International Collaboration

International Information Sharing Conference

Wednesday 1st November 2017

MalwareTech Retweeted

NCSC UK @ncsc · May 13

Finding the kill switch to stop the spread of ransomware bit.ly/2qDoW6r

21 716 847

MalwareTech @MalwareTechBlog · May 13

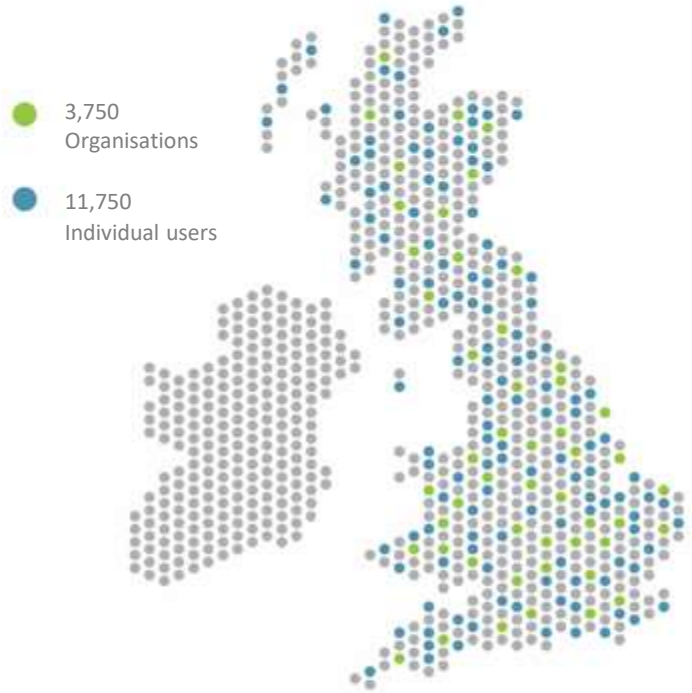
Well, that went about as well as anything i do does.

33 34 427

FACEBOOK FOR CYBER THREATS

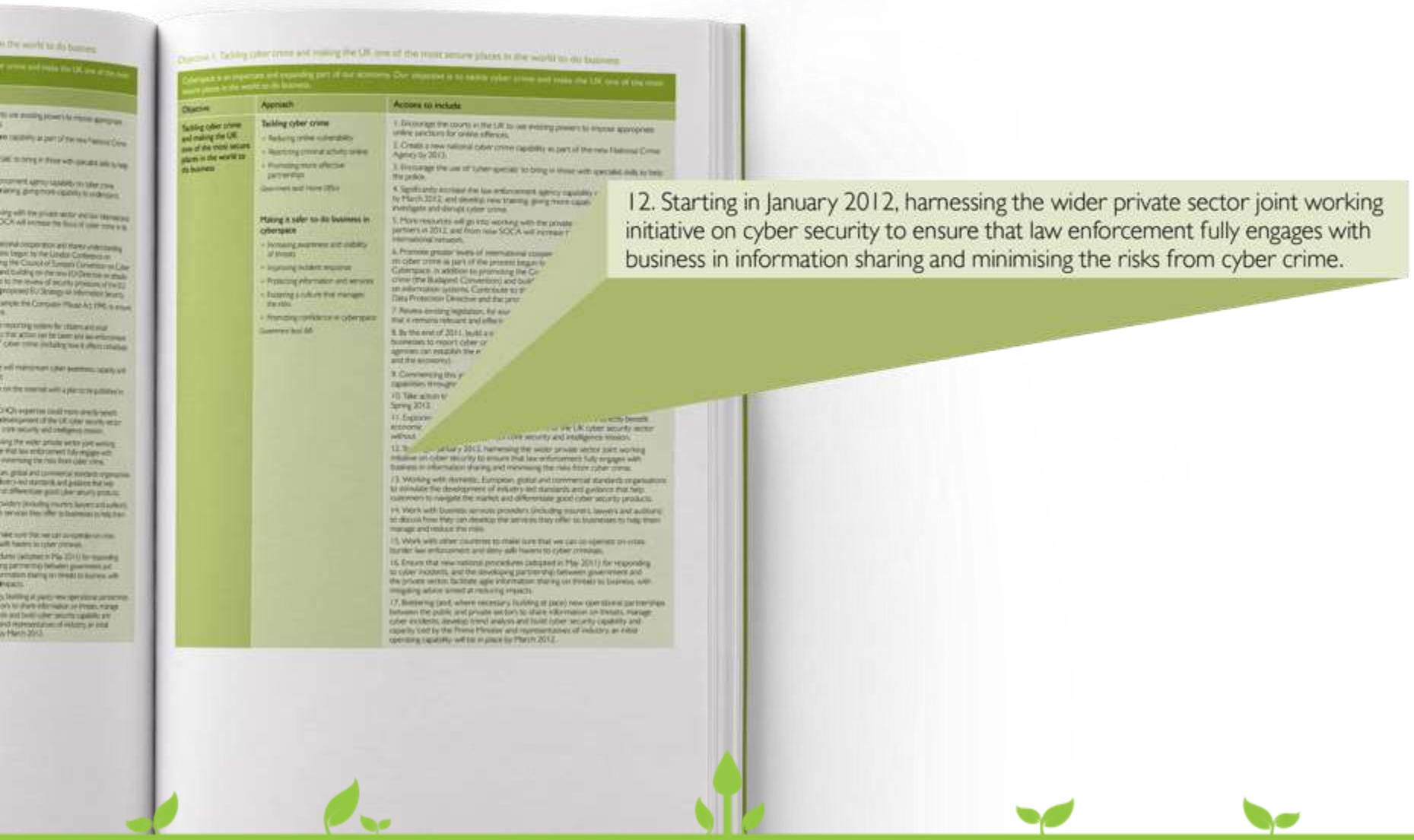
Proven success
With CiSP

Industry and
government work together



Across 25+ industry sectors

UK CYBER STRATEGY 2011-2016



NCSC RESPONSIBLE FOR CISP

Who we work for

The National Cyber Security Centre serves a wide range of UK organisations across the entire spectrum of cyber security issues.

Consequently the service provided will be multi-layered, reflecting the different threats that organisations face, and the skills and resources they have to address them. Owners of networks, systems and data will remain responsible for managing the risks to their organisations; the NCSC will not represent a change to this principle of risk-ownership.

We have defined four categories of engagement to describe the scope of our offer:

The NCSC will provide general advice & guidance. The NCSC will be the lead technical authority in the UK, with overall responsibility for the technical delivery of all cyber security advice issued by HMG. The NCSC will work closely with CPNI, Law Enforcement, DCMS and other partners to ensure these messages are delivered as effectively as possible.

For organisations that have their own networks, **the NCSC will run the Cyber Security Information Sharing Partnership (CiSP)**. This will enable organisations to share information with each other and the NCSC about what they are seeing on their networks, and provide a forum for discussion from beginner through to expert level.

We propose that **the N… tailored advice and… sectors, and pr… companies o…** that the NC… form th… UK, … re…

…ffer an enquiries line for the general public:

"Action Fraud will continue to be the first port of call for victims to report suspected cyber crime".

However, when there is a significant cyber incident affecting the UK, the NCSC will have the leading role for government in communicating to the public, to provide reassurance and guidance on what individuals and organisations can do to better protect themselves.

For organisations that have their own networks, **the NCSC will run the Cyber Security Information Sharing Partnership (CiSP)**. This will enable organisations to share information with each other and the NCSC about what they are seeing on their networks, and provide a forum for discussion from beginner through to expert level.

UK RESPONSIBILITY

National Cyber Security Centre
a part of GCHQ

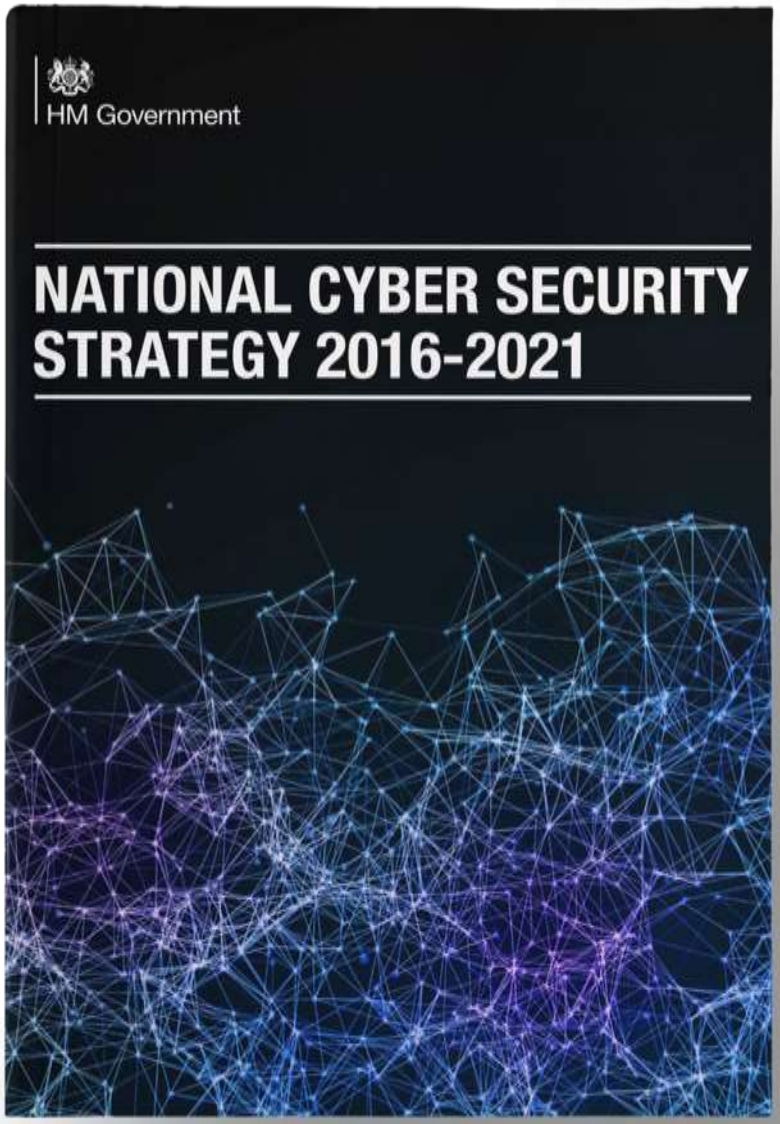
CPNI
Centre for the Protection of National Infrastructure

CERT-UK

CESG

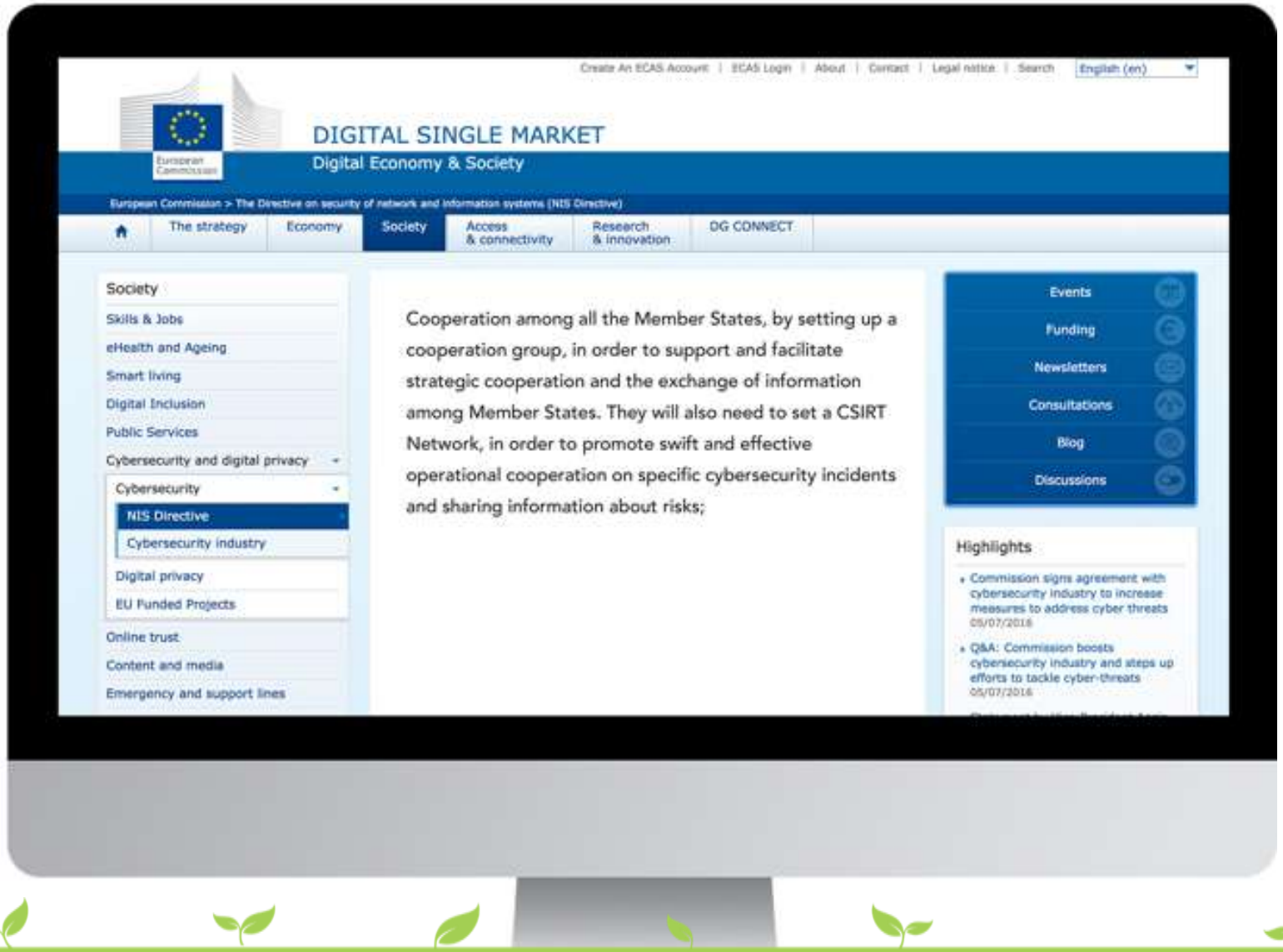
GovCertUK
COMPUTER EMERGENCY RESPONSE TEAM

SHARING IS STRATEGIC



SHARING IN THE US

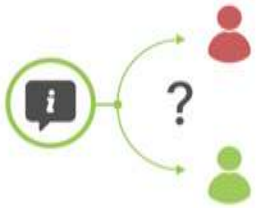
EUROPE NISD


Create An ECAS Account | ECAS Login | About | Contact | Legal notice | Search
English (en)
DIGITAL SINGLE MARKET
Digital Economy & Society
European Commission > The Directive on security of network and information systems (NIS Directive)
The strategy
Economy
Society
Access & connectivity
Research & innovation
DG CONNECT
Society
Skills & Jobs
eHealth and Ageing
Smart living
Digital Inclusion
Public Services
Cybersecurity and digital privacy
Cybersecurity
NIS Directive
Cybersecurity industry
Digital privacy
EU Funded Projects
Online trust
Content and media
Emergency and support lines
Cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among Member States. They will also need to set a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;
Events
Funding
Newsletters
Consultations
Blog
Discussions
Highlights
Commission signs agreement with cybersecurity industry to increase measures to address cyber threats
05/07/2016
Q&A: Commission boosts cybersecurity industry and steps up efforts to tackle cyber-threats
05/07/2016

DIB – MANDATORY SHARING

WHERE INFORMATION GOES TO DIE

CHALLENGES



NOT SURE WHO TO TRUST
WITH YOUR INFORMATION

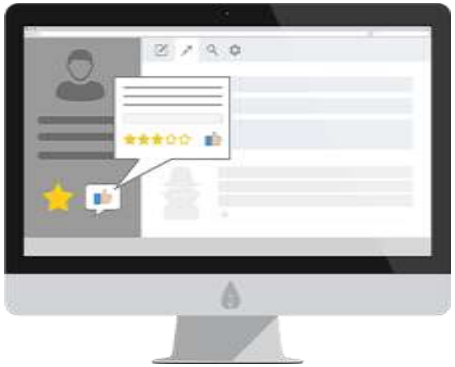
WAITING FOR OTHERS TO
SHARE PUBLICALLY IS SLOW

NO EASY WAY FOR THIS
INFORMATION TO BE SHARED

NOT SURE WHOSE
INFORMATION YOU CAN TRUST

PUBLIC DISCLOSURE DOES
NOT ALWAYS HAPPEN

FEATURES



COMMUNITY

ANONYMITY

INFORMATION HANDLING

INCIDENT REPORTING

SECURE PLATFORM MAINTAINED
BY TRUSTED PARTY

QUICK AND EFFICIENT SHARING
THROUGH STRUCTURED DATA

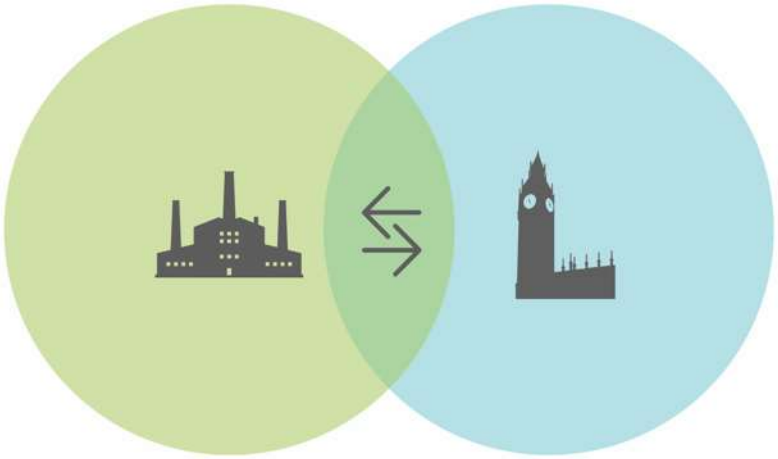
HOW?

USE INDUSTRY-RECOGNIZED TRAFFIC
LIGHT PROTOCOL
(TLP) TO CONTROL SHARING

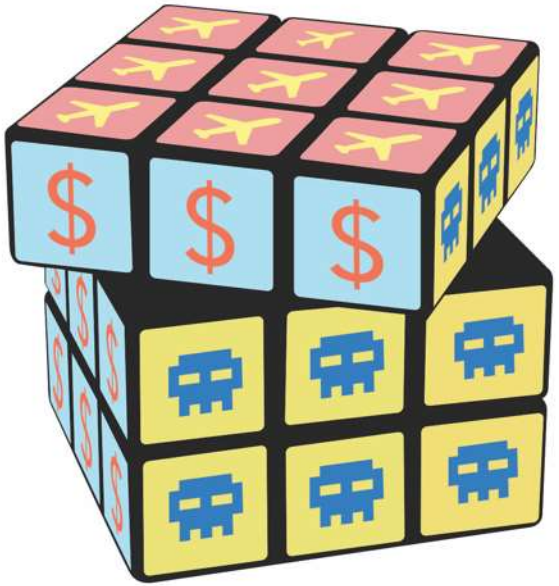
TERMS & CONDITIONS
THAT ALL MEMBERS
MUST AGREE TO

NEW MEMBERS ARE REVIEWED
BEFORE JOINING TO
MAINTAIN TRUST

OVERSIGHT…



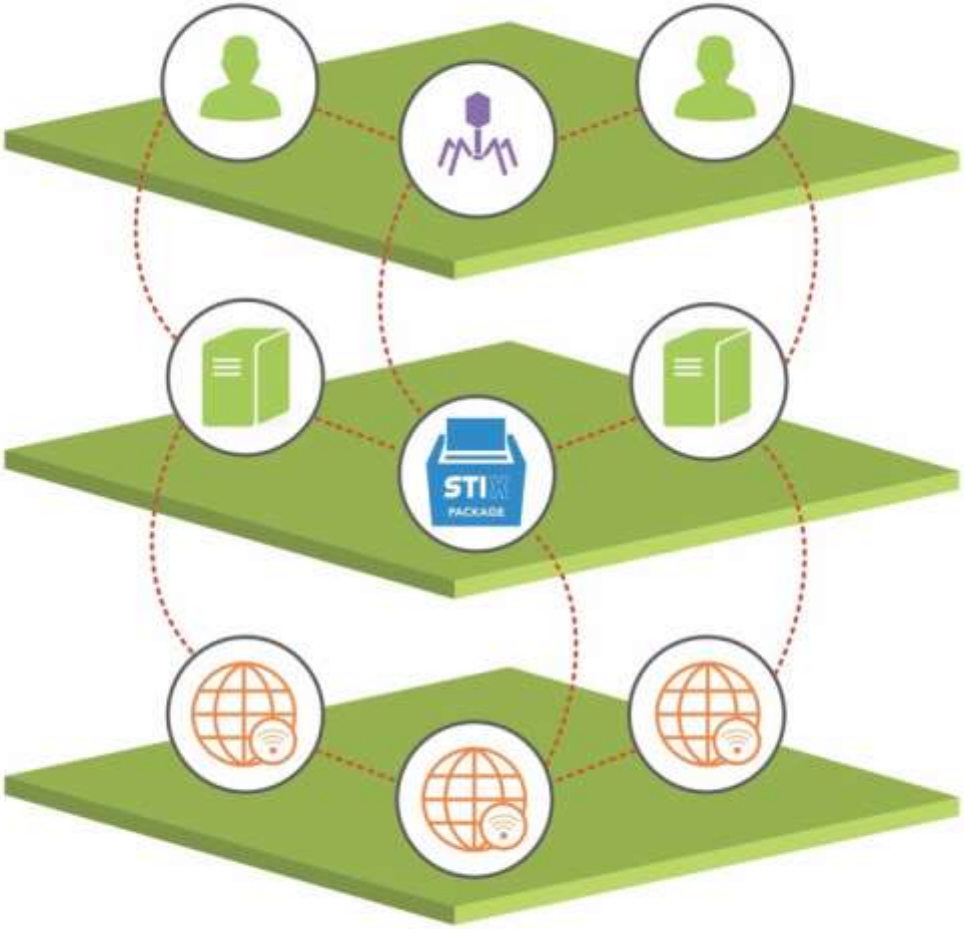
FUSION CELL



ANALYSE PATTERNS
ACROSS ALL SECTORS,
PROVIDE CONTEXT

GLOBAL DEMAND

SHARING GOES DEEP



GLOBAL ALLIANCES





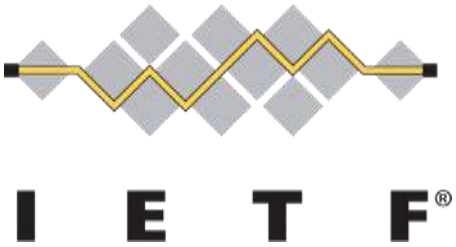

BORDERLESS OR SOVEREIGN?

HUB vs FEDERATION

- Centralised model - trusted authority
- National level collaboration
- Challenge: collaboration across boundaries

- Federated model
- Control who, what
- Protect data sovereignty

PLAY BY THE RULES



Secure Government and military communications nationally and trans-nationally

Secure Information Sharing

Cyber-security information sharing platform designed for secure cross-organisational **collaboration** and collaborative intelligence analysis.

Participate | Collaborate | Innovate