

E S I S S

emMAN
East Midlands Metropolitan Area Network

Playing Detective DISC Guest Talk 2009

9th December 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

- ▶ Why are we playing detective?
- ▶ What are we seeing?
- ▶ How to playing detective.
- ▶ Tools and examples.
- ▶ Network Based Anomaly Detection.
- ▶ Reputational monitoring.
- ▶ Futures.
- ▶ <http://escarpment.net/> and <http://esiss.ac.uk/>

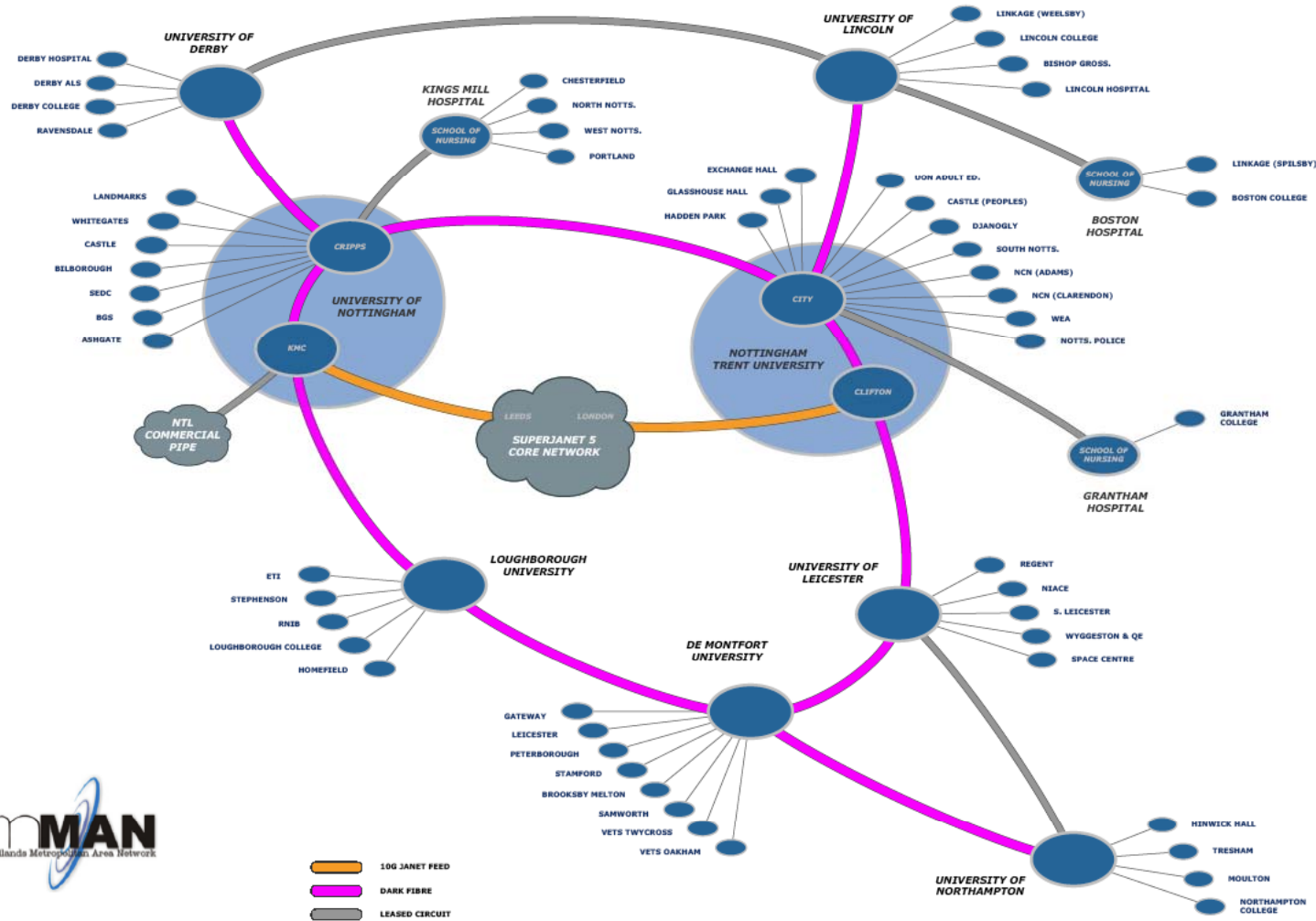
A bit more about Loughborough

- ▶ A 437 acre campus University
- ▶ 3,000 Staff and 15,000 Students
- ▶ 5,500 Study Bedrooms

- ▶ 1,200 network switches/routers
- ▶ 24,000 network connections
- ▶ 650 wireless access points

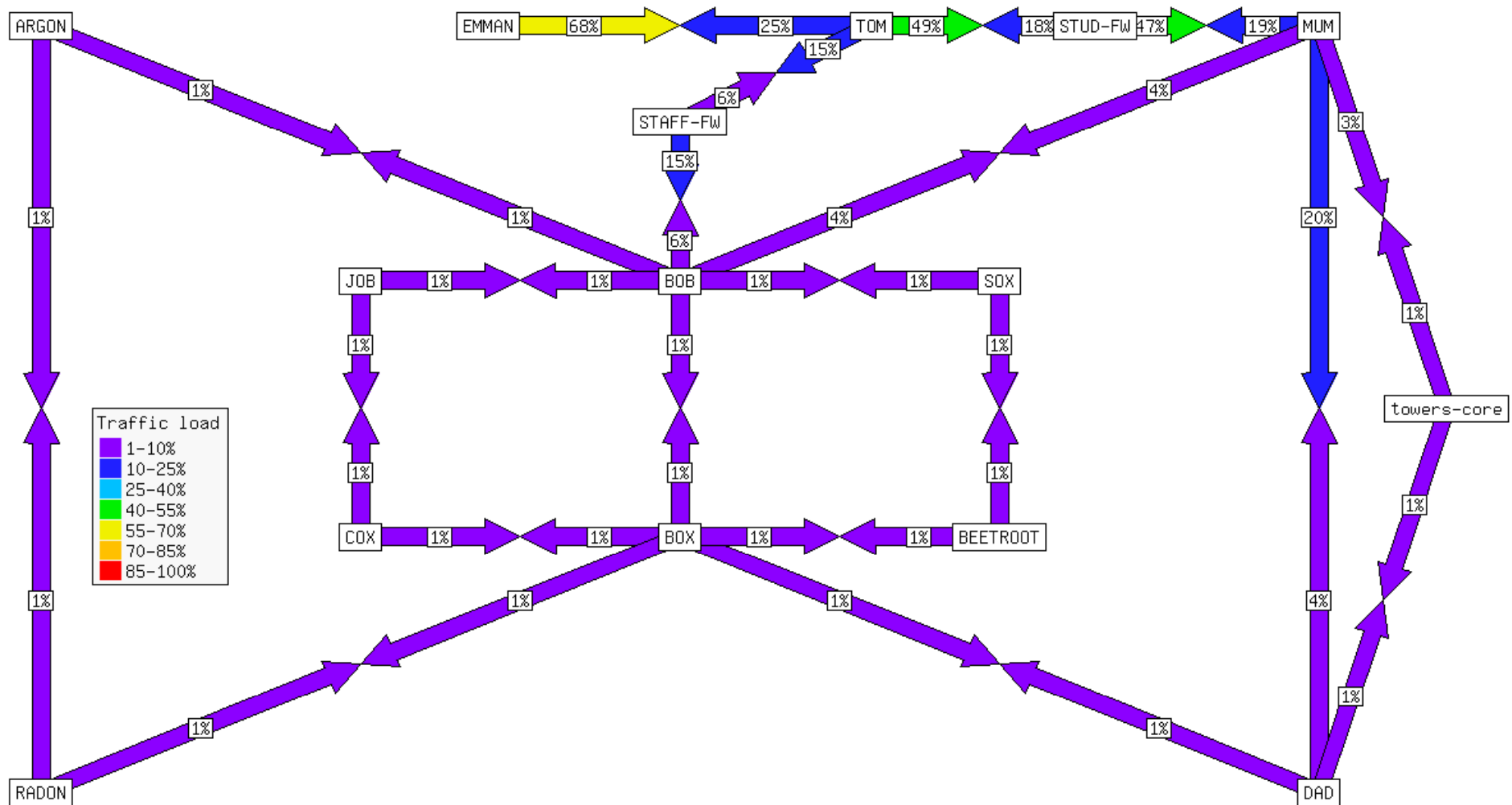
- ▶ IT Service with 110 FTEs, 13 Network & Security

East Midlands Region



EMMAN Overview Schematic
Revised: 28 September 2009

Network at a Glance



Why we are playing detective?

- ▶ Investigating Peer to Peer Usage
- ▶ Breach in internal AUP Policy
- ▶ Forensics Required
- ▶ Assistance required by government agency
 - ▶ Police Force, CEOP, MI5, HMRC etc
 - ▶ RIPA Act - Section 22(4)
 - ▶ Data Protection Act - Section 29
- ▶ For reasons to keep the network available
 - ▶ A person with a right to control the system
 - ▶ Has the express or implied consent, AUP Policy

What are we seeing?

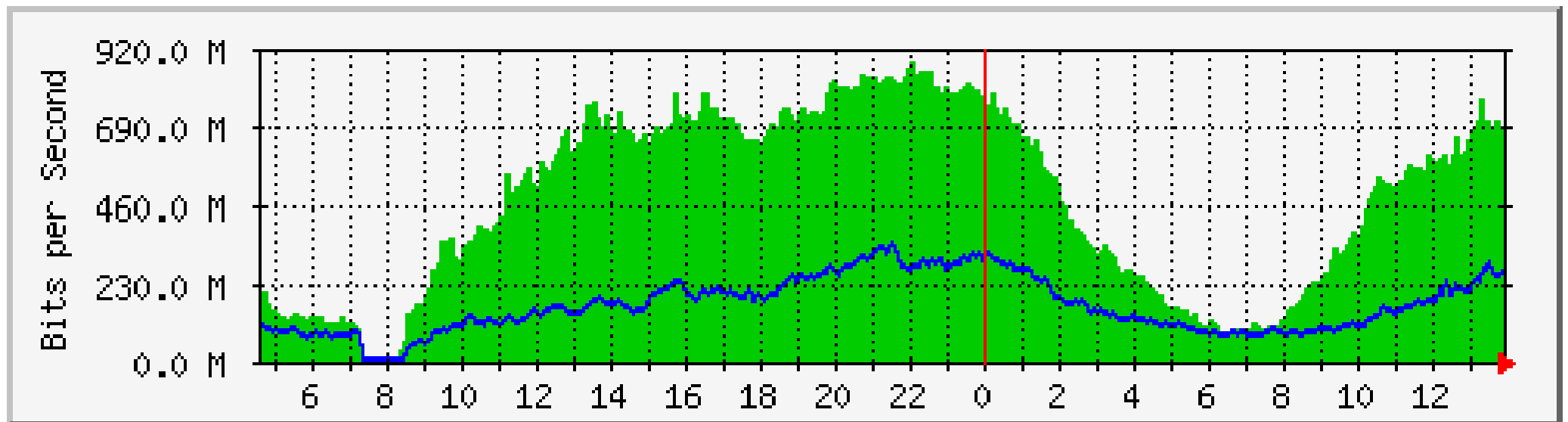
- ▶ A lot of peer to peer traffic
- ▶ External abuse attempts
- ▶ Mis-configured internal devices, printers etc
- ▶ Internal worm outbreaks
- ▶ SPAM bots
- ▶ Internal enquires regarding AUP breach
- ▶ Enquires from government bodies

- ▶ Playing detective on a bigger scale

Dealing with Incidents

- ▶ Important to have a policy to follow
- ▶ Incidents dealt with in a uniform manner
- ▶ Appropriate people managing the process
- ▶ Minimum information tracked in Service Desk
- ▶ Verify the requestor
- ▶ Encrypted storage of data
 - ▶ Important when sharing data
- ▶ Internally all data gathered from incidents provided to HR or Student Services

A lot of bandwidth, and growing




	Max	Average	Current
In	882.0 Mb/s (88.2%)	468.8 Mb/s (46.9%)	685.5 Mb/s (68.5%)
Out	345.4 Mb/s (34.5%)	164.7 Mb/s (16.5%)	258.7 Mb/s (25.9%)

Tools

- ▶ Experienced Professionals
- ▶ Registration systems
- ▶ NetDISCO
- ▶ Aggregated Logfiles
- ▶ Netflow
- ▶ IDS, replacing Snort
- ▶ Lancope Stealthwatch
- ▶ Orion NPM

NetDISCO

Netdisco



[Network Map]
[Device Search]
[Device Inventory]
[Node Search]
[Port Report]
[Duplex Mismatch Finder]
[Node Inventory]
[Backend Log]
[Documentation]
[Administration Panel]
[About]
User [redacted] [Logout]
[Change Password]

Search Results

MAC	Vendor	Match	Device or Node	First Seen	Last Seen
00:25:00: [redacted]		IP -> MAC	131.231. [redacted] (blackslab)	Jun 3 19:04 2009	Dec 9 14:04 2009
		Switch Port	131.231. [redacted] [FastEthernet0/41] (cisco-2960-48tt-n105-rack27-1)	May 27 10:19 2009	Dec 9 10:15 2009
		MAC -> IP	131.231. [redacted] (diss-83-50)	May 27 09:02 2009	Oct 21 14:16 2009

Matched 1 nodes.

Node Search

MAC, Hostname, IP, NetBIOS:
* and ? are wildcards.

Time Stamps: On Off
Archived Data:
Show Vendor: On Off

Advanced Node Search

[+] Search on Vendor or OUI

Specific Searches

- These aren't guaranteed to be wireless access points, they just have MACs that fall into the right range. Also remember people can hide them under fake MAC addresses as well.
-

* Advanced Searches can be slow to load.

IDS Systems

06/16-05:17:26.101855 [**] [1:2181:1] P2P

BitTorrent transfer [**] [Classification: Potential
Corporate Privacy Violation] [Priority: 1] {TCP}

131.231.*.*:1559 -> 65.6.195.243:6883

06/16-12:22:19.935235 [**] [1:1432:4] P2P

GNUTella GET [**] [Classification: Potential
Corporate Privacy Violation] [Priority: 1] {TCP}

158.125.*.*:4229 -> 210.24.249.191:6346

Wireless Access Points

The screenshot displays a web-based map application. The main map area shows an aerial view of Loughborough University and surrounding residential areas. Numerous wireless access points are marked with colored circles (red, green, yellow) across the map. The map control panel on the left includes navigation arrows, a zoom slider, and a compass. The search and filter panel on the right has the following sections:

- ENC Type:** [Open](#), [Wep](#), [TKIP](#), [Wpa](#), [other](#)
- Net Type:** [AP](#), [Probe](#), [Ad-Hoc](#), [Data](#), [Turbo-Cell](#), [Unknown](#)
- Search Fields:** ssid: , bssid:
- Checkboxes:** Reachable from center
- Buttons:** Clear Search Values, Search, Interesting

At the bottom of the interface, a status bar reads: "Status: Loading GPS Data", "Rendering Data", and "Depends on browser speed (Firefox is the fastest)".

Wireless Access Points

- ▶ Some are legitimate: SMEs or Sporting Bodies in Innovation Centres, Students Personal Access Points, Vending Machines, Rogue Access Points and Houses surrounding campus.
- ▶ RADAR
- ▶ Unauthenticated Access

```
[root@box huntkill]# ./trackme 158.125.*.*
```

```
Leave IP2MAC with MAC of '00:00:00:00:00:00'
```

```
Seen 00:00:00:00:00:00 on sox interface Po2 going to box
```

```
Seen 00:00:00:00:00:00 on box interface Gi1/2 going to beetroot
```

```
Seen 00:00:00:00:00:00 on beetroot interface Gi0/6 going to cisco-35-  
ZZ
```

```
Seen 00:00:00:00:00:00 on cisco-35-** interface FastEthernet0/15  
(seen19 on port)
```

Logs, Logs and more Logs

- ▶ Logging is key, trivial to set up, difficult to use...
- ▶ WMF vulnerability in January 2006
- ▶ Aggregation to a central location:
 - ▶ DHCP Servers
 - ▶ Authentication Servers
 - ▶ Email Servers
 - ▶ Web Servers (VLE, Intranet, VPN)
 - ▶ Network Devices
 - ▶ Firewalls
 - ▶ IDS
 - ▶ Servers: AIDE, Tripwire, Snare, HIDS

Examples

- ▶ Physical theft of computer RAM
- ▶ Physical theft of whole Computer
- ▶ Malicious email: x-originating-ip: [123.121.x.x]
- ▶ Hijacked accounts (someone in the room)
- ▶ Research Server
- ▶ Projects Server
- ▶ Photocopier
- ▶ Appliance Devices, things you can't patch!

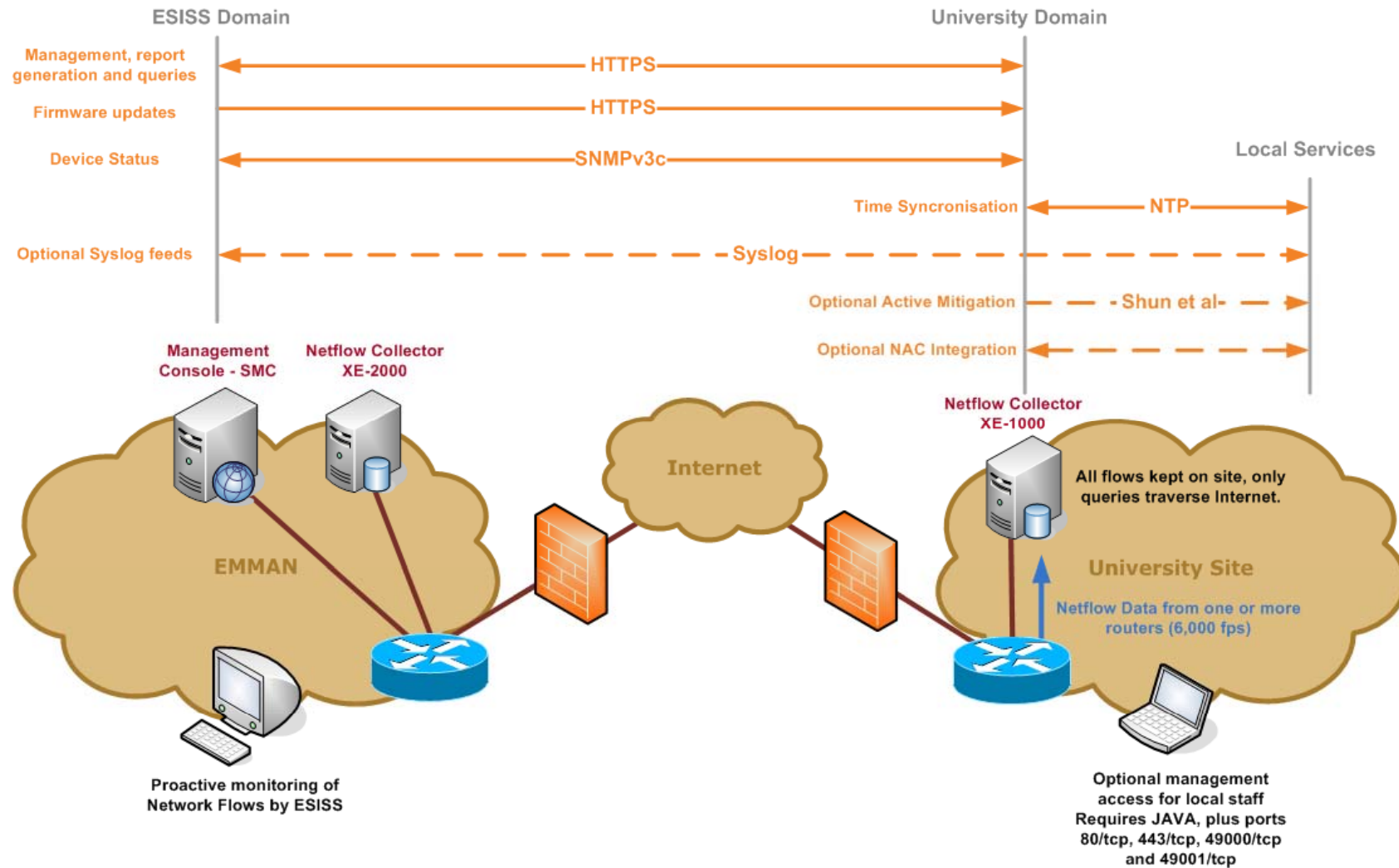
The Beauty of Trend Analysis

- ▶ If it happens to you, it will happen to...
- ▶ Looking at trends within the sector
- ▶ Looking at trends across the global

- ▶ SSH Scans
- ▶ BotNet Controllers
- ▶ Credential dictionary attacks – Email
- ▶ Email Spam bots

Network Based Anomaly Detection

Campus Network Anomaly Detection Service [Per Site]



Lancope StealthWatch

File Edit View Status Security Hosts Traffic Reports Analysis Configuration Help

Enterprise

- EMMAN
 - Inside Zones
 - Loughborough
 - Dark Net
 - HallNet
 - Labs
 - Loughborough grammar
 - Servers
 - VPN Clients
 - Wireless
 - Outside Zones
 - All-Outside
 - AGS - Test
 - AGS - Test 2
 - Conficker Collisions
 - Countries
 - Appliances
 - NTU-G1c
 - UoN-G1c
 - Xe-1000
 - Exporters
 - Peripherals
 - External Devices

Loughborough Dashboard

Domain : EMMAN
Zone : Loughborough

Zone Index Counts - 56 records

Zone	CI	FSI	TI
Elvyn			
Towers		1	
Faraday			
Telford-Whitworth		1	
William Morris			
Forest Court-Royce			

Zone Traffic, Inbound (+) and Outbound (-)

Zone Service Traffic, Traffic Inbound (+) and Outbound (-)

Alarm Report by Type

Last updated at: 09-Dec-2009 16:26:03
Next update in: 4:21

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

What can we monitor?

- ▶ Twitter
- ▶ Google Search
- ▶ Facebook
- ▶ BeBo
- ▶ Blogosphere
- ▶ New Sites
- ▶ Wikipedia
- ▶ TheStudentRoom.co.uk
- ▶ WhatUni.com
- ▶ RateMyProfessor.com
- ▶ YouTube
- ▶ Graduate Jobs Forum
- ▶ Web Server Directory List
- ▶ Default Installs/files
- ▶ Web Stats Pages
- ▶ RBL Checks
- ▶ Open SMTP Relay
- ▶ Recursive DNS Check
- ▶ Web Forgery
- ▶ Bug-Me-Not
- ▶ PHP versions
- ▶ Safebrowsing Alerts
- ▶ IRC/IRQ Chat
- ▶ Much, much more

Reputational Monitoring from ESISS

Welcome MattCook



[Logout](#)

Contact Us

New Business: 07774 251 556
Tel: 01509 22 5978/5979
Fax: 01158 48 4724
Email: esiss@emman.net

EMMAN Ltd
c/o Information Systems
The Nottingham Trent University
Burton Street
Nottingham
NG1 4BU

Organisation: Loughborough University

Your Role(s): Admin

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	1.000	2009-12-09 02:34:03 See results
Webcam Finder [edit parameters]	Network visible webcams More info...	0.5	1.000	2009-12-08 18:15:12 See results
Open Proxy Servers [edit parameters]	Open Proxy Testing More info...	0.5	1.000	2009-12-08 22:12:02 See results
JANET RBL presence [edit parameters]	Check Lboro Hosts for RBL entries More info...	0.2	1.000	2009-12-08 20:45:02 See results
Check for banned words [edit parameters]	Look for banned words in Loughborough University More info...	0.5	0.538	2009-12-09 04:23:01 See results
Vulnerable Wordpress Versions [edit parameters]	Checks for dodgy versions of WordPress More info...	0.2	1.000	2009-12-08 18:18:06 See results
Vulnerable Gallery Versions [edit parameters]	Check for vulnerable versions of the Gallery photo album software. More info...	0.5	1.000	2009-12-08 19:03:03 See results
Vulnerable PHPMyAdmin Version [edit parameters]	Look for dodgy PHPMyAdmin MySQL database front ends. More info...	0.3	1.000	2009-12-09 03:19:02 See results
BugMeNot [edit parameters]	BugMeNot username and password exposure More info...	0.7	1.000	2009-12-09 12:28:04 See results
WhatUni.com [edit parameters]	Check reviews in WhatUni.com More info...	1.0	1.000	2009-12-09 09:54:05 See results

Futures

- ▶ Increasing bandwidth
- ▶ 802.1X and NAC
- ▶ Site Visitors
- ▶ VPN Portal Abuse
- ▶ IPv6
- ▶ SSL Proliferation
- ▶ Encryption
- ▶ Appliances, things you cannot patch!
- ▶ Cloud Computing: SaaS and IaaS
- ▶ Emerging ISO Standards



Questions, and safe journey home!

<http://escarpment.net/> and <http://esiss.ac.uk/>

