LOGPOINT

Using Logpoint to Meet the NHS Data Security and Protection Toolkit

www.logpoint.com

Table of Contents

"The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practicing good data security and that personal information is handled correctly."

https:// www.dsptoolkit.nhs.uk

Introduction

The Data Security and Protection Toolkit (DSPT) replaced the Information Governance toolkit from April 2018.

The DSPT has moved away from levels of assurance, and towards mandatory evidence-based system which is more precise. It is aligned with the 10 data security standards and the General Data Protection Regulation (GDPR).

As part of this assessment, all of the mandatory items need to be completed, and be deemed 'satisfactory'.

This document aims to provide insights and guidance as to where the Logpoint SIEM solution would assist in meeting the requirements outlined in the DSPT, and where additional value may be gained by the use of the Logpoint SIEM technology for any NHS trust.

A key focus for the Logpoint SIEM solution is enabling customers to gain visibility into their entire security ecosystem. To improve security through proactive alerting, machine learning, and to address compliance and reporting requirements. This enables access to incident and security information in a quick and effective manner.

A modern SIEM such as Logpoint is therefore a key enabling technology to address the requirements outlined in the NHS Data and Security Protection toolkit.

Data Security and Protection Toolkit: Logpoint Value Assessment

Based upon an analysis of the DSPT, Logpoint have assessed where the Logpoint SIEM solution can provide significant value, enabling NHS organisations to achieve DSPT compliance.

The analysis details of the assertions and evidence items that either benefit from, or fundamentally require, the deployment of a SIEM solution.

- Assertions highlighted in blue are a mandatory requirement for Category 1 and 2 (NHS Trusts, CSU, ALBs and ICBs)
- Assertions not highlighted are optional

Assertion	Evidence Ref	Evidence text	Tool Tips	Logpoint Value
The organisation assures good management and maintenance of identity and access control for it's networks and information systems	4.2.3	Logs are retained for a sufficient period, reviewed regularly, and can be searched to identify malicious activity.	Organisational policy should set out the rules defining log retention. The average time to detect a cyber-attack is over three months and it is not uncommon for incidents to take significantly longer to detect. The most important logs for identifying malicious activity should be held for six months as a minimum. Organisations should consider the ability to trace an incident end to end e.g. network address translation logs can help organisations trace traffic back to the original source address. Please refer to National Cyber Security Centre guidance.	Logpoint is a modern SIEM providing a centralised log storage and big data platform that scales to any organisation's size. Logs in Logpoint are stored out-of-band, away from the source systems. The Logpoint platform provides role-based access to log data, including "data privacy" functionality that can mask sensitive data until approved under a four-eye principle. Log data cannot be modified or removed by users once ingested into the platform. All data held in Logpoint is indexed and fully searchable, including based on key/value pairs as well as full text searches.
	4.2.4	Unnecessary user accounts are removed or disabled.	Former employees', guest and other unnecessary accounts are routinely and promptly removed or disabled from internal workstations, Active Directory domains and other user directories. Privileged user access is also removed when no longer required or appropriate. This should be included in polices covering access control.	Logpoint provides account auditing facilities for Active Directory that allow administrator to quickly identify dormant accounts. Logpoint can help identify user accounts misused as service accounts. Using Logpoint Security Orchestration, Automation and Response (SOAR), such accounts can immediately removed right from within

				the platform and even automated, or automated after manual review.
You closely manage privileged user access to networks and information systems supporting the essential service	4.4.1	The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel. They are stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate.	Organisational policy should set out the rules defining log retention, the approach to storage of logs, including details on maintaining the integrity of the logs and offline backup for disaster recovery purposes. The average time to detect a cyber-attack is over three months and it is not uncommon for incidents to take significantly longer to detect. The most important logs for identifying malicious activity should be held for six months as a minimum. Guidance from NCSC on maintaining security of logs is available. Note: you are not expected to purchase a CSOC."	Also see 4.3.2 Logs in Logpoint are stored out- of-band, away from the source systems. The Logpoint platform provides role-based access to log data, including “data privacy” functionality that can mask sensitive data until approved under a four-eye principle. Log data cannot be modified or removed by users once ingested into the platform. Logs held in Logpoint are only accessible to authenticated users, based on role-based access integrated with Active Directory. Logpoint supports audit functionality for a variety of platforms, such as Windows (Active Directory, Office 365, servers, and workstations), Unix and databases. Using audit logging, Logpoint can provide dashboards, alerts and reports for user logging activity, including failed login, apparent brute-force attempts, and bad password management practices. Logpoint UEBA can identify unusual behaviour patterns based on machine learning against a baseline of activities of users and their peer group.
You ensure your passwords are suitable for the information you are protecting	4.5.2	Technical controls enforce password policy and mitigate against password guessing attacks	Examples of technical controls are provided by the National Cyber Security Centre.	Logpoint can audit user login attempt and alert on multiple failed login attempts in short succession. This is a useful additional layer of security on top of existing operating system policies to verify that these are applied successfully. There are often gaps – users who

				have their password policies disabled or overridden, or systems that do not adhere to organisation wide policies
Process reviews are held at least once a year where data security is put at risk and following data security incidents	5.1.1	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security incident, with finding acted upon	Explain how the organisation identifies the root cause of data security and protection incidents, how it uses this to design and implement mitigating controls to either prevent similar incidents from occurring in the future or to be in a position to better manage them if they do occur. This should be undertaken with a multi-disciplinary team. Provide details where process review findings have informed the immediate future technical protection and remediated any systemic vulnerabilities of the system or service, to ensure identified issues cannot arise in the same way again	Any root cause analysis relies on the evidence and evidence impossible to obtain without effective log management in place to capture and retain this information as well as making it accessible for quick retrieval when required. Once evidence has been obtained, additional alerts can be configured to proactively identify and act upon breaches going forward.
Action is taken to address problems processes as a result of feedback at meetings or in year	*5.3.1*	*Actions to address problem processes are being monitored, and assurance is given to the board or equivalent senior team.*	*Explain the governance around escalation of any issues and findings to the board equivalent, such as through reports and briefing notes, during the last twelve months.*	*If the business processes are changed or improved to address the problems, a SIEM can be the technical control to monitor the effective technical application of these process changes as they are usually evident in log messages and can be monitored and audited.*
All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.	6.2.3	Anti-malware and Anti-Virus is kept continually up to date.	Provide an explanation of how this is achieved. This could be through Automatic update, central deployment, ATP.	The Logpoint SIEM is able to monitor and report on Anti-Virus update failures for a multitude of Antivirus vendors. This information can be used to create blacklist of systems that warrant a higher level of alerting if their Antivirus systems are out of date.
Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses	6.3.1	If you have had a data security incident, was it caused by a known vulnerability?	Provide details of incidents over the reporting period (a year). Known vulnerabilities are those listed on the Cyber Alerts portal. If no incidents have occurred, state: ”None”.	Logpoint integrates with a wide variety of third-party threat feeds that provide information about specific know threat payloads/hashes and destination domains/addresses. Logpoint also integrates with various Vulnerability Management tools and can

				use their findings in updated white- and blacklists for vulnerable devices.
	6.3.2	The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.	Your response (chould cover 'high severity' cyber alerts issued over the last 12 months.	Being able to collate and present all information responsive to a security incident is a key functionality of a SIEM solution and almost impossible to achieve in the required timeframes if manual retrieval and analysis of log files is required. Using Logpoint Security Orchestration Automation and Response (SOAR), playbooks can be identified to automatically collect additional evidence and carry out specific checks before a human analyst investigates a case, dramatically decreasing response times.
	6.3.3	The Organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Since 1st July 2022, all systems monitoring requirements have been assessed and technology solutions and processes have been implemented to detect cyber security events. A risk-based approach to monitoring for all systems should be in place ensuring that the organisation's most critical services and assets are in scope of its monitoring solutions. Where any gaps have been identified, mitigations have been put in place.	Logpoint can audit and monitor a virtually limitless number of systems and activities both for administrative access and changes as well as login activities, file access, database queries etc. and proactively alert on access or configuration changes.
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 security changes in response to new threats, e.g. a widespread outbreak of very damaging malware*		*Logpoint integrates with a wide variety of threat sources, paid for and free, to enrich log and traffic data with potential indicators of compromise. Logpoint can proactively alert when evidence of these connections and activities is seen within the customer's environment. Logpoint also aligns to the Mitre ATT&CK framework, giving alignment, visibility and intelligence of security threats against a recognised security standard.*

You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.	9.4.4	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way		Being able to collate and present all information responsive to a security incident is a key functionality of a SIEM solution and almost impossible to achieve in the required timeframes if manual retrieval and analysis of log files is required.
You securely configure the network and information systems that support the delivery of essential services	9.5.3	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.	Provide details of your organisation's change management process that prevents changes to its IT environment from being implemented without being approved by the appropriate individuals and security implications being considered.	Also see 6.2.3. By monitoring all configuration and system change events on both infrastructure as well as systems and endpoints, unauthorised configuration changes can be identified and alerted on, or alternatively documented and audited.

The Logpoint approach to the NHS

Logpoint is able to deliver a best-in-class SIEM solution, with a seamless initial deployment providing a stable and scalable platform that will meet NHS organisational needs now and in the future.

Logpoint's uniquely unlimited enterprise NHS license model, based upon the guiding principle that customers should not be restricted in the use of their software or the volumes of log data the solution digests, **enables unrestricted data (EPS) ingestion, with special pricing aligned for the NHS.**

- ***Scalable Enterprise Solution*** - Logpoint adopts an agile approach to deployment of SIEM capability, designed around a modular solution. This ensures that we can provide functionality and deliver value quickly, whilst providing a scalable platform able to support the organisation as data complexity and volumes increase over time. The Logpoint solution has already been deployed by a number of NHS and healthcare organisation as well as global enterprises and large government departments.

- ***Ease of Deployment and Continuous Support*** - Logpoint have supported many hundreds of deployments. A common response from customers is their surprise at how simple the process is and how quickly the platform is deployed, configured and presenting events and information previously not available. Logpoint takes logs from any source and has a huge range of pre-configured use cases which customers can deploy out-of-the-box. The support provided by Logpoint's dedicated team of support analysts and developers is second to none.

- ***Pricing Assurance*** - Whilst most enterprise SIEM providers price their solutions based on the amount of data taken into the platform, the Logpoint standard pricing model is based on the number of devices (nodes). For the NHS, Logpoint has also aligned the option to purchase an **unrestricted enterprise license at a significant discount**. With data volumes ever increasing, the Logpoint approach enables customers to very easily and accurately budget future costs, providing greater cost certainty over the short, medium and longer term.

- ***Enabling the full potential of SIEM*** - The unlimited enterprise license model enables NHS organisations to bring in as much data as possible to provide further context; opposed to SIEM solutions that charge based on data volume which may deter an organisation from bringing in as much data as they could, would or should. Logpoint enables the full potential of SIEM.