

E S I S S

emMAN
East Midlands Metropolitan Area Network

ESISS Launch Event

EMMAN Shared Information Security Service

9th September 2009

Matthew Cook

- ▶ Managing ESISS within EMMAN
- ▶ Network and Security Manager for Loughborough University
- ▶ ESISS integrated into team of 13
- ▶ Over ten years of IT experience
- ▶ Work on international research projects; generating an income in excess of £175k.
- ▶ JANET(UK) projects/services £105k PA.
- ▶ Budget turnover in excess of one million



Agenda

- ▶ History
- ▶ Inception
- ▶ Service Drivers
- ▶ Service Catalogue
- ▶ Future Developments
- ▶ Demonstration
- ▶ Progress to date
- ▶ Governance
- ▶ How to find out more information

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]

Inception

- ▶ Service development started 1st April 2009
 - ▶ Recruitment of two full time staff into ESISS
 - ▶ Infrastructure development
 - ▶ Website launch
- ▶ ESISS started providing service 1st August 2009
- ▶ Developed initial service offerings:
 - ▶ External campus network anomaly detection service
 - ▶ Network Security “Health Check”
 - ▶ Forensic Investigation and Support
- ▶ Launch event 9th September 2009

Service Drivers

- ▶ Strong support from EMMAN community
- ▶ Individual requests from other academic institutions
- ▶ Feedback from JANET CSIRT events
- ▶ UCISA Directors 'Top Ten Concerns'

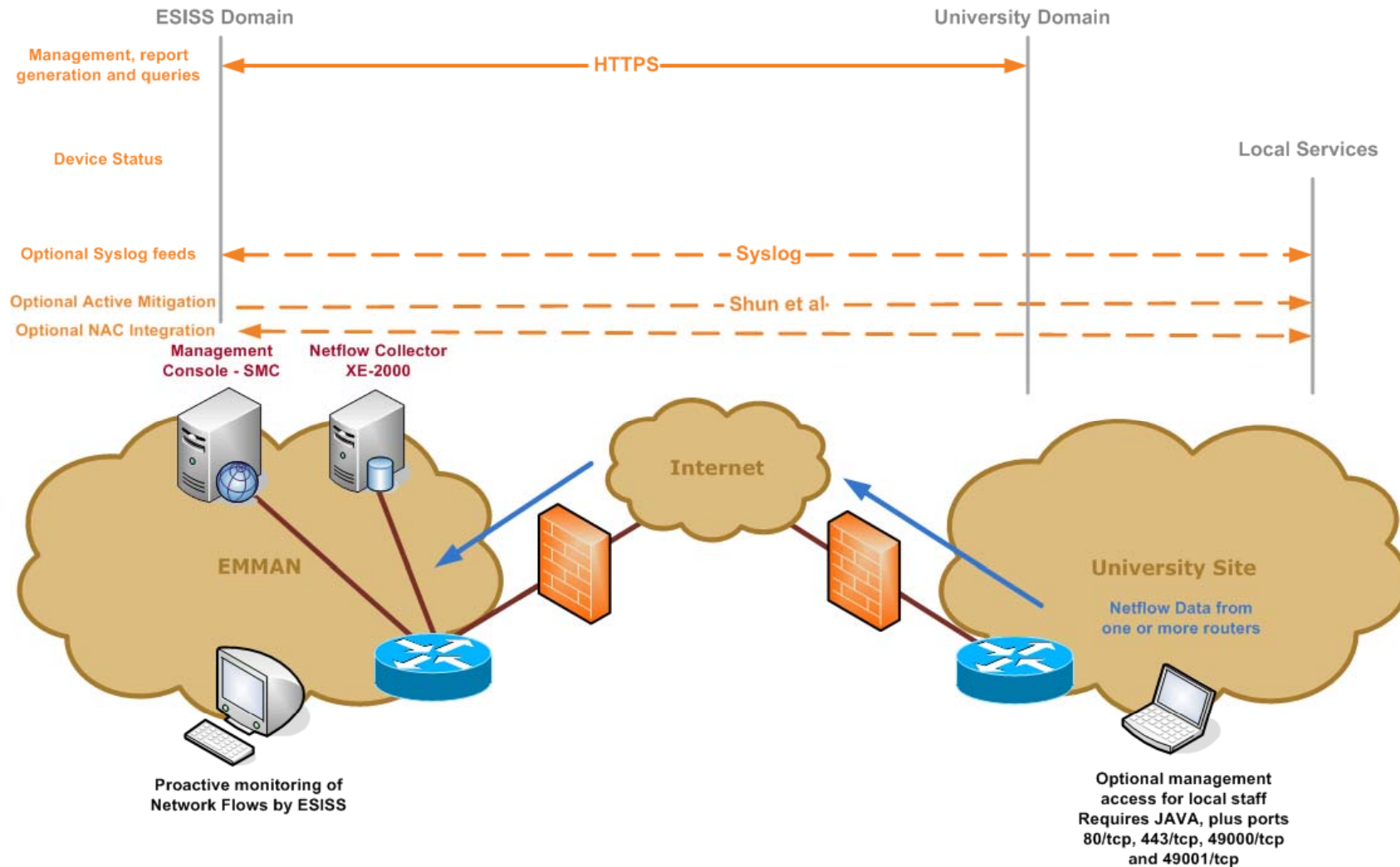
- ▶ Organisations are broadly facing the same challenges which do not provide distinct competitive advantage.

Service Catalogue



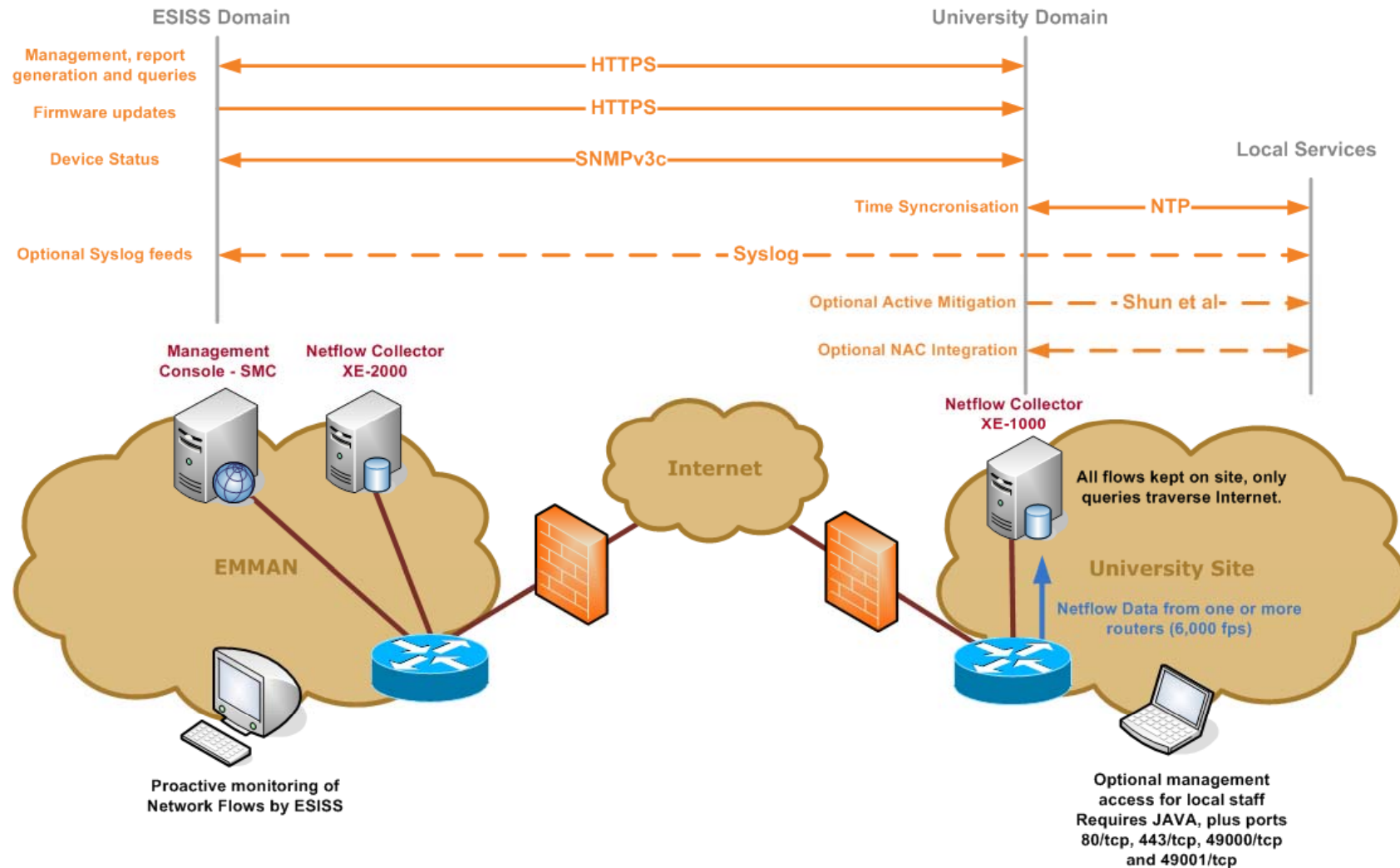
Network Based Anomaly Detection

Campus Network Anomaly Detection Service [Per MAN/RNO]



Network Based Anomaly Detection

Campus Network Anomaly Detection Service [Per Site]



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 [edit parameters]	Checking the name "Loughborough University" against home page URL More info...	0.9	1	2009-09-09 02:34:02
Webcam Finder [edit parameters]	Network visible webcams More info...	1.0	1	2009-09-08 18:15:08
Open Proxy Servers [edit parameters]	Open Proxy Testing More info...	1.0	1	2009-08-25 16:48:52
JANET RBL presence [edit parameters]	Check Lboro Hosts for RBL entries More info...	1.0	1	2009-09-08 20:45:02
Check for banned words [edit parameters]	Look for banned words in Loughborough University More info...	0.5	-2.498e-16	2009-09-09 04:23:10

ESISS Team Background

- ▶ Extensive experience of IT in public sector
- ▶ Two CCSP qualified staff
- ▶ Discovered vulnerabilities in major IT software from HP, Cisco and Aleph
- ▶ International invited conference speakers, over 50 events since 2001
- ▶ TF-CSIRT members (FiRST and Trusted Introducer)
- ▶ Access to a variety of experts in wider team
- ▶ Relationships with major vendors:
 - ▶ Cisco IPv6 Council
 - ▶ Cisco Wireless Assurewave Programme
 - ▶ Cisco Security/Remote Access Programme

Demonstration

- ▶ ESISS web based content
- ▶ Reputational Monitoring Service

Progress to date

- ▶ Additional turnover of £13k since service launch
- ▶ Arranging meetings with staff from all eight EMMAN members
 - ▶ Initial Service Briefing
 - ▶ On site Stealthwatch base lining activity
- ▶ Two additional Universities in advanced stages of signing up to the service.
- ▶ 14 further Universities have expressed an interest in ESISS services
- ▶ Extensive service development

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.”

Governance

- ▶ **Steering Group**
 - ▶ Ian Griffiths (EMMAN)
 - ▶ Pete Darby (EMMAN)
 - ▶ Paddy Walker (HEFCE)
 - ▶ Paul Kennedy (University of Nottingham)
 - ▶ Alison Brook (University of Northampton)
 - ▶ Matthew Cook (Loughborough University)
- ▶ **Reporting to EMMAN groups and HEFCE**
- ▶ **Complete Professional Indemnity Insurance**
- ▶ **Accreditation through partnership arrangements**

What do EMMAN members get?

- ▶ Network based anomaly detection.
- ▶ Option to send one Netflow feed from your site.
- ▶ Proactive, notification of incidents.
- ▶ Four mailing lists, RSS feed/blog:
 - ▶ infosec, windows, unix and mac
- ▶ Information Security templates, documentation, advice and guidance.
- ▶ Four training events per annum.
- ▶ Reputation monitoring service.
- ▶ 5 IP Automated Pentest every month.

How to find out more information

- ▶ Please chat with any member of the ESISS team:
 - ▶ Paul Whitton
 - ▶ Mohamed Imran
 - ▶ Matthew Cook
- ▶ New business enquiries:
 - ▶ Peter Darby
- ▶ Integration with EMMAN Ltd:
 - ▶ Ian Griffiths

Summary

The EMMAN Shared Information Security Service (ESISS) can provide a complete portfolio of services to your organisation. These services are designed to reduce the risk of significant information security breaches and reduce the associated costs of prevention, management, remediation and audit activities.