Gigamon for the NCSC Cyber Assessment Framework for the NHS

Gigamon Mapping Guide

January 2025

Table of Contents

Introduction

The National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) collection consists of the CAF itself, together with a range of linked guidance and some background on its intended use. It is aimed at helping an organisation, including critical national infrastructure entities such as the National Health Service (NHS), achieve and demonstrate an appropriate level of cyber resilience. This resilience is crucial in protecting vital functions performed by these organisations, which are at risk of disruption due to serious cyber incidents.

This paper presents a comprehensive mapping guide, offering Gigamon as a support for organisations navigating the compliance landscape of the NCSC CAF. Specifically, it is designed for:

- Organisations subject to the Network and Information (NIS) regulations
- Organisations within the UK critical national infrastructure (CNI), including the NHS
- Organisations managing cyber-related risks to public safety
- Public sector organisations that support core government functions

This checklist is structured to provide a systematic breakdown of the legislative provisions and articles related to Gigamon's capabilities, enabling organisations such as the NHS to implement the necessary measures to meet the CAF's requirements.

CAF and cyber resilience in the NHS

Network and information systems and the essential functions they support play a vital role in society, from ensuring the supply of electricity, water, oil, and gas, to the provision of healthcare through institutions such as the National Health Service (NHS), and the safety of passenger and freight transport. The reliability and security of these systems are crucial for maintaining the daily operations and wellbeing of society.

These systems are not only essential but also attractive targets for malicious actors and are susceptible to disruptions caused by system failures. The Cyber Assessment Framework (CAF) establishes comprehensive guidelines to strengthen the overall security of the Critical National Infrastructure (CNI), which includes the NHS, against potential cyber threats and disruptions. These guidelines particularly focus on essential functions, such as those provided by the NHS, where any compromise could result in significant harm to the economy, society, the environment, and individual welfare—including loss of life.

Gigamon Solutions for CAF Compliance

Gigamon provides a deep observability pipeline that efficiently delivers network-derived intelligence to cloud, security, and observability tools aligns with NCSC Cyber Assessment Framework.

Gigamon goes beyond security and observability log-based approaches by extracting real-time network intelligence derived from packets, flows, and application metadata to deliver defense-in-depth and complete performance management, a crucial step in compliance with the overarching objectives of NCSC CAF.

Objective A – Managing Security Risk

	NCSC CAF	Gigamon
A1 Governance	The organisation has appropriate management policies, processes and procedures in place to govern its approach to the security of network and information systems.	Gigamon plays a vital role in helping organisations establish and maintain effective management policies, processes, and procedures to govern the security of their network and information systems providing full visibility into network traffic and system interactions, ensuring that management policies are based on accurate and complete information about the organisation's network environment. Gigamon's traffic analysis capabilities allow organisations to monitor compliance with security policies, providing detailed reports that help ensure policies are being followed and are effective. Gigamon can enforce security policies by ensuring that only legitimate traffic and activities are allowed within the network. This includes filtering and controlling traffic based on predefined rules that align with the organisation's security policies

Objective A – Managing Security Risk, cont'd

	NCSC CAF	Gigamon
A2 Risk Management	The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	Gigamon assists organisations in identifying, assessing, and understanding security risks to the network and information systems that support the operation of essential functions. Gigamon provides comprehensive visibility into all network traffic, including east-west (lateral) and north-south traffic. This allows organisations to see all data flows, applications, and interactions within the network, helping them identify potential risks that could otherwise go unnoticed. Gigamon enables deep packet inspection (DPI), which allows for detailed analysis of network traffic. DPI can reveal hidden threats, suspicious activity, or anomalies that could indicate potential security risks. Gigamon provides a move to a proactive security posture that goes beyond conventional MELT-based approaches
A3 Asset Management	Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	Gigamon plays a crucial role in helping organisations understand and manage everything required to deliver, maintain, or support networks and information systems that are necessary for the operation of essential functions. This includes ensuring a clear understanding of data, people, systems, and supporting infrastructure such as power or cooling. Gigamon provides a holistic view of the entire network, enabling organisations to see all data flows, system interactions, and dependencies. This visibility is essential for understanding how different components, such as data, people, and systems, interact to support essential functions. Gigamon helps organisations discover and map out all assets, including managed/unmanaged servers, network devices, applications, and data repositories, that are necessary to support essential functions.
A4 Supply Chain	If an organisation relies on third parties (such as outsourced or cloud-based technology services) it remains accountable for the protection of any essential function. This means that there should be confidence that all relevant security requirements are met regardless of whether the owning organisation or a third party operates the function. For many organisations, it may make good sense to use third party technology services.	Gigamon helps organisations maintain accountability and ensure that security requirements are met when relying on third parties, such as outsourced or cloud-based technology services, in the following ways. Gigamon provides visibility into both on-premises and cloud environments, allowing organisations to monitor network traffic regardless of where it resides. This ensures that the organisation has continuous oversight over its data and operations, even when they are managed by third parties. Gigamon allows organisations to monitor and verify that third-party service providers are adhering to the agreed-upon security standards. By analysing traffic to and from third-party services, organisations can ensure that these providers are implementing proper security controls and that their network behaviour aligns with security expectations, a move to proactive security posture that goes beyond conventional MELT-based approaches

Objective B – Protecting against cyber attacks

	NCSC CAF	Gigamon
B1 Service Protection Policies, processes and procedures	The organisation defines, implements, communicates and enforces appropriate policies, processes and procedures that direct its overall approach to securing systems and data that support the operation of essential functions.	Deep observability into network traffic, encrypted traffic is crucial for ensuring security policies are being applied correctly and no malicious activity is bypassing security controls, also validating that security policies are enforced across the entire network. By integrating with security tools, Gigamon helps verify that security policies are working as intended. For example, it can help ensure that firewalls are blocking prohibited traffic or that data loss prevention (DLP) systems are catching sensitive data leaks. Gigamon maximises the effectiveness of security processes by optimising the flow of data to security tools by filtering and deduplicating traffic, which ensures that these tools operate efficiently. and reduces the chances of missing critical threats due to performance bottlenecks.
B2 Identity and Access control	The organisation understands, documents and manages access to networks and information systems and supporting the operation of essential functions. Users (or automated functions) that can access data or services are appropriately verified, authenticated and authorised.	Gigamon helps organisations understand, document, and manage access to networks and information systems, ensuring that users or automated functions are properly verified, authenticated, and authorised. Gigamon provides deep visibility into all network traffic, including data from both internal and external sources. This visibility allows organisations to see exactly who or what is accessing their networks and systems, giving them a clear understanding of access patterns and potential vulnerabilities. Gigamon monitors and logs all user activity on the network. This includes tracking access attempts, successful logins, and any actions taken by users. These logs are crucial for understanding who is accessing what resources and when.
B3 Data Security	Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on essential functions. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of essential functions. It also covers information that would assist an attacker, such as design details of networks and information systems.	Gigamon helps protect data stored or transmitted electronically from unauthorised access, modification, or deletion by providing comprehensive security solutions that ensure the integrity, confidentiality, and availability of critical data. Comprehensive data visibility by providing deep visibility into all network traffic, including data in motion. This ensures that all data transmitted across the network is monitored and inspected for potential security threats. By having complete visibility, security teams can detect unauthorised access or attempts to modify or delete data. Gigamon also offers the ability to decrypt SSL/TLS encrypted traffic, allowing security tools to inspect the content for any unauthorised actions. This prevents attackers from hiding malicious activities within encrypted data streams.
B4 System Security	Network and information systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to essential functions informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	Risk-Based Visibility - Gigamon helps organisations prioritise their focus on the most critical areas of the network based on risk assessments. By understanding the specific risks associated with essential functions, organisations can apply more robust protective measures where they are most needed. Gigamon integrates with threat intelligence platforms to provide up-to-date information on the latest cyber threats. This enables the organisation to continuously assess risks and adjust security measures accordingly.

Objective B – Protecting against cyber attacks, cont'd

	NCSC CAF	Gigamon
B5 Resilient Networks and systems	The organisation builds resilience against cyber attack into the design, implementation, operation and management of systems that support the operation of essential functions.	Security by design – Gigamon provides visibility into network traffic from the outset, ensuring that security is integrated into the design phase of system development. This allows for identifying potential vulnerabilities and ensuring that systems are built with robust security measures from the ground up. By offering solutions that integrate seamlessly with existing security tools and infrastructure, Gigamon helps organisations design networks that are both secure and resilient. This includes ensuring that critical assets are protected and that there are no blind spots in network visibility.

Objective C – Detecting cyber security events

	NCSC CAF	Gigamon
C1 Security Monitoring	The organisation monitors the security status of the network and information systems supporting the operation of essential functions to detect potential security problems and to track the ongoing effectiveness of protective security measures.	Gigamon plays a crucial role in helping organisations monitor the security status of their networks and information systems, particularly those supporting essential functions. This capability is key to detecting potential security problems and tracking the ongoing effectiveness of protective security measures. Gigamon provides deep and comprehensive visibility into all network traffic, including both east-west (lateral) and north-south communications. This visibility is critical for detecting potential security issues across the entire network infrastructure in addition Gigamon provides visibility into encrypted traffic, ensuring that security monitoring is not hindered by encryption. This helps in identifying potential threats that may be hidden within encrypted data flows.
C2 Proactive Security event discovery	The organisation detects, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature-based security prevent/detect solutions (or when standard solutions are not deployable).	Gigamon helps to detect and remediate challenges with HTTP, HTTPS, and DNS traffic by providing visibility into: • Unusual DNS Traffic • Shadow IT • Suspicious DNS Traffic • Abnormal activities in HTTPS/Web traffic • HTTP Traffic Policy Violations • Suspicious HTTP Traffic • HTTP Error Codes Also helps to detect and remediate issues related to unmanaged devices, suspicious connections, and traffic outside norms • IoT Unmanaged Devices • Unwanted Services and Port Misuse • Traffic Outside Norms Finally detect rogue activities related to unsanctioned applications that can pose challenges to network and security • Unsanctioned P2P Apps • Crypto Jacking

Objective D – Minimising the impact of cyber security incidents

	NCSC CAF	Gigamon
D1 Response and recovery planning	There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.	In the event of a security incident, Gigamon provides the necessary data for forensic analysis. This helps in understanding whether policies were bypassed, how the breach occurred, and what adjustments need to be made to prevent future incidents.
D2 Lessons learned	When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.	Deep observability ensures that security teams have full visibility into all network traffic, which is essential for identifying and understanding the scope of an incident. This includes both real-time and historical data allowing teams to pinpoint when and how an incident occurred. Gigamon provides enriched metadata and contextual insights from network traffic to help quickly identify the route cause of an incident. This context is essential to help understand the sequence of events leading to an incident. Gigamon integrates with SIEM and SOAR platforms to streamline incident response process ensuring all relevant data is available for a coordinated response

Conclusion

As organisations, including the National Health Service (NHS), strive to adhere to the comprehensive guidelines laid out in the NCSC Cyber Assessment Framework, Gigamon emerges as a strategic partner in fortifying cyber resilience. This paper has highlighted how Gigamon's ability to provide a deep observability pipeline aligns with each CAF objective, offering organisations like the NHS a robust and proactive approach to cybersecurity and regulatory compliance.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com