National Cybercrime Programme

Detective Superintendent Martin PETERS

NPCC National Police Chiefs' Council

National Cybercrime Programme

UK | DICE
DARKWEB INTELLIGENCE, COLLECTION AND EXPLOITATION

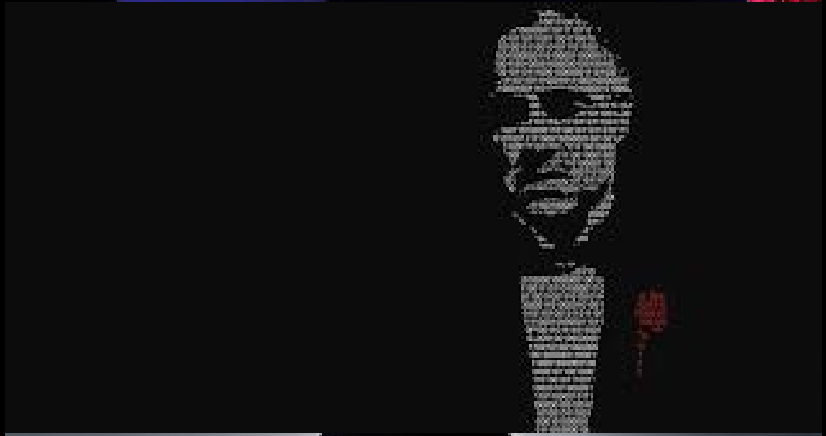
THE CYBER RESILIENCE CENTRE

CDSV
CYBER AND DIGITAL SPECIALS AND VOLUNTEERS

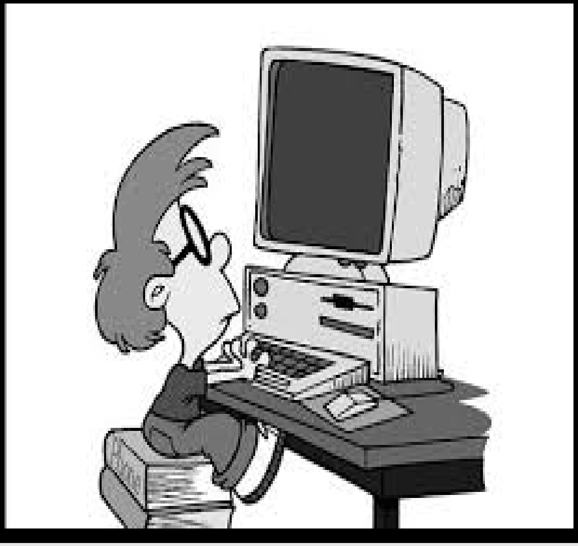
POLICE CYBERALARM

Agenda

- Introductions
- Threat
- Policing Response
- Police CyberAlarm
- Cyber Resilience Centres



2017 EDITION
Data Breach
Cyber Attack
Protection
BEST HACKING TOOLS



Cybercrime-as-a-Service

Action Fraud

- 41,000 cybercrimes to April 2024

Crime Survey of England & Wales 2023

- 898,000 to September 2023

DCMS Cyber Breaches Survey 2024

- 1 in 2 businesses suffered breach or incident

Challenges for public & SMEs

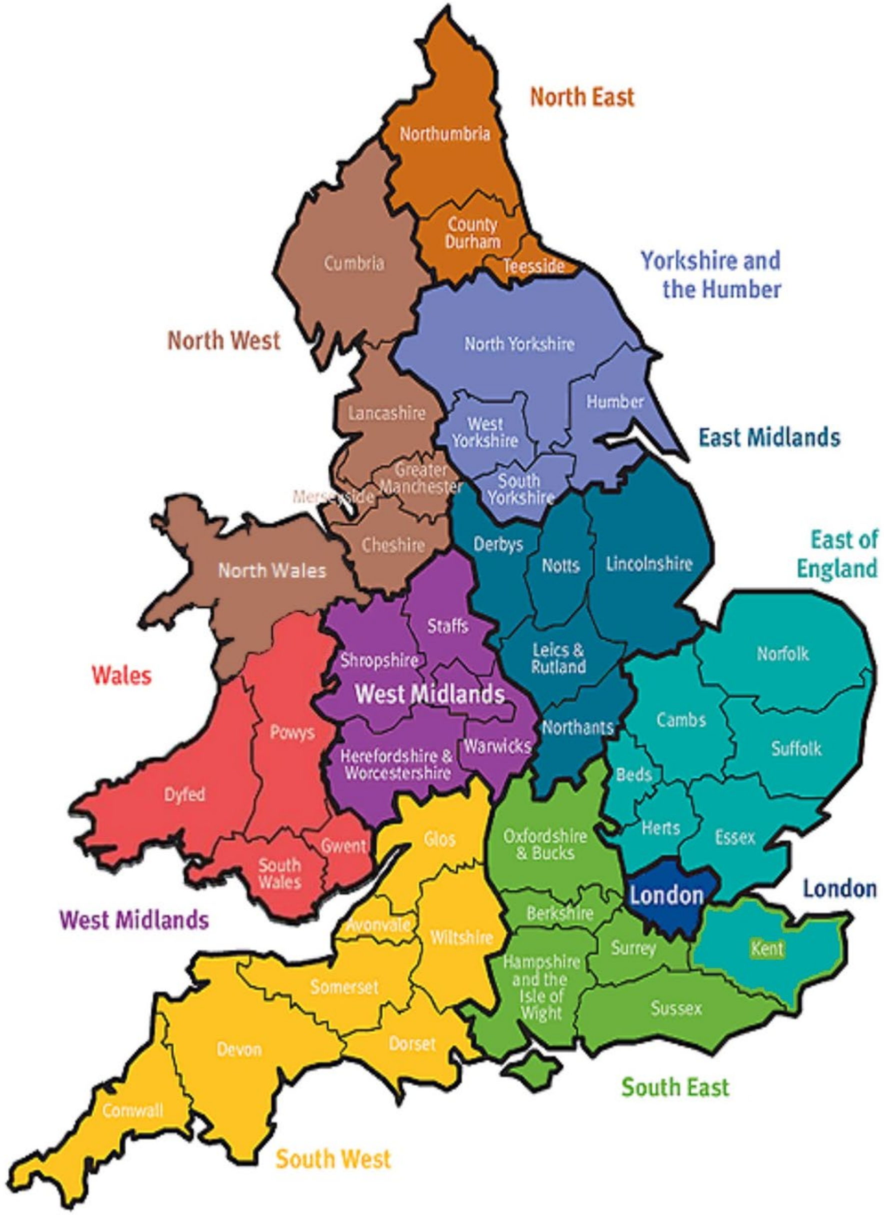
- Complexity understanding how to protect yourself or your business
- Cyber security can be expensive
- Where do you go for help?

- Est 5.6 million UK private sector businesses - SMEs account for 99%

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Office for National Statistics

Department for Digital, Culture Media & Sport



National Cyber Security Centre

a part of GCHQ

NCA

National Crime Agency

Force & ROCU Cyber Crime Units

Cyber PURSUE

Cyber PREPARE

Cyber & Digital Specials & Volunteers

Cyber PROTECT

Cyber PREVENT

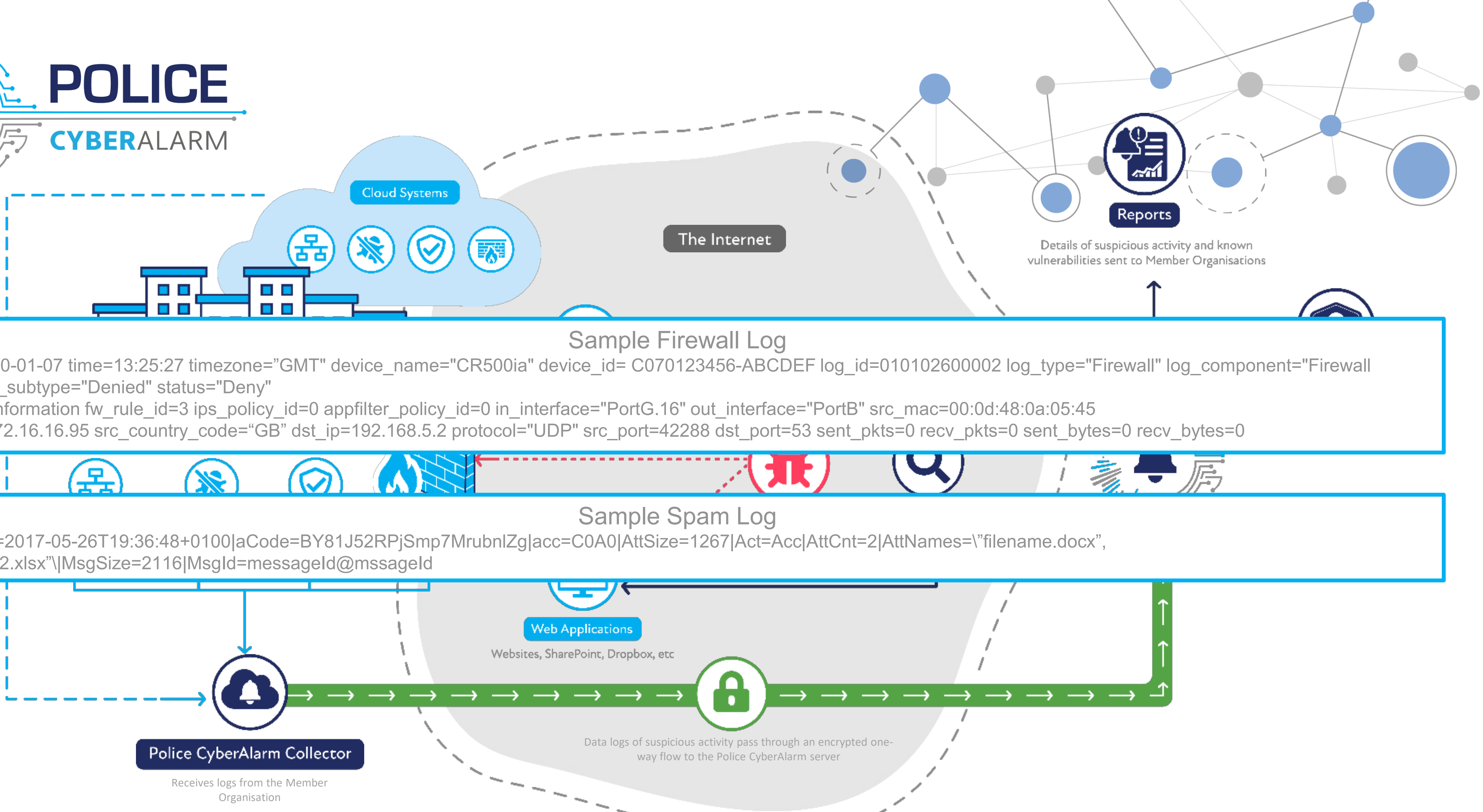
POLICE CYBERALARM

> *“To provide policing with a more comprehensive picture of the cyber threat landscape, inform cyber defence strategy and collect evidence that can be used in the identification, pursuit and prosecution of Cyber Criminals.”*

National
Cybercrime
Programme

NPCC
National Police Chiefs’ Council

POLICE CYBERALARM


Cloud Systems
The Internet
Reports
Details of suspicious activity and known vulnerabilities sent to Member Organisations
Web Applications
Websites, SharePoint, Dropbox, etc
Police CyberAlarm Collector
Receives logs from the Member Organisation
Data logs of suspicious activity pass through an encrypted one-way flow to the Police CyberAlarm server

Sample Firewall Log

```
date=2020-01-07 time=13:25:27 timezone=”GMT" device_name="CR500ia" device_id= C070123456-ABCDEF log_id=010102600002 log_type="Firewall" log_component="Firewall
Rule” log_subtype="Denied" status="Deny"
priority=Information fw_rule_id=3 ips_policy_id=0 appfilter_policy_id=0 in_interface="PortG.16" out_interface="PortB" src_mac=00:0d:48:0a:05:45
src_ip=172.16.16.95 src_country_code=“GB” dst_ip=192.168.5.2 protocol="UDP" src_port=42288 dst_port=53 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0
```

Sample Spam Log

```
datetime=2017-05-26T19:36:48+0100|aCode=BY81J52RPjSmp7MrubnlZg|acc=C0A0|AttSize=1267|Act=Acc|AttCnt=2|AttNames=\”filename.docx”,
“filename2.xlsx”\|MsgSize=2116|MsgId=messageId@mssageId
```

Current Picture

Members: Over **7300** member applications.

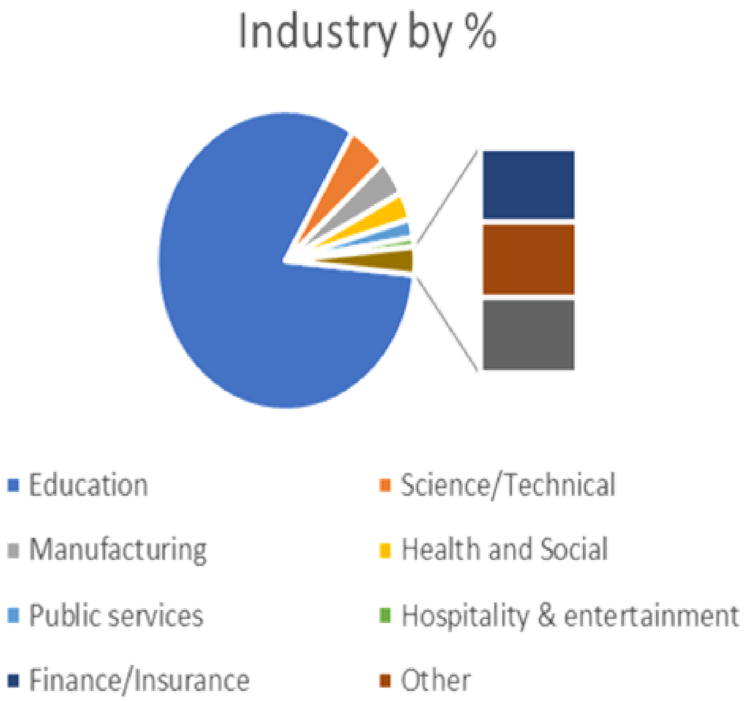
2022

394 Million suspicious incidents

62,000	vulnerability scans
<2,100	critical/high vulnerabilities
<14,200	medium vulnerabilities
<3,300	Low risk vulnerabilities

2023

50,100	vulnerability scans
1,726	critical/high vulnerabilities
5,966	medium vulnerabilities
725	Low risk vulnerabilities



Premier League

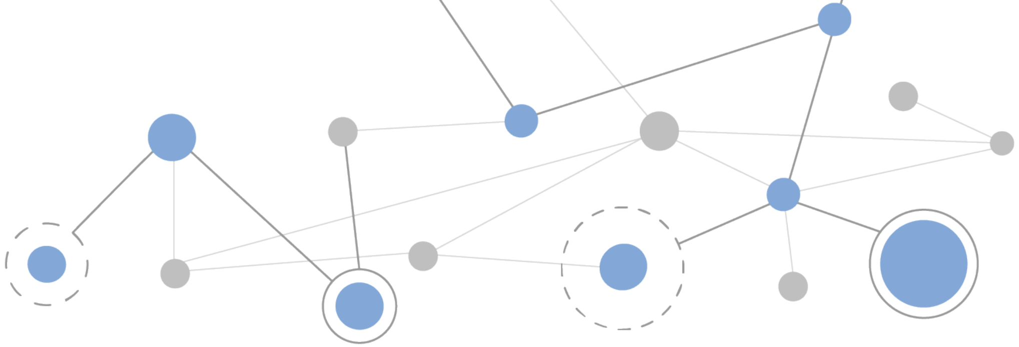
Threats

Top sources of suspicious traffic

- Netherlands
- United States
- Russia
- United Kingdom
- Bulgaria
- Denmark
- Germany
- China

Top vulnerabilities

- SSL Certificate: Cannot Be Trusted
- TLS Version 1.1 Protocol Deprecated
- Web Application Potentially Vulnerable to Clickjacking
- TLS Version 1.0 Protocol detection
- HSTS Missing From HTTPS Server



Top Common attack ports

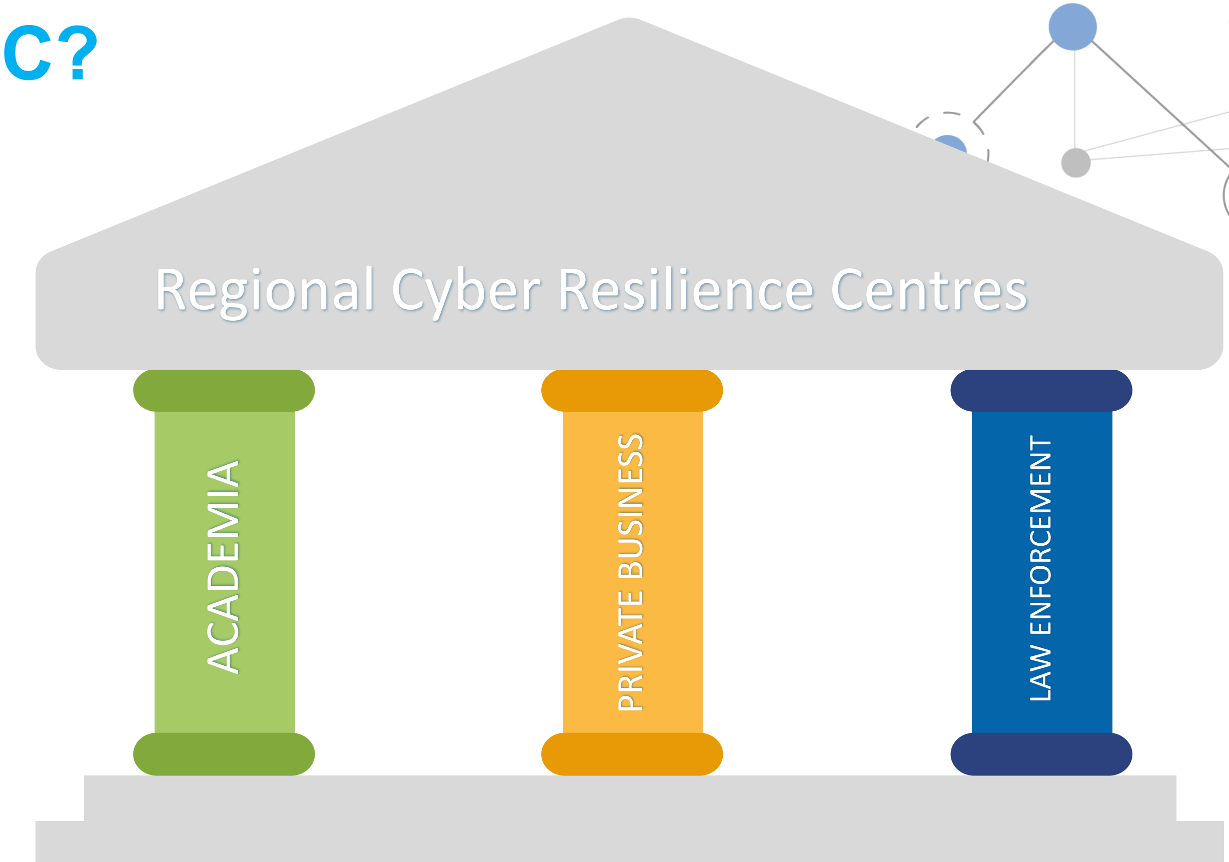
Jan 2023	April 2023	May 2023
137	58343	443
139	58463	53
23	51402	80
21	51446	23
53	22058	10443
5353	1143	40746
8080	67	5355
3306	**32760**	10051
3389	12118	547
32760	5678	20297

THE
CYBER
RESILIENCE
CENTRE

NPCC
National Police Chiefs' Council

National
Cybercrime
Programme

What is a CRC?



Regional Cyber Resilience Centres

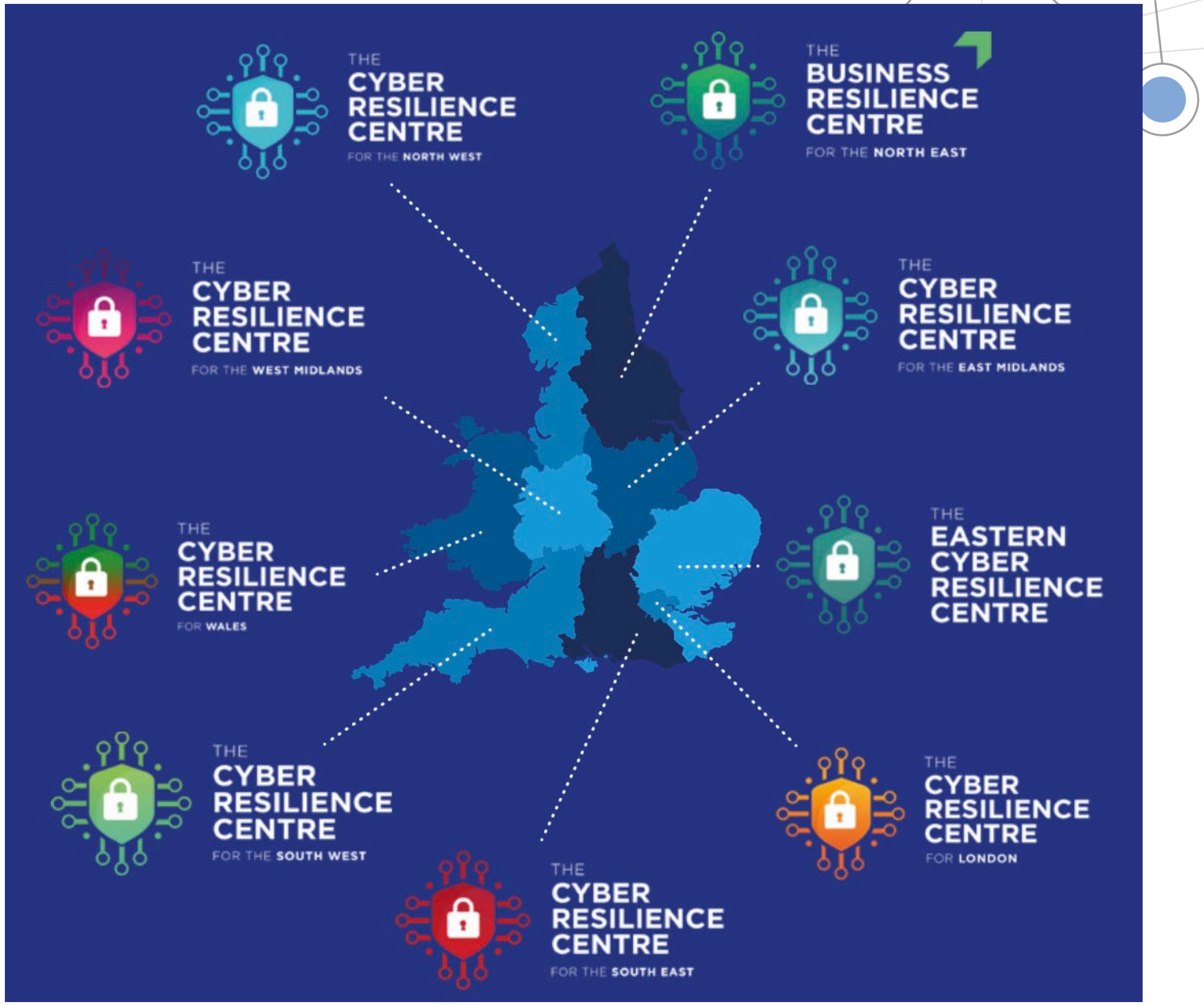
ACADEMIA

PRIVATE BUSINESS

LAW ENFORCEMENT

Trust and Confidence

Regional CRC network


THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST
THE BUSINESS RESILIENCE CENTRE FOR THE NORTH EAST
THE CYBER RESILIENCE CENTRE FOR THE WEST MIDLANDS
THE CYBER RESILIENCE CENTRE FOR THE EAST MIDLANDS
THE CYBER RESILIENCE CENTRE FOR WALES
THE EASTERN CYBER RESILIENCE CENTRE
THE CYBER RESILIENCE CENTRE FOR THE SOUTH WEST
THE CYBER RESILIENCE CENTRE FOR LONDON
THE CYBER RESILIENCE CENTRE FOR THE SOUTH EAST

National Ambassadors

KPMG

CGI

NatWest Group

Chainalysis

THE VERY GROUP

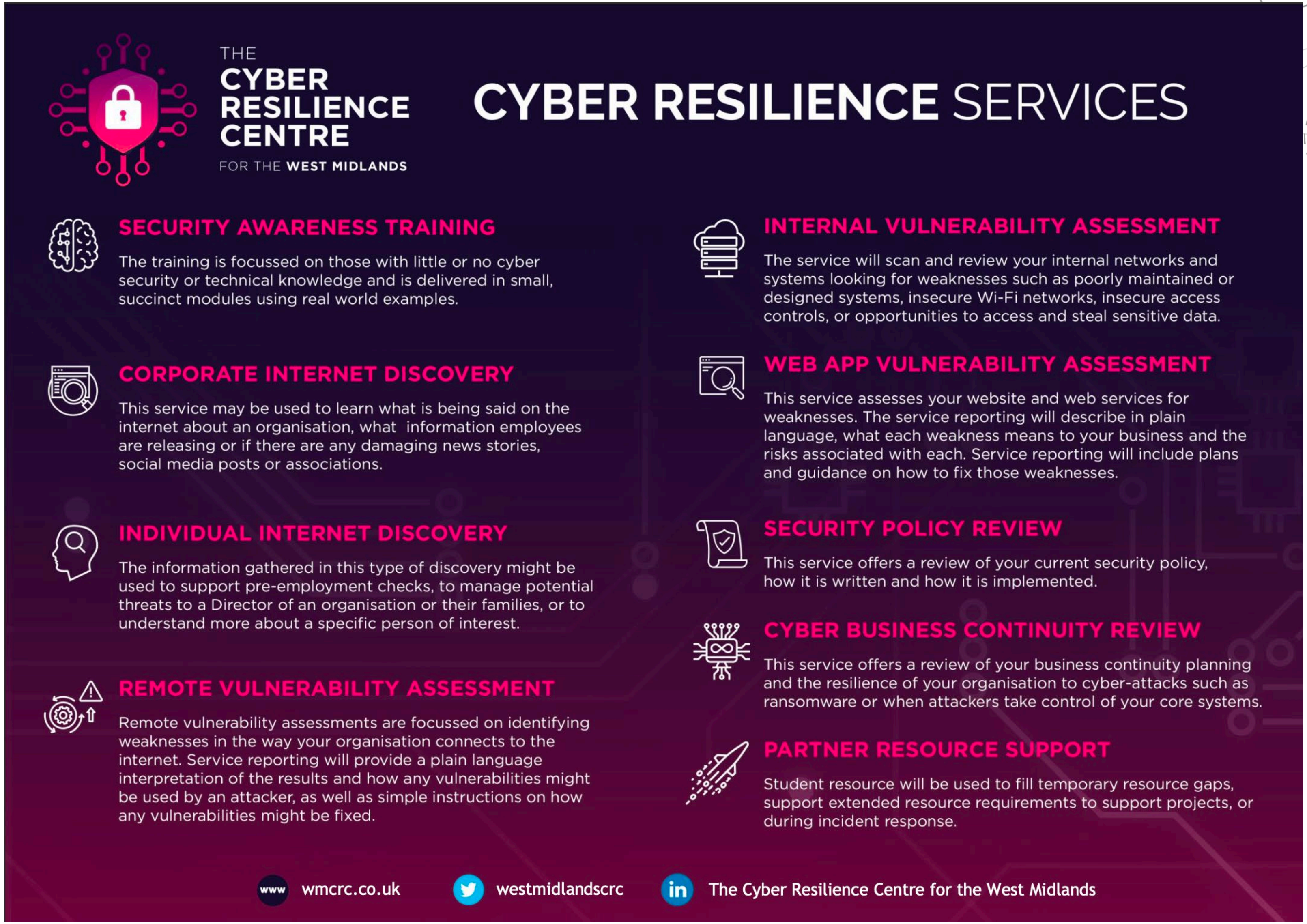
accenture

SANS

Microsoft

mastercard

Cyber PATH Services



THE
CYBER RESILIENCE CENTRE
FOR THE WEST MIDLANDS

CYBER RESILIENCE SERVICES

SECURITY AWARENESS TRAINING

The training is focussed on those with little or no cyber security or technical knowledge and is delivered in small, succinct modules using real world examples.

CORPORATE INTERNET DISCOVERY

This service may be used to learn what is being said on the internet about an organisation, what information employees are releasing or if there are any damaging news stories, social media posts or associations.

INDIVIDUAL INTERNET DISCOVERY

The information gathered in this type of discovery might be used to support pre-employment checks, to manage potential threats to a Director of an organisation or their families, or to understand more about a specific person of interest.

REMOTE VULNERABILITY ASSESSMENT

Remote vulnerability assessments are focussed on identifying weaknesses in the way your organisation connects to the internet. Service reporting will provide a plain language interpretation of the results and how any vulnerabilities might be used by an attacker, as well as simple instructions on how any vulnerabilities might be fixed.

INTERNAL VULNERABILITY ASSESSMENT

The service will scan and review your internal networks and systems looking for weaknesses such as poorly maintained or designed systems, insecure Wi-Fi networks, insecure access controls, or opportunities to access and steal sensitive data.

WEB APP VULNERABILITY ASSESSMENT

This service assesses your website and web services for weaknesses. The service reporting will describe in plain language, what each weakness means to your business and the risks associated with each. Service reporting will include plans and guidance on how to fix those weaknesses.

SECURITY POLICY REVIEW

This service offers a review of your current security policy, how it is written and how it is implemented.

CYBER BUSINESS CONTINUITY REVIEW

This service offers a review of your business continuity planning and the resilience of your organisation to cyber-attacks such as ransomware or when attackers take control of your core systems.

PARTNER RESOURCE SUPPORT

Student resource will be used to fill temporary resource gaps, support extended resource requirements to support projects, or during incident response.

www wmcrc.co.uk   westmidlandscrc   in The Cyber Resilience Centre for the West Midlands