2021-2022学年春季学期

网络空间安全态势感知

CyberSecuritySituationalAwareness

授课团队：刘宝旭，卢志刚，刘玉岭

助　　教：李　宁

网络空间安全态势感知

CyberSecuritySituationalAwareness

[第18次课]网络空间安全态势感知 --爱因斯坦计划

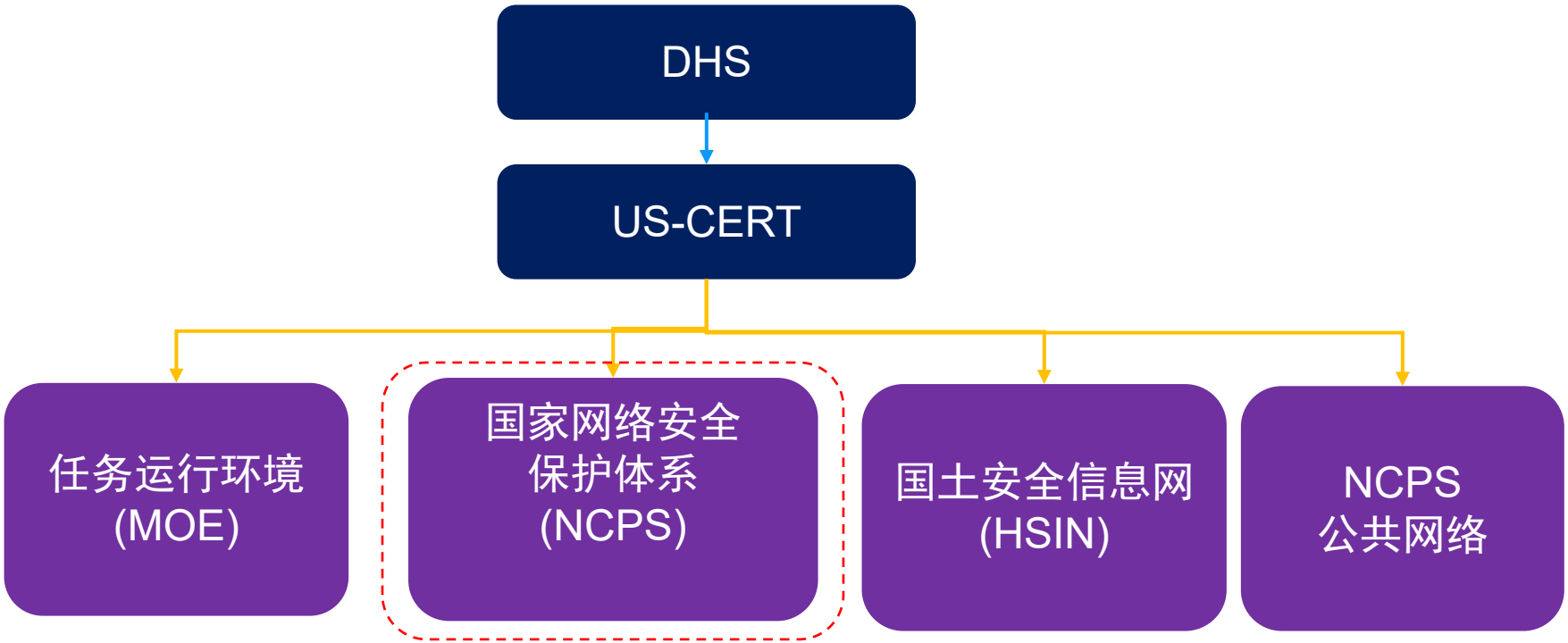
授课教师：卢志刚

授课时间：2021年5月13日

概要

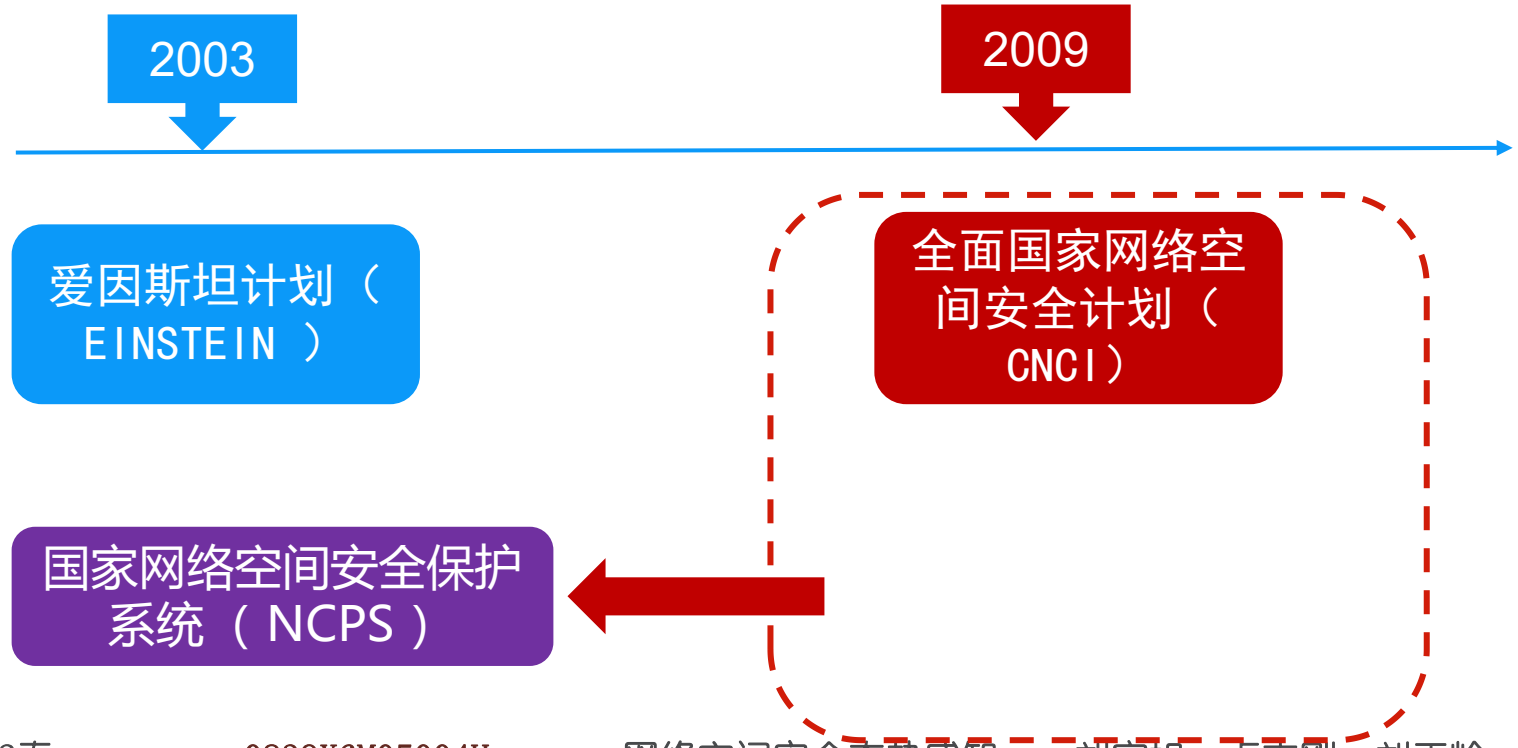
项目背景

- “爱因斯坦”计划是美国联邦政府主导的一个网络安全自动监测项目，由国土安全部（DHS）下属的美国计算机应急响应小组（US-CERT）开发，用于监测针对政府网络的入侵行为，保护政府网络系统安全
- US-CERT共启动四个项目，NCPS是其中之一



项目背景

- 爱因斯坦计划（EINSTEIN）于2003年启动
- 在2009年美国政府启动了CNCI（全面国家网络空间安全计划）
- 爱因斯坦计划并入CNCI，并改名为NCPS（国家网络空间安全保护系统），但依然称为爱因斯坦计划



项目概要

概述

该计划是一个政府主导，各商业机构参与的国家级大项目，并在法律上由美国政府签署和投资，美国国家安全局全面执行的跨度大、项目众多的国家计划

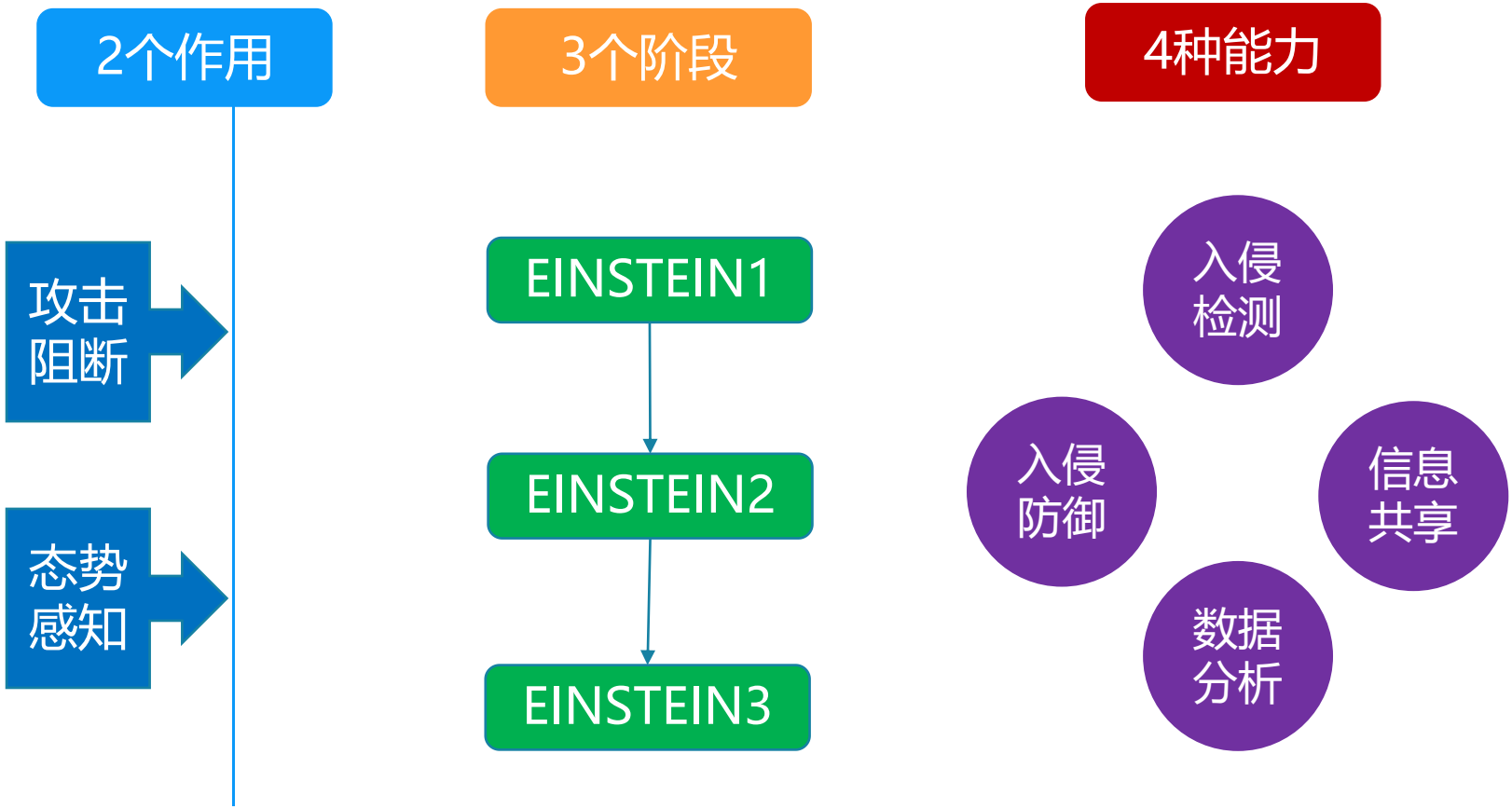
目的

把美国联邦机构各自的互联网出口数据汇集并分析、感知，获取整个联邦政府的安全态势，提高相互之间的信息共享、信息安全的协同

阶段

爱因斯坦计划包括1、2、3，分别启动于2003、2008、2010年

项目概要


2个作用
3个阶段
4种能力
攻击
阻断
态势
感知
EINSTEIN1
EINSTEIN2
EINSTEIN3
入侵
检测
入侵
防御
信息
共享
数据
分析

项目概要

代号	部署时间	目标	描述
EINSTEIN 1	2003	入侵检测	通过在政府机构的互联网出口部署传感器，形成一套自动化采集、关联和分析传感器抓取的网络流量信息的流程
EINSTEIN 2	2009	入侵检测	对联邦政府机构互联网连接进行监测，跟预置的特定已知恶意行为的签名进行比对，一般匹配上就向US-CERT发出告警
E^3A	2010	入侵检测 入侵防御	自动地对进出联邦政府机构的恶意流量进行阻断，这是依靠ISP来实现的。ISP部署了入侵防御和基于威胁的决策判定机制，并使用DHS开发的恶意网络行为指示器（Indicator）来进行恶意行为识别

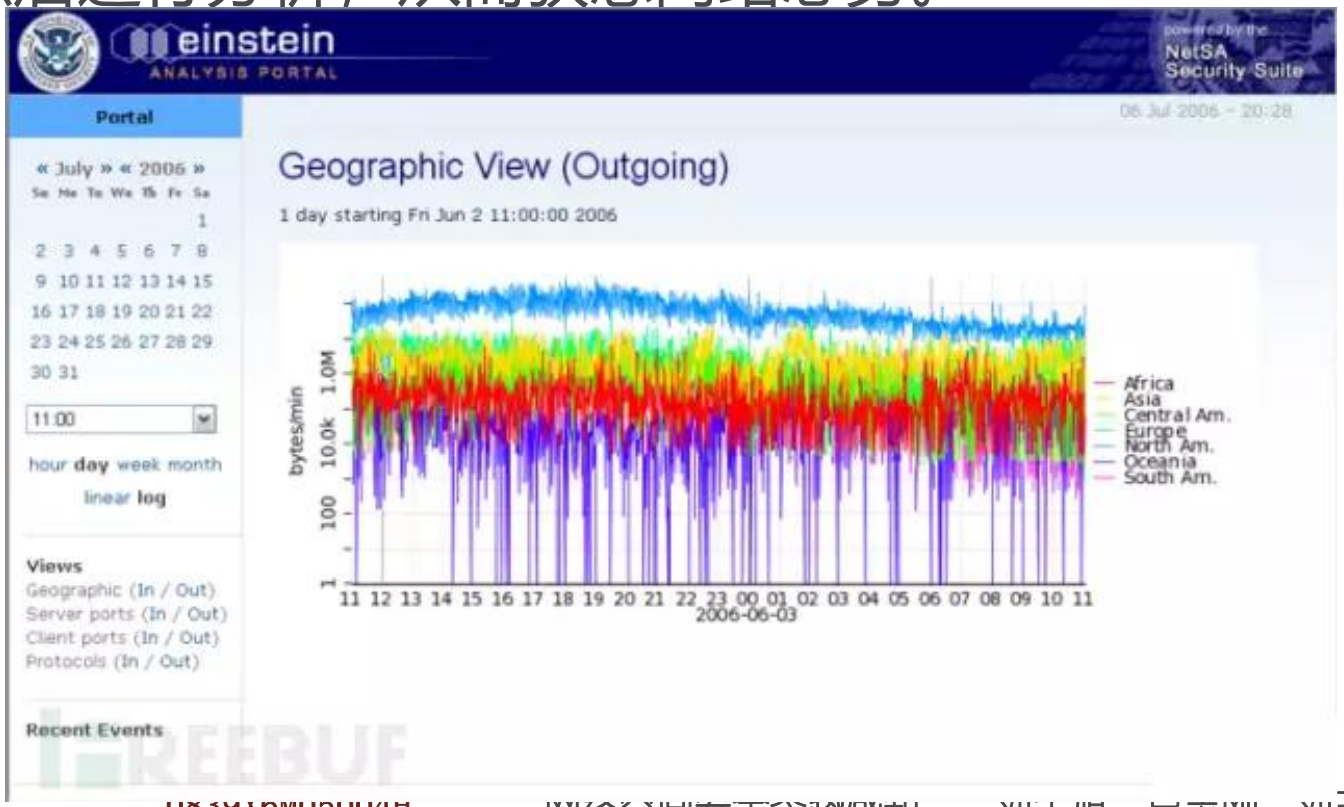
概要

EINSTEIN1 介绍

- 通过收集参与该计划的联邦政府机构的信息，US-CERT能够建立和增强对美国网络空间态势感知的能力，以更好的响应网络威胁与攻击
  - 蠕虫检测：可以形成一幅跨政府部门的蠕虫攻击图
  - 异常行为检测：通过跨政府部门的带内和带外的异常行为分析，能够更加全面的分析异常行为，并对其它部门提供预警信息和攻击线索
  - 配置管理建议：通过爱因斯坦计划，US-CERT能够为联邦政府机构提供更有价值的配置管理建议
  - 趋势分析：帮助联邦政府从整体上了解政府网络的健康度

EINSTEIN1 介绍

- 爱因斯坦1的技术本质是基于流量的分析技术（DFI深度流检测）来进行异常行为的检测与总体趋势分析
- US-CERT通过采集各个联邦政府机构的这些Flow信息，然后进行分析，从而获悉网络态势。

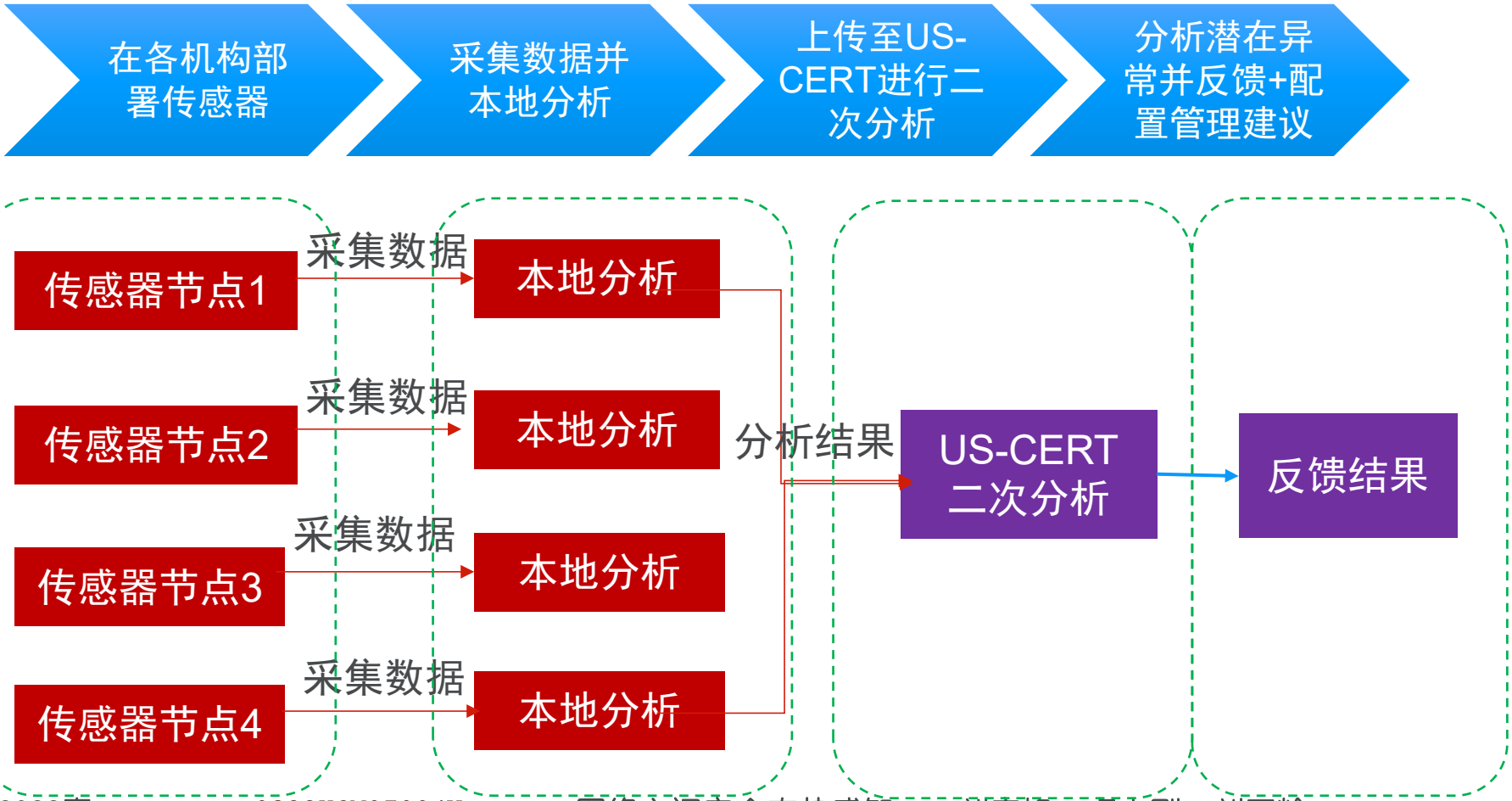


EINSTEIN1 介绍

- 爱因斯坦1通过采集Flow信息，获得的数据包括以下几个部分：

- 1）ASN自治域号；
- 2）ICMP类型/代号；
- 3）流字节长度；
- 4）TCP/IP协议类型；
- 5）传感器编号：整个系统将在参与的联邦政府机构的网络中部署Flow采集传感器；
- 6）传感器状态；
- 7）源IP地址（IPv4）；
- 8）目的IP地址（IPv4）；
- 9）源端口；
- 10）目的端口；
- 11）TCP标志位信息；
- 12）时间戳；
- 13）持续时间

系统工作流程

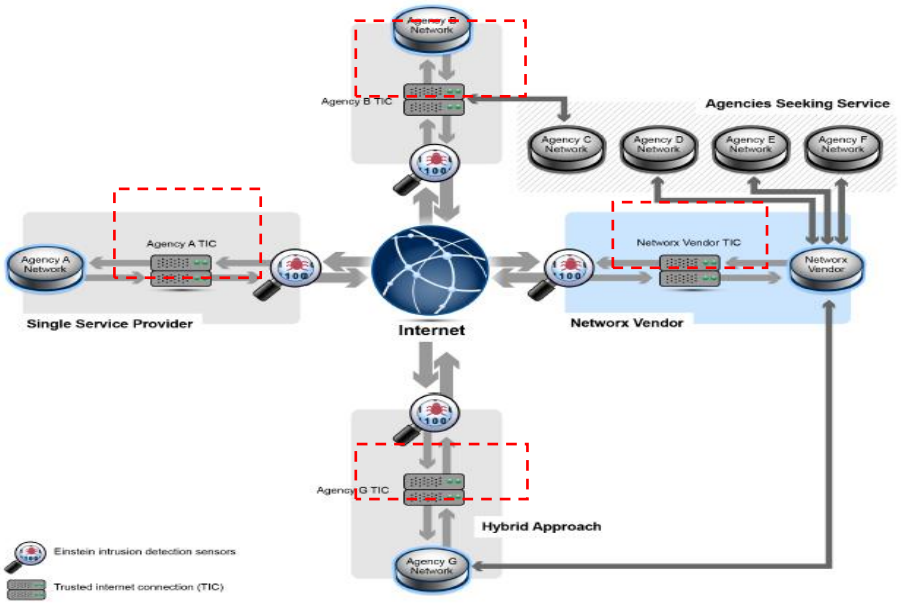

在各机构部署传感器
采集数据并本地分析
上传至US-CERT进行二次分析
分析潜在异常并反馈+配置管理建议
传感器节点1
采集数据
本地分析
传感器节点2
采集数据
本地分析
分析结果
US-CERT二次分析
反馈结果
传感器节点3
采集数据
本地分析
传感器节点4
采集数据
本地分析

概要

- 爱因斯坦2计划是爱因斯坦1计划的增强，进一步分解为三个阶段

EINSTEIN2 介绍——Block 2.0

- 核心工作是在电子政务网络的边界部署IDS，并且这项工作与TIC（“电子政务互联网收口计划”）同步进行。
- IDS传感器部署在联邦机构的互联网出口处（IAP，Internet Access Point），并且最终就是TIC计划中的那些统一互联网出口



EINSTEIN2 介绍——Block 2.0

- 目标：收集整个联邦政府的网络流量，提升对网络事件的检测、阻止和通知能力
- 增强功能：
  - 包捕获技术
  - 恶意代码分析中心
  - 增强的分析中心
  - 突发事件管理系统
  - 网络空间指标体系库（CIR）
  - 网络空间指标分析平台（CIAP）
  - 与CyberScope集成
  - 建立US CERT的公共网站
  - 建立US CERT的HSIN门户

EINSTEIN2 介绍——Block 2.1

- 核心工作：
  - ✓核心是搭建SIEM（Security Information and Event Management）系统，实现SIEM能力来归一化和关联不同数据源的事件
  - ✓建立具有聚合和增强能力的数据存储机制
  - ✓多数据源关联技术
  - ✓可视化技术
- 数据来源
  - ✓NETFlow数据
  - ✓NETFlow数据标签
  - ✓IDS告警
  - ✓外部情报
  - ✓CERT的各种黑白名单

EINSTEIN2 介绍——Block 2.2

- 核心工作：
  - ✓ 各类网络空间安全信息的共享与协作（ISCE）
  - ✓ 基于搜索技术的网络调查分析追踪能力
- 项目指标
  - ✓ 项目的各参与方能够在30分钟内分享到任何一方检测并确认的网络空间安全事件的数据和相关信息。

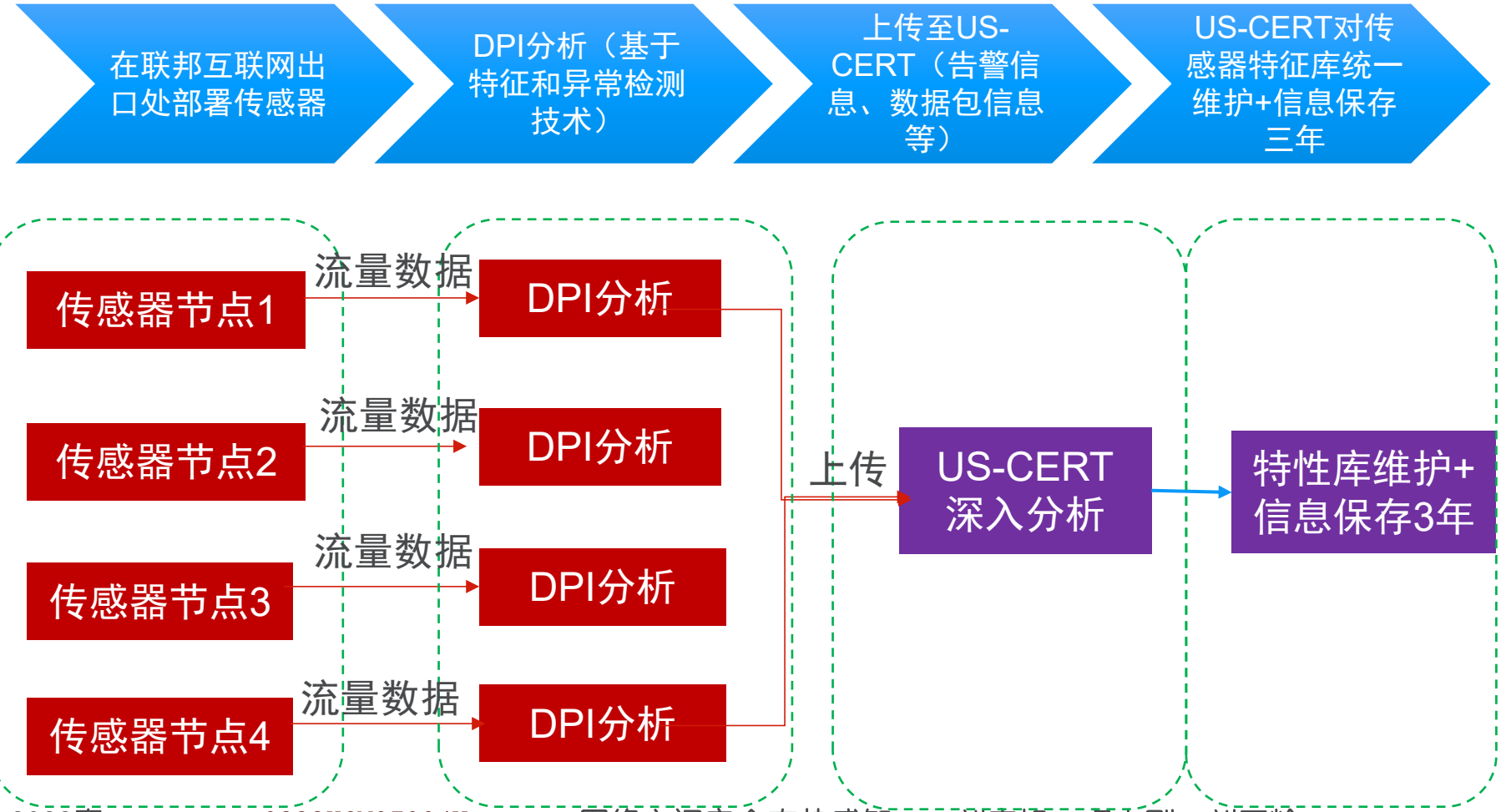
EINSTEIN2 介绍

- 爱因斯坦2计划的技术本质是IDS技术，它对TCP/IP通讯的数据包进行DPI分析，来发现恶意行为（攻击和入侵）
- 爱因斯坦2通过DPI，获得的数据包包括以下几个部分

```
127.0.0.1|192.168.0.20|52119|25|6|10|600|S|2008/04/28T00:02:47.958|44.9
85|2008/04/28T00:03:32.943|SENSOR1|out| S|
sIP|dIP|sPort|dPort|protocol|packets|bytes|flags|sTime|dur|eTime|sensor
|type|initialFlags|
```

- 1） 源IP：sIP；
- 2） 目的IP：dIP；
- 3） 源端口：sPort；
- 4） 目的端口：dPort；
- 5） 协议类型：protocol
- 6） 包数量：packets，通过传感器计算出来的一次连接的包数量；
- 7） 字节数：bytes；
- 8） 连接开始时间：sTime；
- 9） 连接持续时间：dur；
- 10） 连接结束时间：eTime；
- 11） 传感器编号；
- 12） 数据流方向：type
- 等

系统工作流程


在联邦互联网出口处部署传感器
DPI分析（基于特征和异常检测技术）
上传至US-CERT（告警信息、数据包信息等）
US-CERT对传感器特征库统一维护+信息保存三年
传感器节点1
传感器节点2
传感器节点3
传感器节点4
流量数据
流量数据
流量数据
流量数据
DPI分析
DPI分析
DPI分析
DPI分析
上传
US-CERT 深入分析
特性库维护+信息保存3年

概要

EINSTEIN3 介绍

- 爱因斯坦3计划：美国DHS(国土安全部)称其为下一代爱因斯坦计划。(目前披露的信息甚少)
  - 在进入爱因斯坦3之前，DHS在2010年进行了一个名为“第三阶段演练”的先导性项目，用于进行可行性论证和试点。
  - 根据 “第三阶段演练”项目，可以得知，爱因斯坦3计划的主要技术支撑是IPS。
  - 该IPS技术是由NSA（国家安全局）主导开发出来的，代号为Tutelage（已经用于保护军方网络），主要是一套识别特定攻击的特征库（Signature）

EINSTEIN3 介绍——基本信息

二者融合

TIC（可信互联网连接）计划

爱因斯坦计划

→ 为联邦政府网络基础设施提供保障

NSA(国家安全局)

DoD(国防部)

→ 明确加入爱因斯坦3计划

商业技术

NSA的技术

→ 对政府机构网络出入流量全包检测（FPI）+基于威胁的决策分析

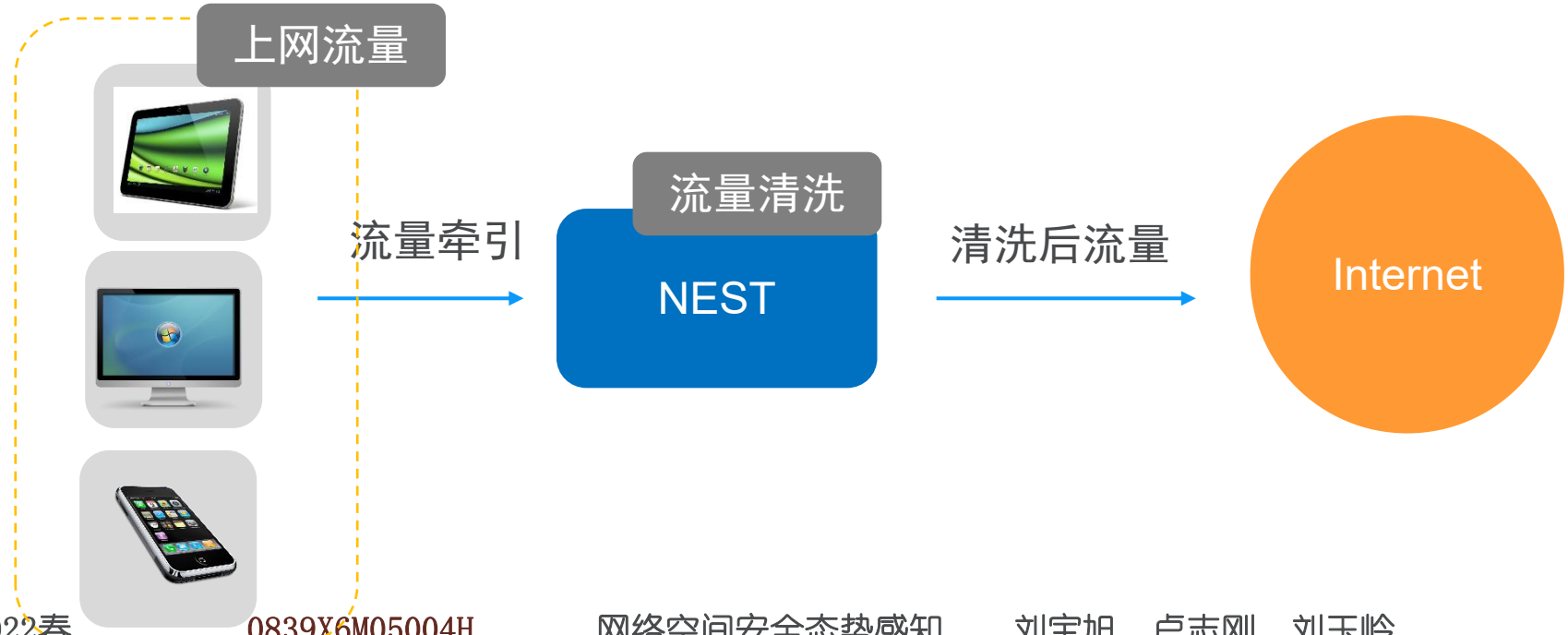
在电信运营商处部署传感器，能够在攻击进入政府网络之前就进行分析和阻断

EINSTEIN3 介绍

- 总体目标：
  - 识别并标记恶意网络传输，主要解决的问题是网络空间威胁
    - 钓鱼攻击
    - IP欺骗
    - 僵尸网络
    - DDoS
    - 中间人攻击
    - 恶意代码插入攻击等

EINSTEIN3 介绍 — —创新之处

- 在分析端，亮点在于加入了IPS技术，还有实时FPI全包分析技术
- 由于入侵防御能力是部署在签约的ISP那里，因此，在那些ISP里面部署了一个称作“Nest”的保密设施。
- “Nest”负责将政府机构上网的流量牵引到其中，进行检测和阻断，然后再将清洗后的流量送回互联网



EINSTEIN3 介绍 — —技术实现

- 恶意流量阻断
  - 自动地对进出联邦政府机构的恶意流量进行阻断，这是依靠ISP来实现的
- DNS阻断
  - 也就是DNS Sinkhole技术，用于阻止已经被植入政府网络的恶意代码与外部的恶意域名之间的通讯
- 电子邮件过滤
  - 使得DHS能够在网络上对所有发给政府网络用户的邮件进行扫描，能够识别含有恶意代码的附件、恶意URL等，将其过滤掉，并可以转发到特定位置，以供分析人员进一步检测

概要

爱因斯坦项目动态——各方观点

- 2016 年1月，美国审计署（GAO，General Accounting Office）提交的一份报告《DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System》称该系统仅“部分达标”，提出了严厉的批评

入侵检测能力	仅支持基于签名的检测方法，尚不支持基于异常和状态的检测方法，而且数据类型目前也有限，无法检测加密网络流量、邮件、文件传输中的攻击。
入侵防御能力	NCPS（爱因斯坦3）部署的入侵防御能力具备近实时的的入侵阻断功能，但无法仅针对某些协议流量进行细粒度阻断
信息共享能力	NCPS（爱因斯坦3）的信息共享能力还处于手工和无序的状态

爱因斯坦项目动态——各方观点

- 针对美国审计署的指责，DHS（国土安全部）新闻办公室在2016年1月30日发表声明，在声明中DHS部长Jeh C. Johnson指出：
  - 价值：
    - 审计署在报告中承认了爱因斯坦系统的显著效益，爱因斯坦事实上已被证明是在发现重大事故上是非常有价值的
    - 一年以前，EINSTEIN 3A仅仅保护20%的政府网络，现在实际保护了50%，而且有能力保护整个政府网络，其已经阻断了超过70万次网络威胁
    - 国会授权所有联邦机构在2016年年底前采用该系统
  - 缺陷：
    - 当前版本的EINSTEIN只阻止已知网络威胁，但是DHS会研发新的技术以发现未知攻击

爱因斯坦项目动态——最新动态

- 目前现状——部署

部署数量

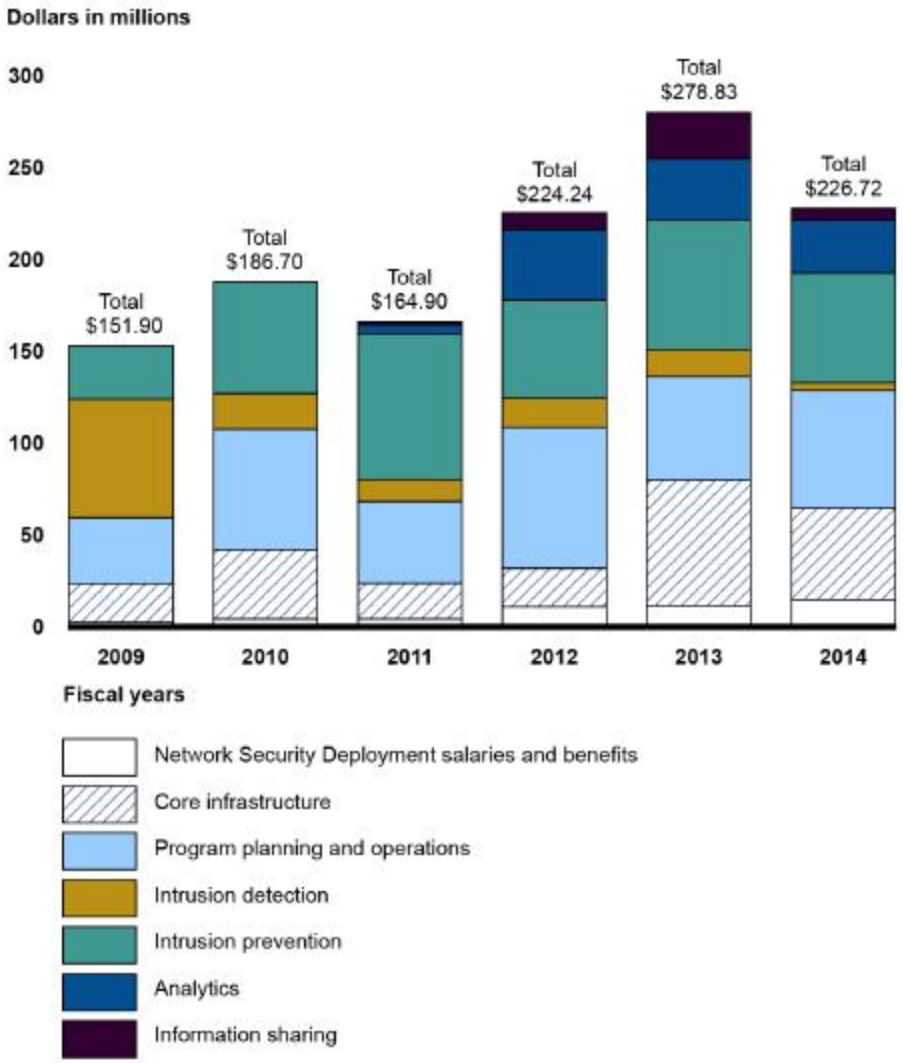
NCPS(爱因斯坦3)项目已经在.gov政府网络出口部署了229台入侵检测传感器

规则状态

部署了超过9000条入侵检测特征，其中大约2300条处于全天候激活状态

爱因斯坦项目动态——最新动态

- 美国“爱因斯坦”计划迄今已经历时17年
- 截至2014财年，DHS（国土安全部）已经花费了超过12亿美元在NCPS项目之上



爱因斯坦项目动态——后续发展

- 尽管存在非议，然后美国政府仍然支持该计划，这表现在2016年2月美国总统奥巴马发布的《网络安全国家行动计划》，
- “计划”中指出将要拓展“爱因斯坦”项目，总统的 2017年预算中支持所有联邦民事机构都具备记录、分析网络流量并针对政府网络信息进行入侵检测的能力。

Q&A