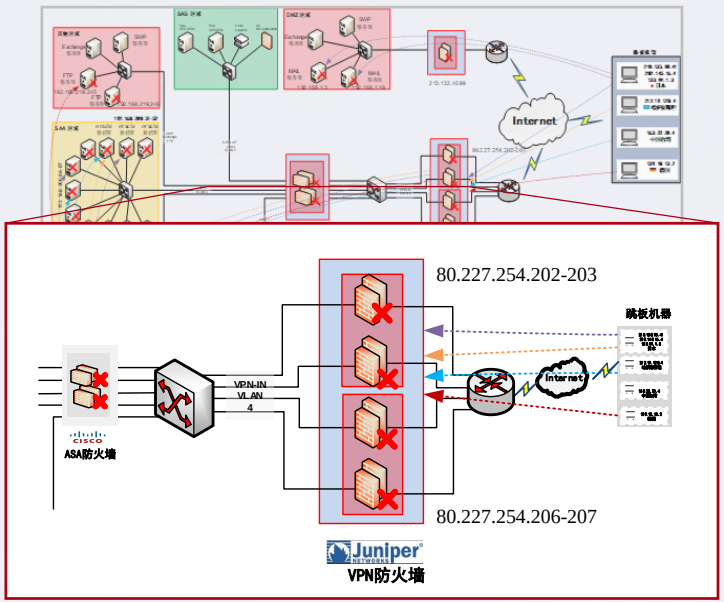
步骤2：
通过VPN防火墙攻击
内网企业级防火墙

步骤3：
通过内网企业级防火墙攻击
管理服务器

步骤4：
通过管理服务攻击
SAA服务器



攻击步骤1：通过外网跳板机攻击内网VPN防火墙（1）



通过漏洞攻击并控制VPN防火墙

被攻陷资产Tag

类型：防火墙　**版本型号**：Juniper SSG 520M

用途：提供VPN接入服务

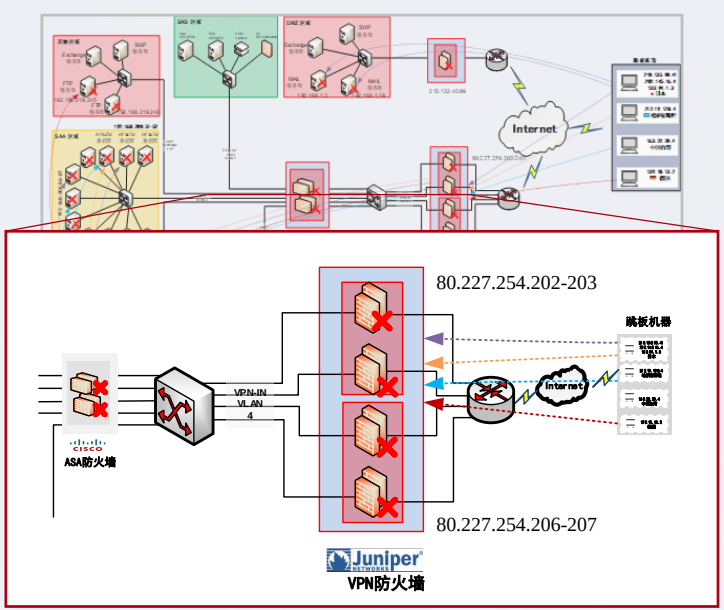
被攻陷资产对象已有的防护措施

强密码 登录认证 | 网段访问控制策略 | syslog日志记录 | 分离的管理接口

攻击行为的ATT&CK映射

攻击动作	攻击行为映射		攻击动作技术分析
①通过跳板机利用漏洞攻击防火墙	初始访问	有效账号	在VPN防火墙中进行凭证转储，查看配置内容中存在的凭证；
	初始访问	外部远程服务	发现其可以利用的外部远程服务，**使用漏洞进行攻击CVE-2015-7755**；
②植入持久化攻击装备到防火墙中	命令与控制	远程文件复制	通过隐蔽通道利用装备进行文件传输与复制；
	执行	命令行界面	攻击所使用的方式都是基于命令进行控制；
	持久化	Bootkit	FEEDTROUGH**持久化**攻击装备可能具有BootKit功能；
	持久化	组件固件	FEEDTROUGH持久化攻击装备可能存在组件固件；
③通过持久化装备植入两款后门攻击装备，实现对防火墙的完全控制	命令与控制	远程文件复制	通过隐蔽信道利用装备进行文件传输与复制；
	命令与控制	创建多级信道	通过多种重定向装备进行多级信道建立隐蔽信道；
	执行	命令行界面	攻击所使用的方式都是基于命令进行控制；
	命令与控制	利用不常用端口	攻击中所**使用端口**444、555等；
	收集	收集本地系统数据	收集防火墙配置信息规则信息；
	数据渗出	自动渗出	将收集到的有价值信息进行回传；

攻击步骤1：通过外网跳板机攻击内网VPN防火墙（2）



通过漏洞攻击并控制VPN防火墙

被攻陷资产Tag

类型：防火墙　**版本型号**：Juniper SSG 520M

用途：提供VPN接入服务

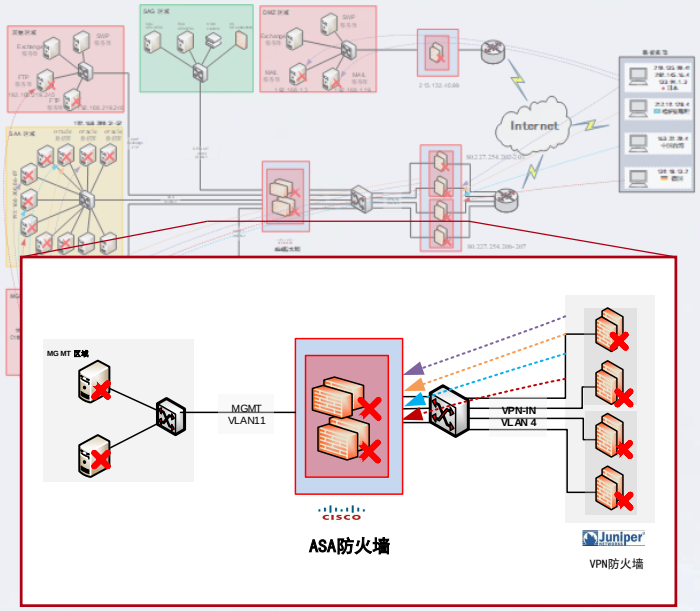
被攻陷资产对象已有的防护措施

强密码 登录认证 | 网段访问控制策略 | syslog日志记录 | 分离的管理接口

对应攻击行为的防护措施分析

攻击动作	攻击行为映射		对应的防护措施分析
①通过跳板机利用漏洞攻击防火墙	初始访问	有效账号	**设置远程接入区（DMZ区）、设置远程接入白名单**、多因子认证、特权帐户管理、身份验证日志记录与审计、流量监控
	初始访问	外部远程服务	
②植入持久化攻击装备到防火墙中	命令与控制	远程文件复制	深包解析、网络全要素记录、网络协议分析
	执行	命令行界面	
	持久化	Bootkit	固件校验
	持久化	组件固件	
③通过持久化装备植入两款后门攻击装备，实现对防火墙的完全控制	命令与控制	远程文件复制	**深包解析、网络全要素记录、网络协议分析**、Netflow采集、日志采集与审计
	命令与控制	创建多级信道	
	执行	命令行界面	
	命令与控制	利用不常用端口	网络协议分析、Netflow采集、日志采集与审计
	收集	收集本地系统数据	
	数据渗出	自动渗出	网络全要素记录、日志采集与审计

攻击步骤2：通过VPN防火墙攻击内网企业级防火墙（1）



通过漏洞攻击并控制区域边界防火墙

被攻陷资产Tag

类型：防火墙　**版本型号**：CISCO PIX Ver. 8.0

用途：区域边界访问控制

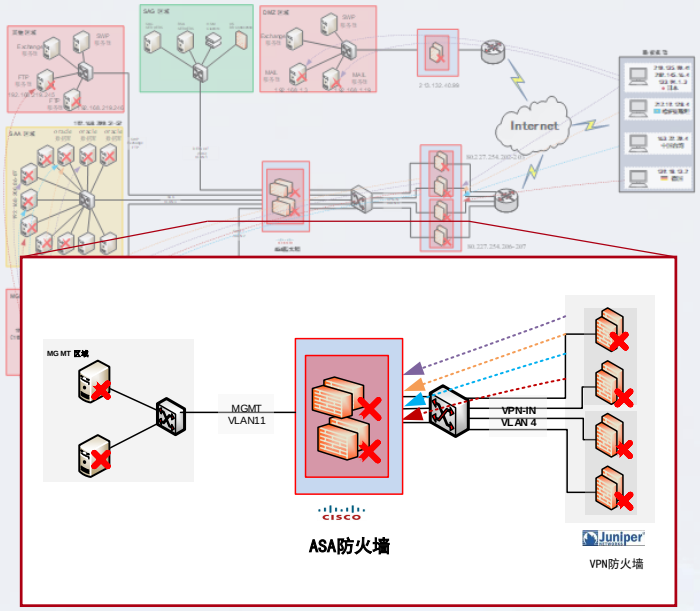
被攻陷资产对象已有的防护措施

强密码 登录认证 | 网段访问控制策略 | syslog日志记录 | 分离的管理接口

攻击行为的ATT&CK映射

攻击动作	攻击行为映射		攻击动作技术分析
①通过横向以动利用漏洞攻击防火墙	发现	网络嗅探	对内部网络结构进行扫描探测收集相关信息
	横向移动	利用远程服务漏洞	Cisco 设备的SNMP服务（端口161、162）漏洞攻击;
	提权	利用漏洞提权	针对Cisco ASA and PIX设备中command-line interface (CLI)解析器的CVE-2016-6367漏洞攻击;
	命令与控制	拷贝远程文件	通过隐蔽信道利用装备进行文件传输与复制;
	命令与控制	创建多级信道	通过多种重定向装备进行多级信道建立隐蔽信道;
②植入持久化攻击装备到防火墙中	命令与控制	拷贝远程文件	通过隐蔽信道利用装备进行文件传输与复制;
	命令与控制	创建多级信道	通过SCREAMINGPLOW等装备建立多级信道;
	执行	利用命令行	其整个攻击框架所使用的方式都是基于命令进行控制;
	持久化	使用Bootkit	针对 Cisco ASA and PIX设备进行持久化的攻击装备JETPLOW和SCREAMINGPLOW;
	持久化	利用系统固件	
③通过持久化装备植入后门攻击装备，实现对防火墙的完全控制	命令与控制	拷贝远程文件	通过隐蔽信道利用装备进行文件传输与复制;
	执行	利用命令行	其整个攻击框架所使用的方式都是基于命令进行控制;
	命令与控制	创建多级信道	通过多种重定向装备进行多级信道建立隐蔽信道
	命令与控制	利用不常用端口	攻击中所使用的端口都不是常用的端口如(4426、555);
	凭证访问	网络嗅探	对内部网络结构进行扫描探测收集相关信息

攻击步骤2：通过VPN防火墙攻击内网企业级防火墙（2）



通过漏洞攻击并控制区域边界防火墙

被攻陷资产Tag

类型：防火墙　**版本型号**：CISCO PIX Ver. 8.0

用途：区域边界访问控制

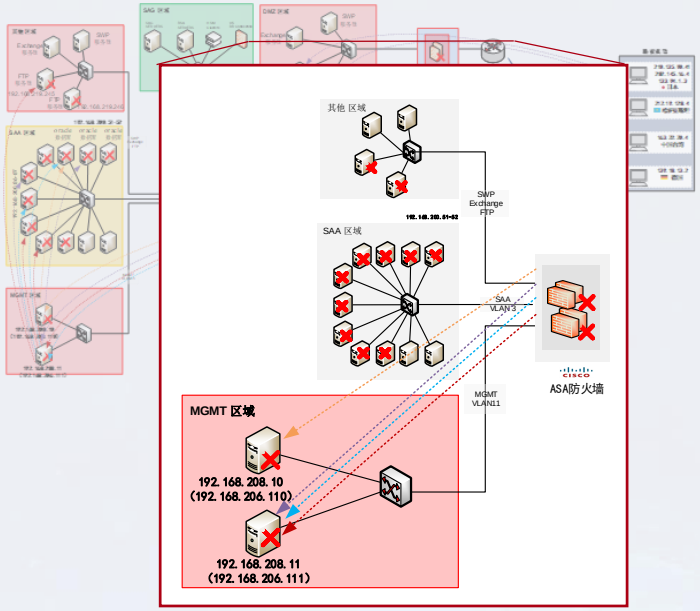
被攻陷资产对象已有的防护措施

强密码 登录认证 | 网段访问控制策略 | syslog日志记录 | 分离的管理接口

对应攻击行为的防护措施分析

攻击动作	攻击行为映射		对应的防护措施分析
①通过横向以动利用漏洞攻击防火墙	发现	网络嗅探	Netflow记录、网络全要素采集、全流量记录、网络协议分析、防火墙设备日志采集与审计、端口白名单
	横向移动	利用远程服务漏洞	
	提权	利用漏洞提权	防火墙设备日志采集与审计
	命令与控制	拷贝远程文件	网络深包解析、网络全要素记录、网络协议分析 Netflow、日志采集与审计、全流量记录
	命令与控制	创建多级信道	
②植入持久化攻击装备到防火墙中	命令与控制	拷贝远程文件	
	命令与控制	创建多级信道	
	执行	利用命令行	
	持久化	使用Bootkit	固件校验
	持久化	利用系统固件	
③通过持久化装备植入后门攻击装备，实现对防火墙的完全控制	命令与控制	拷贝远程文件	网络深包解析、网络全要素记录、网络协议分析
	执行	利用命令行	
	命令与控制	创建多级信道	Netflow、网络协议分析、网络设备日志采集与审计 网络全要素、全流量记录、、端口白名单
	命令与控制	利用不常用端口	
	凭证访问	网络嗅探	多因子认证、加密

攻击步骤3：通过内网企业级防火墙攻击管理服务器（1）



通过漏洞攻击并控制Mgmt管理服务器

被攻陷资产Tag

类型：服务器　**版本型号**：win2k8 SP2 x86

用途：Mgmt 管理服务器

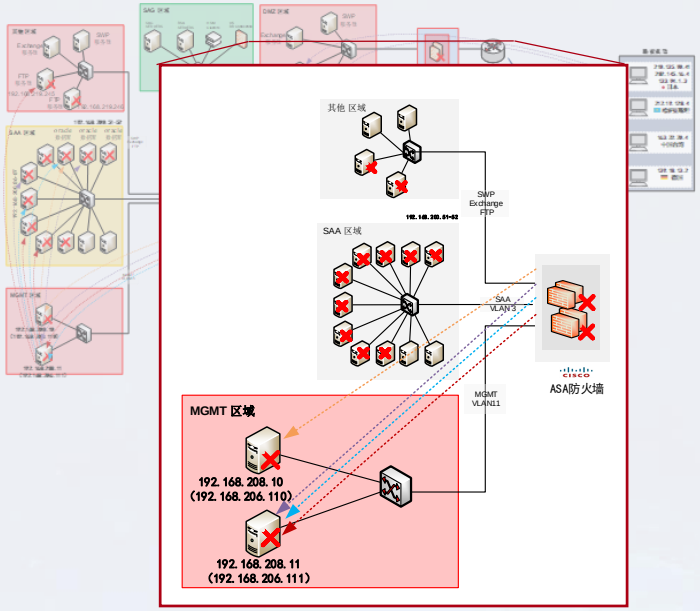
被攻陷资产对象已有的防护措施

强密码 登录认证 | Symantec Endpoint Protection 11（部分未装）

攻击行为的ATT&CK映射

攻击动作	攻击行为映射		攻击动作技术分析
①通过横向以动利用漏洞攻击管理服务器	发现	网络嗅探	对内部网络结构进行扫描探测收集相关信息；
	发现	扫描网络服务	使用ping命令和DS平台的扫描模块收集端口和服务信息
	发现	发现网络共享	在扫描到在线主机后会尝试链接其IP地址的默认共享
	横向移动	利用远程服务漏洞	可能使用永恒系列漏洞攻击装备，针对Windows Server 008 R2 的SMBv1远程代码执行漏洞；
②植入持久化攻击装备到管理服务器中	命令与控制	利用常用端口	利用“永恒”系列漏洞针对445端口进行漏洞利用；
	命令与控制	使用标准加密协议	DS攻击平台使用的是标准的加密协议；
③通过植入的攻击装备进一步植入DanderSpritz后门进行远程控制。	防御规避	进程注入	DanderSpritz平台生成的后门载荷投放并注入系统进程；
	执行	通过模块加载执行	DanderSpritz平台插件以模块内存加载执行；
	命令与控制	使用标准加密协议	DS攻击平台使用的是标准的加密协议；
	命令与控制	利用不常用端口	DS攻击平台反弹shell端口可自定义一些不太常用的端口
	命令与控制	创建多级信道	据有多种信道进行通信；
	命令与控制	端口敲门	DS攻击平台监听端口对数据包进行过滤符合的才会激活
	凭证访问	凭证转储	通过DS攻击平台投放凭证转储插件；

攻击步骤3：通过内网企业级防火墙攻击管理服务器（2）



通过漏洞攻击并控制Mgmt管理服务器

被攻陷资产Tag

类型：服务器　**版本型号**：win2k8 SP2 x86

用途：Mgmt 管理服务器

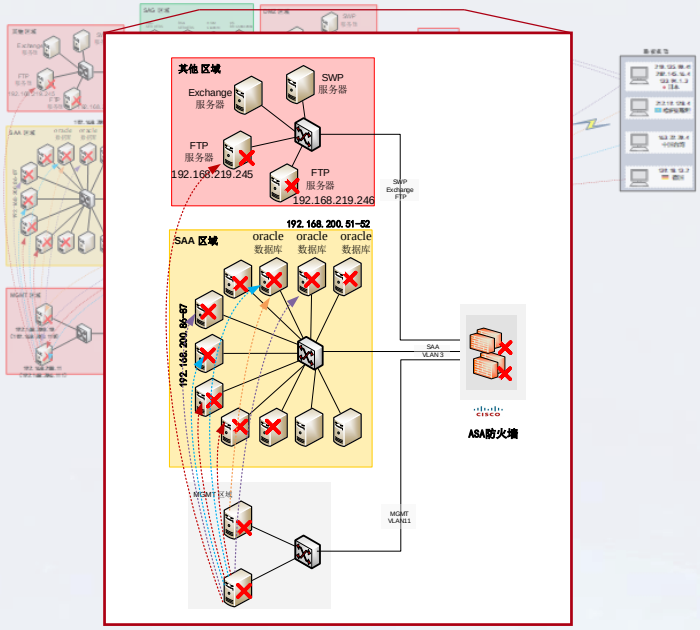
被攻陷资产对象已有的防护措施

强密码 登录认证 | Symantec Endpoint Protection 11（部分未装）

对应攻击行为的防护措施分析

攻击动作	攻击行为映射		对应的防护措施分析
①通过横向以动利用漏洞攻击管理服务器	发现	网络嗅探	**多因子认证、加密**
	发现	扫描网络服务	Netflow记录、网络协议分析、数据包捕获、网络全要素、全流量记录、网络深包解析
	发现	发现网络共享	
	横向移动	利用远程服务漏洞	进程监控、进程命令行参数、windows 错误报告、网络全要素、全流量记录、网络深包解析
②植入持久化攻击装备到管理服务器中	命令与控制	利用常用端口	**进程监控、进程命令行参数**、网络协议分析、进程请求网路监控、windows 系统日志、网络全要素、全流量记录、网络深包解析、进程请求网路监控
	命令与控制	使用标准加密协议	
③通过植入的攻击装备进一步植入DanderSpritz后门进行远程控制。	防御规避	进程注入	API监控、Windows 注册表信息、文件监控、DLL监控 进程监控、windows 系统日志
	执行	通过模块加载执行	
	命令与控制	使用标准加密协议	网络协议分析、网络全要素、全流量记录
	命令与控制	利用不常用端口	进程监控、进程命令行参数、网络协议分析、进程请求网路监控、网络全要素、全流量记录、网络深包解析
	命令与控制	创建多级信道	Netflow记录、网络协议分析、网络设备日志采集与审计、网络全要素、全流量记录
	命令与控制	端口敲门	
	凭证访问	凭证转储	文件进程监控、 PowerShell日志、进程命令行参数

攻击步骤4：通过管理服务攻击SAA服务器（1）



通过漏洞攻击并控制SAA业务服务器

被攻陷资产Tag

类型：服务器 **版本型号**：wind 2008 r2 SP1(64) **用途**：SAA业务服务器

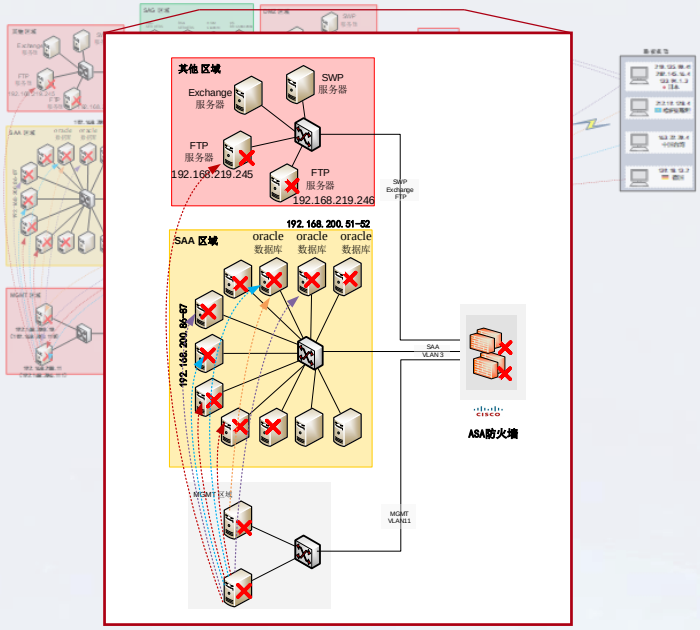
被攻陷资产对象已有的防护措施

强密码 登录认证 | Symantec Endpoint Protection 11

攻击行为的ATT&CK映射

攻击动作	攻击行为映射		攻击动作技术分析
①通过横向移动利用漏洞攻击9台SAA业务服务器	发现	网络嗅探	对内部网络结构进行扫描探测收集相关信息；
	发现	扫描网络服务	通过使用ping命令和DS平台的扫描模块进行收集端口和服务信息；
	发现	发现网络共享	
	横向移动	利用远程服务漏洞	利用“永恒”系列漏洞攻击装备，对Windows全平台的SMBv1远程代码执行漏洞；
	提权	利用漏洞提权	
②植入持久化攻击装备到管理服务器中	命令与控制	利用常用端口	**利用“永恒”系列漏洞针对445端口进行漏洞利用；**
	命令与控制	使用标准加密协议	DS攻击平台使用的是标准的加密协议；
③通过植入的攻击装备进一步植入DanderSpritz后门进行远程控制。	防御规避	进程注入	DanderSpritz平台生成后门载荷投放并注入系统进程；
	执行	通过模块加载执行	使用DanderSpritz平台插件以模块内存加载执行；
	命令与控制	使用标准加密协议	DS攻击平台使用的是标准的加密协议；
	命令与控制	利用不常用端口	使用DS攻击平台反弹shell端口可自定义不太常用的端口；
	命令与控制	创建多级信道	**据有多种信道进行通信**；
	命令与控制	端口敲门	DS攻击平台监听端口会对数据包过滤符合的才会激活；
	凭证访问	凭证转储	通过DS攻击平台投放凭证转储插件；

攻击步骤4：通过管理服务攻击SAA服务器（2）



通过漏洞攻击并控制SAA业务服务器

被攻陷资产Tag

类型：服务器　**版本型号**：win2k8 SP2 x86

用途：Mgmt 管理服务器

被攻陷资产对象已有的防护措施

强密码 登录认证 | Symantec Endpoint Protection 11

对应攻击行为的防护措施分析

攻击动作	攻击行为映射		对应的防护措施分析
①通过横向移动利用漏洞攻击9台SAA业务服务器	发现	网络嗅探	多因子认证、加密、进程监控
	发现	扫描网络服务	Netflow记录、网络协议分析、数据包捕获、HIDS防护
	发现	发现网络共享	
	横向移动	利用远程服务漏洞	进程监控、进程命令行参数、windows 错误报告、网络协议分析、网络全要素、全流量记录、网络深包解析
	提权	利用漏洞提权	API 监控、DLL 监控、进程监控、windows 系统日志
②植入持久化攻击装备到管理服务器中	命令与控制	利用常用端口	进程监控、进程命令行参数、网络协议分析
	命令与控制	使用标准加密协议	网络协议分析、网络全要素、全流量记录
③通过植入的攻击装备进一步植入DanderSpritz后门进行远程控制。	防御规避	进程注入	API监控、Windows 注册表信息、文件监控、DLL监控
	执行	通过模块加载执行	进程监控、windows 系统日志
	命令与控制	使用标准加密协议	网络协议分析、网络全要素、全流量记录
	命令与控制	利用不常用端口	进程监控、进程命令行参数、网络协议分析、网络全要素、全流量记录、网络深包解析
	命令与控制	创建多级信道	Netflow记录、网络协议分析、网络设备日志采集与审计、网络全要素、全流量记录
	命令与控制	端口敲门	
	凭证访问	凭证转储	进程监控、 PowerShell日志、进程命令行参数

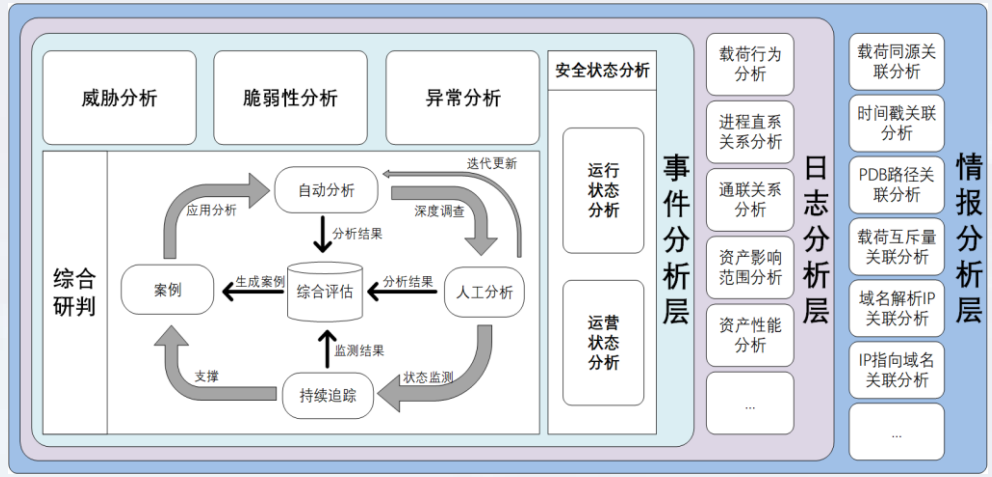
态势感知需要的数据支撑

ATT&CK中与**端点相关TTP占95%**以上，**网络相关占24%**，是最重要的两个数据源
有效的全面的采集、处理、理解、使用这些数据是态势感知成败的关键。

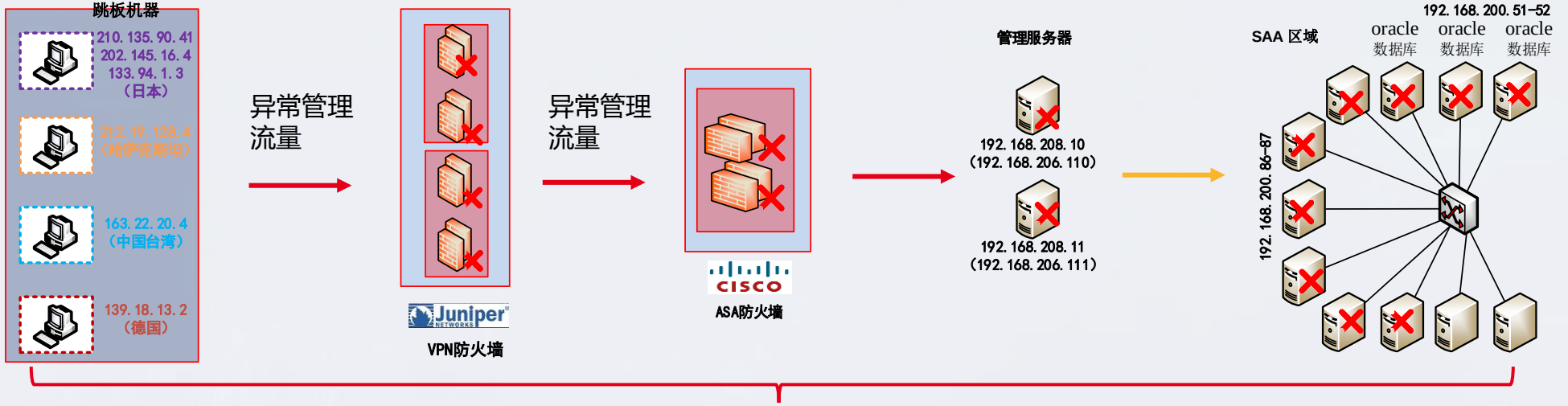
态势感知所需威胁发现能力

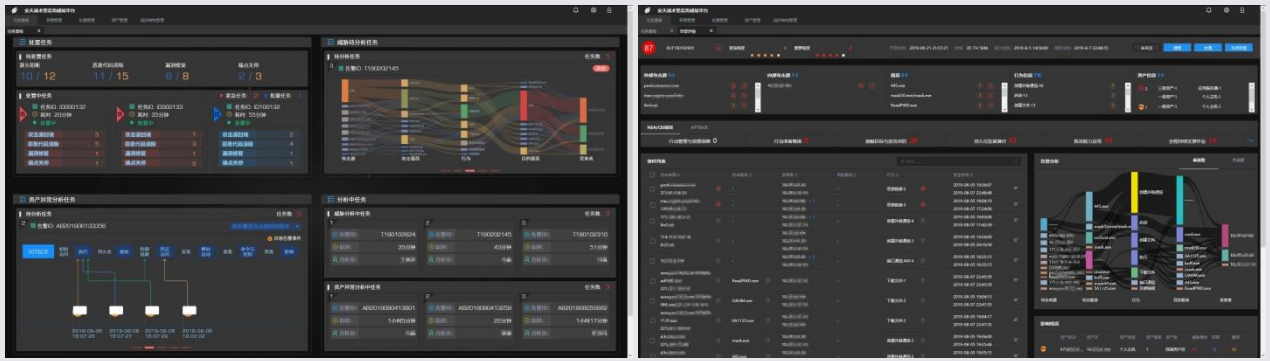
本次攻击使用了大量的0Day漏洞，态势感知需要具有异常分析和未知威胁发现能力。

攻击步骤	攻击手段	攻击装备	防护结果
攻击Juniper VPN防火墙	0day漏洞利用（身份认证漏洞：CVE-5-7755）	未知攻击装备A（漏洞攻击装备）、FEEDTROUGH（持久化）、ZESTYLEAK（后门）、BARGLEE（后门）	被控制，防护失效
攻击Cisco企业级防火墙	0day漏洞利用	PICBANANA（漏洞攻击装备）、EXTRABACON（漏洞攻击装备）、JETPLOW（持久化）SCREAMINGPLOW（持久化）、BANANAGLEE（后门）	被控制，防护失效
攻击两台管理服务器	0day漏洞利用	“永恒”系列的0Day漏洞攻击装备、DoublePulsar（Rootkit）、Darkpulsar（Rootkit）、未知攻击装备、(DanderSpritz平台生成的后门)	被控制，防护失效
攻击SAA业务服务器	0day漏洞利用	ETERNALROMANCE（永恒浪漫）、ENTERNALCHAMPION（永恒冠军）、ETERNALSYNERGY（永恒协作）ETERNALBLUE（永恒之蓝）	被控制，防护失效

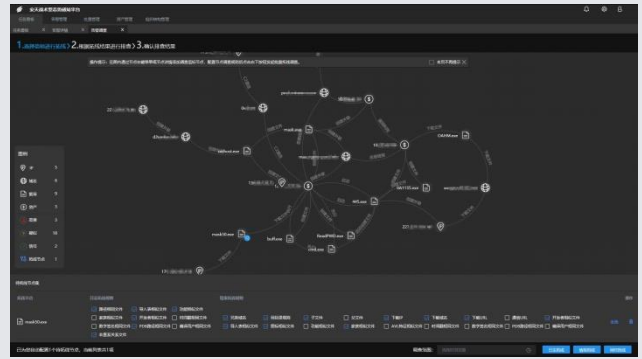


态势感知人机结合的分析能力，排查还原事件链





基于基线的异常自动分析



日志辅助人工分析

由SWIFT攻击事件引发的思考

- 高价值（政治、经济）目标，必然会受到以高能力攻击者为首发起大量持续的攻击
- 高能力对手有足够的方法绕过当前防御体系

攻击视角

防御视角

“敌已在内”是基础的敌情想定，防御方应充分考虑防御措施失效的情况，以**“面向失效的设计”**为基本原则指导防御。

具有**可管理性网络**是防御效果达成的基础支撑；例如合理的网络架构设计，资产信息、网络协议、通联关系等基础信息的记录和基准的建立是支撑上层态势感知异常行为分析的基础。

在合理网络结构上**叠加纵深布防的防御措施、监测措施**是限制、阻断、延缓攻击行动的有效方法，同时也为态势感知的综合分析提供安全日志和按需采集支撑，降低态势感知分析判定的成本代价，分析的数据量、提升判定的成功率；也为态势感知联动响应提供防御和处置手段；例如流量侧的全要素采集能力，端点侧的综合防护与检测响应能力等。

基于良好的基础结构安全能力与纵深防御能力，通过人机结合的安全分析以及威胁情报的利用，才能真正有效支撑态势感知指控积极防御，快速发现异常、支撑威胁猎杀和防御体系的持续优化。

防御体系的防御能力与持续的安全运营成正比，防御核心对象清晰的情况下，**实战化的安全运行**可以大幅提升防御能力。

02 动态综合防御体系

面向失效建设高对抗能力的防御体系

基于叠加演进模型构建动态综合网络安全防御体系

总体思路

以基础结构安全和纵深防御为主体的综合防御体系为基础，叠加动态的积极防御以应对高级复杂威胁，同时结合威胁情报缩短防御响应周期并提高针对性，构建动态综合网络安全防御体系。

- **综合发展**：从前到后逐步加强、逐步演化，且前面的层次要为后面的层次提供基础支撑条件。
- **深度结合**：将安全能力落实到信息系统的各个实现层组件，逐层展开防御，为及时发现和响应赢得时间。
- **全面覆盖**：将安全能力最大化覆盖信息系统的各个组成实体，避免因局部能力短板导致整体防御失效。
- **动态协同**：依托持续监测和自动响应能力，结合大数据分析、威胁情报、专家研判，实现积极防御。

基础结构安全体现

合理架构

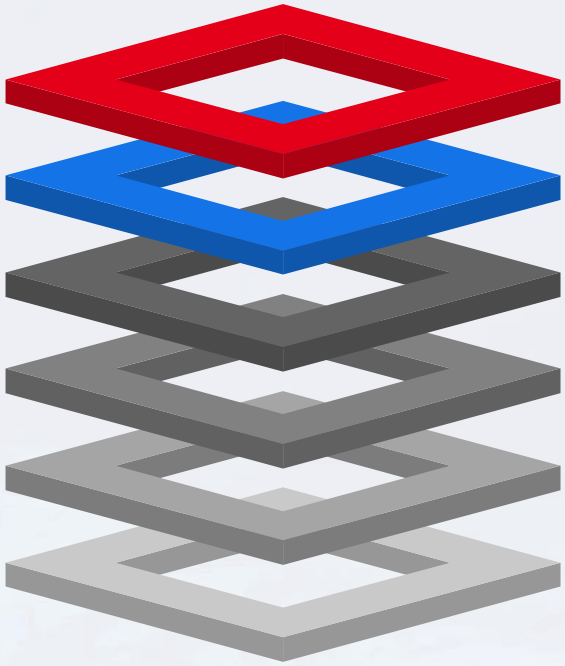
通过精心设计架构体系，不仅提高信息系统的可靠性，还有助于良好的网络分区 。

网络分区

通过良好的网络分区，特别是结合业务的功能内聚特性的网络分区，有利于实现有效的纵深防御机制。

应用内建安全

面向风险在应用系统中设计并实现内建的安全机制， 能够提高信息系统应对风险的抵抗力。



组件自身安全

通过在信息系统等IT架构组件中落实一系列安全要求， 能够提升安全防护能力并支撑其他更高成熟类别的安全机制。

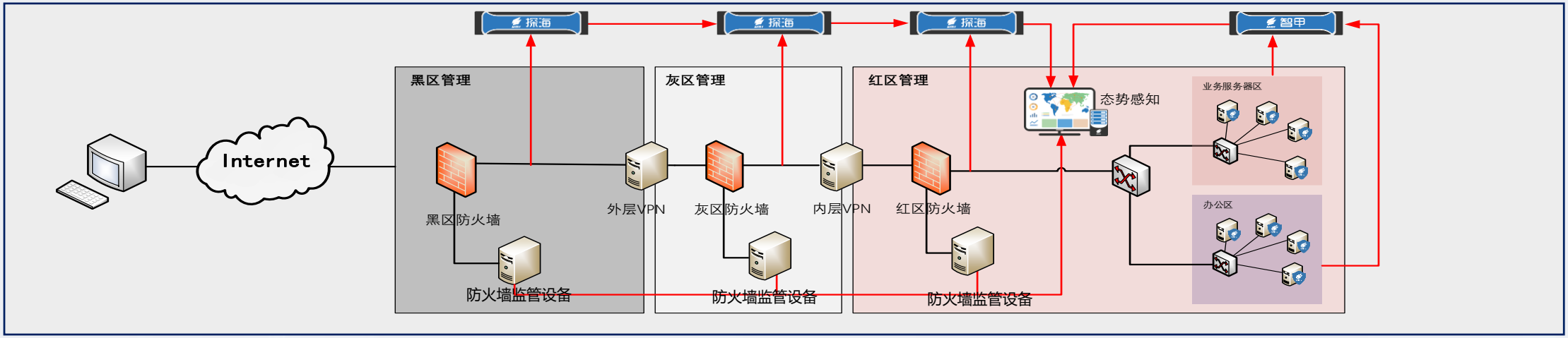
安全加固

通过实施操作系统安全加固和严格安全配置，提高IT架构组件的自我防护能力，同时增强防御纵深。

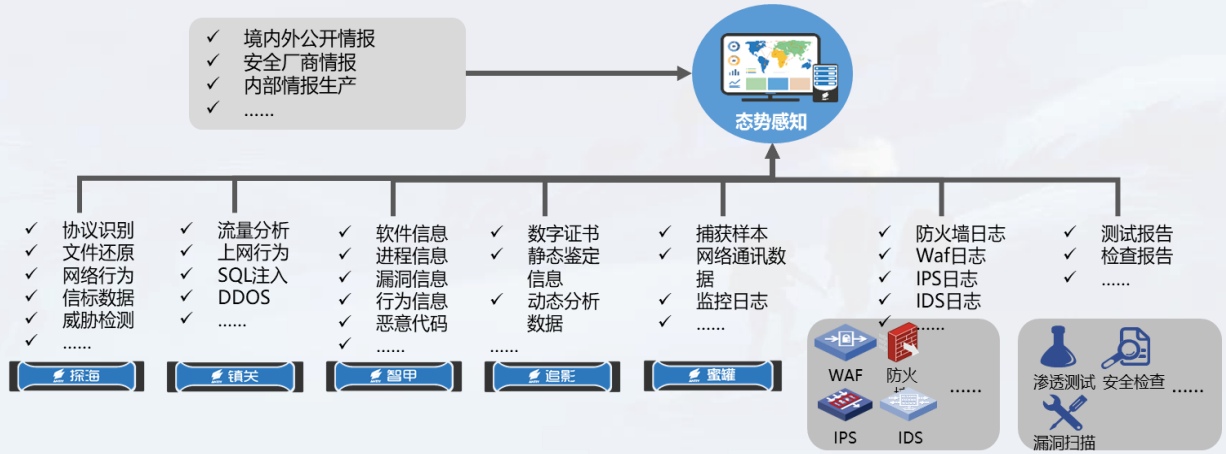
补丁管理

落实与标准化运维体系紧密结合的补丁管理工作，在确保系统正确、可靠运行的同时有效收缩IT架构的攻击面。

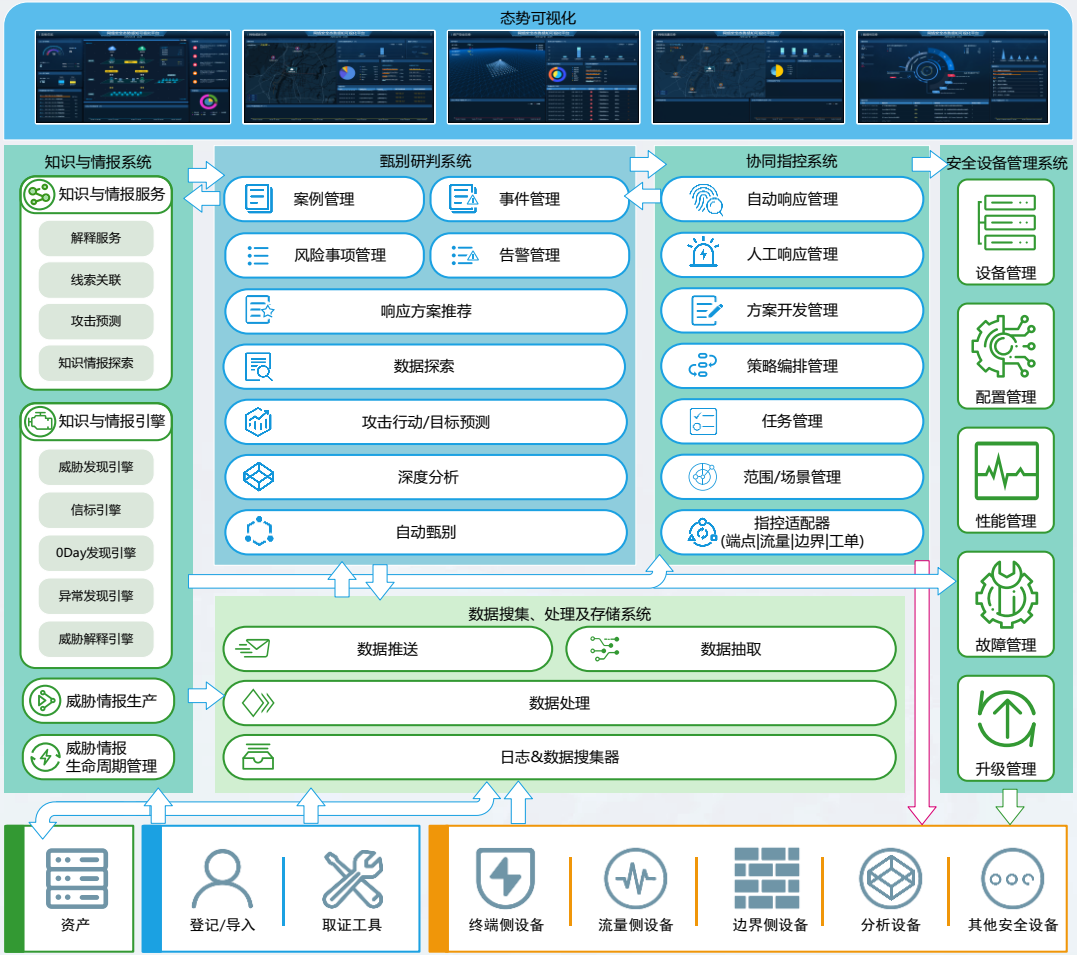
全面覆盖协同联动的纵深防御



智甲终端安全防御系统	探海威胁检测系统	威胁情报
端点数据采集能力	网络数据采集能力	威胁情报支撑能力
◘ 威胁事件采集	◘ 全要素采集	◘ 情报采集与分析
◘ 异常行为采集	◘ 数据预处理	◘ 威胁识别
◘ 环境信息采集	◘ 情报触发按需采集	◘ 漏洞识别
端点响应与防御能力		◘ 威胁关联分析
◘ 端点响应能力		◘ 知识库支撑
◘ 端点防御能力		



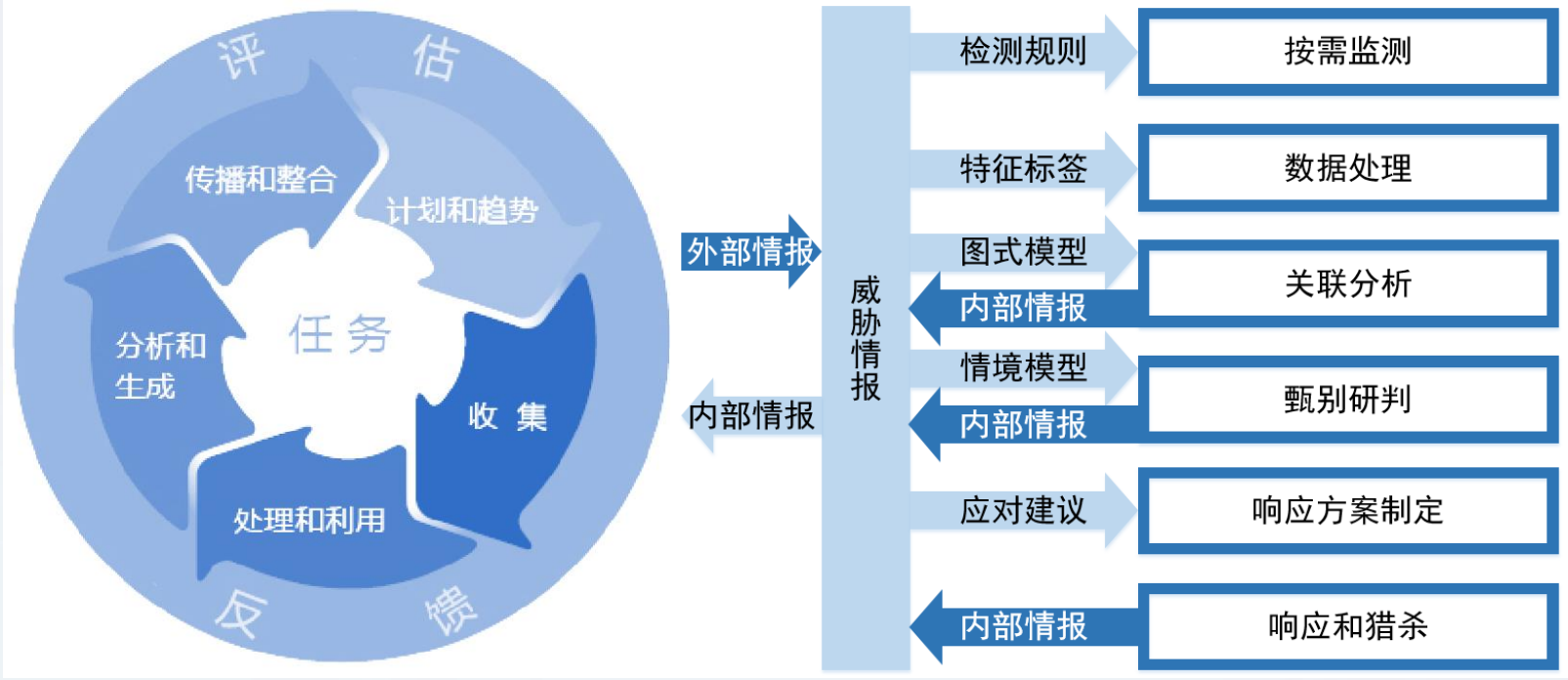
战术型态势感知与积极防御



- 全面持续监测及发现威胁
- 自动化的甄别威胁
- 高效的理解和分析威胁
- 有效的遏制和缓解威胁
- 集约化的资产安全运维
- 持续性的防御体系评估和优化
- 更多价值

多源威胁情报应用与私有化内部情报生产

基于安全研究知识与威胁深度检测能力，将外部获取到多源威胁情报通过整理分析进而转化成向量特征和应对措施，达到加固基础防御、强化威胁甄别研判能力、支撑协同响应指控、指导内部威胁猎杀等效果。基于自动分析、内部取证、威胁猎杀等过程生产内部威胁情报，赋能私有化威胁发现能力，实现对威胁的持续追踪，从而持续提升威胁对抗能力。



谢谢大家