Training

Current Offerings

28 June 2023

Contents

1 Description

We can provide training related to any of the services that we provide. That nature and price of that training can be matched to your needs, as follows:

a) If you are an existing customer and we are aware of any open source or free training which will meet your needs, we will in the first instance direct you to those resources so that you may consider whether these are appropriate.

b) We can provide you access to any existing training courses (free or chargeable) that we provide where such courses exist.

c) We can create a bespoke training course for you.

d) If your training needs are specialist, it may be more appropriate and cost effective to deliver training as a consultancy activity on a time and materials basis where we:

   i) Work with you to define the goals and objectives of your staff.

   ii) Carry out the activities that you require your staff to be able to carry out, observed by them and documented by them.

   iii) Monitor them repeating the activity and providing guidance as required to verify that they understand and are confident to carry out the activity in the future.

e) Where we have partners who can deliver training courses where we get a resellers margin, we will direct you to these courses and make clear the business relationship between us and the reseller.

f) We may also be able to recommend you third party training courses if there are any that meet your needs.

Most of our courses are related to Cyber Security offerings that we provide. However, we have reasonable understanding of generic training needs for project management, solution architecture and particular technologies such as those from IBM, Red Hat, AWS, MariaDB, Actian and Microsoft to name but a few.

The courses that we author and deliver can be provided via a number of channels: Face to face, Instructor led online or online self-paced. Delivery of courses from third parties will be in accordance with their standard terms and conditions.

The following are examples of training material that we can direct you to or deliver:

a) At no additional cost as part of our Cyber Security product CSPM:

   i) “How to…” training in carrying out tasks related to achieving and maintaining Cyber Essential accreditation, such as,

   ii) How to encrypt a drive with Windows 10.

   iii) How to disable autostart for external devices.

   iv) How to disable USB ports if required.

   v) Configuring and managing SE Linux rules.

   vi) Enabling security using third party certificates on all devices.

   vii) Enabling disk encryption on a Linux machine.

   viii) Sandboxing virtual machines.

   ix) Disabling SNMP V1 and V2 on Epson ET-5800 and similar printers.

   x) Planning for carrying out a vulnerability scan using Qualys.

   xi) Setting up routers running Untangle.

xii) Managing your network.

b) A range of courses available on youtube to help you with common tasks:

i) Setting power on and administrator passwords in Lenovo laptops.

ii) Enabling virtualization to run VMWare.

c) Risk Management

i) Carrying out a risk review of your business.

ii) Carrying out a WFH risk assessment.

iii) Business continuity and disaster recovery planning.

iv) Creating an incident management plan.

d) Where you develop your own applications, training to ensure security by design:

i) Understanding the obligations placed upon an organization to meet development standards such as OWASP.

ii) Verifying that organizations meet CCS standards where they are contracted on government framework contracts such as G-Cloud, DSP or DOS.

We use a third-party training platform for the on-line self-paced training that we develop and deliver which allows us to monitor progress of people through each course and link progress to completion of CSPM tasks associated with specific training.

In addition, we can run exercises to test that training has been properly adopted:

a) Online penetration testing.

i) Phishing attacks

ii) Other email attacks where we seek to investigate user behavior when sent dangerous material over email.

iii) Vulnerability scans.

Physical penetration testing of premises to see if access can be gained.

2 Commercial Terms

Our training as a service is a low-cost subscription offered at a low cost on the basis that all people in the organization that have access to any electronic device through which they can access company data will be subscribed.

Training as a service is bundled into our standard pricing for our security policy offering but it can be taken as a lower cost subscription for training only through our CSPM platform.

We provide an easy-to-understand table of training which includes:

a) Schedule of the costs of training we provide and the length of time that you have access to the course material and your responses.

b) The program for updating a course and whether a subscription to a previous version means you also have access to replacement material.

c) Gives you access in perpetuity while you continue to take other services, for example our security policy service.

Where you take training courses from third party vendors that we resell, we will ensure that the terms and conditions are summarized by us and that you have easy access to the detailed terms and conditions of the vendor, before you purchase.

These will cover:

a) Cost of the course.

b) Time you have from purchase to take the course before any subscription expires.

c) The length of time that you have access to any course material and whether any such access constraints are linked to the time access is granted or the time when the course is passed or any other limitation.

You can take our training as a service offering as a standard subscription offering in which case you will have access to all our training offerings provided you continue to take our training as a service offering.

When you take our Training as a Service subscription, there is an initial 3-month commitment. You can terminate use of the service completely giving 30 days' notice on completion of the 3-month commitment.

If you terminate the service then we stop managing your training and have no further responsibilities to you.

Your charge is monthly in advance for payment within 15 days. We can take check or credit card but request you set up regular ACH payments to minimize administration and costs for both parties.

A small discount is available for increased long-term commitment or annual payments in advance provided payments are via ACH.

3 Service benefits

There are some absolutely fundamental technical protections that all organizations should deploy to have any semblance of defense against cyber security attacks, such as deploying a router to protect equipment from direct attack across the internet, deploying anti-malware software to detect common attacks and ensuring all software is regularly updated with the latest patches to remove vulnerabilities that have been discovered.

However, the next most common attacks rely very heavily on training people to ensure they remain aware of the common types of attack and avoid being hoodwinked into participating in those attacks. For example:

a) Most ransomware attacks arise from people "clicking" on dangerous content and downloading damaging applications that damage their systems.

b) Phishing, CEO and mandate fraud arise because fraudsters build up a picture of people via social media or other information bases and then convince or persuade them to take actions that damage their company, for example:

   i) Changing the bank payment details of an invoice to a fraudsters account and then paying that account.

   ii) Telephoning them using the information gleaned and persuading them to provide account details or make improper payments, for example by convincing them that they are talking to their bank or to the police and then giving away login details.

It is therefore vital that organizations:

a) Provide basic training their staff

b) Have follow up reminder training to maintain awareness.

c) Ensure that each person understands the importance of their actions and reports incidents promptly if they think they might have been compromised.

d) Practice how to respond to an incident if one should occur.

Following training, the organization should run exercises to test whether training has been adopted and has become ingrained in the business processes of the business.

Effective training and awareness should dramatically reduce the probability and impact of a successful attack occurring.

Minimizing the risks of a large fine by a regulator if a successful attack does occur because an organization can show through its training records that it has met its obligations to train staff.

You can define and manage your training needs through our platform (not yet deployed in CSPM but in the original platform).

4 Deploying and Operating the Service

Where an organization purchases our training as a service, it accesses training through our CSPM platform and is billed through CSPM.

Where we resell third party training products and services, we expect the vendor to provide a training portal. However, where an API exists, we may build an integration with that API so our customer can manage all training needs and delivery through our single portal.

Payment of training is generally upfront and prior to delivery though may be billed through our payments engine that collects fees through GoCardless but specific terms may apply depending on the vendor of the service and their terms.

5 Supporting Documentation

Details of all training requirements specific to carrying out tasks associated with maintaining protection as described in a security policy are described in the security policy.

Where the details of training courses are maintained in CSPM, the details of all courses are provided in our platform.

CSPM holds details of all training needs, minimum trained staff requirements and warns organizations if they have or are likely to fall below their minimum trained staff requirements.

6 How Support Works

As our training service is included within CSPM our support model is maintained within our standard CSPM support approach. The following is a brief description of our support mechanism. This is explained fully in our support manual:

- We identify where we provide training to meet you expected needs and in addition, we maintain a list of vendors for these and other common training needs that we do not currently support.
- Access to our training provision is standard functionality within the solution.

- If a problem arises around any aspect of training provision, a new issue is then raised in our service desk environment, on behalf of the nominated user associated with the item of equipment concerned.
- If you take our remote management services, you may raise a support issue directly for any item of equipment we are managing by using the Company's icon on your machine. As soon as this appears on our service desk environment, you can then add further comments or information related to the problem.
- All information related to the issue should be entered via service desk but we will accept calls to escalate urgent/serious issues by email or phone.
- Once an issue is raised, you can then track the issue through to resolution.

Support is provided during the working day between 0800 and 1800. You cannot purchase extended support for out of hours or 24 x 7 only for training, but if you have purchased this for our other services then support for training is included automatically in extended support.

Onsite support is not included as part of this service though training may be delivered face to face in your offices if that is an option for a particular course.

At the end of each month, you are provided with a report describing our performance against agreed KPIs.

Our service desk is available at the following URL
https://cysure.atlassian.net/servicedesk/customer/portal/2

7 What is not included

Currently all provided materials are those available online. We do not provide downloads of training materials or of worked examples or exercises unless explicitly stated in a course schedule as a deliverable.

Support is related to the technical delivery of the course. It does not include services to explain or expand the details of the course being delivered, i.e., additional training or expansion of an element of a course using additional trainer resources.

That said we will accept support requests related to an aspect of the course which a student does not feel is adequately explained and will forward this to the training provider. We do not offer any warranty or other obligation that the provider must respond. However, we will maintain an FAQ related to course enquiries and will encourage the provider to address and then promulgate any revisions or clarifications to the course as a consequence (and update the standard material appropriately as soon as is practical) to maintain the quality of training deliverables offered by or through us.

8 How we may change the service from time to time

We will publish any revised prices on our website and will notify you of any price rises giving you 3 months' notice of such price rises related to our service or any training materials that we provide directly. By taking this service you agree to accept any such price rises. You may terminate the service if you wish.

We may change the product we use to provide this service at any time. It is then our responsibility to ensure that the change of product has no impact for you. Note:

a) the most likely reason for a change would be that an alternative product either provides significantly more functionality at a comparable price or is more cost effective for the capability delivered.

b) As we would bear to cost of any transition, this is not something we would do lightly!

9 Terminating our service

If you decide to terminate our service, then for this service you must provide us 30 days' notice of termination.

You may terminate our training service independently of any other service we provide to you, except where the service is a bundled component of another service that you do not terminate. An example is our security policy service.

On termination and provided we have received payment in full on all outstanding invoices, we will provide to you on request details of your staff and their training records on the date that our services terminate at the end of your notice period, in a format that we describe to you.

After one month following termination, or sooner if you request, we will remove details of your staff and their training needs and records if these are not required for any other service that we provide you.

It is your responsibility to archive any reports important to you before you terminate as once we remove your organization from the platform all historic data is deleted.

If you require any assistance from us when terminating, for example to transfer to an in-house solution or to an alternative vendor, then as a responsible supplier we will assist you in this process if requested and charge you at our standard professional services rates on a time and materials basis.