Simon Clifford

The Digital Blue line

Insight into the Cyber Policing Landscape

The Police ICT Company

21 New Street, London, EC2M 4TP

PO Box 36451, 182 Bishopsgate, London EC2M 4WN

Simon.clifford@ict.police.uk | https://ict.police.uk | @simonaclifford

CYBER CRIME

CONTEXT
Current Landscape
Future Considerations

RESPONSE
NCSC / Cyber Essentials
Cyber Resilience Centres
Cyber Specials / Volunteers & Beyond
Evolution of Action Fraud
Cyber Alarm

PoliceICT

Pandora's box

A process that once begun generates many complicated problems

STOCHASTIC RISK

Dictionary

stochastic

stochastic

/stəˈkastɪk/

adjective *technical*
adjective: **stochastic**

having a random probability distribution or pattern that may be analysed statistically but may not be predicted precisely.

Origin

GREEK stokhos — aim → GREEK stokhazesthai — aim at, guess → GREEK stokhastikos → stochastic — *mid 17th century*

mid 17th century: from Greek *stokhastikos*, from *stokhazesthai* ‘aim at, guess’, from *stokhos* ‘aim’.

Translate stochastic to Choose language

Use over time for: stochastic


Cyber Crime
4.1 Billion records stolen in 2019
54% increase on 2019
Over 15 Billion records stolen in the past 7 years

Hackers steal £650 million in world's biggest bank raid

Investigators uncover what is thought to be the biggest ever cybercrime with more than £650 million going missing from banks around the world

ave stolen £650 million from banks Photo: Alamy

£183,390,000
GDRP Fine

Uber

By Martin Evans, Crime Correspondent
4:09PM GMT 15 Feb 2015

Follow 4,225 followers

British banks are thought to have lost tens of millions of pounds after a gang of Russian based hackers spent the last two years orchestrating the largest cybercrime ever uncovered.

As much as £650 million is thought to have gone missing after the gang used computer viruses to infect networks in more than 100 financial institutions worldwide.

Crime
News » UK News »
Banks and Finance »
Technology »
Technology News »

In Crime


167 Million
LinkedIn
Hacked accounts on SALE!
Free

QUANTUM COMPUTING

Impact of Security & Cyber

53 Qbits – 200 seconds

IBM's Summit, the world's most powerful supercomputer, 10,000 years.

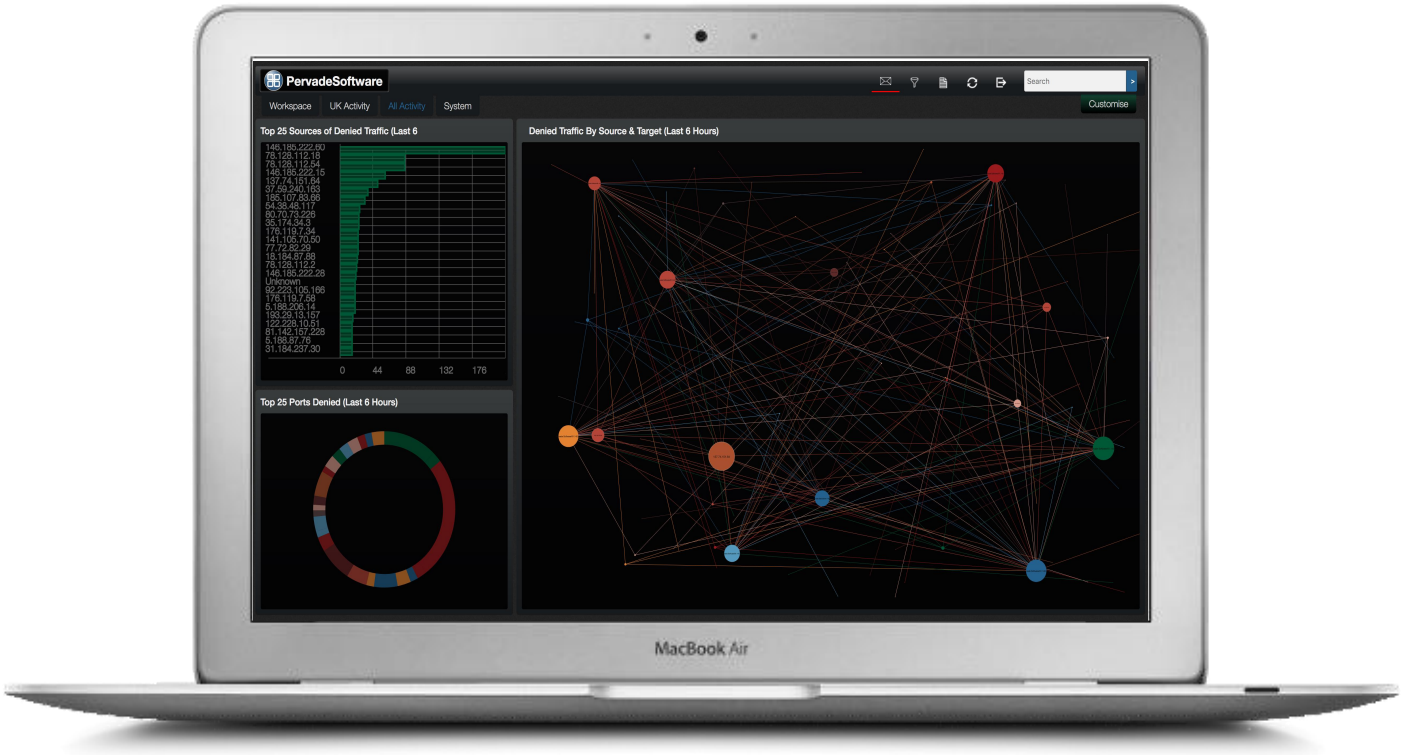
CYBER CRIME

CONTEXT
Current Landscape
Future Considerations

RESPONSE
NCSC / Cyber Essentials
Cyber Resilience Centres
Cyber Specials / Volunteers & Beyond
Evolution of Action Fraud

Cyber Alarm

POLICE CYBER ALARM



WHY IS CYBER ALARM NEEDED

* Reporting cyber crime, is difficult and inconsistent
* Attempted Cyber Crime is not reported
* Funding follows reporting
* Cost of cyber investigation (Ensuring value for money)
* Efficient & effective use of finite specialist resource
* The Voice of security/cyber leads lack management support
* Dynamic Threat landscape
* Evidence prioritisation for new capabilities

THE GENESIS OF CYBER ALARM

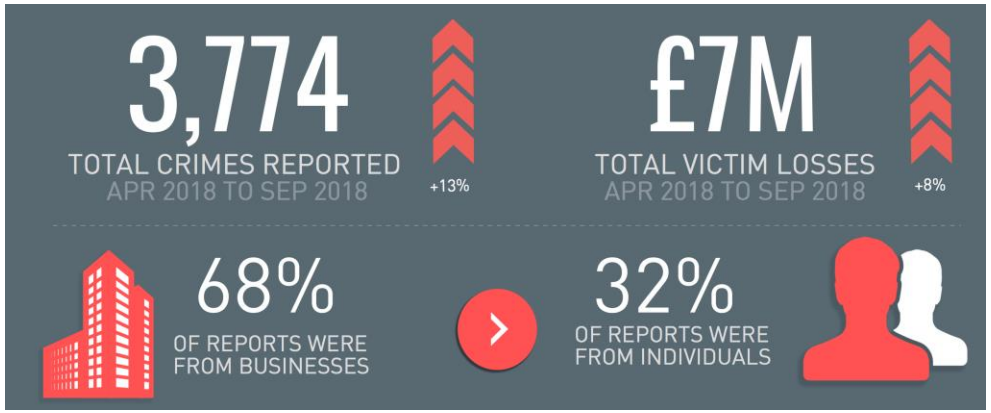
* User need
* Stakeholder engagement
* Identify emerging threat landscape

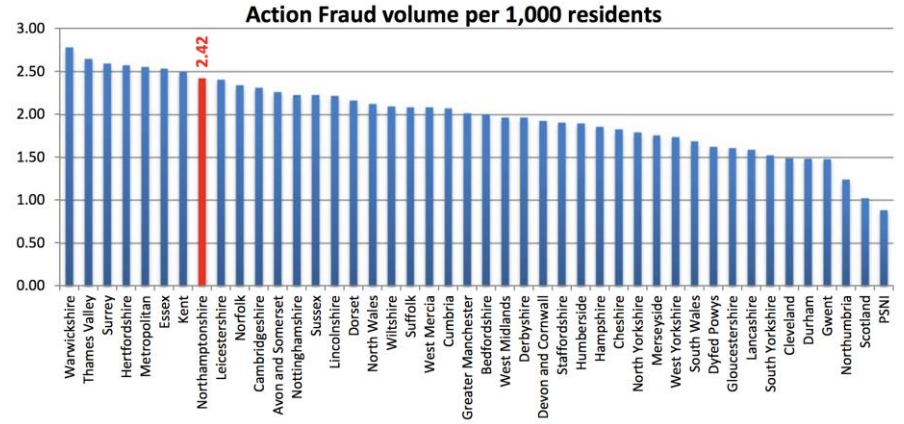
* Minimum viable product proof of concept
* Pilot introduction
* Multi-level stakeholder engagement
* Delivery at Pace
* Independent validation

WHY NORTHAMPTONSHIRE

Crimes

Northants has an abnormally high rate of reported cyber and fraud crime, despite being the 34th largest force it is 9th on the ranking of reported crimes per 1,000 residents with over £7m in estimated victim loss.

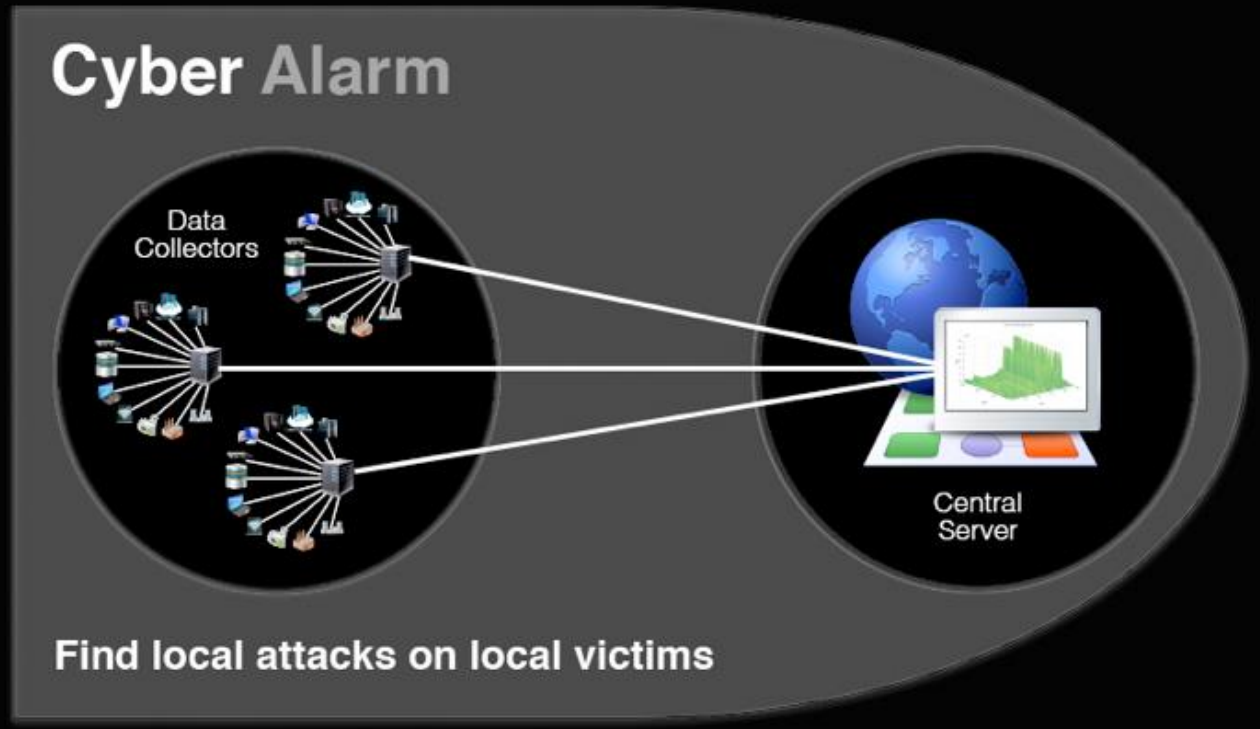




People

Northamptonshire Police has both Chief Constable and Police Fire & Crime Commissioner who want to draw on the benefits of digital capability and leadership of CC Peter Goodman around Cyber Capability

PoliceICT



A unique award-winning monitoring system

Cyber Alarm is built on the Pervade OpView™ Platform which leverages an innovative new database architecture to provide unique capabilities:-

- ✓ Successfully gather data with no VPN, NAT rules or onsite engineering work
- ✓ Automatically detect and geo-locate the source IP address of attacks (where possible)
- ✓ Forces are alerted if attackers are in their area of jurisdiction
- ✓ Forensic evidence of the attack can be analysed and relied on in court
- ✓ Trend patterns of attacks can be communicated back to data contributors
- ✓ Data analytics can be used to inform national policy and statistics

This solution supports all strands of the UK Police Strategy:-

- ✓ PREPARE – by encouraging organisations to share their data
- ✓ PURSUE – attackers that are identifiable & reachable
- ✓ PROTECT – future victims through better intelligence and more arrests
- ✓ PREVENT – by making local businesses "higher risk" targets

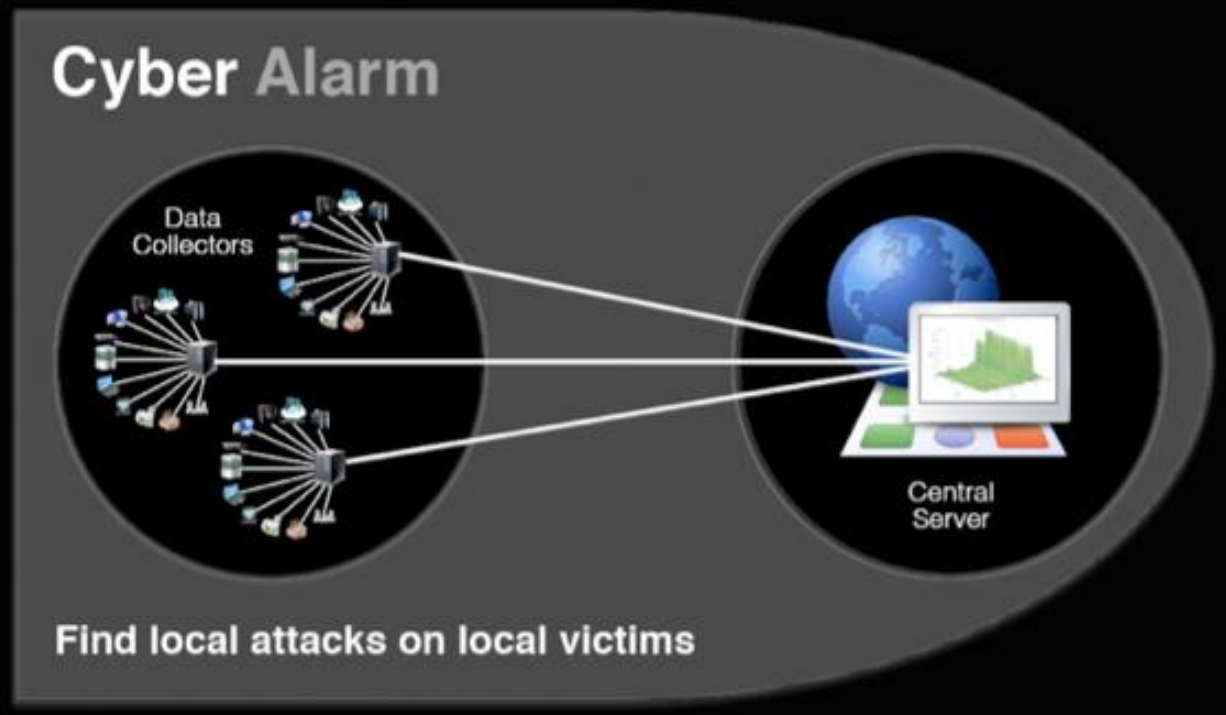
Cyber Alarm helps local Police to fight local cyber crime

CYBER ALARM ROLLOUT

Police Cyber Alarm pilot capability planned to scale out in 2020.

Currently Cyber Alarm is a regional programme deployed in the East Midlands region.

Discussions with Nation Cyber Security Centre regarding links to Active Cyber Defense.



Currently Cyber Alarm is receiving information from:-

- Councils
- Schools
- Mental Health Clinics
- SME Tech Companies with valuable IP
- IT Managed Services Company
- Formula 1 Race Team

Great example of business and community out reach.

Work is underway to increase participation to thousands of contributors in 2019.

With regional and local coordination and coopertation.

Details of current solution at: Cyberalarm.org.uk

Not Cyberalarm.org

PervadeSoftware

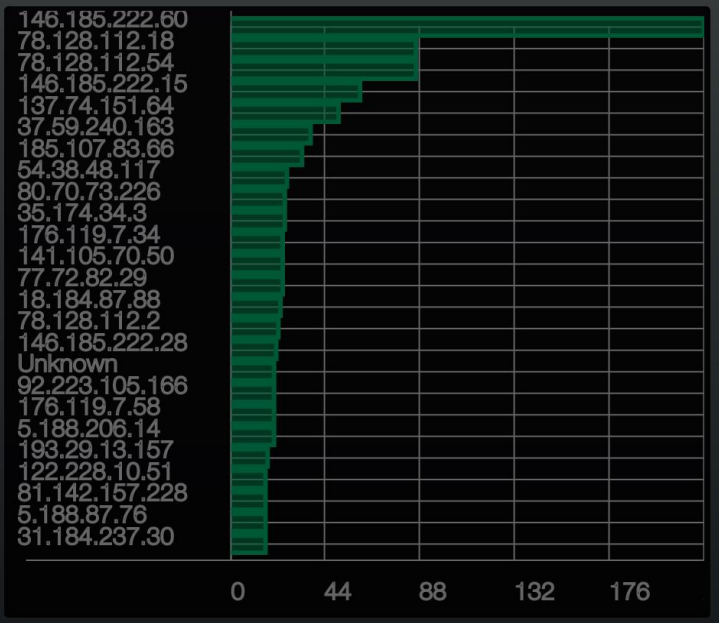
Police Cyber Alarm

Search

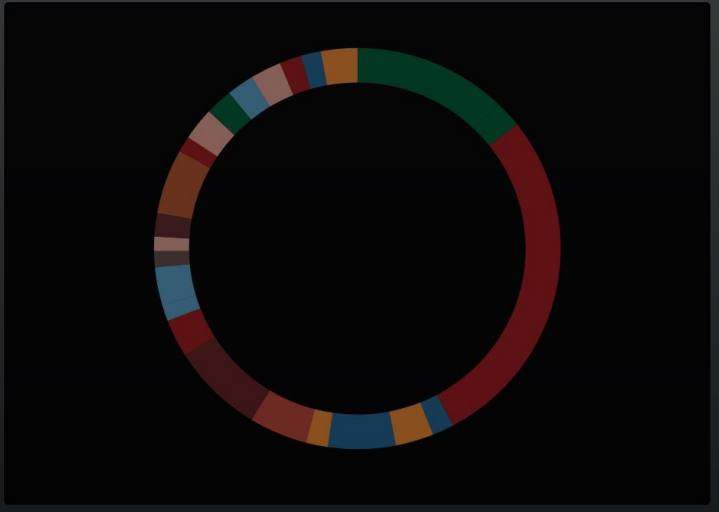
Workspace | UK Activity | All Activity | System

Customise

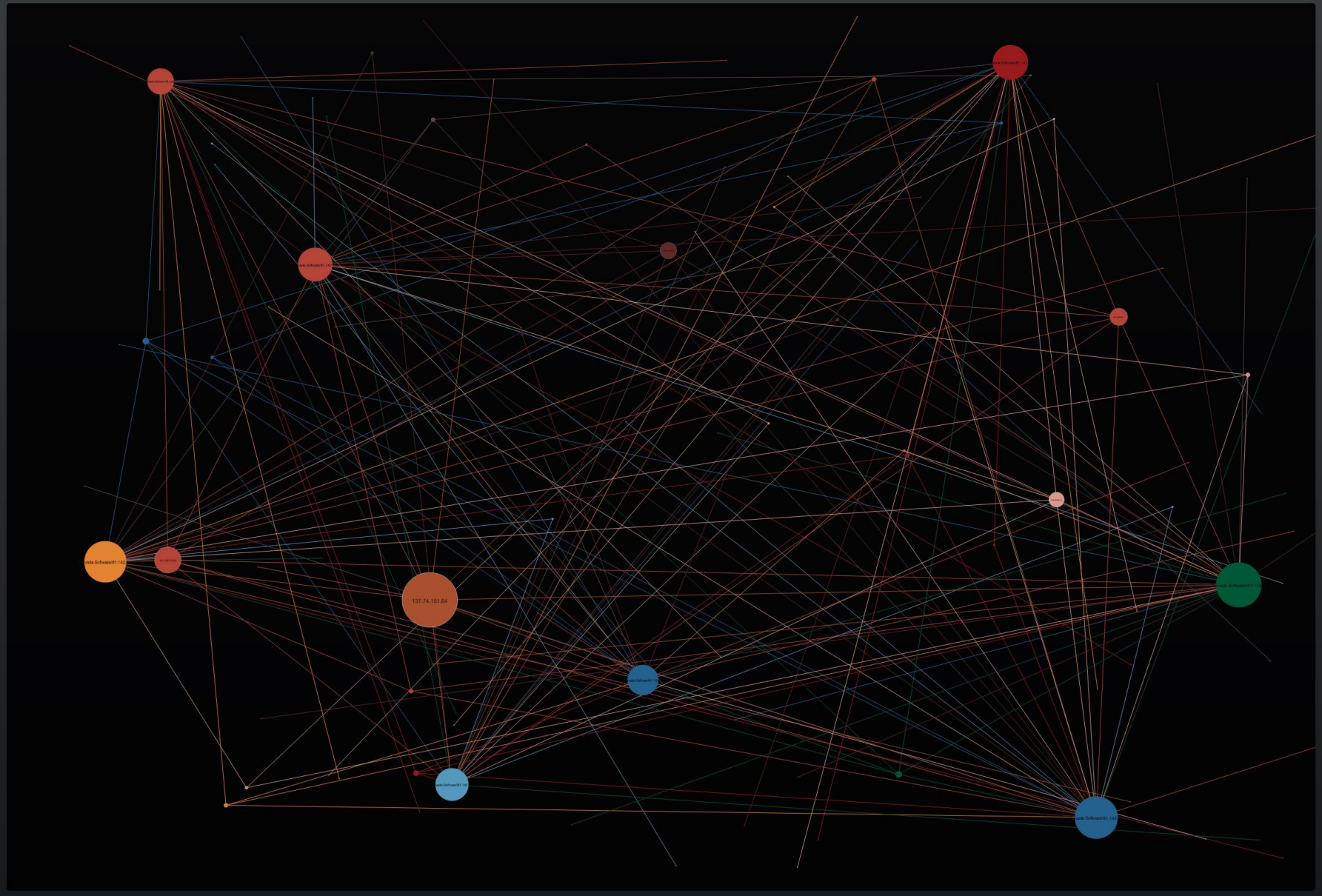
Top 25 Sources of Denied Traffic (Last 6



Top 25 Ports Denied (Last 6 Hours)



Denied Traffic By Source & Target (Last 6 Hours)



Thank you

Questions

The Police ICT Company

21 New Street, London, EC2M 4TP

PO Box 36451, 182 Bishopsgate, London EC2M 4WN

Simon.clifford@ict.police.uk | https://ict.police.uk | @simonaclifford