NHS England

# Barcelona CISO 360

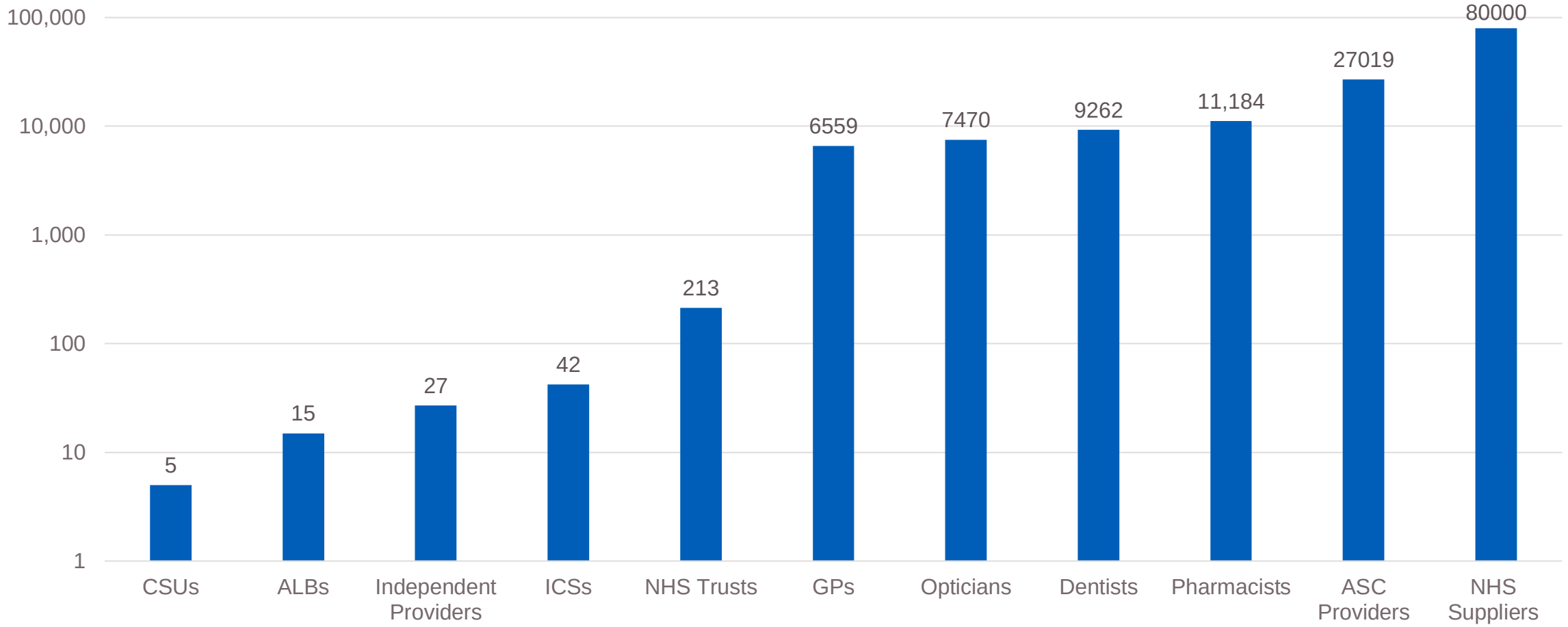
Mark Logsdon, CISO, NHS England

# Context

Who we are

# The Health and Social Care Cyber Community

## 141,795 Organisations, Roughly 12% of UK's GDP



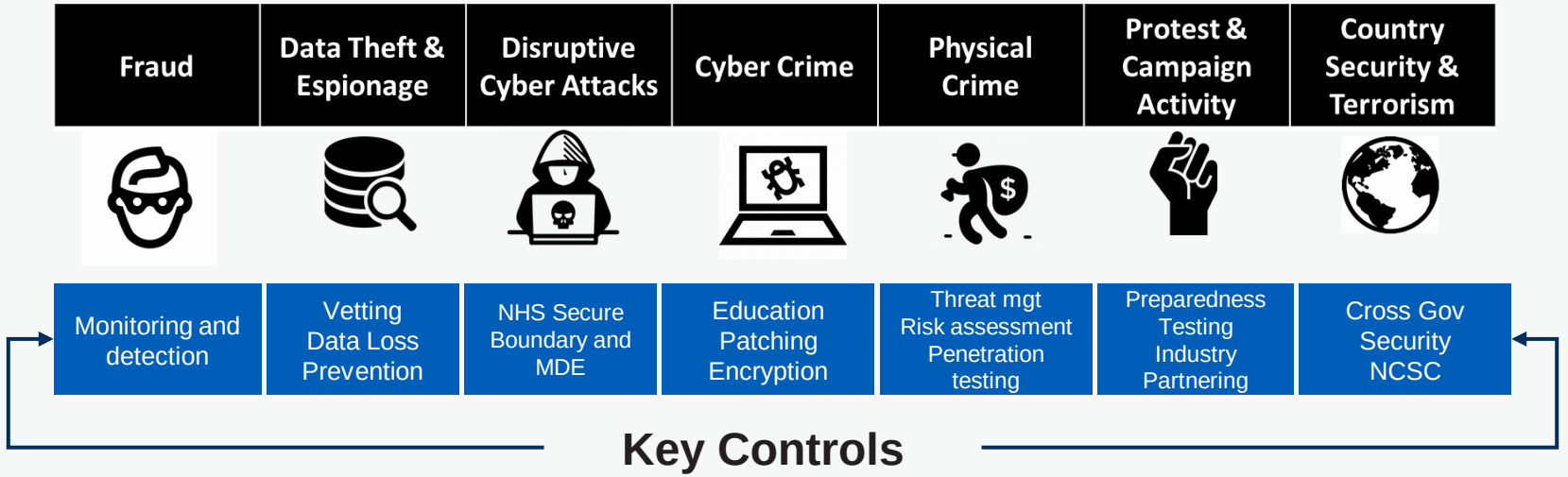
# We’re often a person’s first point of contact with NHS care

We build and run NHS.UK, NHS login and the NHS App. NHS 111 and most 999 centres run on our algorithms, reducing demand on the front line


**Over 35 million verified registrations of the NHS App,** allowing people to manage their own care, for example order repeat prescriptions, book appointments and view health records securely

# Threats to the NHS

The NHS is considered a high value target for malicious cyber actors, including nation states and cyber criminals, because of the quantity and sensitivity of the information held about UK citizens, and the potential for criminal financial gain through fraud.




- The NHS takes a holistic approach to managing security risk, ensuring that for Cyber, Physical, Personnel, Supplier Security and Business Continuity all attack vectors are considered together
- Unsupported and legacy systems are a security risk and could cause serious harm to patients
- NCSC provides advice of the key threat vectors to the NHS, specifically calling out ransomware, phishing, legacy unpatched systems, IT supply chain and cyber-enabled fraud as real and imminent threats to our business

# Supporting frontline staff

## Internal security

**100**

**Security Champions**

Across NHS Digital we have 100 security champions who are actively engaged. They act as ambassadors within their teams and regularly take part in security activities

## Data Security and Protection Toolkit

**41k**

**submissions**

Over 41,000 organisations submitted a DSPT return; the online self-assessment tool that allows organisations to measure their performance against the National Data Guardians standards

## Incident volumes

**300%**

**rise in cyber incidents**

Since 2019 there has been a 300% rise in incident volumes; requirement to scale-up and increase automation

## Cyber Associates Network

**2100**

**CAN members**

Peer to peer network aimed at improving cyber security across health and social care. Giving opportunities to discuss key issues in a safe space and learn from each other

## High severity alerts

**15**

**High severity alerts**

A 54% increase on the previous year's high severity alerts. These are cyber security alerts that require immediate action to prevent damage to the network

## Protecting the NHS

**23.2bn**

**transactions**

Protection of 23.2 billion transactions over a five day period through NHS Secure Boundary

## Protecting patients

**Several**

**Significant attacks**

The cyber security operations centre prevented several significant ransomware attacks that could have severely impacted patient care

## Security education

**5k**

**downloads**

Over 5000 downloads of security awareness materials from our Keep IT Confidential campaign. Topics include: social engineering, passwords, tailgating and be aware of what you share.

## Devices protected

**1.9m**

**devices enrolled**

Devices enrolled onto Microsoft Defender for Endpoint which feeds directly into the cyber security operations centre enabling them to detect nefarious activity across the NHS network

## Blocking malicious activity

**21m**

**malicious items a month**

On average CSOC blocks over 21 million items of malicious activity every month, Working directly with local team to respond to the cyber threats

## Prevention

**Several**

**global scale attacks**

Several global scale attacks prevented before anyone else noticed it was happening

## Active defence

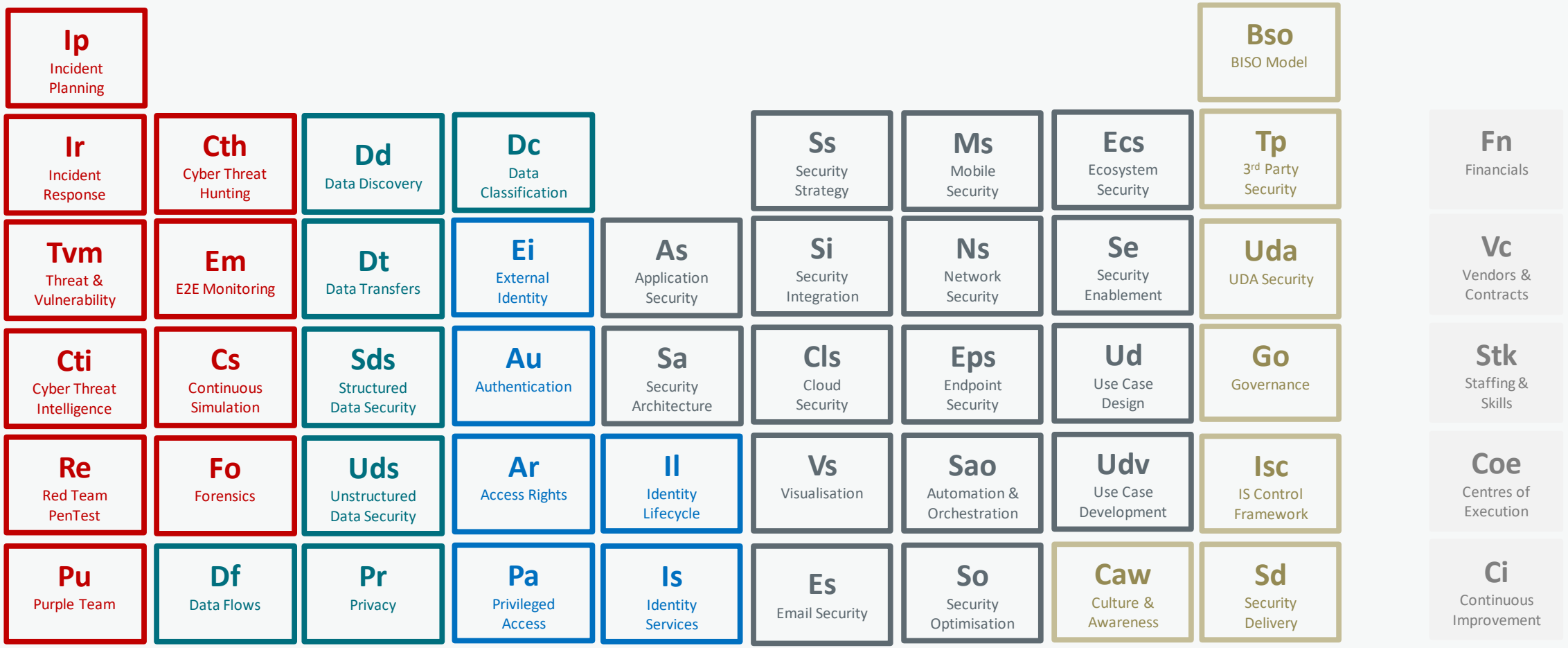
**5m**

**transactions a week**

We actively monitor and protect devices across the NHS and work directly with local teams in response to cyber threats

# Our Structure

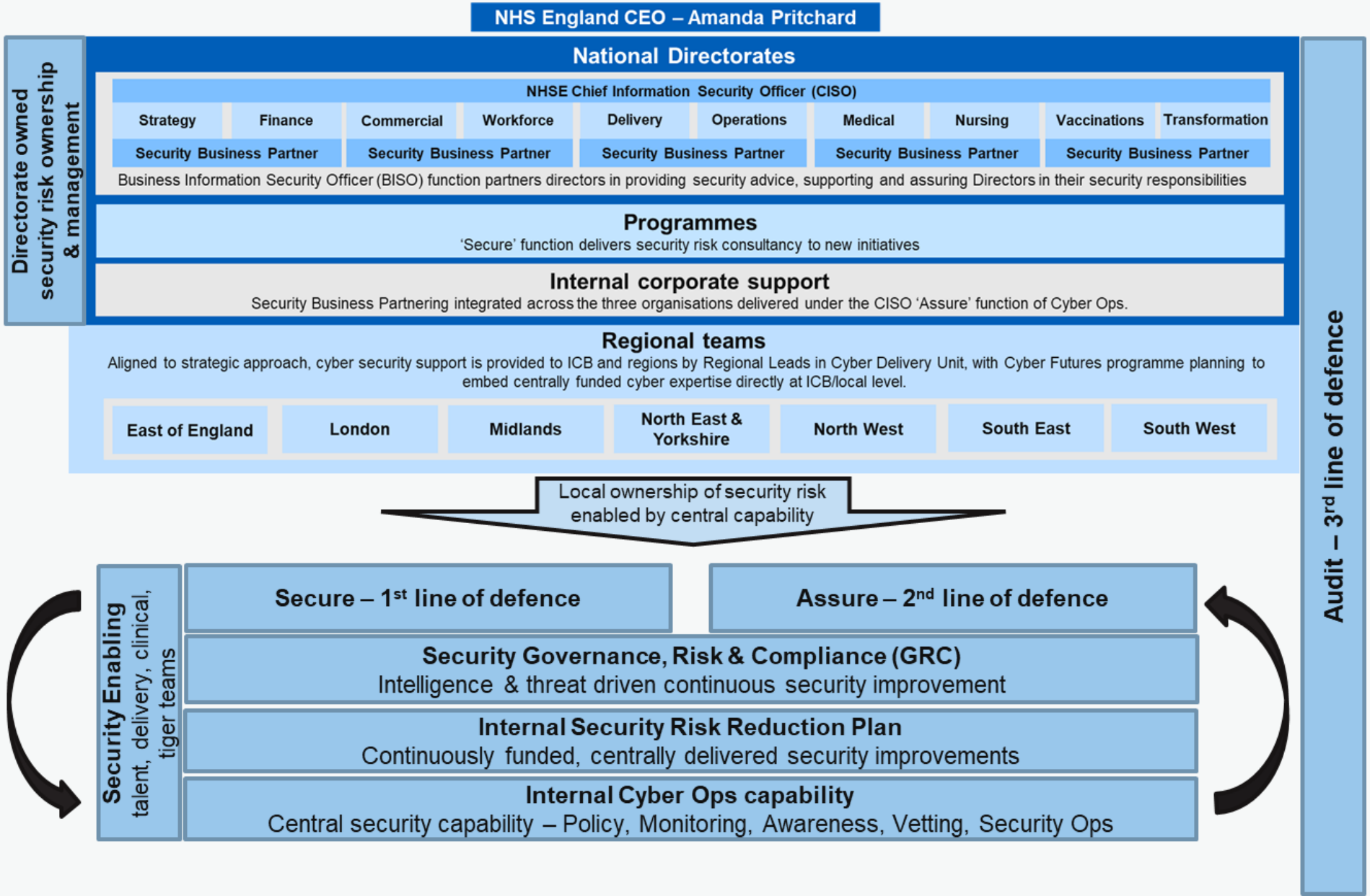
# Security “Periodic Table”




**Incident, Vulnerability & Threat Management**
**Identity & Access Management**
**Risk & Security Management**

**Privacy & Data Protection**
**Automation, Security Architecture & Services**

# Integrating Cyber Operations in NHS England



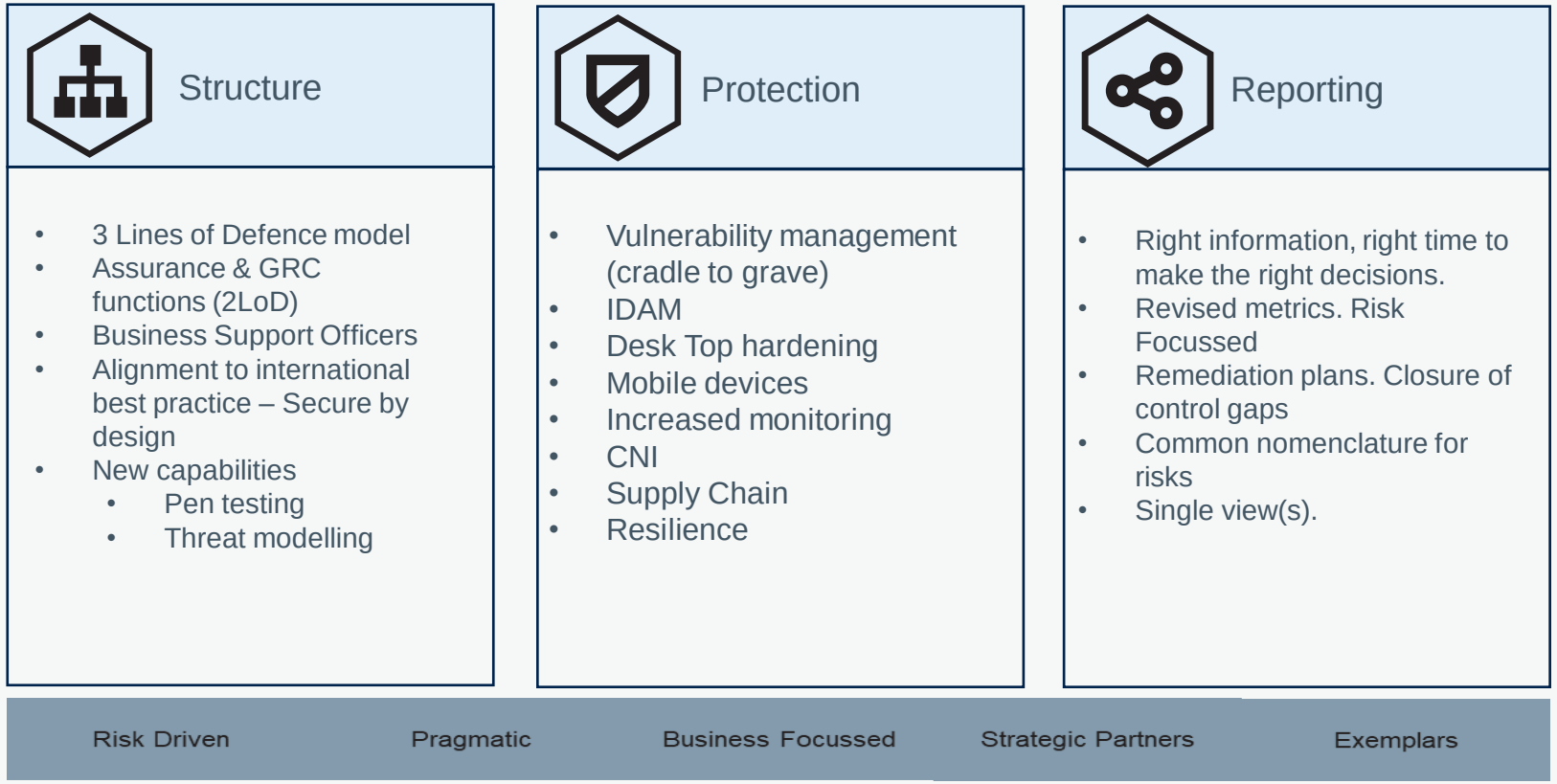
# CISO Risk Reduction Plan

# Transforming Cyber Security within NHSE

At NHS England, we have a diverse IT estate; many cloud instances, on prem and, of course, legacy. We also have a several development teams. We are a very big MS shop, complemented by large AWS and Splunk instances.

Cyber maturity can be patchy, but equally there are some areas of real excellence and high maturity.

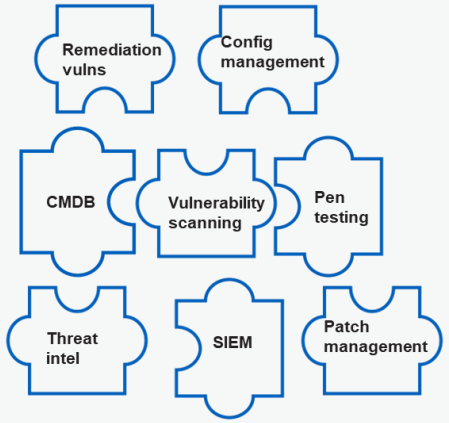
We have what is colloquially known as the CISO Risk Reduction Plan. Progress is Board reportable. Broadly speaking it has 3 pillars



# Vulnerability Management (VM) - Conception to Grave

Vulnerability management is a continuous, proactive, and often automated process that keeps systems, networks, and enterprise applications safe from cyberattacks and data breaches. It should be a continuous process to keep up with new and emerging threats and changing environments.

The goal is to reduce the organization's overall risk exposure by mitigating as many vulnerabilities as possible. However, for various reasons risk acceptance is not necessarily a bad answer.




There are several elements to good VM, it’s not just about patching. We have some pockets, green shoots, of this, but we need to broaden this out.
What I’m seeking to do is to piece together the jigsaw, ideally into one view & crucially into our development lifecycle. One of the first steps is continuous testing.
I’m looking for the developers to become security people, and for my 1.5 and 2 LoD teams to move towards “trust but verify”.

I appreciate this is not without its challenges and for us probably one of the biggest will be around cultural changes. We are about to start a continuous monitoring pilot with one of the dev teams. It may well prove unsuccessful, hopefully not, but regardless our intention is to learn, adjust and to implement it elsewhere

# Third Party Assurance

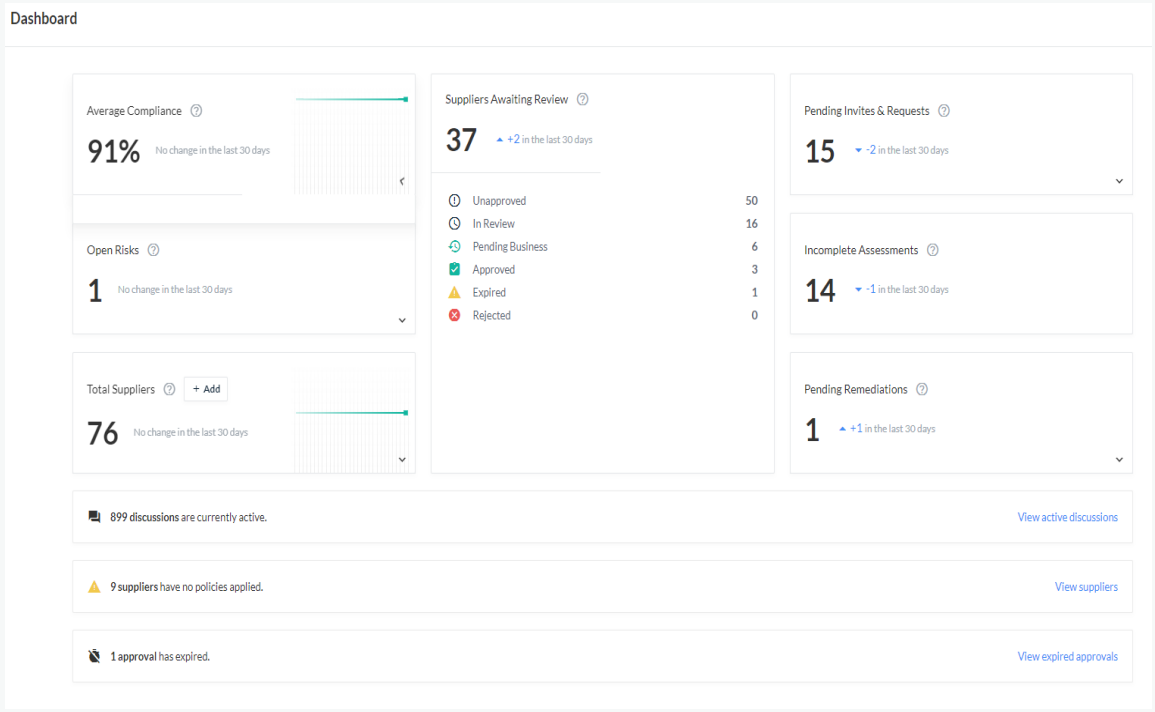
Our supply chain is large and complex and recent events have shown it to be vulnerable and a risk to us.

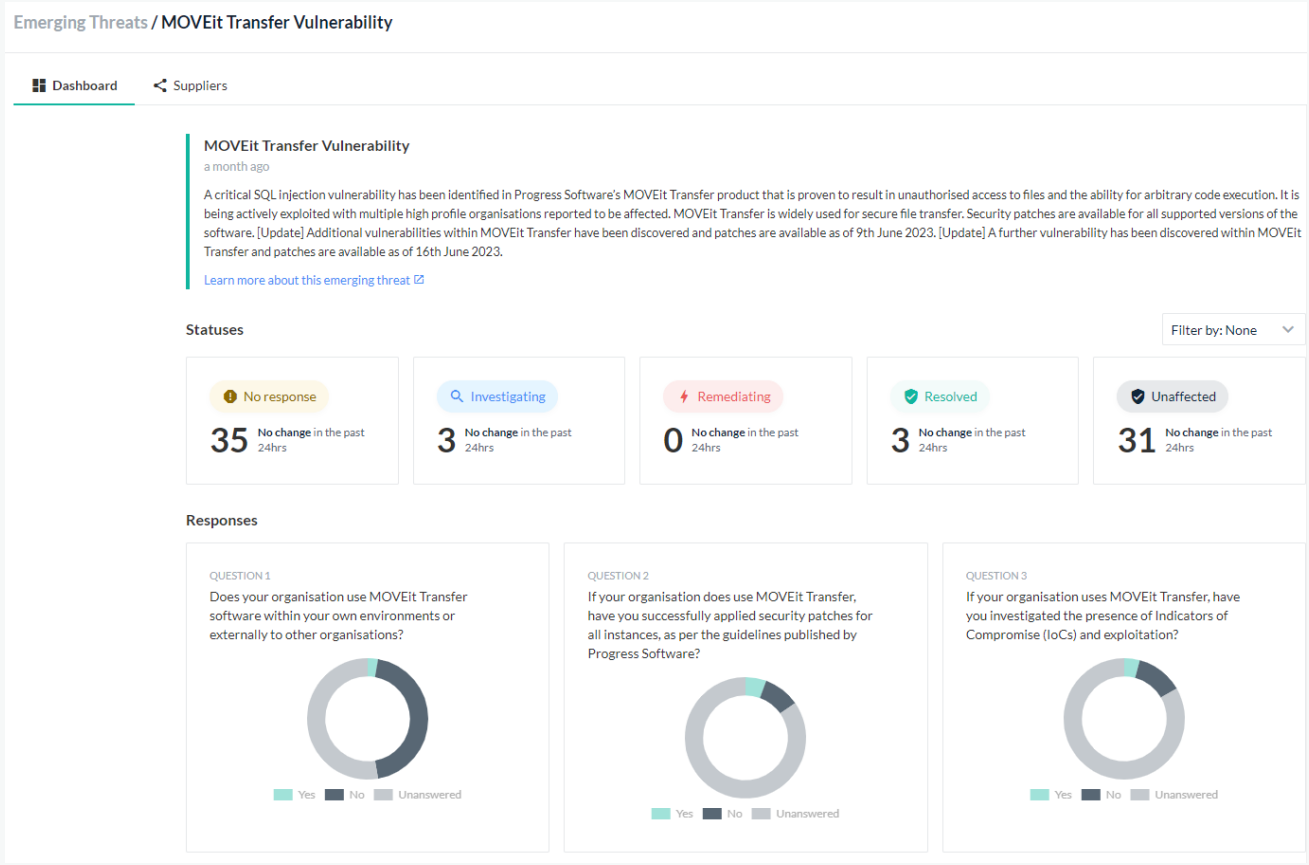
We want to address several issues:

- Ability to manage our supply chain holistically, throughout its ‘lifecycle’.
- Identify our concentration risks, our 4th, 5th party suppliers.
- Product assurance, not just vendor assurance.
- Real time, ongoing engagement with suppliers.
- A solution that works for us and the suppliers.

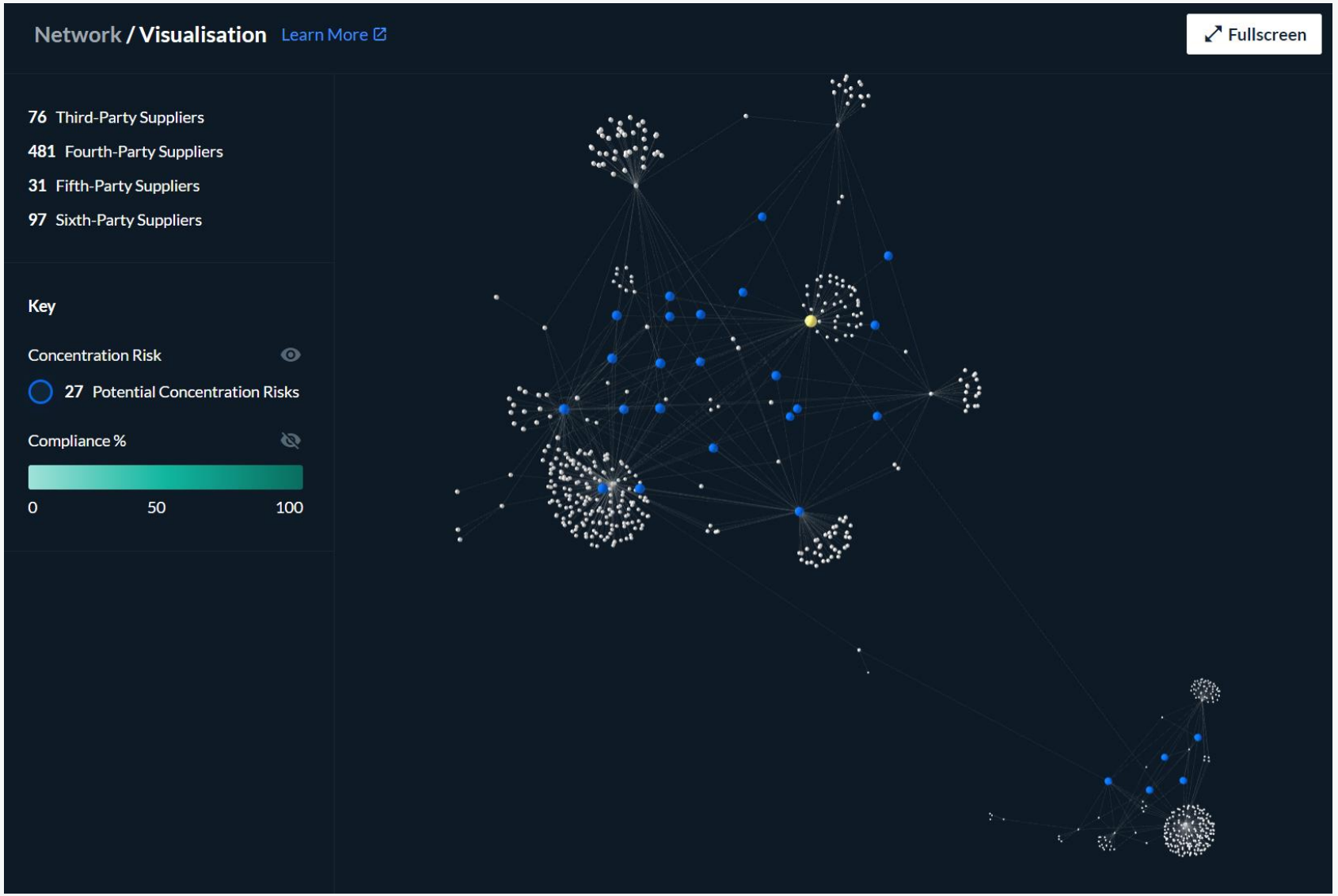
We recently conducted a small pilot (approx. 70 odd suppliers) to test these issues.

# Dashboard Screenshots



# Visualization of supply chain




Yellow dot is NHS England

Blue dots are potential concentration risks

The blue dots have a relationship with us, but they are potentially reliant on 4th, 5th etc parties.

# Visualization of supply chain


Once again, we are the yellow dot.

The Green dots are our suppliers.

Filters, Highly Conf and Holds PII, applied to show that there is a link between two unrelated suppliers holding our data.

This may prompt further investigation.

# Thank You

digital.nhs.uk

NHS England