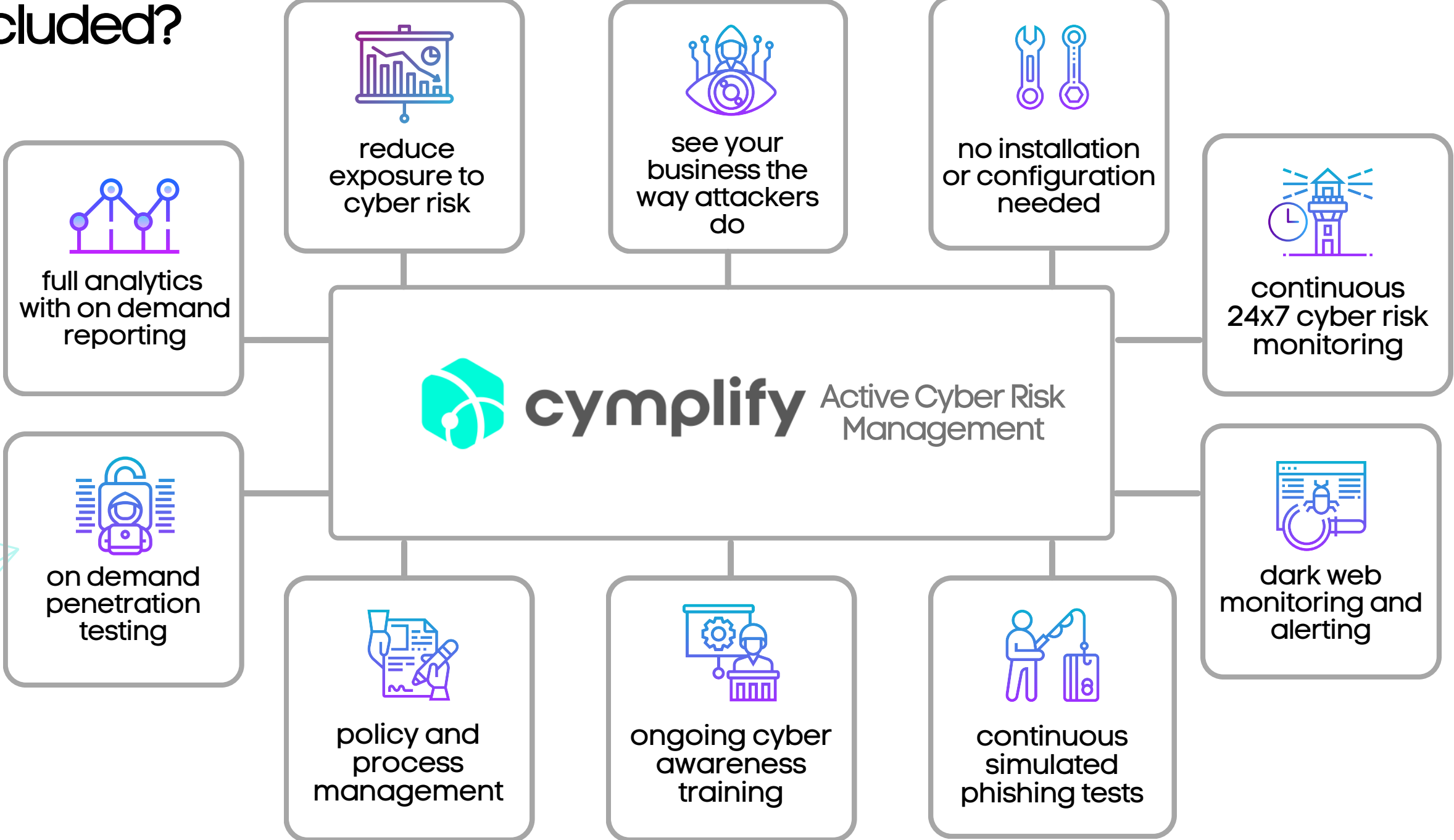


cymplify


Active Cyber Risk Management Platform
Overview



What is included?



Current Cyber Risk Exposure Report



Executive Summary

Target >> eXample™

Overview


This report is intended to provide a high level 'Red Flag' report to the target organisation on their current Visible Cyber Risk Exposure. The report provides insight into several key areas of Cyber Risk so that the target organisation can better understand their current exposure, their 'Attack Surface' and serve as the basis for further actions. To compile this Report, investigations and reconnaissance have been carried out to ascertain the current state of Visible Cyber Risk and determine a current 'Attacker View' of the Target organisation.

Example - Current Cyber Risk Exposure


Low

eXample™


Severe




Ransomware




Exposure has been identified




Open Access



Exposure has been identified



Dark Web



Exposure has been identified



Cyber Risk Exposure

Target >> eXample™

Ransomware

Database exposed & directly visible

Example Co - A MySQL database is currently using port 3306 on IP address 195.224.xxxx. This is an open port which is directly visible and accessible from the Internet. At worst this may expose sensitive information directly to the Internet, at best it elevates the risk of sustained efforts to compromise your systems, and we recommend this is urgently addressed.

- Ransomware
- Malware
- Public/unsecured assets
- Control of assets

Open Access

Remote Desktop Protocol **visible and accessible from the Internet.**

When remote desktop services are visible to the Internet, hackers are able to identify services with vulnerabilities which they will then exploit. Having a visible remote desktop makes an organisation **extremely vulnerable** to cyber attack and service failure, we recommend this is urgently addressed.

- Public/unsecured assets
- Control of assets
- Ransomware
- Security

Dark Web

Dark Web Breach Exposure

This report identifies breached credentials from users with email addresses under the mail domain '@exampleco.com'.

These credentials are obtained from websites, databases and various online services that have been breached, likely due to either a technical vulnerability or social engineering attack.

- 6 Compromised Accounts **3,413**
- *** Passwords Leaked **3,128**
- b Data Items Leaked **915**



Cyber Risk Exposure

Target >> eXample™

What to do next - Top 3 Issues to Address

1

Close Public Access to Database Services

Why is this important?
There are **1x** SQL Databases open to the public, allowing others to control assets or install malware / ransomware. Even if these databases are protected by passwords, open access allows attackers to easily launch their attacks and gain entry into these systems. Databases should be protected behind firewalls and access restricted to internal networks to prevent attackers gaining access to Example Co's internal and customer data.

2

Close RDP Access to your Infrastructure

Why is this important?
There are **2x** Remote Desktop Protocol (RDP) services open to the public. RDP is commonly exploited to deploy ransomware and steal data, making Example Co extremely vulnerable to these types of attacks. RDP services should be protected behind firewalls and restricted to internal networks. Additionally, RDP access should only be granted to Example Co systems and accounts where absolutely necessary, and multi-factor authentication (MFA) should be required in these limited cases.

3

Implement Email Policies

Why is this important?
@exampleco.com does not have a DMARC policy to prevent spoofed emails from being delivered that appear to be legitimately sent from your business. Even if you have inbound mail protection solutions, these will not prevent criminals from sending spoofed outbound emails to your clients, suppliers and other vital business contacts. This puts Example Co at significant risk of Financial Loss due to Business Email Compromise, which can lead to issues like payment of fraudulent invoices or unauthorised payments being made which you could be liable for.

Example Dashboards

Active Cyber Risk Management Platform



Home
Cyber Risk
Dark Web
Penetration Testing
Cyber Training
Phishing Simulator
Policy Hub
Cyber Insurance
Report Generator

Cyber Risk Exposure

Top 3 Critical Risks

- 1 Close public TeamViewer access to your organisation
- 2 Close public access to database services
- 3 Close all developer access on external services

Dark Web Exposure

Penetration Test Data

Access Test Report

Cyber Awareness

Compliance Hub

Home
Cyber Risk
Dark Web
Penetration Testing
Cyber Training
Phishing Simulator
Policy Hub
Cyber Insurance
Report Generator

Current Cyber Risk

13 36

Top 3 Critical Risks

- 1 Close public TeamViewer access to your organisation
- 2 Close public access to database services
- 3 Close all developer access on external services

Service Locations

We have identified the locations your internet services are running from so you can check there are no surprises

Visible Services

These are your visible, internet facing services that we are able to see your business is running online

Domain Discovery

These are the domains that have been associated with your organisation. Click the dropdown for further details or the button below for a full list.

Full List of Domains

- aacmexample.co.uk
- aacme.co.uk
- aacmcp.com

Data Breach Risk

Be alerted to any unauthorised access or breach of your sensitive databases, helping you respond quicker to incidents and comply with standards like GDPR, CPPA etc.

Synthetic ID's

Home
Cyber Risk
Dark Web
Penetration Testing
Cyber Training
Phishing Simulator
Policy Hub
Cyber Insurance
Report Generator

Report Generator

Generate a variety of Reports to visualise and understand your Organisation's Cyber Risk Exposure, what to do about it, and see how your Active Cyber Risk Management Programme is helping to reduce your Organisation's exposure to Cyber Risk over time

Executive Summary

An Overview Report detailing the Top 5 Issues exposing your Organisation to Cyber Risk right now

Create Report

Attacker View Report

A detailed Report to help you understand how Attackers can view your Organisation right now

Create Report

Risk Reduction Report

A Report to help show you how your Organisation's exposure to Cyber Risk has changed over time

Create Report

Cyber Risk Report

Create Report

Dark Web Report

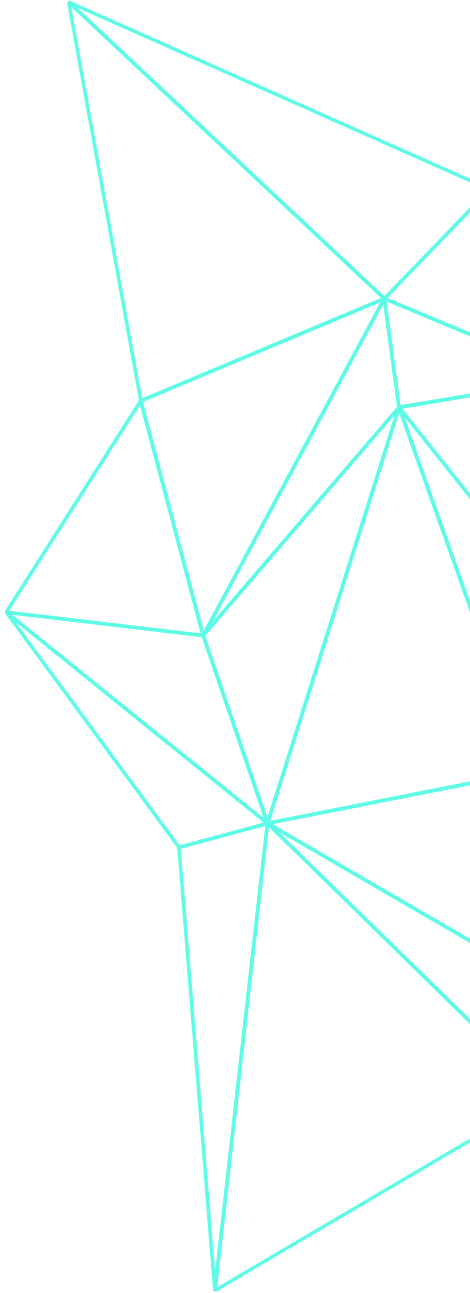
Create Report

Cyber Training Report

Create Report

Policy & Process Report

Create Report



Real Time Cyber Risk Exposure Visibility and Control



Immediate visibility of a wide range of Cyber Risk Insights

The dashboard shows a current cyber risk score of 13 out of 36. The top 3 critical risks are: 1. Close public TeamViewer access to your organisation, 2. Close public access to database services, and 3. Close all developer access on external services. Service locations are shown on a world map, and domain discovery lists domains like aacmexample.co.uk, aacme.co.uk, and aacmpp.com.

Uncover and understand High Risk Issues - what they are, where they are and what to do

The dashboard displays a grid of risk issues. Each issue card includes a title, a brief description, and a 'READ MORE' link. Issues include 'Vulnerable services', 'Email spoofing policy', and 'Email sender protection'.

Drill down into each specific issue for full details, description of potential impacts and advice on how to fix it

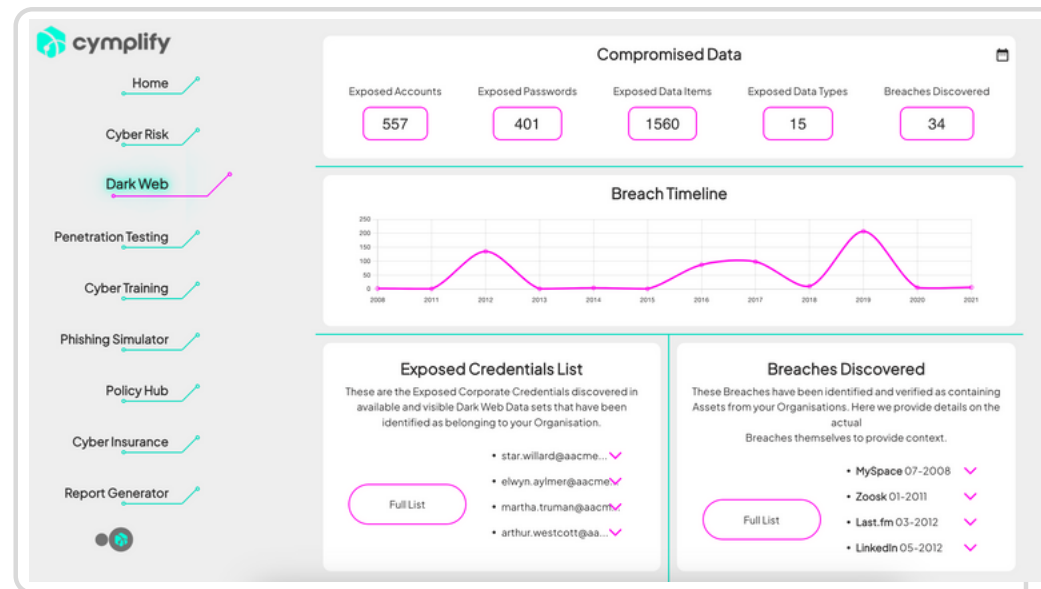
The detailed view for 'Vulnerable services' describes an OpenSSH 8.2p1 Ubuntu-4ubuntu0.3 vulnerability on port 22 at IP 174.55.115.128. It provides instructions on how to resolve the issue by updating the software to the latest version.

+ Email Alerts when new Exposures are detected

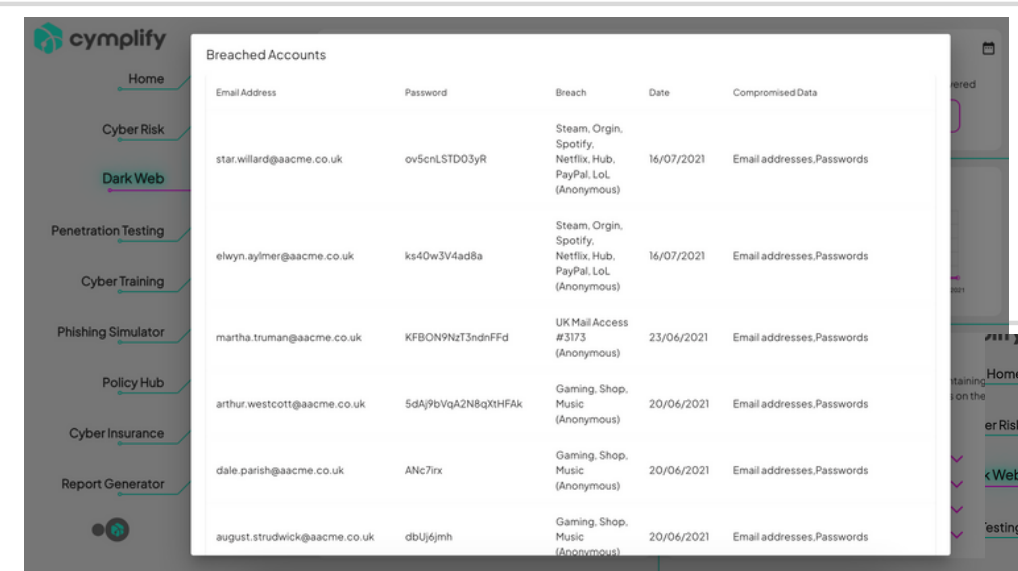
The email alert is titled 'Subject: New Cyber Risk Discovered' and features a red 'Alert!' button. The main content states: 'Cymplify has detected the following new Cyber Risk: Out of date software. Microsoft IIS httpd 10.0 is an older version of this product. This service is using port 80 on IP address 52.97.202.120. Newer versions of products become available to ensure any bugs or vulnerabilities are fixed to maintain maximum security. The older the version, the more vulnerabilities it is likely to have. Older versions of services are less well-supported by the developer, making an organisation more vulnerable to cyber attacks and service failure. What should you do? To maintain optimum security and prevent cyber attacks, a more recent version of this product may be preferable. Refer to the Microsoft IIS httpd website for more detail. Additionally, we're always happy to have a chat to explain any additional queries you have, or to walk you through the required steps. Please log in to the Cymplify platform for more information.'

Dark Web Breach Exposure Visibility and Insight

Immediate visibility of all Corporate Credentials exposed in existing Breach Data on the Dark Web

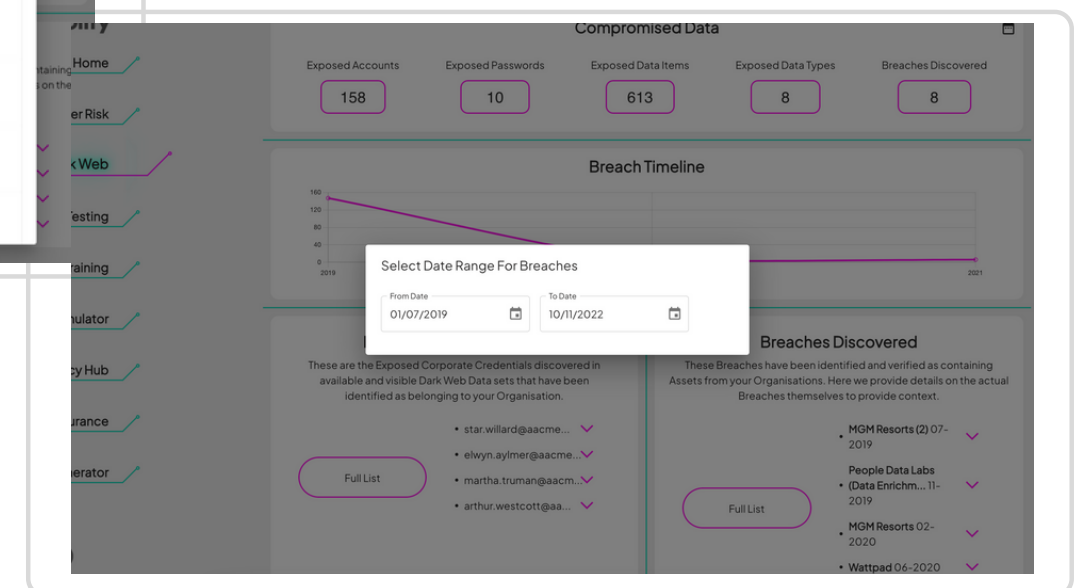


Drill down into your exposure in Dark Web Breach Data - including exposed credentials, passwords, the specific breaches you have been involved in and details of over 100 different Data types

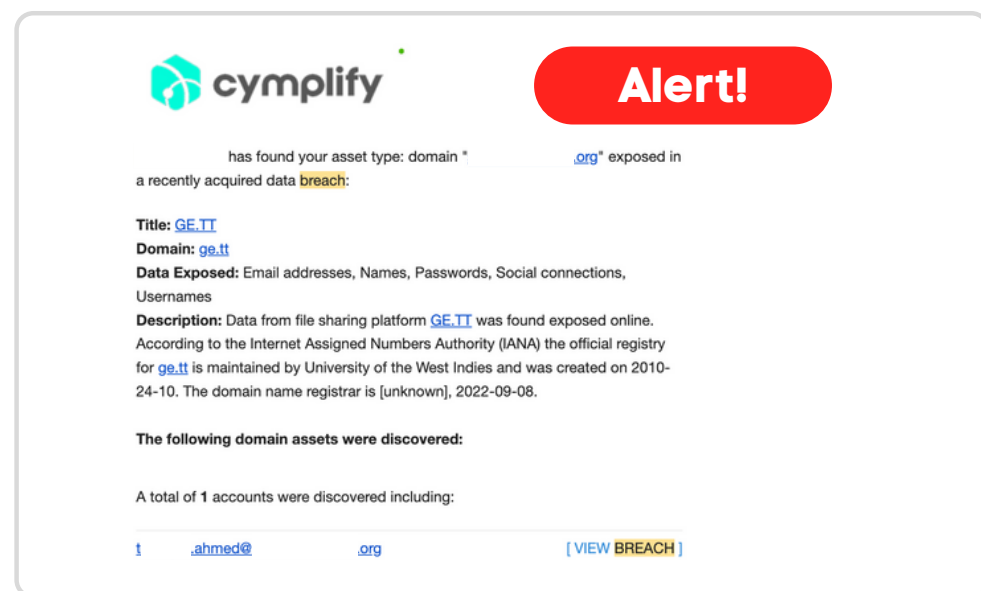


Email Address	Password	Breach	Date	Compromised Data
star.willard@aacme.co.uk	ov5cnLSTD03yR	Steam, Origin, Spotify, Netflix, Hub, PayPal, LOL, (Anonymous)	16/07/2021	Email addresses, Passwords
elwyn.aymer@aacme.co.uk	ks40w3V4ad8a	Steam, Origin, Spotify, Netflix, Hub, PayPal, LOL, (Anonymous)	16/07/2021	Email addresses, Passwords
martha.truman@aacme.co.uk	KFBON9NzT3dnrFfd	UK Mail Access #3173 (Anonymous)	23/06/2021	Email addresses, Passwords
arthur.westcott@aacme.co.uk	SdA9bvQvA2N8qXHfAK	Gaming, Shop, Music (Anonymous)	20/06/2021	Email addresses, Passwords
dale.parish@aacme.co.uk	ANc7ix	Gaming, Shop, Music (Anonymous)	20/06/2021	Email addresses, Passwords
august.studwick@aacme.co.uk	dbUj6jmh	Gaming, Shop, Music (Anonymous)	20/06/2021	Email addresses, Passwords

Refine date range on Breach Exposure information - to see all, some or most recent exposure - or exposure during a specific time period



+ Email Alerts when new Breach Exposure is detected



Alert!

has found your asset type: domain *.org* exposed in a recently acquired data breach:

Title: GE.TI
Domain: ge.tt
Data Exposed: Email addresses, Names, Passwords, Social connections, Usernames
Description: Data from file sharing platform GE.TI was found exposed online. According to the Internet Assigned Numbers Authority (IANA) the official registry for ge.tt is maintained by University of the West Indies and was created on 2010-24-10. The domain name registrar is [unknown], 2022-09-08.

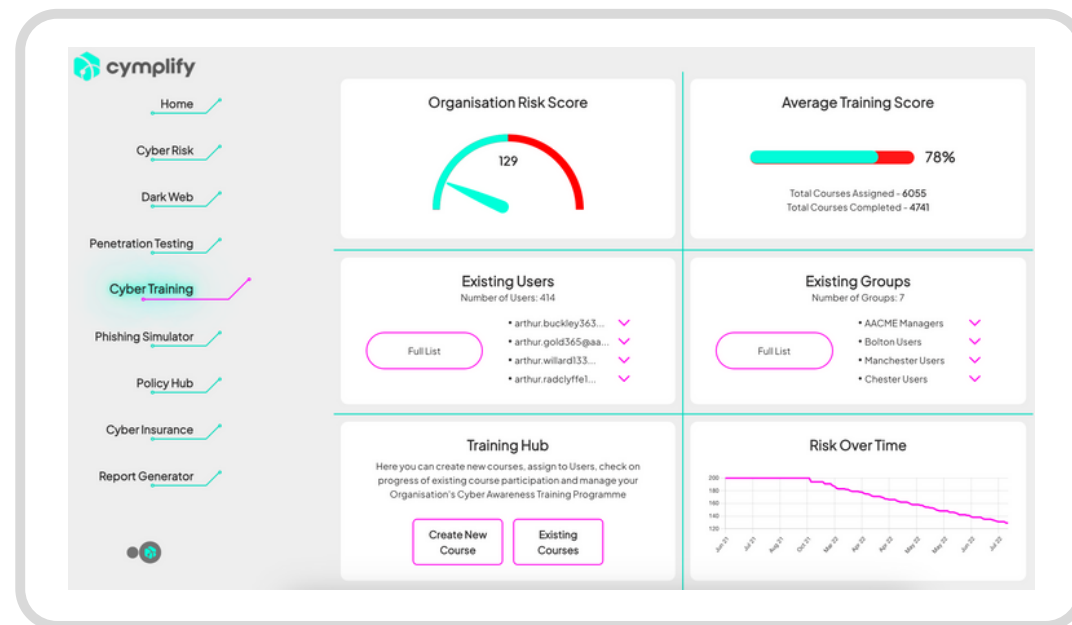
The following domain assets were discovered:

A total of 1 accounts were discovered including:

t .ahmed@ .org [VIEW BREACH]

Ongoing Cyber Awareness Training & Simulated Phishing Programmes

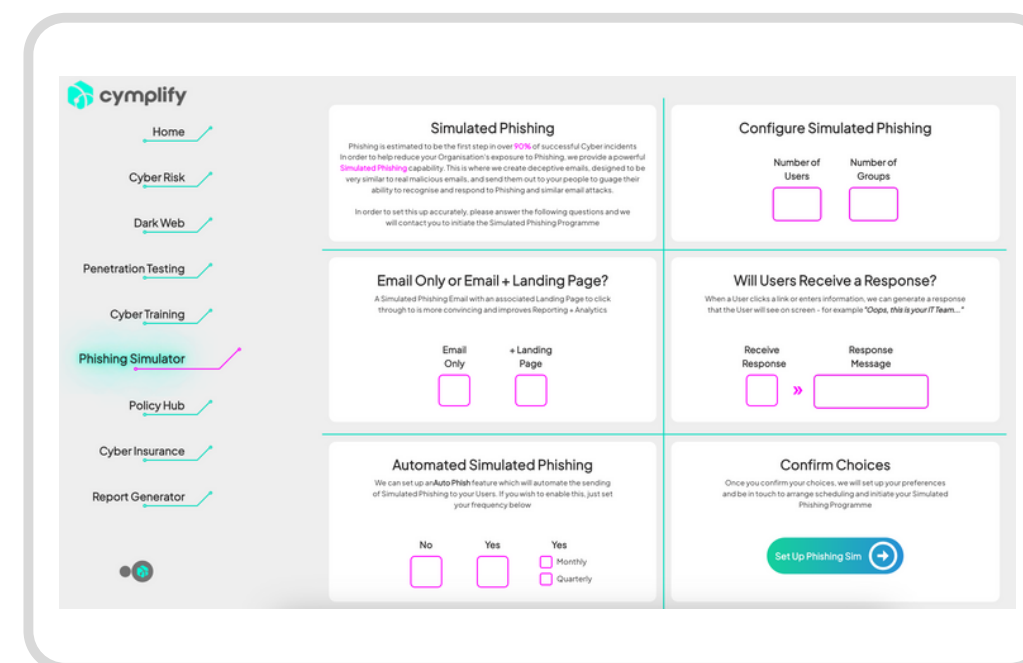
Centralised control of Cyber Awareness Training Programme



The dashboard provides a centralised view of the training programme. Key metrics include:

- Organisation Risk Score:** 129 (represented by a gauge chart).
- Average Training Score:** 78% (represented by a progress bar). Total Courses Assigned: 6055, Total Courses Completed: 4741.
- Existing Users:** 414. List includes: arthur.buckley363..., arthur.gold365@gaa..., arthur.willard333..., arthur.radclyffe...
- Existing Groups:** 7. List includes: AACME Managers, Bolton Users, Manchester Users, Chester Users.
- Training Hub:** A section for creating and managing courses, with buttons for 'Create New Course' and 'Existing Courses'.
- Risk Over Time:** A line graph showing the trend of the Organisation Risk Score over time.

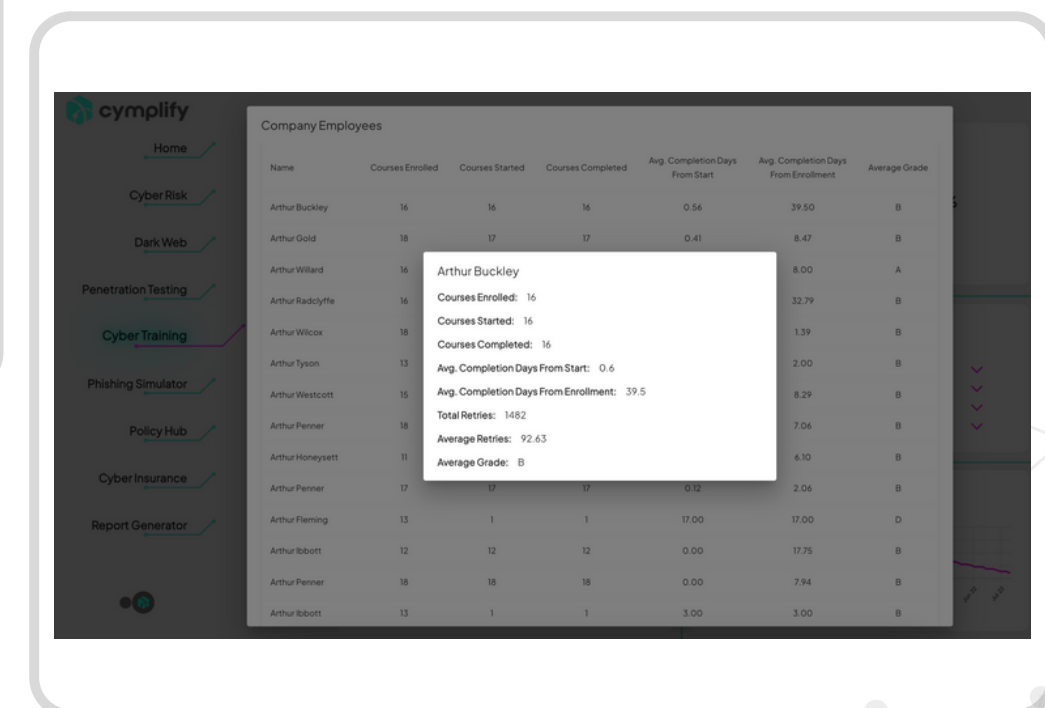
Configure, schedule and deliver an ongoing Simulated Phishing programme



The configuration interface allows users to set up a simulated phishing programme with the following options:

- Simulated Phishing:** Overview of the programme's purpose and goals.
- Configure Simulated Phishing:**
 - Number of Users:** Input field for the number of users to be targeted.
 - Number of Groups:** Input field for the number of groups to be targeted.
- Email Only or Email + Landing Page?:** Selection between 'Email Only' and 'Email + Landing Page'.
- Will Users Receive a Response?:** Selection between 'Receive Response' and 'Response Message'.
- Automated Simulated Phishing:** Options to schedule the programme (No, Yes Monthly, Yes Quarterly).
- Confirm Choices:** A 'Set Up Phishing Sim' button to finalise the configuration.

Drill down into Group or Individual User performance in specific scenarios or over time

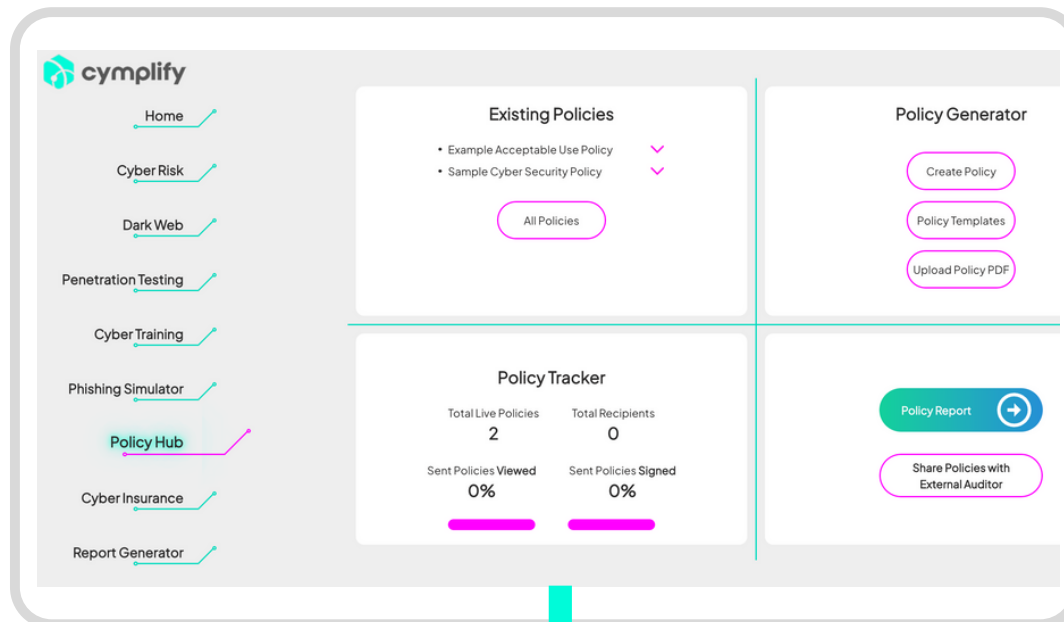


The performance report provides a detailed view of user engagement and completion rates. A tooltip for Arthur Buckley shows the following performance metrics:

- Company Employees:** Table with columns: Name, Courses Enrolled, Courses Started, Courses Completed, Avg. Completion Days From Start, Avg. Completion Days From Enrollment, Average Grade.
- Arthur Buckley Performance Summary:**
 - Courses Enrolled: 16
 - Courses Started: 16
 - Courses Completed: 16
 - Avg. Completion Days From Start: 0.6
 - Avg. Completion Days From Enrollment: 39.5
 - Total Retries: 1482
 - Average Retries: 92.63
 - Average Grade: B

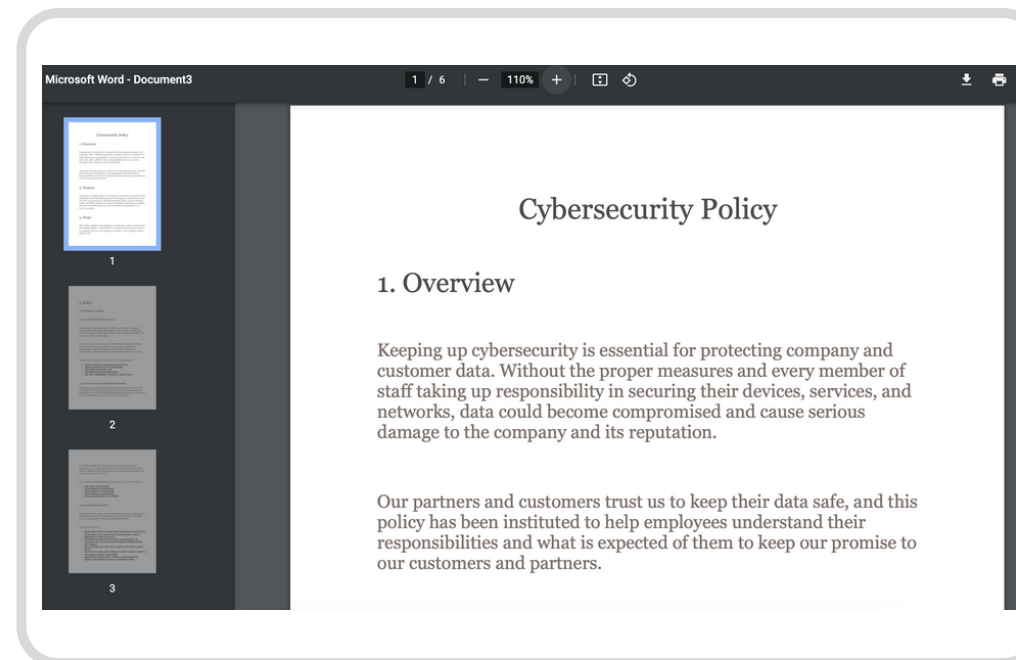
Centralised Policy and Process Management Hub

Centralised Policy Management, Policy creation, send and track views and acceptance across the organisation



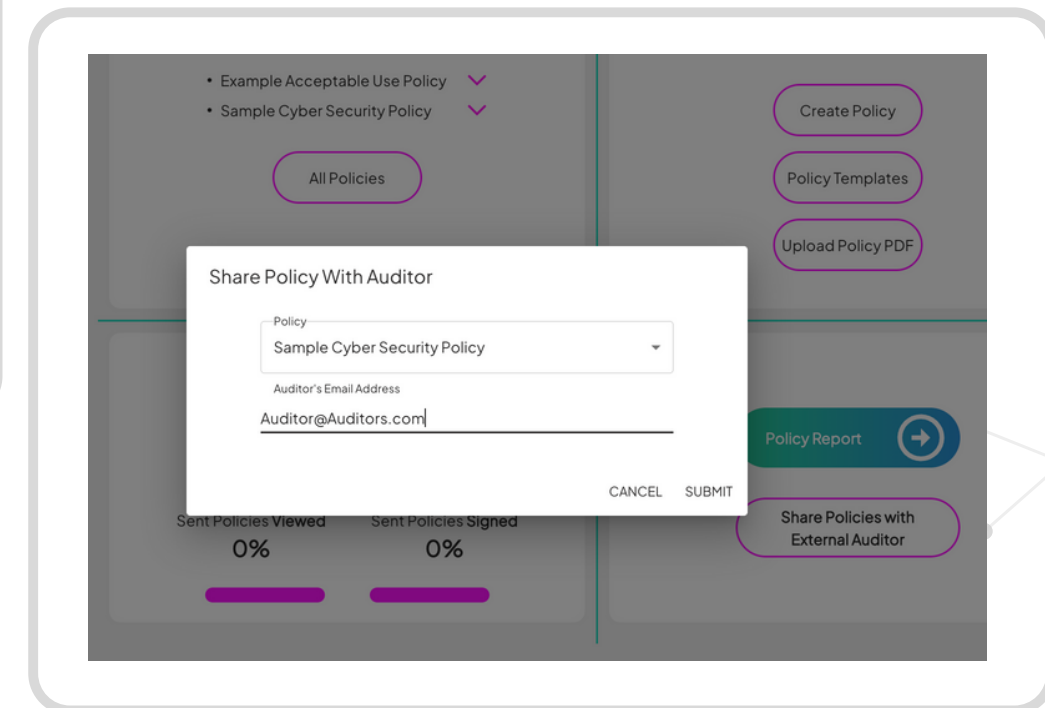
The dashboard features a sidebar with navigation links: Home, Cyber Risk, Dark Web, Penetration Testing, Cyber Training, Phishing Simulator, Policy Hub (highlighted), Cyber Insurance, and Report Generator. The main content area is divided into three sections: Existing Policies (listing 'Example Acceptable Use Policy' and 'Sample Cyber Security Policy' with a dropdown arrow and an 'All Policies' button), Policy Generator (with buttons for 'Create Policy', 'Policy Templates', and 'Upload Policy PDF'), and Policy Tracker (displaying 'Total Live Policies: 2', 'Total Recipients: 0', 'Sent Policies Viewed: 0%', and 'Sent Policies Signed: 0%' with progress bars, and buttons for 'Policy Report' and 'Share Policies with External Auditor').

Access a range of Boilerplate Cyber Policies, pre built and approved templates to help create your own



The document shows a 'Cybersecurity Policy' with an 'Overview' section. The text reads: 'Keeping up cybersecurity is essential for protecting company and customer data. Without the proper measures and every member of staff taking up responsibility in securing their devices, services, and networks, data could become compromised and cause serious damage to the company and its reputation.' It continues: 'Our partners and customers trust us to keep their data safe, and this policy has been instituted to help employees understand their responsibilities and what is expected of them to keep our promise to our customers and partners.'

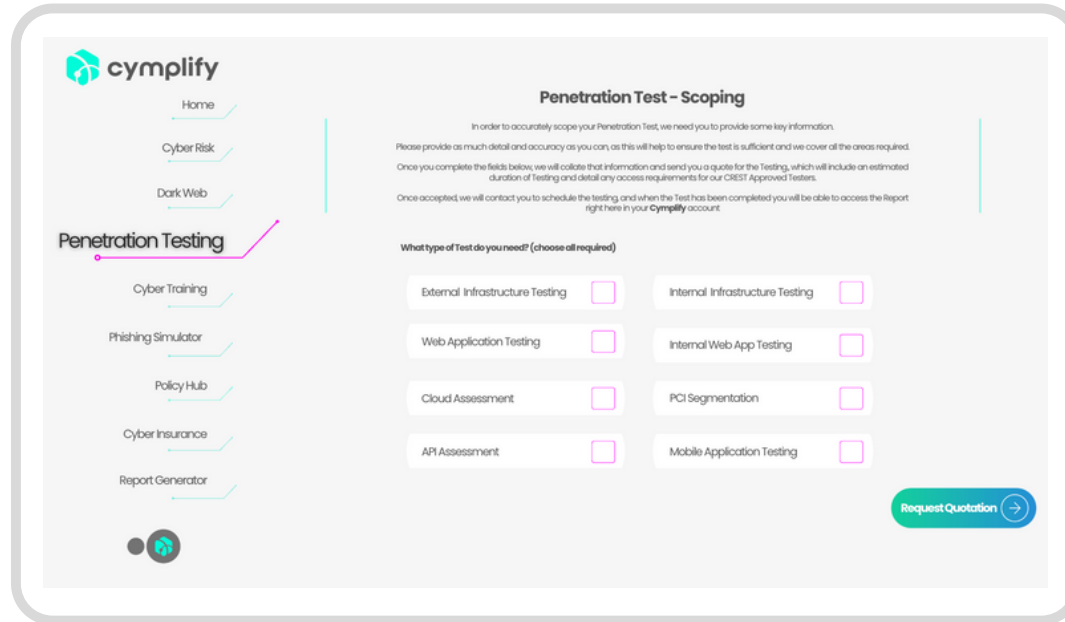
Share your policies directly with a Third Party Auditor for them to review and provide feedback



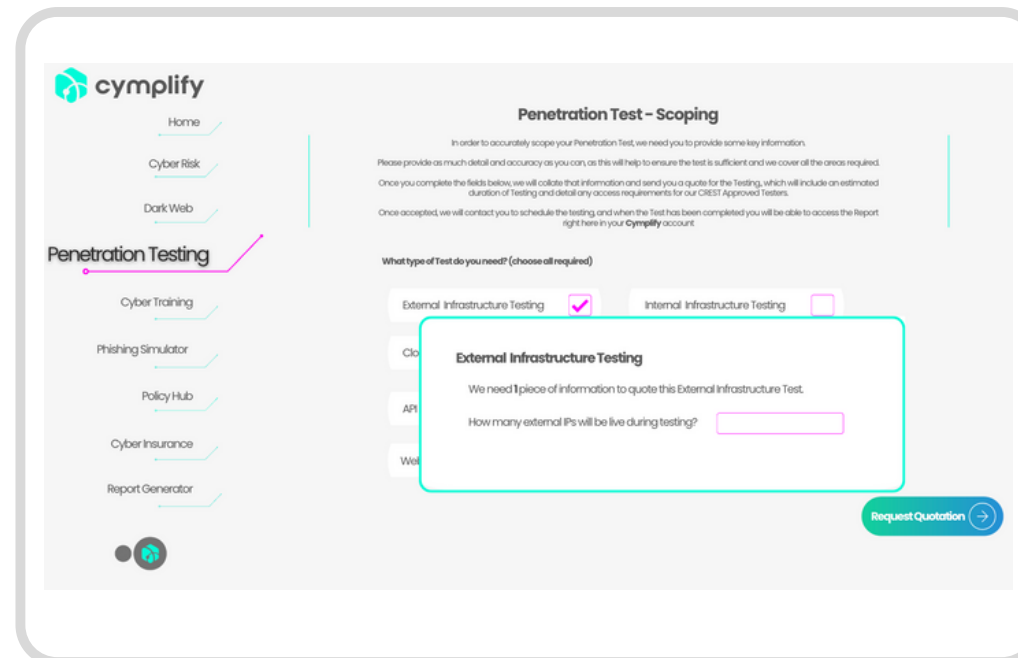
The dashboard is shown with a modal window titled 'Share Policy With Auditor'. The modal contains a dropdown menu for 'Policy' set to 'Sample Cyber Security Policy', a text input field for 'Auditor's Email Address' containing 'Auditor@Auditors.com', and 'CANCEL' and 'SUBMIT' buttons. The background dashboard shows the same 'Policy Tracker' and 'Policy Generator' sections as in the previous screenshot.

Centralised Penetration Testing Scoping, Quoting and Scheduling

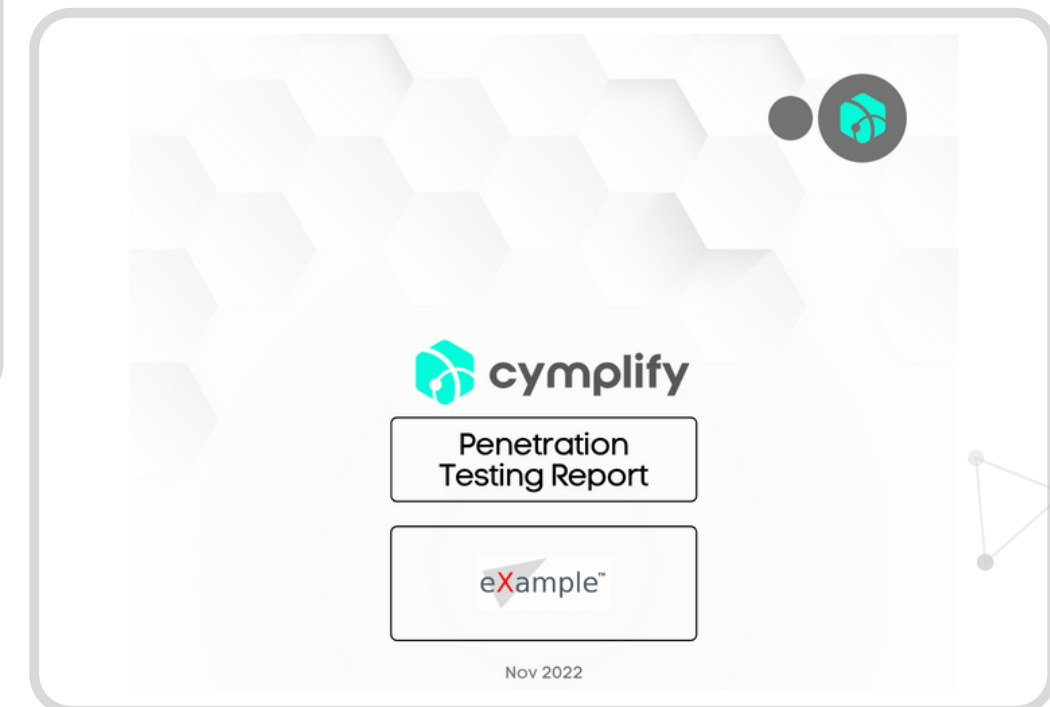
Choose, scope and schedule a wide variety of Penetration Testing in app



Schedule and engage CREST Accredited Ethical Hackers to carry out the required Testing



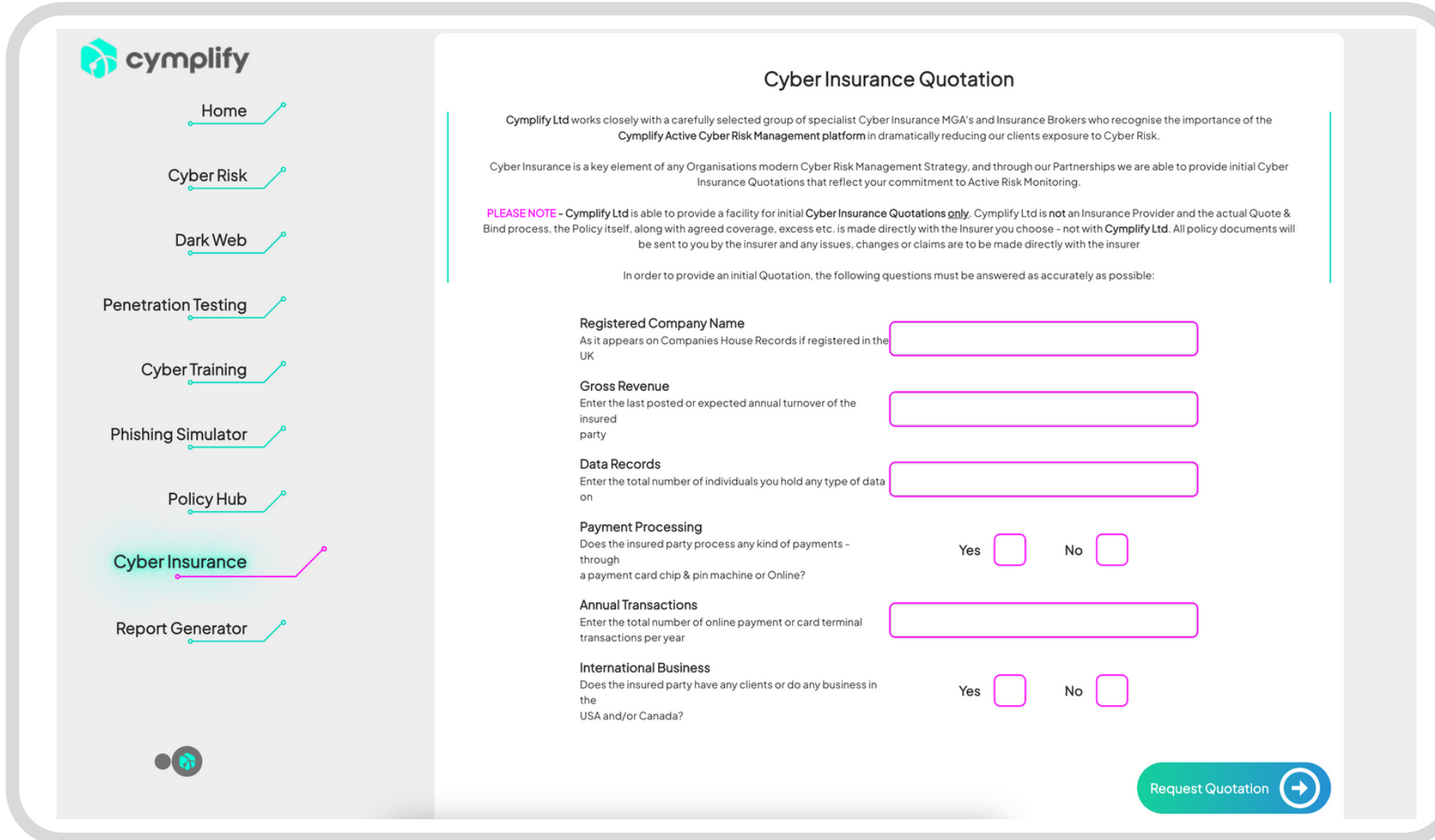
Access Penetration Test results and full Report in app



Integrated **Cyber Insurance** module - direct access to specialist Cyber Insurers and Brokers

Cyber Insurance is now an integral part of both a Cyber Resilience Strategy, and increasingly to Commercial Partnerships and Supplier requirements. However, at the same time as gaining prevalence, actually getting Cover is rapidly becoming much more difficult due to the pace at which the Cyber Threat changes, and the Insurance industry's lack of ability to adapt quickly.

Your Cymplify subscription comes complete with direct access to carefully selected, specialist Cyber Insurers and Brokers who recognise and understand the value of the Active Cyber Risk Management platform you are using - and this is reflected in the Policy Documents and Cover Quotes you will receive directly inside the Cymplify app itself



cymplify

- Home
- Cyber Risk
- Dark Web
- Penetration Testing
- Cyber Training
- Phishing Simulator
- Policy Hub
- Cyber Insurance**
- Report Generator

Cyber Insurance Quotation

Cymplify Ltd works closely with a carefully selected group of specialist Cyber Insurance MGA's and Insurance Brokers who recognise the importance of the Cymplify Active Cyber Risk Management platform in dramatically reducing our clients exposure to Cyber Risk.

Cyber Insurance is a key element of any Organisations modern Cyber Risk Management Strategy, and through our Partnerships we are able to provide initial Cyber Insurance Quotations that reflect your commitment to Active Risk Monitoring.

PLEASE NOTE - Cymplify Ltd is able to provide a facility for initial Cyber Insurance Quotations only. Cymplify Ltd is not an Insurance Provider and the actual Quote & Bind process, the Policy itself, along with agreed coverage, excess etc. is made directly with the Insurer you choose - not with Cymplify Ltd. All policy documents will be sent to you by the insurer and any issues, changes or claims are to be made directly with the insurer

In order to provide an initial Quotation, the following questions must be answered as accurately as possible:

Registered Company Name
As it appears on Companies House Records if registered in the UK

Gross Revenue
Enter the last posted or expected annual turnover of the insured party

Data Records
Enter the total number of individuals you hold any type of data on

Payment Processing
Does the insured party process any kind of payments - through a payment card chip & pin machine or Online? Yes No

Annual Transactions
Enter the total number of online payment or card terminal transactions per year

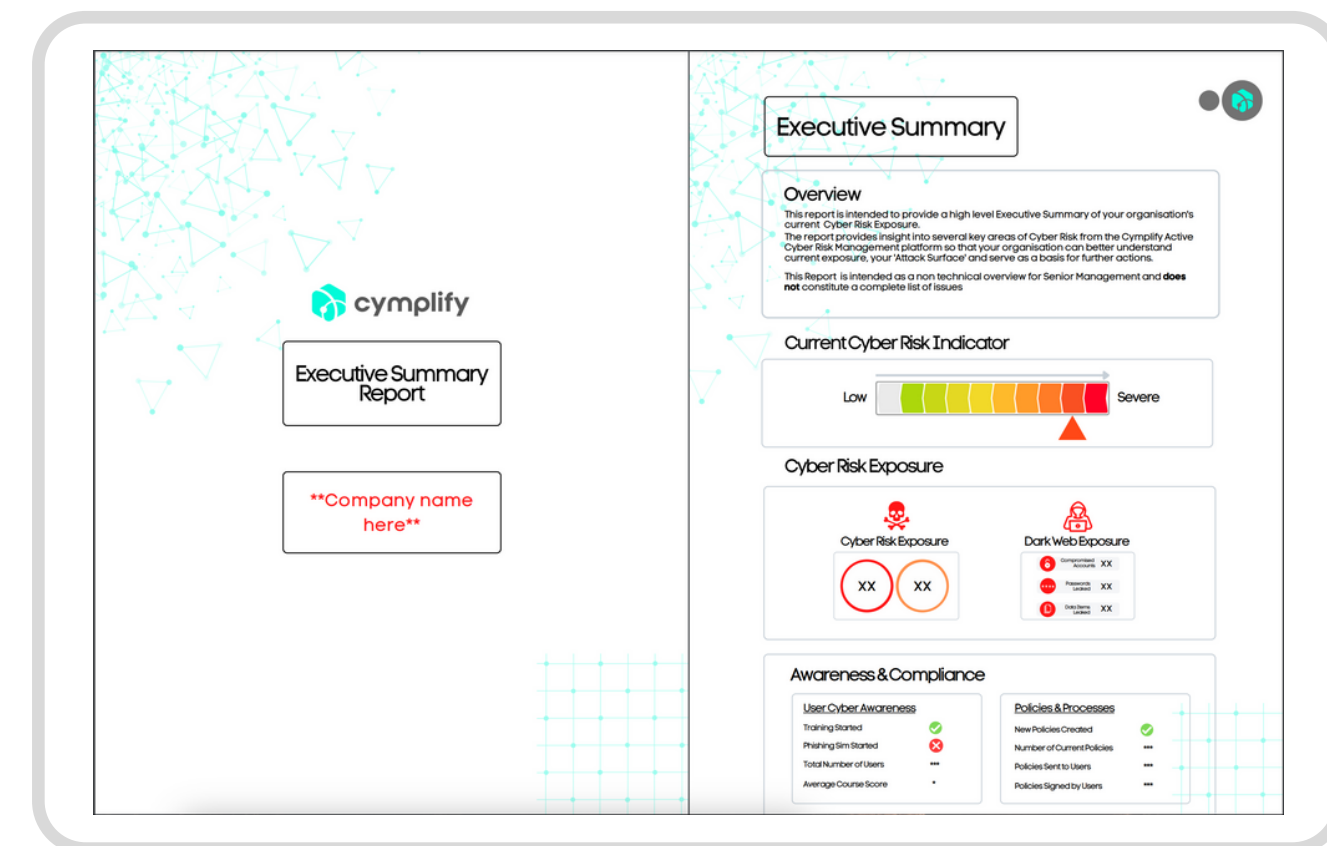
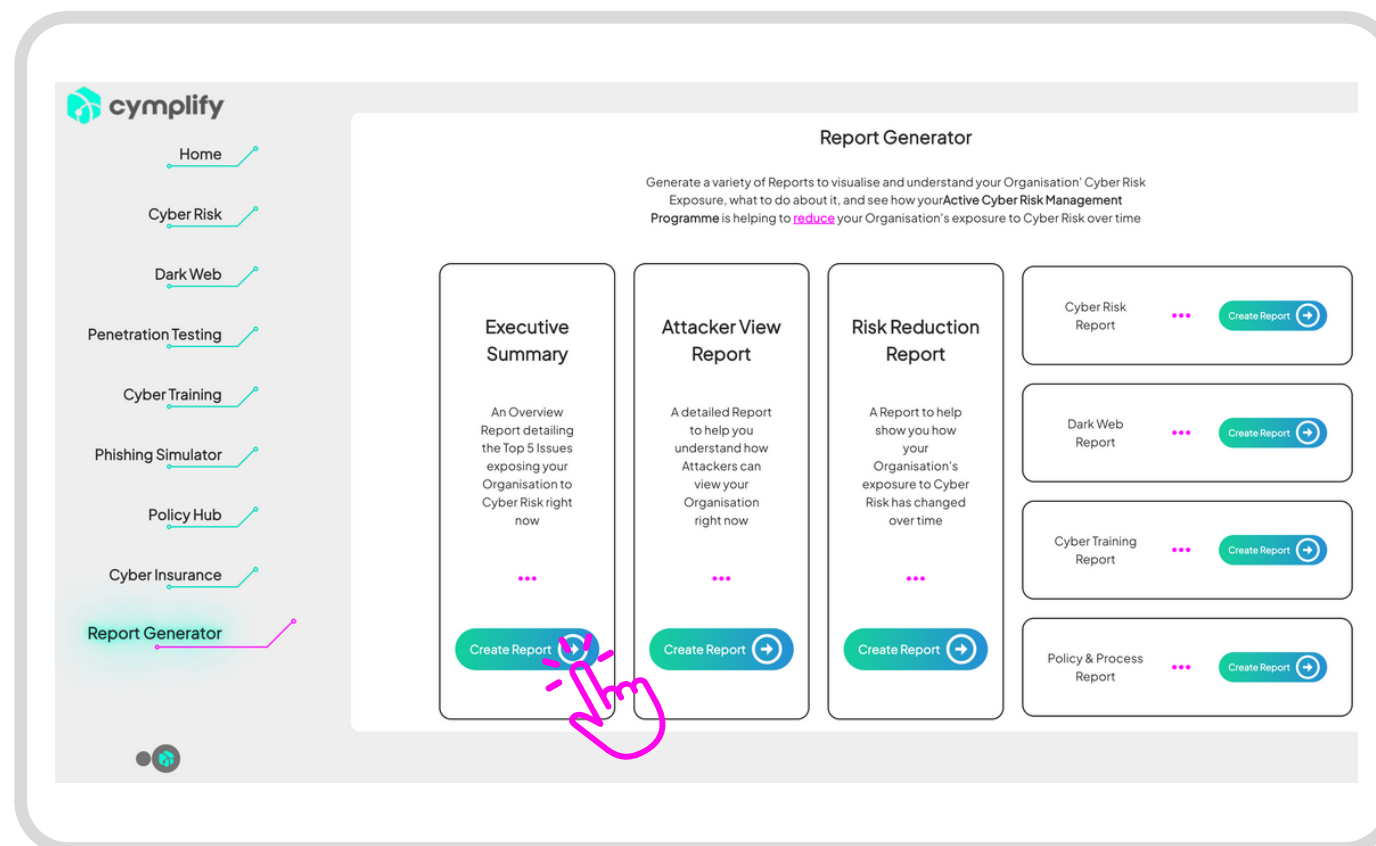
International Business
Does the insured party have any clients or do any business in the USA and/or Canada? Yes No

[Request Quotation](#)

Centralised Report Generator - visualise Risk exposure, evidence improvements over time and demonstrate ROI across the business

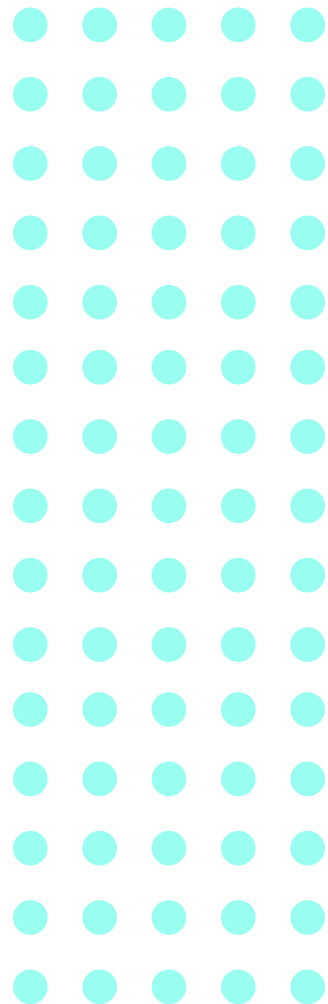
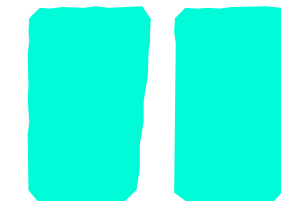
Choose from a variety of Board Level or
Risk Specific Reports

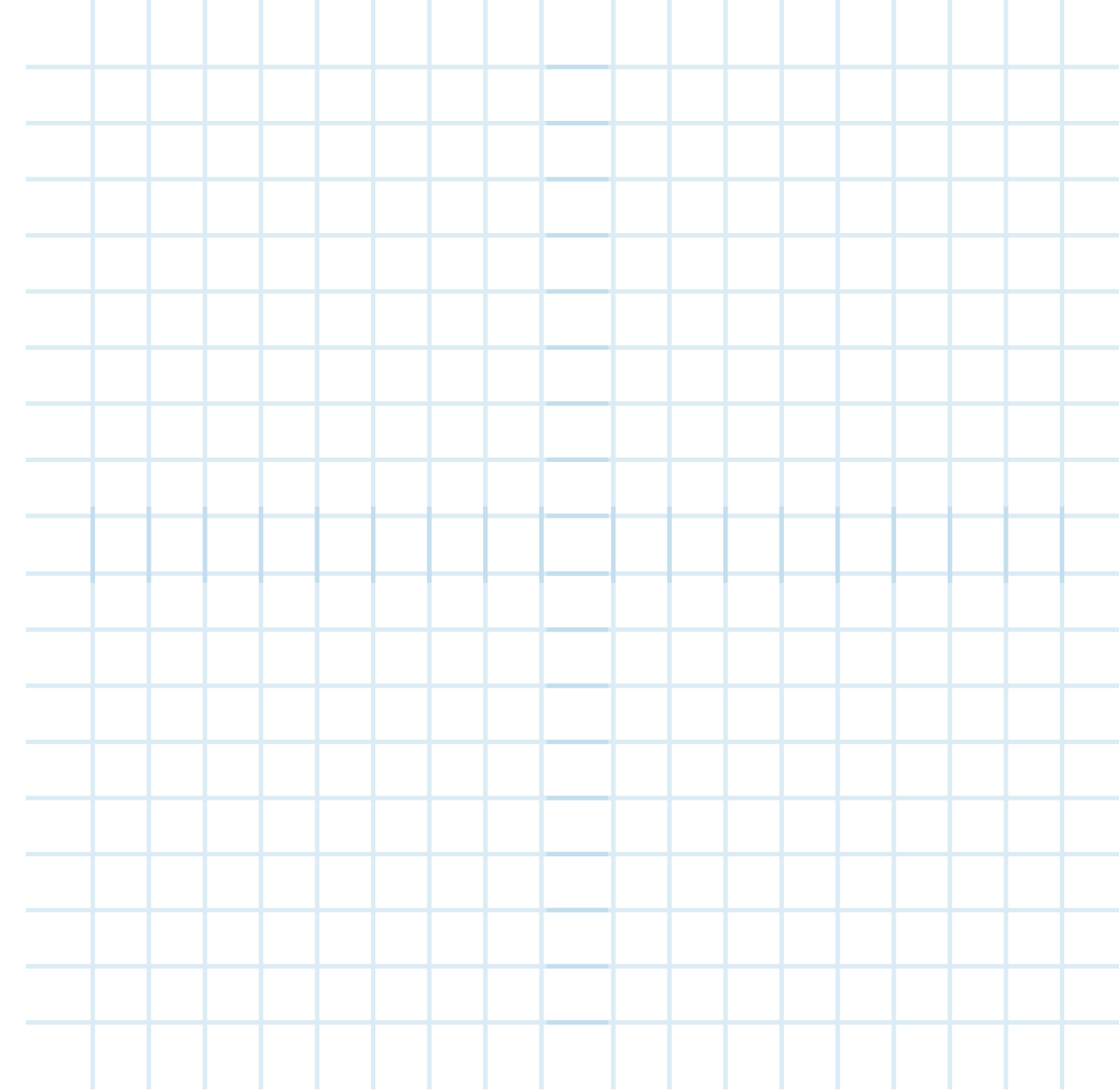
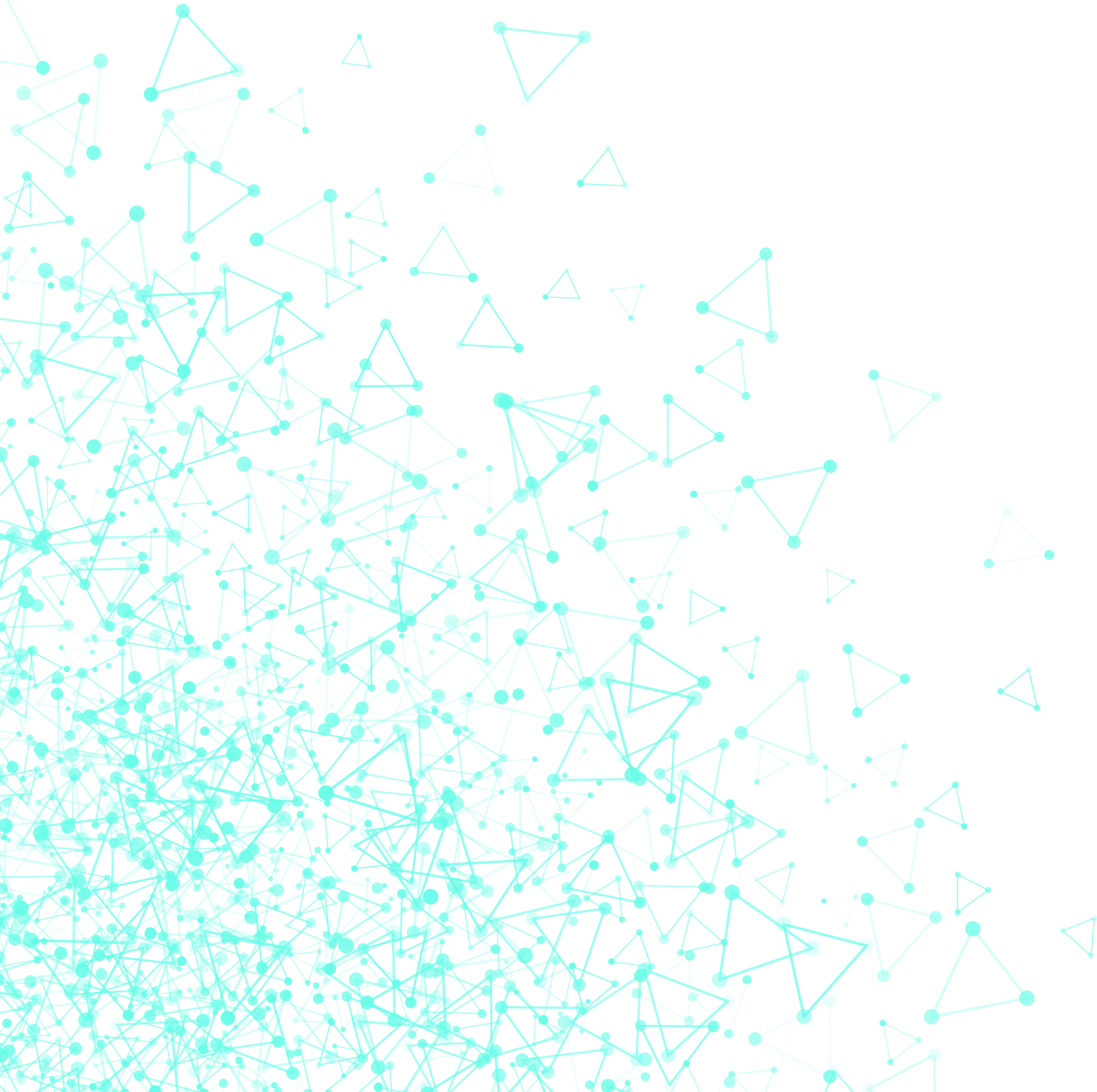
Access reports instantly or download
PDF to share with Key Stakeholders





The Cymplify Active Cyber Risk Management Platform brings powerful, simple, affordable and continuous Cyber Risk Management within the reach of every business. Cutting edge tools, 'Always On' monitoring, real time Alerting and detailed analytics enable any business to **dramatically** reduce their Cyber Risk exposure, promote a culture of Security, and to compete effectively in the digital first, globally connected world





w: www.cymplify.co.uk

e: hello@cymplify.co.uk

t: +44 (0)7801899016

a: 71 Shelton St, London, WC2H 9JQ