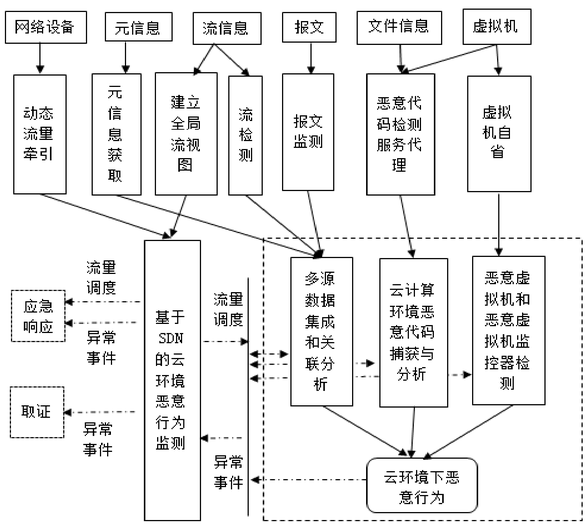
云计算环境下的恶意行为检测、响应与取证平台

丁丽萍 赵粮 刘文懋 裘晓峰 方华 杨卫军 刘斌 季昕华 等
dingliping@gz.iscas.ac.cn

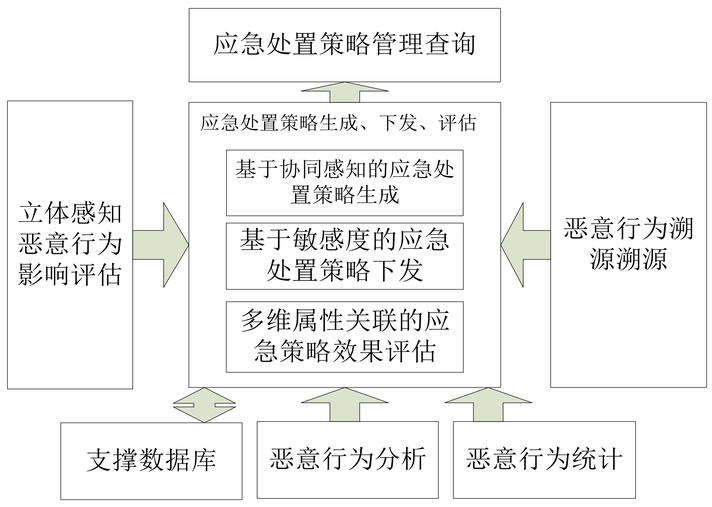
系统简介：针对目前云计算环境中存在的恶意行为难以检测，恶意行为的应急响应和溯源不及时、不到位以及违法证据难以提取和保全等问题，研究面向云环境的恶意行为监测技术、追溯技术、虚拟机自省技术和取证技术，形成云环境下的恶意行为检测系统，恶意行为应急处置与溯源系统和云基础设施服务平台取证系统，为云服务提供者、用户提供一个相对安全、可靠的云环境，为针对云环境的违法犯罪行为提供具有可采用性的电子证据。

云环境下恶意行为检测系统



✓对网络设备进行动态流量牵引，对网络中的流信息建立全局流视图
✓快速检测异常流，并通过网络控制器牵引流量到安全设备
✓对于元信息、流信息和报文进行多源数据集成和关联分析
✓对于云环境下的文件信息和虚拟机通过建立恶意代码检测服务代理进行恶意代码的捕获和分析
✓对于虚拟机通过虚拟机自省技术进行恶意虚拟机和虚拟机监控器检测
✓基于检测出的恶意行为，调度云环境下的取证系统和应急响应系统

云环境下恶意行为应急处置与溯源系统

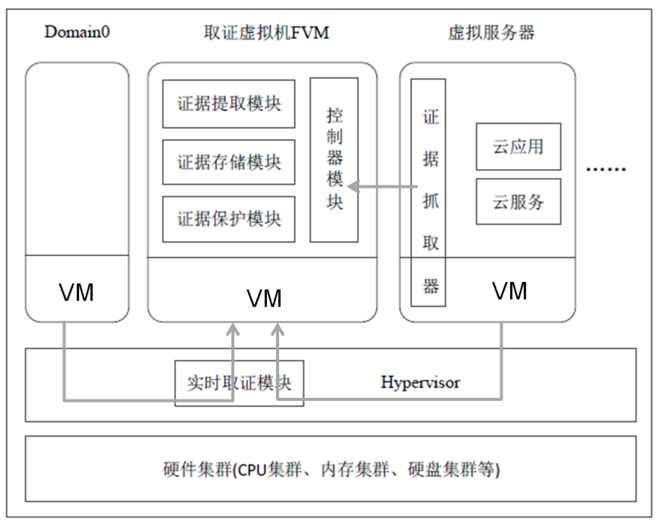


✓获取相关检测数据，对数据进行汇总分析，分析恶意行为类型、分析恶意行为影响、定位恶意行为源头

✓定位恶意行为传播或感染拓扑的关键节点和路径，并针对每个恶意行为自身特性，选择对应的策略进行下发

✓对当前实施的安全策略和历史安全策略进行对比分析，并建立安全策略数据库，提供策略存储、更新和显示等功能

云基础设施服务平台取证系统

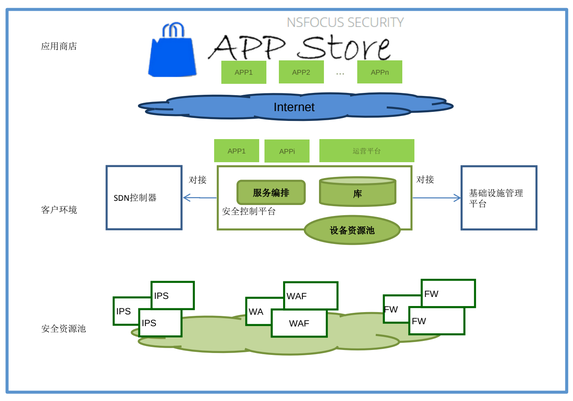


✓证据采集器根据预先设置的规则实时地采集该虚拟服务器中的证据数据，并将这些数据传输到证据仓库FVM中

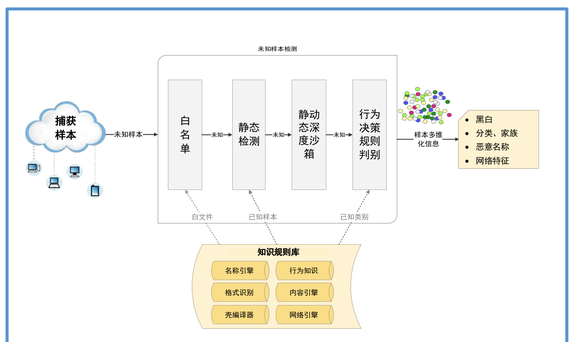
✓实时取证模块根据预先设置的规则获取特定虚拟机实例的实时证据，并将这些数据传输到证据仓库FVM中

✓FVM保存及分析收集到的证据数据，其中证据保护模块主要负责保护证据数据；证据存储模块主要负责将证据数据存储到虚拟磁盘中；证据提取模块提供证据查询接口，供调查人员使用；控制器模块负责整个框架的协作

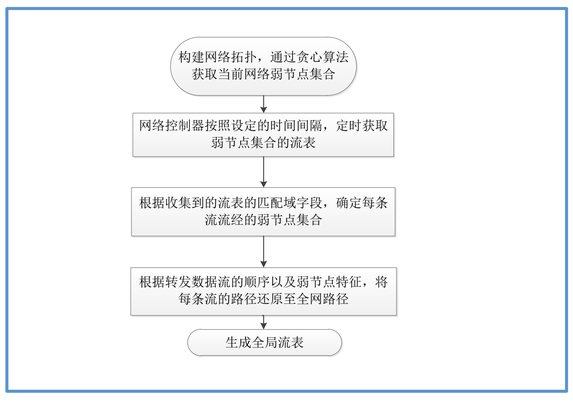
关键技术



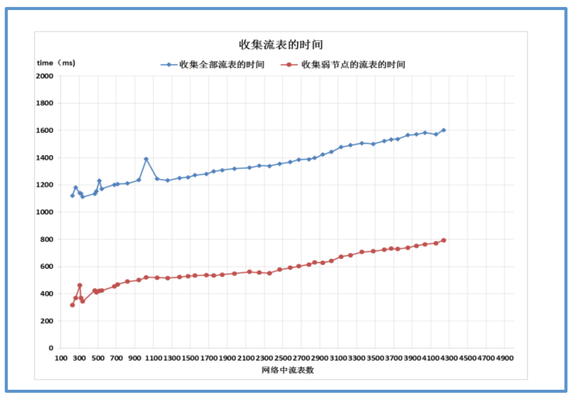
基于SDN的云环境恶意行为检测架构



云环境威胁分析检测技术路线

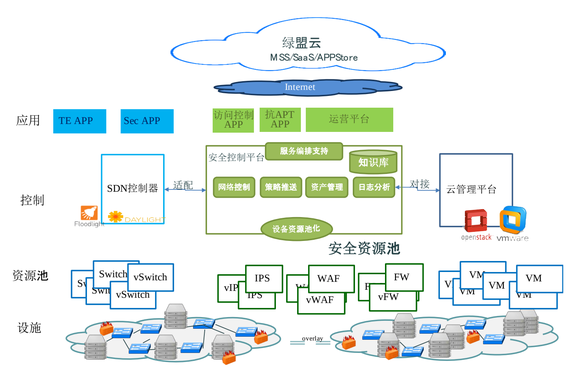


基于弱节点覆盖的全局流算法流程图

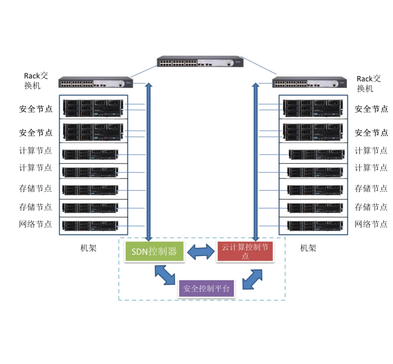


收集流表时间随流表数变化对比图

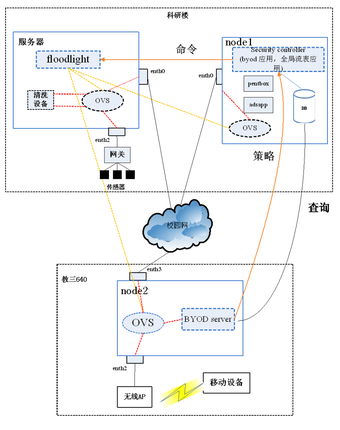
应用情况



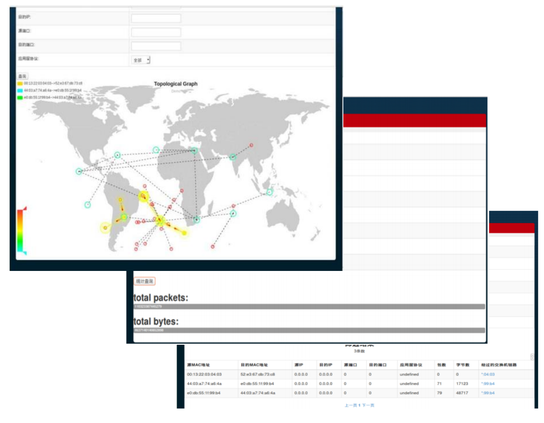
绿盟云应用场景



绿盟安全设备部署图



北邮校园网应用场景



流检索、统计、路径可视化应用视图