

HOW CYLERA SUPPORTS THE NHS DATA SECURITY AND PROTECTION (DSP) TOOLKIT

2022 - 2023

CORE TO  CLOUD™

 CYLERA

What is the Data Security and Protection Toolkit (DSP Toolkit) and its purpose?

The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure and publish their performance against the National Data Guardian's ten data security standards. These security standards are clustered under three leadership obligations to ensure:

- People understand how to handle information with respect and care,
- Processes are in place to proactively respond to incidents and prevent data security breaches, and
- Technology is secure and current.

"Leaders of all health and social care organisations should commit to following the data security standards. They should demonstrate this through audit or objective assurance and ensure that audit enables inspection by the relevant regulator."

- www.dsptoolkit.nhs.uk/Help/Attachment/24

What is the Structure of the DSPT?

The DSPT is composed of ten security standards addressing issues arising from people, processes, and technology.

The standards are wide-ranging and cover items ranging from a greater understanding of their security responsibilities among staff to regular reviews of processes to avoid data security breaches to holding information technology (IT) suppliers accountable to protecting confidential data they may access.

With each standard are assertions and these are specific themes or controls that substantiate the standard. Evidence items then follow and represent the maturity of that area.

Data Standard 9 IT Protection

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Assertion 9.3.8 and 9.3.9

- 9.3 - Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.
- 9.3.8 - The organisation maintains a register of medical devices connected to its network.

Now Mandatory in the 2022 DSPT and addressed later in this document:-

- 9.3.9 - What is the organisation's data security assurance process for medical devices connected to the network

Assessment Documentation Evidence Item 1

Assessment

1. Request and review the organisation's connected medical device register (which may be part of a larger asset register).
2. Sample a number of devices from the asset register to see if the record reflects current status.

How does Cylera Map to the DSP Toolkit?

The Cylera solution focuses on securing the confidential data of its customers within mission critical applications. Use of the Cylera platform assists customers in either partially or fully fulfilling 40+ evidence items within eight data of the ten data protection standards. Cylera's solution is a scalable platform that enables customers to show compliance with a variety of assertions. These assertions include prioritisation of top data security risks to proven auditing of those systems holding confidential data to guiding staff security training to achieve a culture of privacy and security.

It is important to note the DSPT is not intended to be a complete data security and protection framework. From NHS Digital - "The standards, assertions, and evidence items are not intended to be a complete framework to manage data security and protection. They represent indicators of good practice and maturity." These good practices and maturities can be part of a larger effort to work towards a security framework such as ISO 27001 or NIST CSF. Cylera provides a separate mapping guide illustrating how our solution can aid with fulfillment of that framework's controls.

All organisations that have access to NHS patient data and systems must use this toolkit to supply assurances they are practicing thorough data security and that personal information is handled correctly. This mapping guide illustrates how Cylera can aid Category 1 organisations (i.e., the NHS Trusts) to align with the toolkit.



How Cylera Capability Maps to Data Security and Protection Toolkit (DSPT) Overview

Organisation

NHS Trust Foundation

Industry

Healthcare

Challenges

Adherence to DSPT requirements and securing and protecting IoT, medical devices and patient care

Selection criteria

Automate threat detection to reveal hidden attackers across data center and cloud workloads and user and medical IoT devices

Results

- Discover and inventory assets in complex environments
- Detect hidden vulnerabilities and risks in complex IT infrastructure of data center
- Gain unprecedented visibility into hidden attacks
- Reduce workload of IT team with AI-powered threat hunting investigation

"With our DSP Toolkit submission looming, we found Cylera mapped extremely well to most of the requirements, and specifically some of the new 2022 requirements."

- CTO, Director of Digital Transformation, NHS Trust Hospital

The Cylera Platform has the following key functionality:



IoT/Medical Device Asset Discovery

Cylera automatically discovers and classifies every device on the network, including behavior



Risk & Vulnerability Management

Cylera automates the detection of vulnerabilities and cyber hygiene risks to identify devices affected by variety of security, vulnerability, government and industry alerts.



Continuous Threat Monitoring & Threat Intelligence

Cylera utilises multiple detection engines and Industry threat intelligence detect threats and devices that are under active attack.



Zero Trust, Segmentation, and Response

Cylera can automate policies and integrations to segment and prevent risks to devices as well as to quarantine devices with detected risks or threats. Cylera can integrate and share segmentation policies with tools such as firewalls, networking equipment and NACs to secure devices.

	Assertion	Evidence text – NHS Ref Trusts	Cylera Solution	Required to meet standard
Data Security Standard 1: Personal Confidential Data	Assertion 1.1: The organisation has a framework in place to support Lawfulness, Fairness and Transparency	1.1.3 Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.	<p>Cylera passively discovers all connected hardware and software assets and devices such as in traditional IT, unmanaged IoT, medical devices (IoMT), and OT (such as building automation, power generators, etc.)</p> <p>Each asset is automatically identified and classified with exceptionally detailed device characteristics. For many assets, Cylera can identify operators of the systems and who has access.</p> <p>This data can be easily viewed within the Cylera management console dashboard, exported as report, or sent via API to a Change Management Data Base (CMDB) in support of determining ownership and protection responsibilities.</p>	Yes
Data Security Standard 1: Personal Confidential Data	Assertion 1.3: Individuals' rights are respected and supported (GDPR Article 12-22).	1.3.5 Does your organisation operate and maintain a data security risk register, (including risks from supply chain) which links to the corporate risk framework providing senior visibility?	Cylera automatically assesses and scores security risk for individual assets and groupings of assets and can include supply chain risks. This risk ranking can be linked to the corporate risk framework to give an overall risk score for the estate.	Yes
Data Security Standard 1: Personal Confidential Data	Assertion 1.3: Individuals' rights are respected and supported (GDPR Article 12-22).	1.3.6 What are your top three data security and protection risks?	<p>Cylera's risk summary identifies top security and protection risks by whole organisation, department, asset types such as by manufacturer or by functional type such as imaging, and by individual device.</p> <p>Further, Cylera can provide risk mitigation / response plans to assist in remediation and which if enacted, will ultimately lower the overall risk score.</p>	Yes
Data Security Standard 1: Personal Confidential Data	Assertion 1.3: Individuals' rights are respected and Supported (GDPR Article 12-22).	1.3.8 Your organisation understands when you must conduct a Data Protection Impact Assessment and has processes in place, which links to your existing risk management and project management, to action this	<p>Cylera supports hospital processes for understanding, prioritizing, and mitigating risk. A major capability within the Cylera system is the ability to see when network traffic is transferring private patient data along with the security assessment of IoT, IoMT, and OT assets within the healthcare organisation.</p> <p>See previous sections 1.3.5 and 1.3.6, and Cylera's risk scoring examples, which are also not exhaustive.</p>	Yes
Data Security Standard 4: Managing Data Access	Assertion 4.1: The organisation Maintains a current record of staff and their roles	4.1.1 Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	Cylera supports this broader organizational need through providing visibility into networked logins by users of IoT, IoMT, and OT systems, for which typical IT tools do not give visibility. Cylera can integrate with Active Directory (AD) to track user access to AD registered devices and, depending on the protocol, Cylera captures user details from medical devices that do not require a login such as the attending clinician's name plus time and date of the study.	Yes

	Assertion	Evidence text – NHS Ref Trusts	Cylera Solution	Required to meet standard
Data Security Standard 4: Managing Data Access	Assertion 2: Organisation assures good management and maintenance of identity and access control for its networks and information systems.	4.2.3 Logs are retained for a sufficient period, managed securely, reviewed regularly and can be searched to identify malicious activity.	Cylera's aggregates information about devices, threats, and network behaviors from multiple sources, including external threat intelligence feeds such as NHS Cyber Alert (formerly NHS CareCERT) and other global resources, allowing analysis and reporting on suspicious or unusual activity. Records retention can be configured to align with the Trust's policies.	Yes
Data Security Standard 4: Managing Data Access	Assertion 2: Organisation assures good management and maintenance of identity and access control for its networks and information systems.	4.2.4 Are unnecessary user accounts removed or disabled?	Cylera can report "Users not seen in over 90 days" (or for the time period needed by the trust's policy) to support tracking users who should be removed or disabled from systems they previously had access to. Cylera can be a point of validation that unnecessary user accounts have in fact been removed or disabled, and the reporting can be tuned for the window of time required by the trust.	Yes
Data Security Standard 4: Managing Data Access	Assertion 4.3: All staff understand that their activities on IT systems will be monitored and recorded for security purposes	4.3.2 Are users, systems and (where appropriate) devices always identified and authenticated prior to being permitted access to information or systems?	<p>Whilst many organisations want and need to restrict user or system application access based on authenticated, need-to-know access, it is often difficult to identify and anticipate the various needs of applications, users, and devices.</p> <p>Cylera provides an automated way to identify and review the essential services required by each device or type of device and translate those needs into actively enforced policies. Additionally, via integration with NAC systems and/or SIEMs in IT, Cylera can provide networked user login alerts to unauthorised access or anomalous login behaviours.</p> <p>Cylera can create or modify firewall policies through our integrations that can be accepted by IT for assets that deviate from expected or known behaviours and security policies.</p>	Yes
Data Security Standard 4: Managing Data Access	Assertion 4.4: You closely manage privileged user access to networks and information systems supporting the essential service.	4.4.3 The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation	As part of a layered approach to security controls, Cylera can detect if privileged user access rights are being attempted or granted from a non-corporate device and can alert on this activity to IT SIEM solutions for rapid response. Cylera is also integrated with network access control (NAC) systems and can create and support policies for NAC enforcement.	Yes
Data Security Standard 6: Responding to incidents	Assertion 6.1: A confidential System for reporting data Security and protection from breaches and near misses is in place and actively used.	6.1.1 A policy/procedure is in place to ensure data security and protection incidents are managed/ reported appropriately.	<p>Cylera provides a variety of features to monitor and report data security of IoT, IoMT, and OT assets, and supports incident reporting and management. Cylera is not an incident management system, but fully supports incident and forensic investigations and has been used as a tool by those who perform security risk assessments and incident response.</p> <p>Cylera can route alerts to IT NOC/SOC SIEMs, includes risk ranking and artifacts to substantiate built-in response plans for both IT and Medical Engineering, and can map to the trust's policies and procedures</p>	Yes

	Assertion	Evidence text – NHS Ref Trusts	Cylera Solution	Required to meet standard
<p>Data Security Standard 6: Responding to incidents</p>	<p>Assertion 6.2: All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway</p>	<p>6.2.3 Antivirus/ Anti-malware is kept continuously up to date - we can see it talking out.</p>	<p>Cylera can detect if antivirus is in place and turned on, or out of date through configuration settings for many devices that are able to run AV. However, many unmanaged and medical devices and OT assets that are connected to the internet may not be able to run traditional antivirus software or security agents, this creates a significant security risk for a healthcare organisation.</p> <p>Cylera has patented techniques to more deeply analyse network and device traffic and in combination with patented techniques and threat intelligence feeds, can create a type of digital twin of an active physical device and run standard vulnerability scanners against those devices to further examine for weaknesses, changes, vulnerabilities, vendor and government alerts that may apply to the device details we can see.</p>	Yes
<p>Data Security Standard 6: Responding to incidents</p>	<p>Assertion 6.2: All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway</p>	<p>6.2.6 Number of phishing emails reported by staff per month.</p>	<p>Cylera automatically learns and profiles the behaviours of each asset and can then detect and alert on anomalous activity or zero-day activity that can indicate that the asset is compromised and communicating with known and unknown malicious sites.</p> <p>Even though Cylera is not an email-anti-phishing tool, it can support this need by identification of malware Indicators of Compromise (IoCs), bad behaviour such as command-and-control traffic, and communications to malicious destinations. Cylera's detection then perform policy enforcement actions such as quarantining and network segmentation.</p>	Yes
<p>Data Security Standard 6: Responding to incidents</p>	<p>Assertion 6.3: Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses</p>	<p>6.3.1 If you have had a data security incident, was it caused by a known vulnerability?</p>	<p>Cylera supports the organisation's risk and vulnerability assessment and answer the question, "Was the incident caused by or related to the security incident?" Data on vulnerabilities and risks within the estate can be viewed or printed from the management console.</p> <p>Cylera intimately knows the IoT, IoMT and OT assets in the estate and proactively delivers known vulnerabilities through patented, digital twin scanning techniques and can preventatively identify existing, known vulnerabilities for all these devices ahead of an incident happening.</p>	Yes
<p>Data Security Standard 6: Responding to incidents</p>	<p>Assertion 6.3: Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses</p>	<p>6.3.2 The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.</p>	<p>The Cylera Platform is integrated with various cyber threat intelligence (CTI) feeds including NHS Cyber Alert (formerly CareCERT), and other global sources included in the Cylera Labs proprietary database. This, in combination with automatic alerts on risks and rankings that determine high-risk/high impact vulnerabilities throughout the estate can keep users fully apprised at all times, and most definitely equipped with the information needed to respond within 48hrs, and can validate if the alert has been remediated. Through integrations with trouble-ticketing systems like ServiceNow, Cylera can feed the alert workflow.</p>	Yes

	Assertion	Evidence text – NHS Ref Trusts	Cylera Solution	Required to meet standard
Data Security Standard 6: Responding to incidents	Assertion 6.3: Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses	6.3.3 The organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Cylera continually monitors network communications and endpoint assets within the estate and assesses security gaps and risks. Risk scoring capabilities help focus resources on highest risks to its most critical services and assets. Cylera provides alerts and reports of at-risk assets and can detect cyber events in systems, assets, and services and can be sent to IT SIEM systems for aggregation, prioritization and response.	Yes
Data Security Standard 6: Responding to incidents	Assertion 6.3: Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses	6.3.4 Are all new services that are attractive to cyber criminals (such as for fraud) implementing transactional techniques from the outset?	Cylera supports fraud risk assessment through examining the connected systems and digital services and processed data likely targeted by bad actors, knowing the threat landscape and alerts, advisories and field evidence of which services are vulnerable and commonly targeted by cyber criminals.	Yes
Data Security Standard 6: Responding to incidents	Assertion 6.3: Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses	6.3.5 Have you had any repeat data security incidents within the organisation during the past 12 months?	Cylera supports to verify that vulnerabilities from various threat feed sources have been acted upon, (remediated, mitigated, or patched, etc.) and can verify whether or not repeat security incidents may have occurred within the past 12 months.	Yes
Data Security Standard 7: Continuity Planning	Assertion 7.1: Organisations have a defined, planned and communicated response to Data Security incidents that impact sensitive information or key operational services	7.1.1 Your organisation understands the health and care services it provides.	Cylera delivers foundational supporting information on assets, services and communications between systems and the internet. This is needed information to help document and provide details on the organisation's operational services and dependencies, including power, cooling, surveillance, data, people and the impact of losing the availability of the service. Information within the Cylera platform can be made available as needed for examination and alignment with Trust policies and procedures (stored for 12 months within the Cylera management console or exported and stored for the needed periods.)	Yes
Data Security Standard 7: Continuity Planning	Assertion 7.1: Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services.	7.1.4 You use your security awareness, e.g. threat intelligence sources to make temporary changes in response to a new threat, e.g. a widespread outbreak of very damaging malware.	Cylera uses an array of threat intelligence sources as described in several other areas, to include Cylera Labs' proprietary database, intelligence, and experience in defending other networks, along with NIST NVD data, NHS Cyber Alerts/(previously CareCERT), DHS CISA alerts and advisories, vendor/manufacturer alerts and advisories, MHRA, US FDA, etc. The Cylera Platform and its Threat Intelligence Service can provide reports to support threat intelligence policy and processes at the Trust and this output can be maintained and consumed as Trust policies dictate.	No

	Assertion	Evidence text – NHS Ref Trusts	Cylera Solution	Required to meet standard
Data Security Standard 8: Unsupported Systems	Assertion 8.1: All software and hardware has been surveyed to understand if it is supported and up to date.	8.1.1 Provide evidence of how the organisation tracks and records all software assets and their configurations.	<p>Cylera supports and informs the trust's documented process for managing software assets. The Cylera central management console passively surveys all assets for not only hardware and software versions and knows whether they are out of date (in need of patching and whether a patch exists), as well as if the OS is unsupported.</p> <p>Additionally, Cylera surveys many other characteristics without ever touching the actual IoT, IoMT, and OT, including the vendor, make, model, firmware versions, when last updated, where located in the estate, Active Directory, VLAN and vulnerability information. Cylera monitors all devices connected to the network and identifies any moves, adds, and changes, making it easy to identify the introduction of new or unauthorized devices. Cylera's management console has dashboards and reports that can be printed or shared with supporting systems as needed.</p>	Yes
Data Security Standard 8: Unsupported Systems	Assertion 8.1: All software and hardware has been surveyed to understand if it is supported and up to date.	8.1.2 Does the organisation track and record all end user devices and removable media assets?	Cylera profiles and records all connected devices including those used by end users. However, Cylera does not report on removable media used on end user assets.	Yes
Data Security Standard 8: Unsupported Systems	Assertion 8.3: Supported systems are kept up-to-date with the latest security patches	8.3.1 How do your [estate's] systems receive updates and how often?	Cylera's patent-pending IoT Device Emulation technology allows for detailed, centrally-managed insight into the operating system and patch level of all IoT, IoMT, and OT assets connected to the Trust's estate. Cylera also integrates alerts and advisory feeds from various manufacturers, the MHRA, FDA, NHS Cyber Alert/(formerly CareCERT), and others, whereby it can dynamically alert if needed about device and medical device updates that relate to vulnerabilities and recalls. This enables IT and EBME teams to prioritise any remediation action or service scheduling. Cylera is aware, and can verify when and how often software patches are applied, supporting the Trust's policy.	Yes
Data Security Standard 8: Unsupported Systems	Assertion 8.3: Supported systems are kept up-to-date with the latest security patches	8.3.2 How often, in days, is automatic patching being pushed out to remote endpoints	<p>Cylera is aware of changes (such as automatic patching) performed throughout the estate's IoT, IoMT, and OT assets/endpoints, and provides a centrally managed reporting dashboard for current state and when update patches last occurred.</p> <p>This also provides supporting verification that patching as documented policy and per procedure was actually performed.</p>	Yes

	Assertion	Evidence text – NHS Ref Trusts	Cylera Solution	Required to meet standard
<p>Data Security Standard 8: Unsupported Systems</p>	<p>Assertion 8.3: Supported systems are kept up-to-date with the latest security patches</p>	<p>8.3.3 There is a documented approach to applying security updates (patches) agreed by the SIRO</p>	<p>Cylera supports and informs a documented approach where there is a need to identify and deploy critical and/or high-risk security patches, whether within or outside of normal patching schedules. Cylera's risk reporting dashboards for all assets provide verbiage and links for reviewing Common Vulnerability Enumeration (CVE), Common Vulnerability Scoring System (CVSS) scores (including 7 or greater), advisories and alerts, etc., to help organisations determine their remediation plan and timing for patching or mitigations.</p> <p>Dates of when patches were applied, and policies can be created or modified to establish the needed window of time required to achieve DSP Toolkit requirements. Alerts would then be generated if timelines were not adhered-to.</p> <p>The Cylera system reports per asset, and can be also used for validating that patches were or were not in fact applied in support of a trust's needed documentation. Approval on patches/patch schedules by the SIRO can be supported by Cylera's risk reporting and suggested response plans.</p>	<p>Yes</p>
<p>Data Security Standard 8: Unsupported Systems</p>	<p>Assertion 8.3: Unsupported software and hardware is categorised and documented, and data security risks are identified and managed.</p>	<p>8.3.4 Where a security patch has been classed as critical or high-risk vulnerability, it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO.</p>	<p>Cylera can run reports for critical or high-risk vulnerabilities that have been applied within 14 days for reporting to the SIRO for either risk acceptance or escalation (with a view to mitigation or remediation).</p> <p>Cylera can regularly report patch status to management on individual assets within the estate (or groups of assets by type, vendor, etc.). Schedules for patching within 14 days of patch release notification can be created by policy and supporting reports can be regularly provided for escalation to the SIRO for acceptance or remediation.</p>	<p>Yes</p>
<p>Data Security Standard 8: Unsupported Systems</p>	<p>Assertion 8.3: Supported systems are kept up-to-date with the latest security patches</p>	<p>8.3.5 Where a security patch has been classed as critical or high-risk vulnerability has not been applied, explain the technical remediation and risk management that has been undertaken.</p>	<p>Cylera can run reports for critical or high-risk vulnerabilities that have not been applied within 14 days for reporting to the SIRO for either risk acceptance or escalation (with a view to mitigation or remediation).</p> <p>Cylera supports IoT, IoMT, and OT that have high-risk vulnerabilities with response plans that inform the vulnerability details (CVE, CVSS, NHS Cyber Alerts, DHS CISA alerts and advisories, and with vendor details for obtaining the patch or recommended configuration mitigations – all for use by the trust to help decisions to be made on how to technically remediate the risks, and verify what steps have been chosen.</p>	<p>Yes</p>
<p>Data Security Standard 8: Unsupported Systems</p>	<p>Assertion 8.3: Supported systems are kept up-to-date with the latest security patches</p>	<p>8.3.6 Is your organisation actively using and managing Advanced Threat Protection (ATP)?</p>	<p>Cylera is not an ATP solution but can support and enrich the trust's ATP systems with asset details, IoCs, network traffic analysis, risk scoring, etc., on IoT, IoMT, and OT systems that are susceptible to APTs.</p> <p>Cylera's threat detection and intelligence can also contribute much-needed, timely information from its global sources on the threat landscape within the trust estate.</p>	<p>Yes</p>

	Assertion	Evidence text – NHS Ref Trusts	Cylera Solution	Required to meet standard
<p>Data Security Standard 8: Unsupported Systems</p>	<p>Assertion 8.3: Supported systems are kept up-to-date with the latest security patches</p>	<p>8.3.7 Are 95% of your server estate and 98% of your desktop estate on supported versions of operating systems</p>	<p>When Cylera assesses servers and desktop inventory, it automatically reports on each asset's OS version, and whether the OS is out of support. This process also validates whether the OS is at the release and patch level as documented. Whilst information regarding managed devices can be obtained via Microsoft's ATP solution, this will not provide information needed regarding unmanaged devices that include medical, IoT, shadow IT, and OT systems. When Cylera assesses servers and desktop inventory, it automatically reports on each asset's OS version, and whether the OS is out of support. This process also validates whether the OS is at the release and patch level as documented.</p> <p>Cylera gives an overall security posture risk scoring for individual assets, categories of assets, and for the estate overall, with ability to know the high-risk status of out-of-support. Cylera's reporting can contribute to the walkthrough of the analysis, how calculated, and whether all assets of concern in the estate have been examined.</p> <p>In the case that many medical and IoT devices where it is not possible to patch or upgrade their operating systems leaving an organisation exposed, Cylera can proactively reduce risks by dynamically creating segmentation policies that limit exposure for vulnerable devices.</p>	<p>Yes</p>
<p>Data Security Standard 8: Unsupported Systems</p>	<p>Assertion 8.4: You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service</p>	<p>8.4.1 Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?</p>	<p>Cylera analyses and documents configurations and patch levels of all IoT, IoMT and OT by VLAN, subnet, destination, port, protocol, device group, and more. The platform can further identify weak configurations and vulnerabilities that could be exploited. For each asset's risk posture, Cylera provides needed background on the threats through links and built-in, written response guidance to A.Pts. enhance understanding of the severity of risk and how to mitigate.</p> <p>Based on the observed needs and risks of each asset, input from NHS Cyber Alerts and advisories, Cylera Labs threat detection and intelligence, vendor alerts and advisories, knowledge of EOL/EOS software, Cylera can automatically generate and enforce policies on a per device or group basis. These micro-segmentation policies ensure that lateral East-West spread of a cyber-attack does not impact critical devices as they are shielded from attack. The Cylera SCE can also integrate with traditional 3rd party security products such as firewalls and NAC solutions to enforce contextually aware zero-day policies.</p>	<p>Yes</p>
<p>Data Security Standard 8: Unsupported Systems</p>	<p>Assertion 8.4: You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service</p>	<p>8.4.2 All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.</p>	<p>Many unmanaged devices, including medical equipment such as CT Scanners will not be able to be patched or updated by the IT team and often run operating systems that are either end-of-life or end-of-support and do not receive regular updates from their respective vendors. Cylera mitigates the threat posed by these devices through the enforcement of micro-segmentation policies on firewalls, switches, wireless LAN controllers or via network access control (NAC).</p> <p>Cylera's response to the following assertions can inform the full capabilities of the system to aid unsupported, unpatchable software in multiple ways: 8.1.1, 8.1.3 & 4, 8.2, 8.3.4</p>	<p>Yes</p>

	Assertion	Evidence text – NHS Ref Trusts	Cylera Solution	Required to meet standard
Data Security Standard 8: Unsupported Systems	Assertion 8.4: You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service	8.4.3 You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.	The Cylera solution utilises various industry standard threat feeds including NHS Cyber Alert/(formerly CareCERT), and NVD CVE/CVSS, its own research, other global sources, and active threat defense activities to additionally keep current with publicly known vulnerabilities. Cylera's patented and patent-pending techniques allow it to do vulnerability scanning on assets with zero touch on the actual, physical device in use. Estate assets and their vulnerabilities are centrally managed within the Cylera SCE and automatically detected in real-time and categorized to allow IT and security teams to see all IoT, IoMT, and OT assets quickly and easily with a specific vulnerability or criticality level and includes response plans with recommended remediation steps.	Yes
Data Security Standard 9: IT Protection	Assertion 9.1: All networking components have had their default passwords changed	9.1.1 & 9.1.2 The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password.	As part of its analysis of each device, Cylera can identify assets with weak or default passwords. Cylera continuously monitors the behavior of every asset on the network and can support privileged access management solution configurations and pen testing by reporting on what is actually on the network and whether default or weak passwords are still in use or have changed.	Yes
Data Security Standard 9: IT Protection	Assertion 9.2: A penetration test has been scoped and undertaken.	9.2.1 A penetration test has been scoped and undertaken	Cylera does not perform penetration testing, but supports the function in two ways: 1. Enhancing typical pen testing with reporting on assets that cannot be vulnerability scanned in traditional ways, and instead providing zero disruption through patented techniques. 2. Providing reporting evidence to validate asset configurations, patch levels, and mitigating or compensating controls by policy that have been enacted.	Yes
Data Security Standard 9: IT Protection	Assertion 9.3: Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities	9.3.5 The organisation understands and records all IP ranges in use across the organisation	Cylera delivers passive and continuous monitoring that details all network VLAN and subnets to provide a real-time record plus also show inter-subnet and subnet to internet communications to quickly and easily identify and alert on erroneous traffic flows both internally and internet based	Yes
Data Security Standard 9: IT Protection	Assertion 9.3: Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities	9.3.6 The organisation is protecting its data in transit (including email) using well-configured TLS v1.2 or better.	Cylera can determine TLS versions and earlier (and SSL if in use), and identify assets and their communications that may be handling protected data in transit (PCI, PII, ePHI, etc.), and which VLANs they're a part of. This enables an organisation to ensure that devices, such as some medical equipment, that transmit unencrypted and sensitive data are appropriately secured and in the correct VLAN (i.e. have not been connected to a 'Guest' or insecure VLAN).	Yes

	Assertion	Evidence text – NHS Ref Trusts	Cylera Solution	Required to meet standard
Data Security Standard 9: IT Protection	Assertion 9.3: Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities	9.3.8 The organisation maintains a register of medical devices connected to its network.	Cylera passively discovers and inventories all connected medical devices such as infusion pumps, imaging equipment, diagnostic workstations, heart monitors, and many other biomedical assets connected to its network. This register or inventory is continuously updated with all new devices connected to the network and includes vendor, make, model, IP and MAC addresses, OS, software patch level, firmware level and much more (see description in 1.1.1 important identity depth unavailable to IT and security teams. This function within the Cylera platform supports the requirement for visibility into the connected IoMT, IoT, and even OT devices within the network, and can assist with scheduling maintenance and verifying who has access to the assets.	Yes
Data Security Standard 9: IT Protection	Assertion 9.3: Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities	Mandatory in 2022: 9.3.9 What is the organisation's data security assurance process for medical devices connected to the network?	Cylera can support trust requirements for a data security assurance process and policies for asset lifecycle management of assets connected to the network. Cylera can create or adjust security policies to be enforced across the assets within the estate that can align with the trust's requirements. In reference throughout this document, Cylera provides essential visibility upon first provision through to decommissioning, and reports and validates all the asset characteristics as noted.	Yes
Data Security Standard 9: IT Protection	Assertion 9.6: You securely configure the network and information systems that support the delivery of essential services	9.6.3 The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.	Cylera can assess firewall configurations and report on enabled ports and services. If deviations exist per trust policy and known baseline configuration settings, Cylera can alert and provide reporting as well as adjust or create needed policies for enforcement to protect the estate assets. Cylera will also monitor and report or alert on network infrastructure or devices that have been added, moved or changed dynamically real-time. Ports and services which are allowed or disallowed will be known by the Cylera system and can be alerted upon or reported for verification with IT/Security teams.	Yes
Data Security Standard 9: IT Protection	Assertion 9.6: You securely configure the network and information systems that support the delivery of essential services	9.6.10 You have a plan for protecting devices that are natively unable to connect to the Internet, and the risk has been assessed, documented, accepted, and signed off by the SIRO	Cylera includes a integrated threat detection, uses machine learning and artificial intelligence to detect anomalous behavior, and ingests multiple sources containing threat intelligence, advisories, vulnerability databases, FDA recalls, NHS Cyber Alert, banned devices, to identify devices with risks and have been compromised. Utilising this, Cylera automatically creates a risk score and can generate reports.	Yes

	Assertion	Evidence text – NHS Ref Trusts	Cylera Solution	Required to meet standard
<p>Data Security Standard 10: Accountable Suppliers</p>	<p>Assertion 10: The organisation can name its suppliers, the products and services they deliver and the contract durations</p>	<p>10.1.1 The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.</p>	<p>Cylera can support trust efforts to achieve and maintain a list of its suppliers that are handling personal information, and the security risk status of their products.</p> <p>Often, organisations are not entirely aware of all their suppliers across the estate, and may not be current on who has access, what type of access, what types of OS, patch levels, internet browsers and plugins may be in use, etc.</p> <p>Cylera can augment and support other systems for tracking suppliers by centrally identify connected and networked supplier systems that could potentially pose a data security or data protection risk to the organisation based on vulnerabilities, patch levels, OS version, end-of-life and end-of-support (EOL/EOS) OS versions, etc., and with what other assets in the estate the supplier systems are interacting.</p>	<p>Yes</p>

Appendix: Standard Overview

Data Security Standard 1

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes

Data Security Standard 2

All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3

All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

Leadership Obligation 2: Process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

Data Security Standard 4

Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5

Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6

Cyber-attacks against services are identified and resisted and CareCERT / Cyber Advisories security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Leadership Obligation 3: Technology: ensure technology is secure and up-to-date.

Data Security Standard 8

No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Additional Resources to Help from NHS Digital

Overview

www.dsptoolkit.nhs.uk/Help/overview

Video Guides

www.digitalsocialcare.co.uk/latest-guidance/video-guides-how-to-complete-the-data-security-protection-toolkit/

Completing Standards

www.digitalsocialcare.co.uk/latest-guidance/completing-standards-met-on-the-data-security-and-protection-toolkit/

Big Picture Guides

www.dsptoolkit.nhs.uk/Help/big-picture-guides


About Cylera

Cylera is the leading edge in IoT, IoMT, and enterprise OT security and intelligence. The Cylera Platform is a centralized cybersecurity solution that secures the entire connected IoT environment from the enterprise side to patient care medical devices.

Cylera's patented technology delivers unique depth in asset identification and management, network analysis, risk assessment, network segmentation, threat detection and intelligence, operational analytics and fleet optimization. Cylera delivers the strongest, most advanced IoT, medical device (IoMT), and enterprise OT cybersecurity risk management solution for the industry.

Founded in late 2017, Cylera is developed and maintained in the U.S.A, headquartered in New York, with offices in the U.K.

www.cylera.com

 Core to Cloud Ltd

 @CoretoCloud

CORE T~~Ø~~ CLOUD™

Core to Cloud Ltd, The Castle, Cecily Hill, Cirencester, GL7 2EF, United Kingdom

+44 (0) 1285 708 313 | info@coretocloud.co.uk | www.coretocloud.co.uk



ISO 27001:2013 Certificate Number 11945-ISM5-001