Physical & Network Security

1	Does Maytech's platform have adequate hardware/software monitoring that is in place to ensure issues compromising system performance, availability, integrity or security are alerted for remedial action? What proactive/protective monitoring tools, processes and audits (i.e. details of security/ system health checks, penetration tests, scanning, audit and control of key architectural components etc.) are used?	Maytech's services are very extensively monitored, we have more than 125 checks in place. These include low level system health such as: • Weekly vulnerability tests (McAfee) • Weekly PCI conformance tests (McAfee) • Network conditions • Load • Database response times • Storage IO performance And high-level tests – for example: • Can a test user login • Time to authenticate • Time to get file listing • File transactions – upload, download, rename, delete.
2	What kind of alerting for the monitoring is available: SMS, email, etc?	Our systems are extensively monitored alerting our NOC on a range of conditions, but this is not a service we share with customers.
3	How do you monitor the security of your infrastructure?	Firewalls, weekly external vulnerability scanning (McAfee) daily internal vulnerability scanning (Vuls) and Annual Penetration Testing.
4	Detail any DDoS protection in place for the service.	Maytech's platform is protected by a suitable firewall infrastructure with Intrusion Detection System /Intrusion Protection System, DOS/DDoS protection, antivirus filtering, access control and auditing. The service is monitored by over 125 monitoring daemons continuously probing for fault conditions at levels ranging from basic hardware health to emulated file transactions. Ports are monitored for suspicious activity such as password scams or DDoS attack.
5	What boundary protection architecture and governance regarding protective monitoring is used? Is Maytech's platform protected by a suitable firewall infrastructure with Intrusion Detection System /Intrusion Protection System, DOS /DDoS protection, antivirus filtering, access control and auditing?	The Maytech's networks are protected by a stateful packet inspection firewalls. All ports, other than those required for the provision of service are closed. We operate intrusion detection (SNORT). An attempt to gain unauthorised access results in a lockout of offending IP on the firewall.
6	Are Intrusion Detection Systems (IDS) installed either on network or hosts? If yes, describe the solution used and the management/monitoring process.	Maytech have comprehensive IDPS systems that scan traffic for and recognises intrusion attempts and automatically blocks offending IPs on the firewall.
7	Does your Internet gateway provide website filtering to block compromised sites and provide malware protection?	Yes.
8	Does Maytech's platform have any performance constraints and maximum loading for the system?	Maytech's platform is a cloud service that handles hundreds of requests per second. Server load is constantly monitored at our NOC. It is our policy to ensure no part of the system is loaded above specified industry standard trigger points. Our systems are architected for seamless scaling.
9	Do Maytech have any system hardening policies and controls in place?	System hardening is governed by ISMS OP 11 - Systems Security and Network Management Policy and tightens system security by limiting the number of users, setting password policies, and creating access control lists. Unnecessary services are disabled to make the system more secure and to provide better performance. All ports, other than those required for the provision of service are closed.
10	Are there any patch management policies and controls in place?	Governed by ISMS OP 29 Security and Patching Policy. Critical security patches are installed when they become available. A typical time window for non-critical patch release is two working weeks of patches being released. Patch installation failures are monitored.

11	Does Maytech's platform components have active anti-virus installed and maintained? What anti-virus and/or anti-malware controls are in place?	We may provide virus checking, content filtering (spam control) and other similar supplementary services in connection with, or as part of, the services. We will use our best endeavours to provide these supplementary services with reasonable skill and care but we give no other warranty in regard to these supplementary services and, in particular, we do not guarantee that they will be totally effective. It is essential for the protection of your data and systems that you install and routinely maintain your own virus checking and other security services and that you regard the protection available from us as no more than the first line of defence. All files uploaded are scanned using ClamAV to inspect uploaded files.
12	What antivirus software is installed on both servers and workstations? What are scanning and signature update schedules?	Maytech do not use any Microsoft products in production, as such our production systems are not susceptible to Windows malware. We do offer a virus scan service which uses ClamAV to inspect uploaded files. All staff PCs run McAfee antivirus.
13	Is the application/solution subject to regular third-party penetration testing? How frequently such tests take place?	The service is subjected to an annual IT Security Health Check (ITSHC) by a CHECK / CREST approved vendor and a management report and residual risk statement are available for all interested parties upon request and a signed NDA. The CHECK scheme is UK specific and enables penetration testing by National Cyber Security Centre (NCSC) approved companies, employing penetration testing personnel qualified to assess IT systems for Her Majesty's Government and other UK public sector bodies. Vulnerability scanning: Daily scanning for over 40,000 vulnerabilities and weekly PCI scanning using McAfee, an Approved Scanning Vendor (ASV).
14	Which company, or companies, is used for penetration testing?	Maytech alternative third party security companies on a regular basis. Please contact us for specific details for a current year.