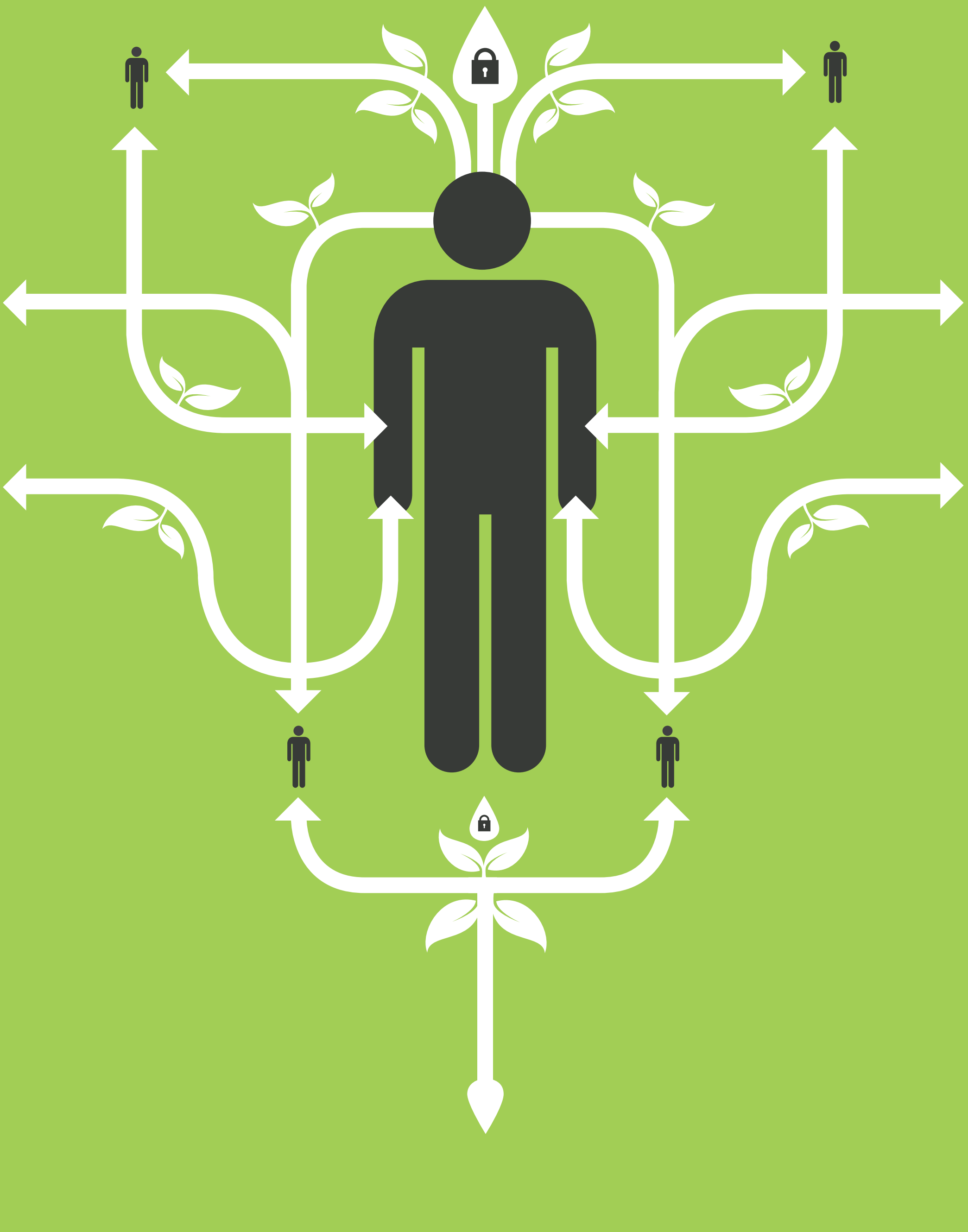
threatvine



Using Threatvine to meet your NISD obligations

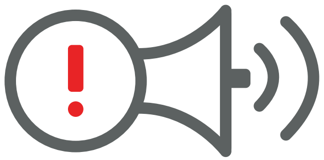
SUREVINE

THE DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS

The NIS Directive requires a CSIRT to be established for each member state, and for that CSIRT Network to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks[1].

Monitor incidents at a national level

Respond to incidents

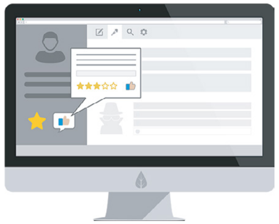


Provide early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents

Provide dynamic risk and incident analysis and situational awareness

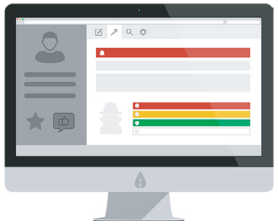
[1] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Threatvine is a cyber-security information sharing platform, designed especially for CSIRTs, to enable communication between them and their Competent Authorities; and to ensure resilience across the wider supply chain.



COOPERATION

Build a trusted network

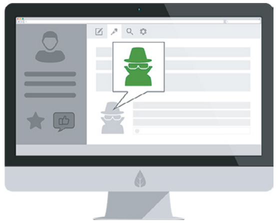


TRAFFIC LIGHT PROTOCOL

Protect your information, maintain control

INCIDENT NOTIFICATION

Swift and effective notification



ANONYMITY

Encourage sharing by preserving confidentiality

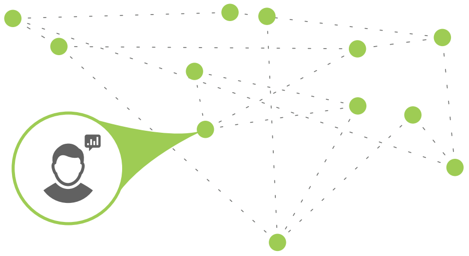
The UK National CSIRT (NCSC) uses Threatvine as it's national cyber-security information sharing platform.

National Cyber
Security Centre

DECENTRALISED APPROACH

Threatvine adapts to different models of sharing with the Competent Authorities.

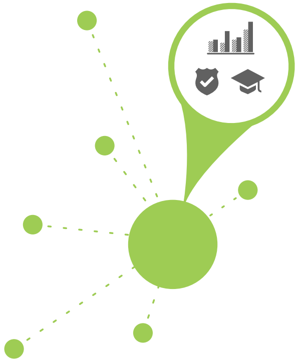
THREATVINE EXCHANGE



A federated platform where each participant retains control of their data and hosts their own "node". Each node is fully autonomous and able to function independently, with the benefit of being able to quickly and easily build up and break down connections with other nodes. Each connection therefore establishes a mutual agreement between nodes to share information.

CENTRALISED APPROACH

One central authority dealing with all sectors and services.



THREATVINE HUB

A national level platform, designed for cross-organisational, cross-sector sharing, powering National cyber strategies worldwide. Threatvine unites critical national infrastructure, law enforcement and academia, moving beyond cyber security information sharing to collaborative cyber security intelligence analysis; keeping you one step ahead of the cyber threat.

OPERATIONAL-TECHNICAL CAPABILITY

Threatvine was designed specifically for CSIRTs, ensuring you comply with the NIS Directive operational technical capabilities for Incident Response.

PROACTIVE APPROACH

Improve the infrastructure and security processes ... before any incident or event occurs or is detected. Prevent incidents and reduce their impact and scope when they do occur."

Threatvine provides or enables:

- ✓ Announcements
- ✓ Security-Related Information Dissemination

REACTIVE APPROACH

"Respond to requests for assistance, reports of incidents from the CSIRT constituency, and tackle threats or attacks against the CSIRT's systems."

Threatvine provides or enables:

- ✓ **Vulnerability Handling**
  - ✓ Vulnerability analysis
  - ✓ Vulnerability response
  - ✓ Vulnerability response coordination
- ✓ **Artefact Handling**
  - ✓ Artefact analysis
  - ✓ Artefact response
  - ✓ Artefact response coordination
- ✓ **Alerts and Warnings**
- ✓ **Incident Handling**
  - ✓ Incident analysis
  - ✓ Incident response support
  - ✓ Incident response coordination

Source:. https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation

SHARING IS STRATEGIC

HELP CREATE AND BE PART OF A TRUSTED COMMUNITY OF EXPERTS WORKING TOGETHER TO KEEP ONE STEP AHEAD OF THE CYBER THREAT.

A SINGLE ORGANISATION

May have good situational awareness of their network

Poor awareness of new, emerging threats

Expensive and time consuming to try and track it all individually

A COLLECTION OF ORGANISATIONS, A TRUSTED NETWORK

Share awareness from ALL networks/sectors

Focus on what is important

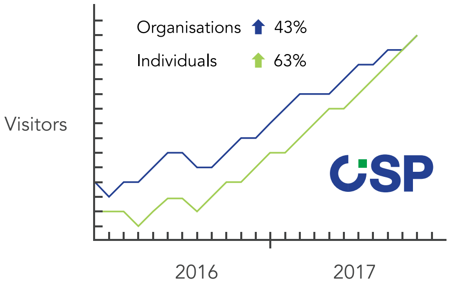
And how to protect against it

ANALYSE PATTERNS ACROSS ALL SECTORS, PROVIDE CONTEXT

Unite operators of essential services, moving beyond cyber-security information sharing to collaborative cyber-security intelligence analysis; keeping you one step ahead of the cyber threat.

SECURE INFORMATION SHARING

CiSP, powered by Threatvine, is the UK's National Cyber-security Information Sharing platform; providing a confidential environment where threat information can be quickly and securely exchanged. CiSP is a joint initiative between government and industry.



Membership from organisations across 30 different sectors.

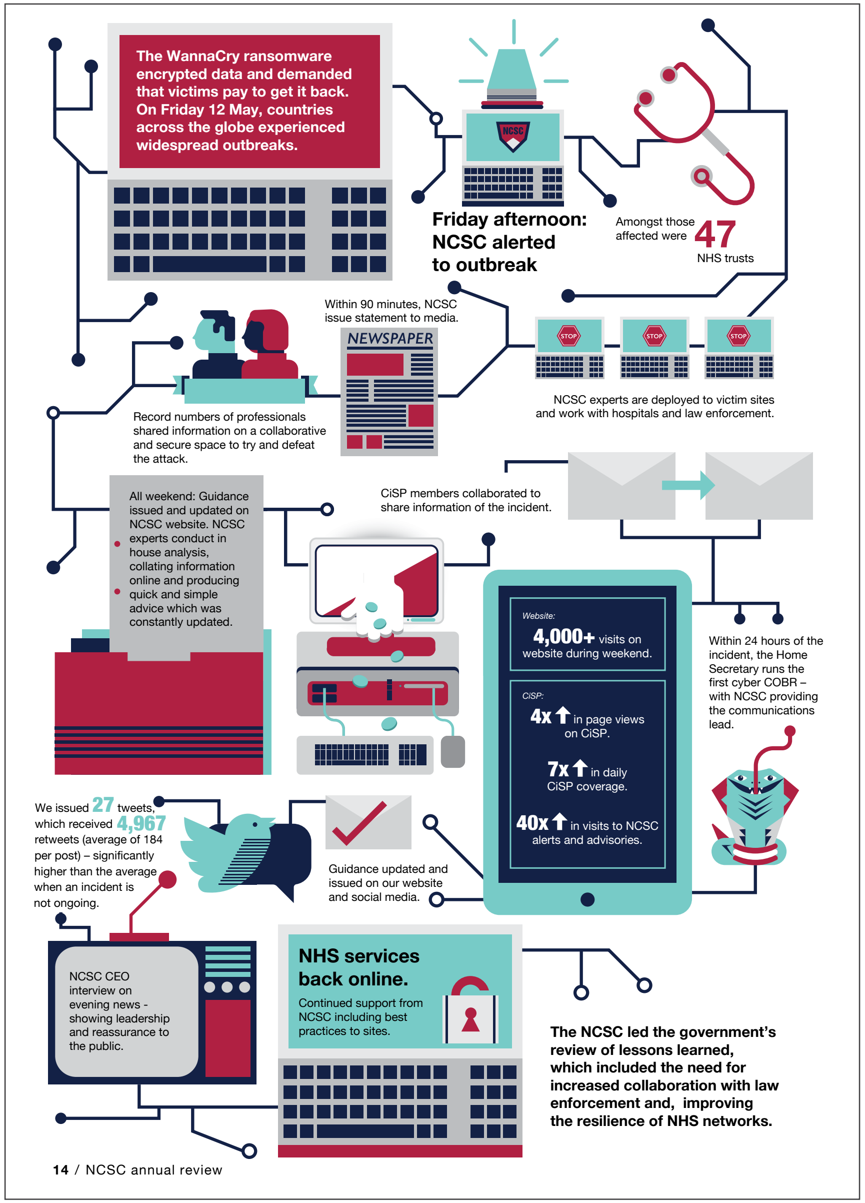
NCSC regularly publishes threat reports, advice and guidance to CiSP, produced with industry partners.

1,131 incident reports created by the community within last 12 months. 590 classed as 'significant'

> *"[The NCSC is] bringing together some of the best cyber security brains in the country in a single place [1]"*

CIARAN MARTIN

CEO OF THE NCSC



The WannaCry ransomware encrypted data and demanded that victims pay to get it back. On Friday 12 May, countries across the globe experienced widespread outbreaks.

Friday afternoon: NCSC alerted to outbreak

Amongst those affected were 47 NHS trusts

Within 90 minutes, NCSC issue statement to media.

Record numbers of professionals shared information on a collaborative and secure space to try and defeat the attack.

NCSC experts are deployed to victim sites and work with hospitals and law enforcement.

All weekend: Guidance issued and updated on NCSC website. NCSC experts conduct in house analysis, collating information online and producing quick and simple advice which was constantly updated.

CiSP members collaborated to share information of the incident.

Website:
4,000+ visits on website during weekend.

CiSP:
4x ↑ in page views on CiSP.
7x ↑ in daily CiSP coverage.
40x ↑ in visits to NCSC alerts and advisories.

Within 24 hours of the incident, the Home Secretary runs the first cyber COBR – with NCSC providing the communications lead.

We issued 27 tweets, which received 4,967 retweets (average of 184 per post) – significantly higher than the average when an incident is not ongoing.

Guidance updated and issued on our website and social media.

NCSC CEO interview on evening news - showing leadership and reassurance to the public.

NHS services back online.
Continued support from NCSC including best practices to sites.

The NCSC led the government's review of lessons learned, which included the need for increased collaboration with law enforcement and, improving the resilience of NHS networks.

14 / NCSC annual review

NCSC 2017 Annual Review, p14

The recent "Wannacry" ransomware attack affected more than 300,000 private and public sector computers across the globe, all in a matter of hours. The attack spread quickly and the effect was felt deeply;" but the response within the UK was uniquely coordinated.

By now we all know the story of @MalwareTechBlog. But did you know his day started with a routine check on CiSP, the UK's cyber threat sharing platform, powered by Threatvine?

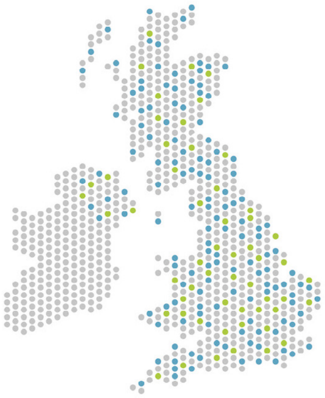
MalwareTech logged in to follow up on an existing malware issue he was following, and found the platform "flooded with posts about various NHS systems all across the country being hit, which was what tipped [him] off to the fact this was something big."

The CiSP community had very quickly rallied around the threat to UK infrastructure, and were sharing openly, honestly, and quickly. And the sharing was happening across a wide range of content; from Twitter links to Indicators of Compromise, such as IP addresses and sample hashes.

Collaborative analysis by CiSP members allowed for accurate, speedy debunking of rumour, and quickly honed in on the detail of the attack. Mitigation advice was provided by the community, for the community. Cross-sector collaboration was the norm; and the advice provided by the community was rapidly picked up by other sectors and businesses not yet affected.

"CiSP has proven to be an extremely valuable resource during large-scale cyber incidents. Following the WannaCry ransomware outbreak there were more than 23,000 visitors to the online platform, including 15,000 during the first weekend. CiSP was invaluable, providing up to the minute mitigation advice whilst also debunking false rumours."

NCSC 2017 Annual review



● 3,750 organisations ● 11,750 individual users

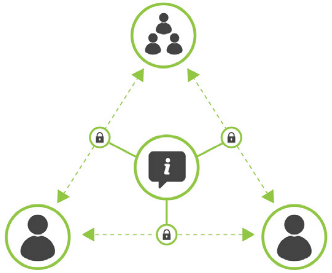
Immensely disruptive, fast-paced incidents like the "WannaCry" outbreak require a similarly fast-paced, **coordinated** response. The response to any incident will rely on individuals with unique insight, skills, and capabilities - and it's only through collaboration that we can truly tap in to that for our common benefit.

Threatvine, designed especially for cyber-threat information sharing, powers this collaboration.

SUREVINE

WHY SUREVINE

Surevine builds secure, scalable collaboration environments for the most security conscious organisations; joining people up and enabling collaboration on their most highly sensitive information.



LEADERS IN SECURE COLLABORATION SOLUTIONS

KEY SUPPLIER TO UK GOVERNMENT AND INDUSTRY

WHO WE WORK WITH

Foreign & Commonwealth Office

Ministry of Defence

Home Office

EUROPOL

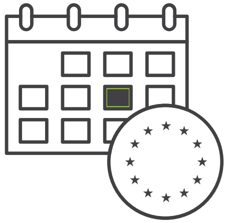
NATO OTAN

HOUSE OF COMMONS

NEXT STEPS

Help create and be part of a community of experts working together to keep one step ahead of the cyber threat.

ENSURE YOU ARE PREPARED FOR EU MEMBER STATES DEADLINE: 9TH MAY 2018



The Cybersecurity Digital Service Infrastructures (DSI) programme of the Connecting Europe Facility (CEF) can provide significant EU funding in assisting Member State CSIRTs to improve their capabilities.

EUROPEAN COMMISSION

Book a demo, arrange a scenario-based exercise or simply find out more about our smart collaboration technology

WWW.SUREVINE.COM/THREATVINE

threatvine

info@threatvine.com | www.surevine.com/threatvine | +44 845 468 1066