# 缩写

|  |  |  |
| --- | --- | --- |
| 缩写 | 全称 | 描述 |
| APT | Advanced Persistent Threat | 高级持久性威胁 |
| ATT&CK | Adversarial Tactics, Techniques, and Common Knowledge | 对抗性的战术、技术和常识 |
| C&C | Command and Control |  |
| CTI | Cyber threat intelligence | 网络威胁情报 |
| CVSS | Common Vulnerability Scoring System | 常见的漏洞评分系统 |
| DARPA | Defense Advanced Research Projects Agency | 国防高等研究计划署 |
| ETW | Event Tracing for Windows | 窗口的事件跟踪 |
| GPM | Graph Pattern Matching | 图形模式匹配 |
| HSG | High-level Scenario Graphs | 高级方案图 |
| IDS | Intrusion Detection System | 入侵检测系统 |
| IOC | Indicator of compromise | 折衷指标 |
| IPS | Intrusion Prevention System | 入侵预防系统 |
| LoC | Lines of Code | 代码行数 |
| PLC | Programmable Logic Controller | 可编程序逻辑控制器 |
| RAT | Remote Administration Tool | 远程管理工具 |
| SIEM | Security Information and Event Management | 安全信息和事件管理 |
| TC | Transparent Computing Project (by DARPA) | 透明计算项目(由DARPA提供) |
| TTP | Tactics, Techniques, and Procedures | 战术、技术和程序 |

# 概述

## 基本概念

### provenance graphs

通过Audit logs生成provenance graphs（溯源图），再根据溯源图进行以下安全行为：

* APT detection 高效持久威胁
* attack scenario reconstruction 攻击场景重建
* cyber threat-hunting 网络威胁探测

### tag-based approach

用于识别subjects, objects and events

### high-level scenario graphs

高级场景图，大概是对当前活动（campaigns）的总结图

### graph pattern matching problem

图匹配问题，把cyber threat-hunting转化为图匹配问题，而这个图匹配，就是query graph（查询图，源自CTI，网络威胁情报）和provenance graph（溯源图，源自内核Audit Logs）。

## 主要研究内容

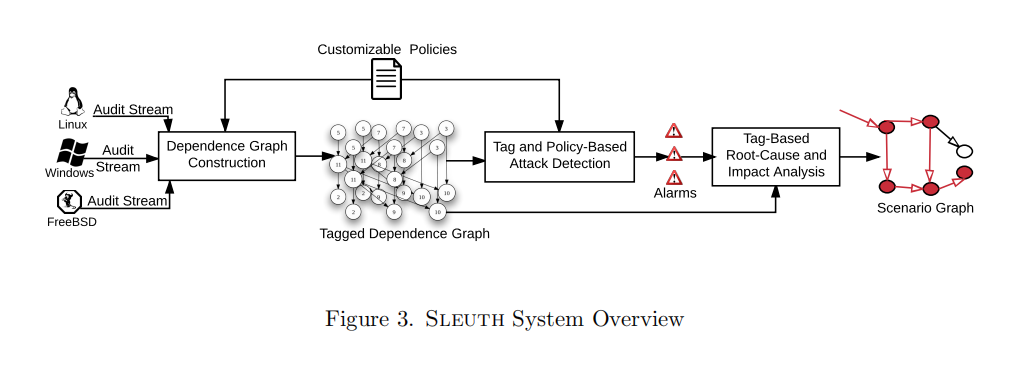
Sleuth，通过内核审计日志构建图（provenance graph？），以实现及时攻击场景重建。

Holmes，在APT检测中，把一堆不可靠告警，转化为强的检测信号。

Poirot，搜索分析溯源图，揭示攻击活动。

# SLEUTH：基于COTS审计数据的实时攻击场景重构

## overview



来自不同操作系统的审计数据被处理成平台独立的图，这个图是攻击检测、关联分析和场景重构的基础。

SLETTH亮点就是全自动，有以下contribution：

1. 将依赖图（紧凑的）存储在内存中，使效率高效。
2. 使用tag-based方法描述Subject、Object和Event。
3. 新的算法，进行root-cause identifification and impact analysis，这里包含backward analysis和forward search算法
4. 可定制的策略框架
5. 提供实验评估（experimental evaluation），更快、更高效、更低的误报率。

## 主存依赖图

图作为数据结构存储依赖关系，一种可行的方法是使用图数据库，例如Neo4J、Titan, 但是除非内存足够大，否则这些数据库在运行许多图算法时会受到限制，而本文提出了一种更省内存的依赖图设计。

图的构成为实体（entity，对应图数据库中的顶点）和事件（event，对应图数据库中的边,）,其中：

实体包含Subject和Objects两种：

1. Subjects

进程，属性值包括：process id（pid）、命令行、所有者（owner）以及代码和数据的标签

1. Objects

实体，例如文件、pipes、网络连接。属性值包括：名称、类型（文件、pipe、socket等）、所有者和标签

事件，用于subjects和objects之间或者两个subjects之间用read､connect､execve来表示。

## 标签和攻击检测

使用标签来评估objects和subjects的trustworthiness和sensitivity。主要是从以下3个方面：

1. 起源：object和subject直接祖先的标记。
2. 系统先验知识：就是对一些应用程序的预了解。
3. 行为：观察sujects行为，并与预期行为比较。