Grid-wide Intrusion Detection

Stuart Kenny*, Brian Coghlan
Dept. of Computer Science
Trinity College Dublin

27th Oct. 2005

Introduction

- **Goal**
  - "To provide the Grid-Ireland OpsCentre with an overall picture of the state of security of the entire Grid-Ireland infrastructure at any time"
    - Starting with intrusion detection
- **Difficulties for Grid**
  - Infrastructure spans multiple networks
  - Don't know about state of security at other sites
  - Similar infrastructure at sites, i.e. OS, services
  - Speed of response depends on speed of access to information
- **Grid-Ireland approach**
  - Develop Grid-wide intrusion detection system
    - Instrument all sites to detect attempted security intrusions
    - All security alerts generated at sites to be visible at OpsCentre

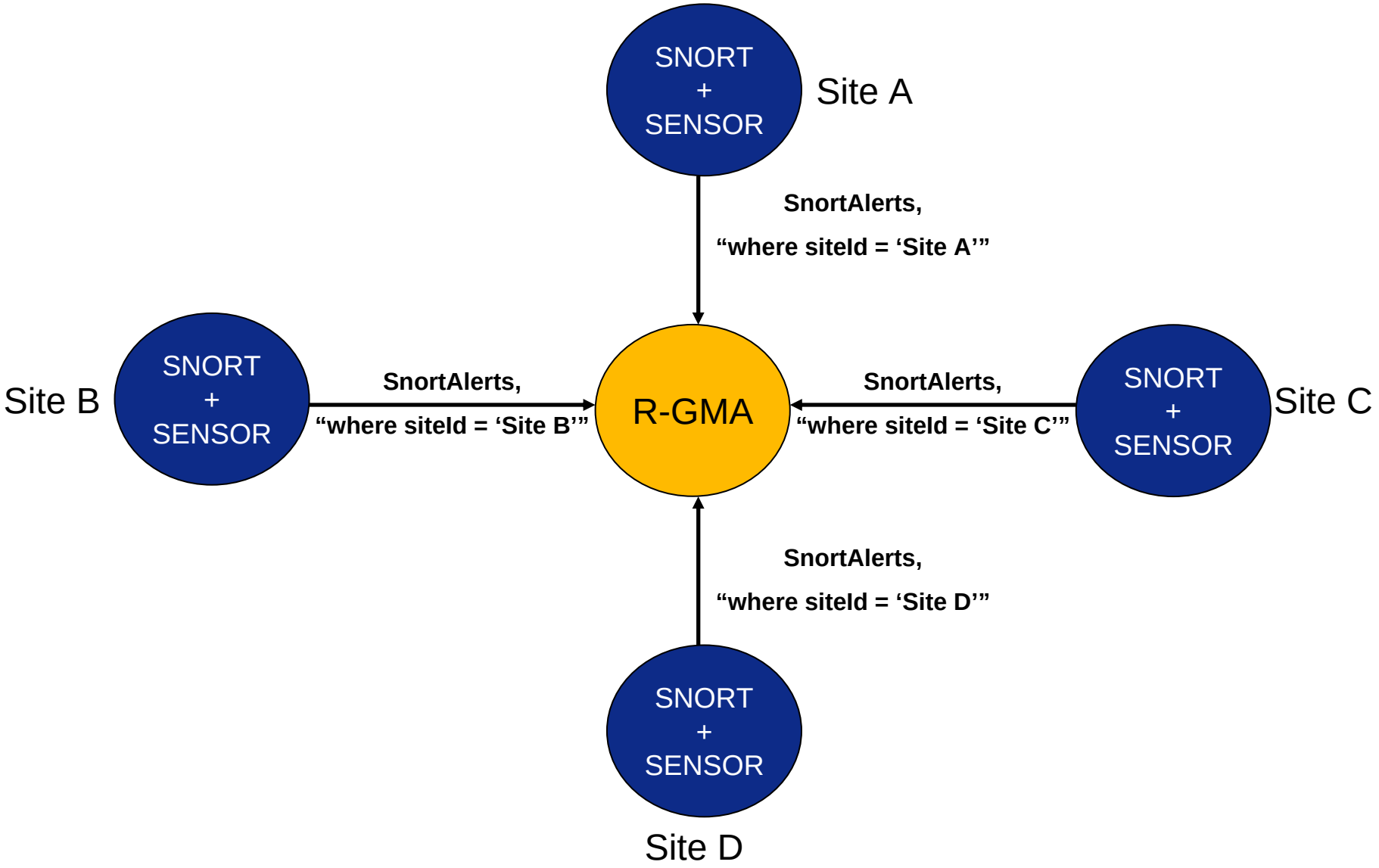
Grid-wide Intrusion Detection

- **System building blocks:**
  - Snort
    - Open-source network intrusion detection system
  - CrossGrid NetTracer
    - System for accessing log files through Grid InfoSys
    - Supports Tcpdump and Snort
  - R-GMA
    - Relational grid monitoring and information system

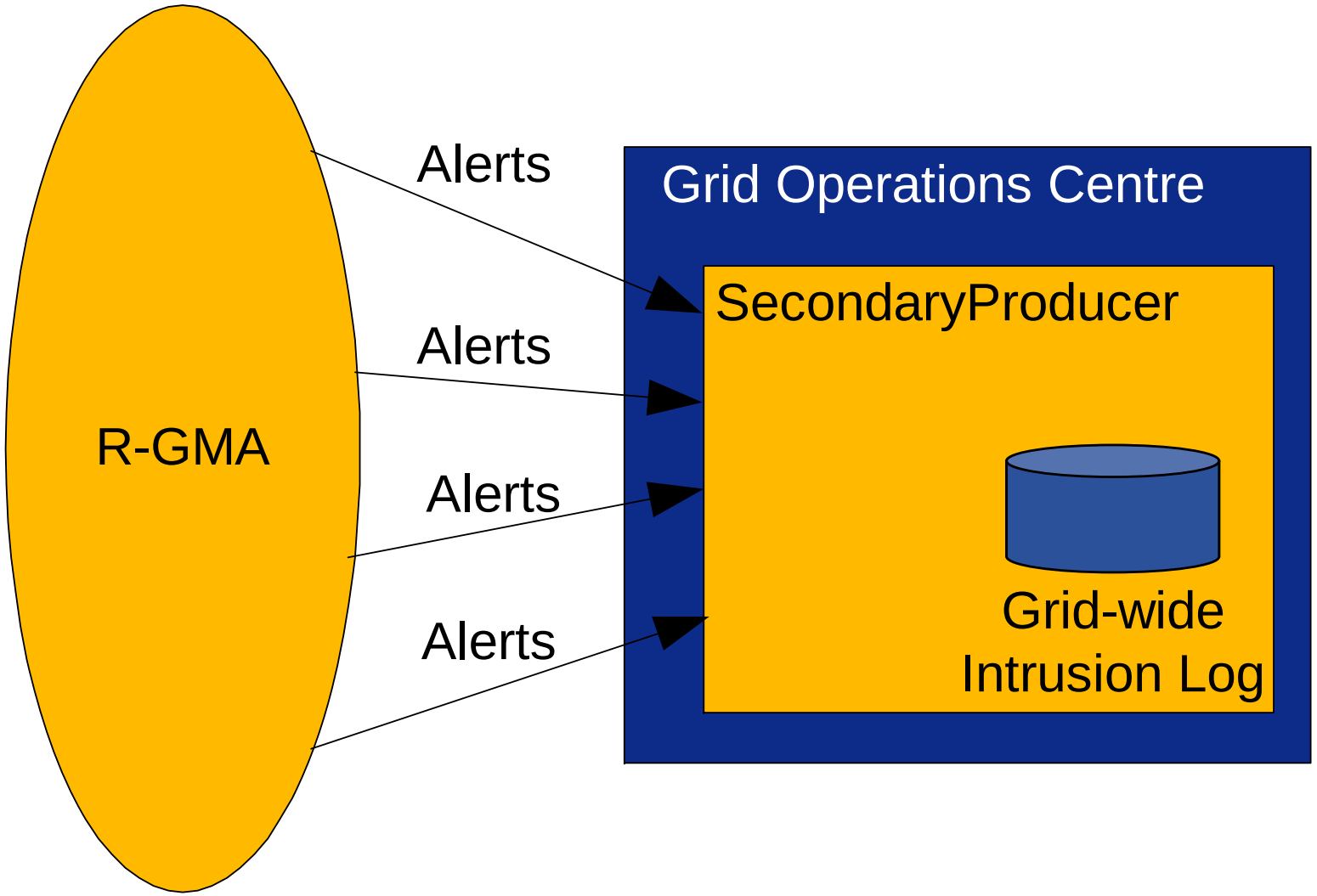
Grid-wide Intrusion Detection

- **System comprised of two levels:**
  1. Alert aggregation
     - Snort + NetTracer Sensor
       - *Snort: generates alerts for suspect packets*
       - *NetTracer: streams alerts to R-GMA*
     - R-GMA Secondary Producer
       - *Collects alerts to central 'Grid-wide intrusion log'*

Alert Aggregation



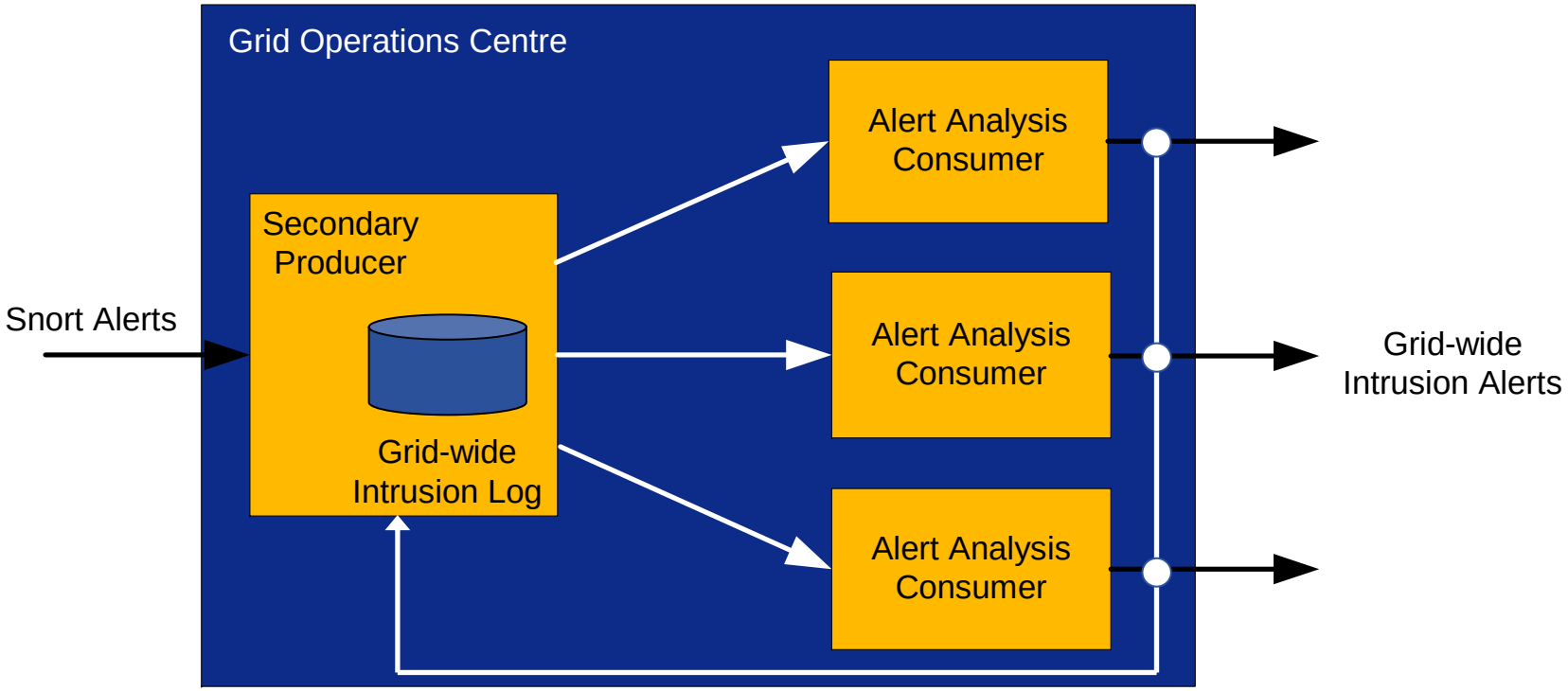
Alert Aggregation



Alert Analysis

- **System comprised of two levels:**
  1. Alert aggregation
     - Snort + NetTracer sensor
       - *Snort: generates alerts for suspect packets*
       - *NetTracer: streams alerts to R-GMA*
     - R-GMA Secondary Producer
       - *Collects alerts to central 'Grid-wide intrusion log'*
  2. Alert analysis
     - Custom R-GMA consumers
       - *Currently 3 different kinds*
     - Detect attempted attack on grid infrastructure
     - Generate 'Grid-alert'

Alert Analysis



Example Analyser

- **Detect scanning of Grid infrastructure**
- **Consumer filters log for portscan alerts**

```
Consumer alert = consumerFactory.createConsumer(timeInterval,
                                                "SELECT * FROM snortAlerts
                                                WHERE generator_id=122",
                                                QueryProperties.CONTINUOUS);
```

- **If multiple sites scanned by single source**
  - Grid infrastructure portscan ‘grid-alert’
  - Alert generated:
    - email
    - published to R-GMA

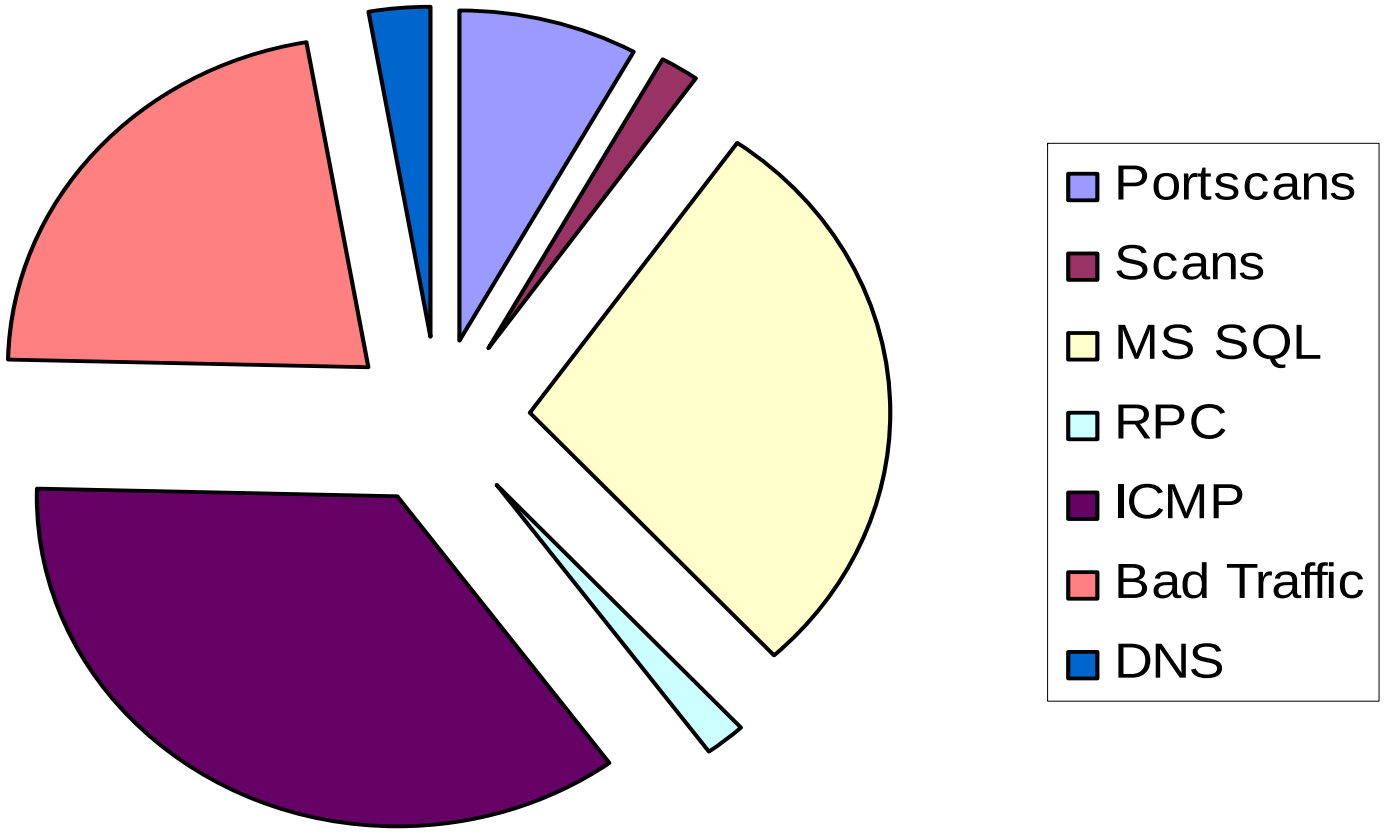
Example Analyser

Grid Alert: Grid Infrastructure Portscan

From: <root@cagraidsvr17.cs.tcd.ie>
To: stuart.kenny@cs.tcd.ie
Date: Yesterday 00:26:05

[**] 08/04-00:26:05.244 Grid Infrastructure Portscan [**]
Source: 59.44.51.80 (59.44.51.80)
Site: giULie
08/04-00:17:56.418485 (portscan) TCP Portscan gridmon.grid.ul.ie (193.1.96.134)
Site: giRCSIie
08/04-00:26:04.005235 (portscan) TCP Portscan gridmon.rcsi.ie (193.1.229.24)
Site: giAITie
08/04-00:13:41.395764 (portscan) TCP Portscan 192.168.32.154
(192.168.32.154)

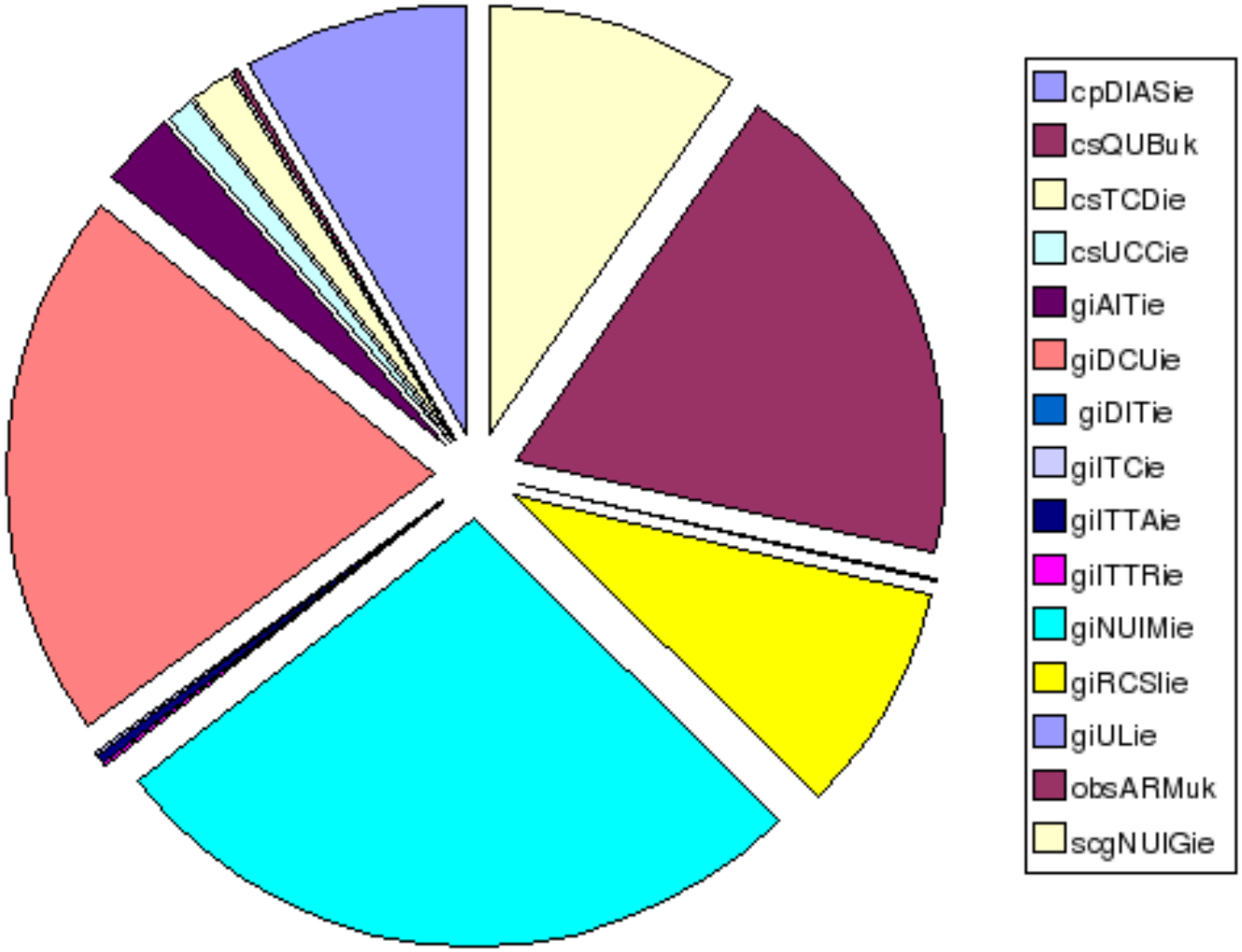
Sample Results



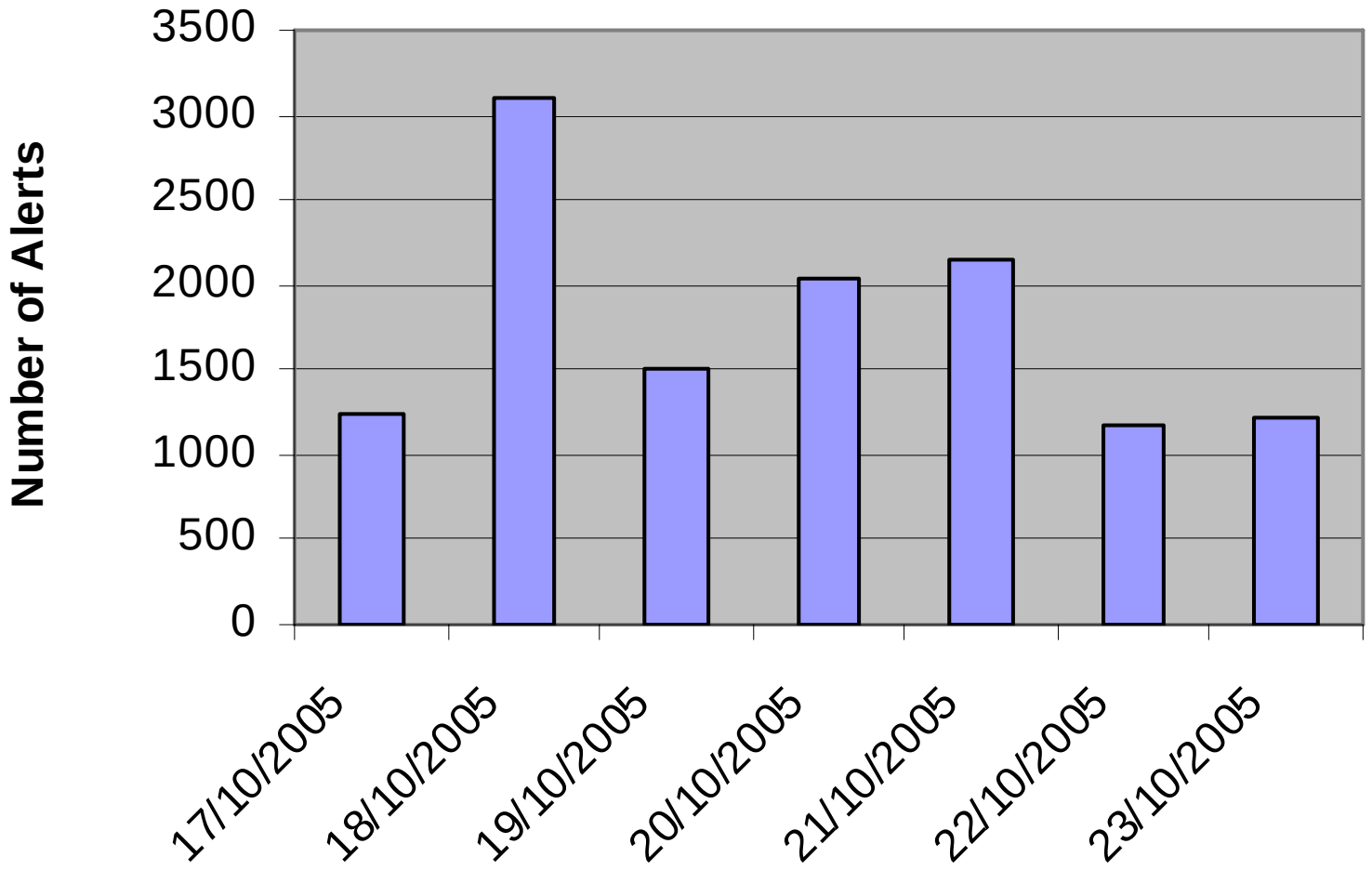
First 4 week period: 25,378

Current Total: 194,390 (16 weeks)

Sample Results



Sample Results



Deployment

- **Deployment**
  - Site
    - R-GMA MON box
    - Snort
    - NetTracer, 2 components:
      - *Sensor – must be co-located with Snort*
      - *QueryEngine – requires the R-GMA API*
  - GOC
    - Intrusion log secondary producer
    - Intrusion log analysers
- **Configuration**
  - Manual
    - configuration script
  - Automatic
    - LCFG component
    - Quattor component (to be tested)
    - YAIM will be provided

Future Work

- **Customise Snort rules for Grid**
  - Based on:
    - Site configurations
    - Host types
    - Services
- **Incorporate additional security components**
  - Tripwire
  - Bro
- **Attack detection**
  - New intrusion log analysers
    - Bayesian
    - AI/Category Theory
- **Active response**
  - Automated responses to detected attacks

The End

- **Any Questions?**

- **Email:**
  - stuart.kenny@cs.tcd.ie