

E S I S S

emMAN  
East Midlands Metropolitan Area Network

# JANET CSIRT Conference

22<sup>nd</sup> October 2009

# Matthew Cook

- ▶ Network and Security Manager for Loughborough University
- ▶ Managing ESISS initiative
- ▶ JANET Contracted Trainer
- ▶ Author of multiple Technical Guides/courses
- ▶ Invited speaker over 50 events in 10 years
- ▶ Personally discovered vulnerabilities in: HP Insight Manager, ExLibris Aleph/MetaLib and Cisco AnyConnect VPN/ASA platform



# Agenda

- ▶ History
- ▶ Service Drivers
- ▶ Service Portfolio
- ▶ Network Based Anomaly Detection
- ▶ Infrastructure Health Check
- ▶ Reputational Monitoring
- ▶ Example Feedback Received

# History

- ▶ Shared Services concept
- ▶ HEFCE expressions of interest
- ▶ Response by Richard Smeeton
- ▶ Feasibility Study [October 2007 – May 2008]
  - ▶ Led by Tony Brookes
  - ▶ Collaboration between six East Midlands Universities
- ▶ HEFCE pump primed service
- ▶ Service delivery award to Loughborough University [April 2009]

# Service Drivers

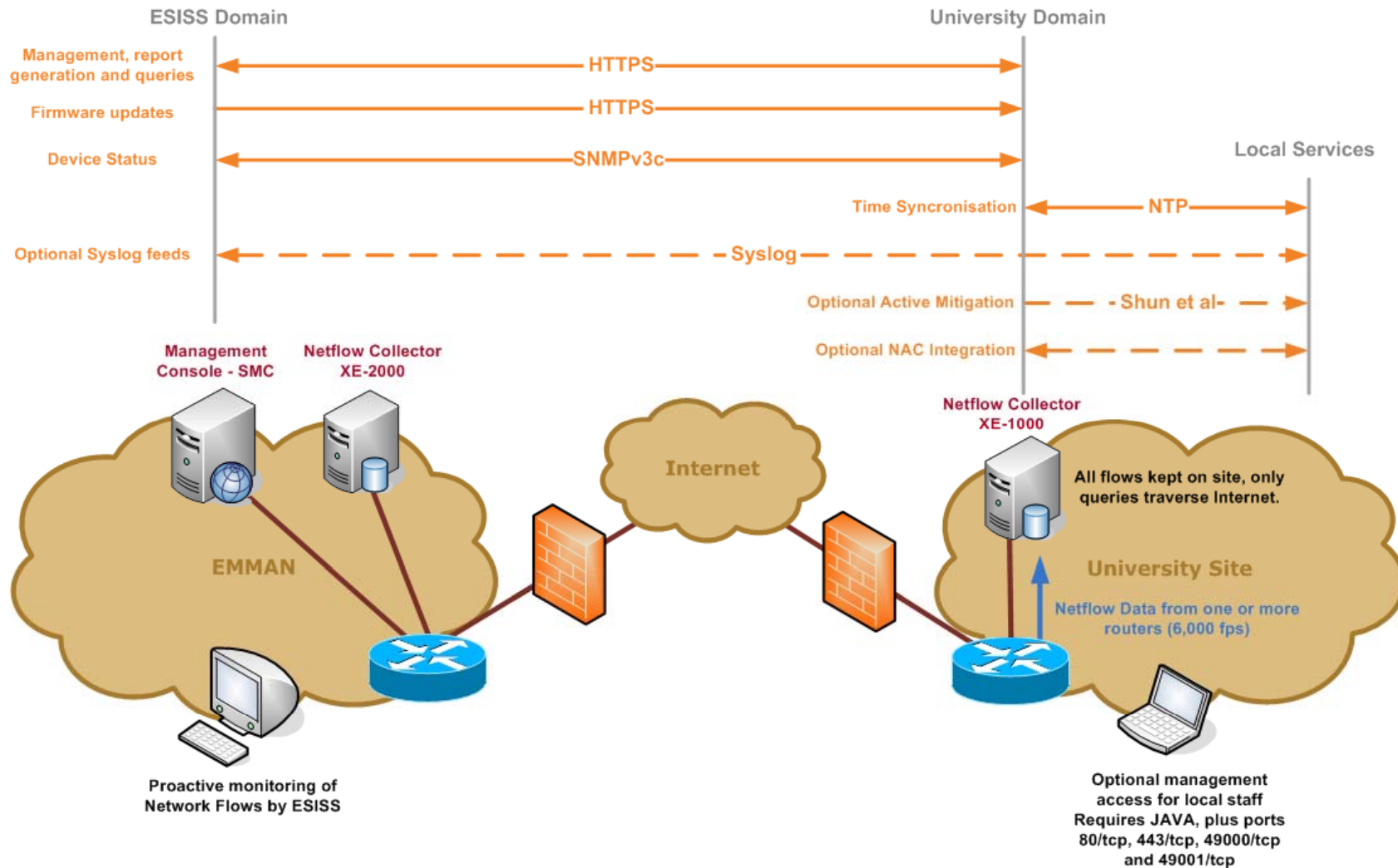
- ▶ Strong support from EMMAN community
- ▶ Individual requests from other academic institutions
- ▶ Feedback from JANET CSIRT events
- ▶ UCISA Directors 'Top Ten Concerns'
  
- ▶ Organisations are broadly facing the same challenges which do not provide distinct competitive advantage.

# Service Portfolio



# Network Based Anomaly Detection

## Campus Network Anomaly Detection Service [Per Site]



# Infrastructure Health Check


- ▶ Modular Infrastructure Health Check Service
- ▶ Starting from £500
- ▶ Penetration Testing
- ▶ Traffic Analysis/Profiling
- ▶ Networking Configuration
- ▶ Service Performance Resolution
- ▶ Security Device Configuration
- ▶ Information Security Policy Discussions
- ▶ Full day, report and briefing is £1,250.

# Reputational Monitoring

- ▶ THE: “University fails to use its own language guidelines in its publications.”
- ▶ Pinsent Mason: “Domain hijacking/squatting”
- ▶ Guardian: “University hosting illegal DVDs”
- ▶ Twitter: “I’ve failed to do any work today, due to network outages!”
  
- ▶ Internet based reputational is critical

# Reputational Monitoring from ESISS

Organisation: Loughborough University

Overall Health Indicator: 

## Test Mechanism Summary

| Test Mechanism  | Description  | Weight | Most Recent Score | Last Update         |
|---|--|--------|-------------------|---------------------|
| Home Page Search<br><a href="#">[edit parameters]</a>       | Checking the name "Loughborough University" against home page URL <a href="#">More info...</a> | 0.9    | 1                 | 2009-09-09 02:34:02 |
| Webcam Finder<br><a href="#">[edit parameters]</a>          | Network visible webcams <a href="#">More info...</a>   | 1.0    | 1                 | 2009-09-08 18:15:08 |
| Open Proxy Servers<br><a href="#">[edit parameters]</a>     | Open Proxy Testing <a href="#">More info...</a>  | 1.0    | 1                 | 2009-08-25 16:48:52 |
| JANET RBL presence<br><a href="#">[edit parameters]</a>     | Check Lboro Hosts for RBL entries <a href="#">More info...</a>                                 | 1.0    | 1                 | 2009-09-08 20:45:02 |
| Check for banned words<br><a href="#">[edit parameters]</a> | Look for banned words in Loughborough University <a href="#">More info...</a>                  | 0.5    | -2.498e-16        | 2009-09-09 04:23:10 |

# Example Feedback Received

Feedback on security notifications:

*“Thanks for this - it's just the kind of helpful message that explains the problem, and the solution, in sufficient plain English for those who are not adept at IT Security to understand and respond to quickly.”*

Feedback on Information Security consultancy:

*“There's been a great buzz here since your visit and we're all fired up now with loads of actions having been suggested already, so the visit was an absolutely resounding success - many thanks again.”*

***More information from <http://esiss.ac.uk/> or [esiss@emman.net](mailto:esiss@emman.net)***