Vulnerability Scanning

Current Offerings

19 October 2022

Contents

1 Description

This service will mean that we scan all the devices on your network and report to you all the vulnerabilities on your network and tell you the level of risk associated with each vulnerability.

We report to you through our online portal or via a point in time report which we can provide to you in PDF or .CSV form.

The team responsible for managing your assets can then act on this report by applying patches to the devices on which vulnerabilities are identified.

Once the devices have been patched, we can then re-scan your network to ensure that the vulnerabilities have been addressed.

It may be that a number of iterations are required before all the relevant patches have been applied.

We will agree with you a schedule for running our scans because there can be some impact on the network while a scan is taking place. More important, we need you to ensure that all your mobile devices are connected to the network at an agreed time so that the scanner can identify them and then scan them.

To perform this service, we need either to have VPN access to your network or to install a scanner on a dedicated device within your network which has access to all subnets and across all switches. The latter is the preferred option.

Some vulnerabilities can be identified where no current patch exists. We will escalate these to you.

If you are already taking our Remote Monitoring service we will immediately, in collaboration with you, plan and then apply any necessary patches to the devices where vulnerabilities have been identified.

If vulnerabilities are identified related to software that is not managed by us, for example to application software products which we are not supporting, then we will identify those so that you can pass to the team providing that support.

It is not our responsibility to ensure applications that we do not manage for you will continue to run after a patch to another item of software is applied. If you believe that there is a risk of a patch impacting a third-party application then you must provide us a test environment on which the patch can be applied. Once we have applied it the test environment and you have checked that there are no such impacts, we will apply the patch to the production environment.

2 Commercial Terms

We offer two options for vulnerability scanning.

2.1 Scanner option

The first is to charge you for a local scanner which is dedicated to your site, is permanently available and from which we can initiate vulnerability scans at any time.

This option comprises a single annual charge paid in advance for the deployment of the scanner, together with a single price per device per year on the network, regardless of the number of scans performed.

2.2 VPN access option

The second option is you provide us VPN access to your network so that we can carry out the scan remotely.

This option comprises a charge for our staff to set up and configure the scanner, plus a charge per year for each device scanned.

If a company considers that they are low risk and only wants an annual scan then option 2 is more cost effective.

However, the level of risk and the frequency with which vulnerabilities are identified means regular scanning is essential for effective protection. The first option is therefore both more secure, more flexible and in most circumstances more cost effective.

2.3 Scanner option costs

For option 1 you pay:

An annual upfront subscription for the scanner which we shall deploy on a dedicated machine in your environment, ideally in a VMWare or Hyper-V platform if you have one.

You pay a single monthly subscription charge for each device to be scanned. There is a discount to this charge for any device that is being managed through our remote service.

You do not directly pay for own any underlying perpetual licenses or third-party subscriptions for our service. We manage all of the underlying technology.

When you take our service 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 scanning your network and have no further responsibilities to you related to this service.

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.

The remainder of this description assumes that you take option 1.

3 Service benefits

One of the most frequent paths for criminals to attack organizations is by exploiting known vulnerabilities in operating systems and in application software. When a vulnerability is found by ethical hackers or other organizations, the vendor responsible is given 30 days to issue a patch to correct the vulnerability, after which the details of the vulnerability is added to publicly available lists of known vulnerabilities, which means hackers can understand the vulnerability and start to develop viruses to exploit it.

Responsible vendors provide regular updates and patches to their software to address these vulnerabilities which is then the responsibility of the organization running software with the vulnerability to install those patches.

Vendors such as Microsoft automatically deploy updates to computers running supported Windows operating systems, for example Windows 10 or Windows server. However, these updates are not always installed by the user, and Windows Server installations are generally not rebooted automatically to enable the updates even if they are installed.

This service ensures that all vulnerabilities present on your computers are identified as soon as they are known, prioritized for resolution based on importance and that the level of risk is escalated directly to the board if it is material and requires executive support.

By taking this service an organization demonstrates that it takes cyber security seriously, it shows it can detect and resolve vulnerabilities promptly and that is managing this key area of risk effectively.

4 Deploying and Operating the Service

Deploying this service involves the following steps:

4.1 Scanner deployment

Deploying a scanner into your organization and connecting it to your organization's networks that need to be scanned.

This includes configuring access to any cloud platforms that you run which need to be scanned.

Defining a business case for opening up a port to allow our scanner to communicate with the product vendor's controller to allow the scanner to register, download details of the latest vulnerabilities, upload details of the assets discovered then configure and run scans.

4.2 Configuration

Configuration involves ensuring all networks are accessible to the scanner. It may be necessary to create a domain account with appropriate privileges to enable access to each machine to be scanned.

We identify the networks or sub-nets in your organization then perform a map operation to identify all the equipment on the network. (We do this even if we are providing remote support and believe we have discovered all your equipment.)

This map operation loads details of all equipment identified which we then organize into groups against which we run scans.

We then run scans on an agreed schedule to check for any new vulnerabilities so that they can be addressed, we re-run maps on an agreed schedule to identify any new hardware that has joined the network, and generate alerts to investigate any such equipment then add those devices to a scan group.

We then escalate to those responsible details of any new equipment that needs to be managed or any vulnerabilities identified so that they can be patched.

Once configured, this Service is run by us, its operation should be transparent to the people in your organization in most respects, until an alert is generated requiring your attention.

You can inspect the level of risk through our console from time to time.

4.3 Reporting

We will provide you with regular reports and alert you to any activity of interest for which management action might be required.

5 Supporting Documentation

As the operation of this service is transparent to your organization, there is no requirement for extensive documentation on the service itself.

We create a short operations guide or manual for ourselves so that any of our team who are appropriately authorized can perform scanning on your network and report back to you. This describes:

a) Our understanding of your environment and network including the subnets of it.

b) The agreed location of the local scanner and your obligations ensure it is running and connected to the network.

c) Our agreed protocol for the frequency with which we run maps and scans and any obligations to alert you in advance.

d) Your responsibilities to inform us in good time of any changes you make to your network that might impact the configuration of our scanner, such as for example additional subnets deployed, new switches, routers or security domains to scan.

e) Protocols for rebooting devices that have been patched and now require to be restarted.

f) Mechanisms for requesting reports and the meaning of the reports we deliver to you.

g) The operation of our support system, how you can track any issue that has arisen and the SLAs and KPIs by which you can measure our performance.

6 How Support Works

The following is a brief description of our support mechanism. This is explained fully in our support manual:

- When an issue occurs on your network related to a detected vulnerability that crosses an agreed threshold, it is automatically reported to us and we document then triage that problem.
- A new issue is then raised in our service desk environment, on behalf of the nominated user associated with the item of equipment concerned where attention is required.
- We may merge incidents reported for many devices if they are fundamentally the same problem, and particularly if you take another of our services that would report problems with the network.

- You may raise a support issue directly for any item of equipment that you are concerned about by using the Cysure icon on your machine through the support portal. 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. Optionally you can purchase extended support for out of hours or 24 x 7.

Onsite support is not included as part of this service: we work with your onsite representative. However, we are able to provide onsite support as part of our Equipment Managed service offering.

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

This does not include any service to monitor or remediate vulnerabilities identified, which we will carry out if you take our remote monitoring service, or alternatively if you wish to contract us based on our Assistance Services offering on a Time and Materials basis.

8 How we may change the service from time to time

Part of our service is based on purchasing software licenses and subscriptions for vulnerability scanning which we then use to deliver the service. From time to time the technology vendors of these products increase their prices and we need to similarly increase our prices.

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. 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. Any charges already invoiced, for example the annual charge for a scanner will not be refundable.

On termination we will no longer carry out vulnerability scanning of your network and we will have no further responsibility regarding reporting vulnerabilities to you.

On termination and provided we have received payment in full on all outstanding invoices, we will provide to you details of all passwords, details of network ports you have opened to operate the scanner and other confidential information related to scanning your network that you have provided to us so that you may make appropriate changes to suspend any accounts you have provided to us or close ports opened only for the purpose of scanning.

After one month or sooner if you request, we will remove details of the devices from our management platform and then remove all details of your organization from the platform.

It is your responsibility to archive any reports important to you before you terminate because 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.