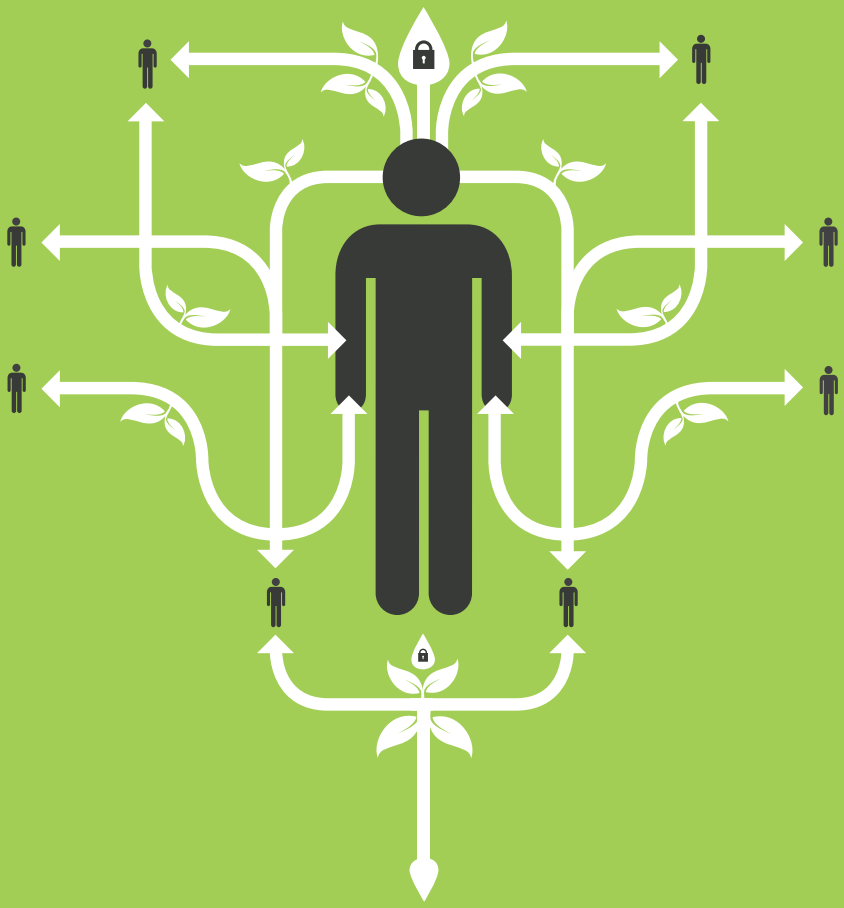
threatvine

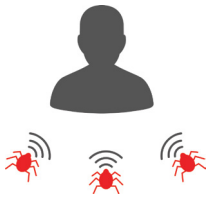


SECURE INCIDENT NOTIFICATION
FOR NATIONAL CERTS

SURFVINE

SHARING IS STRATEGIC

The sharing of cyber threat intelligence is no longer optional; for many countries it is now the core of their National Cyber Security Strategy.



A SINGLE ORGANISATION

May have good situational awareness of their network

Poor awareness of new, emerging threats

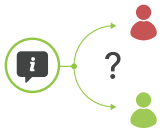
Expensive and time consuming to try and track it all individually

A COLLECTION OF ORGANISATIONS, A TRUSTED NETWORK

*Share awareness from **ALL** networks/sectors*

Focus on what is important

And how to protect against it



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

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 felt deeply; but the response within the UK was uniquely coordinated.

By now we all know the story of @MalwareTechBlog; a modern day hero. 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. CiSP's intuitive security labelling of information, a key feature of the platform that utilises the industry standard Traffic Light Protocol (TLP), allowed each participant to control how far their information was shared.

"Here are some details about our current response to this incident - TLP AMBER"

"This is TLP WHITE - so feel free to share with others, and publicly"

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

3,000 Organisations 8,000 Individual users

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. In a statement released by NCSC they highlighted that "private sector efforts have made a very significant contribution to mitigate the cyber attacks".

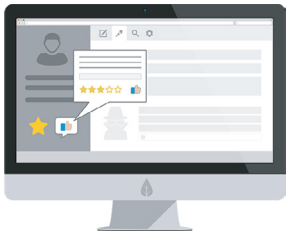
Immensely disruptive, fast-paced incidents like the "WannaCry" outbreak require a similarly fast-paced, **coordinated** response. The response to any incident will rely on individuals with unique insight, skills, and capabilities - and it's only through collaboration that we can truly tap in to that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

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

threatvine

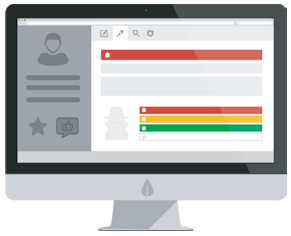
DESIGNED FOR NATIONAL CERTS

Cyber-security information sharing platform designed for cross-sector cooperation and incident notification for CERTs, CSIRTs, NCSCs and National competent authorities.



COOPERATION

Build a trusted network



TRAFFIC LIGHT PROTOCOL

Protect your information, respect your security

INCIDENT NOTIFICATION

Swift and effective notification through open standards

ANONYMITY

Exchange best practice and preserve confidentiality

“Secure Facebook for cyber threats”

FINANCIAL TIMES

ANALYSE PATTERNS ACROSS ALL SECTORS, PROVIDE CONTEXT

Unite 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.

BENEFITS

- A key enabler of a National cyber security strategy
- Designed for National CSIRTs and competent authorities
- Specifically built for cyber-security incident reporting
- Secure cross-sector cooperation on incidents and threats
- Maintain real-time situational awareness
- Help operators of essential services to defend themselves against threats
- Incident notification which complies with the NIS Directive

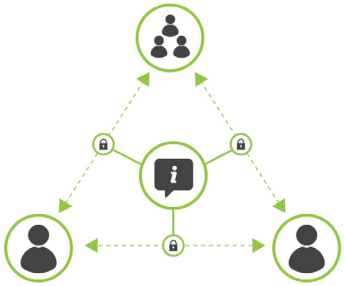
Private nodes
for each essential service

Open nodes
for cross-sector exchange

Focused nodes
for specific events, such as sporting events

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

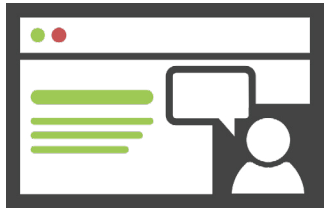
'ONE OF THE TOP UK CYBER COMPANIES'

"One of the UK's leading cyber security companies"

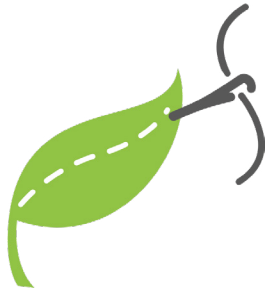
DAVID CAMERON
Former British Prime Minister

NEXT STEPS

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



DEMO ENVIRONMENT AVAILABLE TO
TRIAL/TEST/EVALUATE



OTHER TRIAL ARRANGEMENTS
CAN BE MADE

CURRENTLY HOSTED TRIAL ENVIRONMENT CLOUD HOSTED
Do not add sensitive data

Book a demo, start your FREE trial or simply find out more about our smart collaboration technology

WWW.SUREVINE.COM/THREATVINE

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