Pentera & Kubus Achieving CAF Readiness

WHITEPAPER FOR HEALTHCARE TRUSTS

November 2024

Navigating the CAF Framework with process and Validation

About this document:

This document is intended to assist NHS staff who are involved in protecting their environment (Cyber Security) and for those involved in implementing the Framework's processes and guidelines, such as Cyber Essentials, ISO27001, NHS DSP Toolkit and CAF. It works as an easy-to-read document for C-suite and cyber security teams who are tasked with strategy around meeting framework requirements.

At Pentera, we understand the challenges of cyber professionals in the healthcare sector who are typically working within environments where there is a lack of resources and an abundance of legacy infrastructure and third-party systems to manage. These conditions make it difficult to map out attack surfaces and prioritise true risk. Within this context, the need for security validation is compounded, to ensure that inherent vulnerabilities are managed and remain benign.

In this guide, you will find details on how security validation software helps you meet framework requirements, and even better, supports you to automate the process, linking in with ISO27001 and continuous checking. Both of which are otherwise quite complicated to address and extremely manual and time-consuming without validation software.

What is CAF?

From the NCSC website:

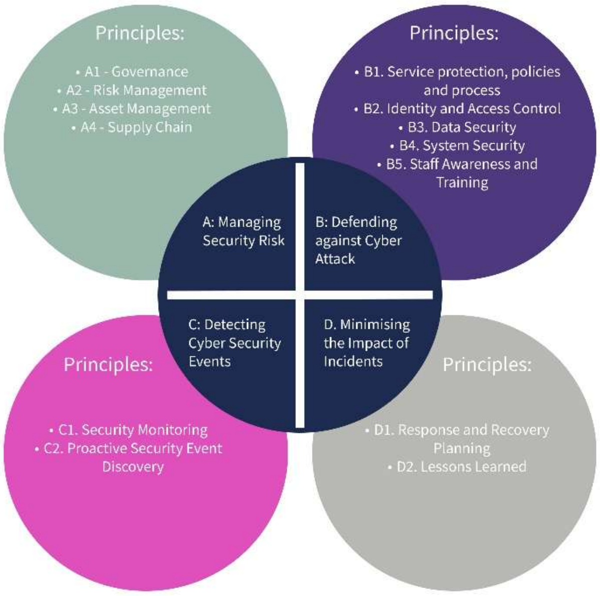
"Cyber incidents can result in a number of different consequences, depending on the nature of the network and information systems targeted and the intention of perpetrators. Circumstances in which the possible consequences of cyber incidents are extremely serious or even, perhaps catastrophic, generally require very robust levels of cyber security and resilience. It is for these circumstances that the NCSC has developed the Cyber Assessment Framework (CAF) collection.

The 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 achieve and demonstrate an appropriate level of cyber resilience in relation to certain specified vitally important functions performed by that organisation, functions that are at risk of disruption as a result of a serious cyber incident."

Using validation software with CAF

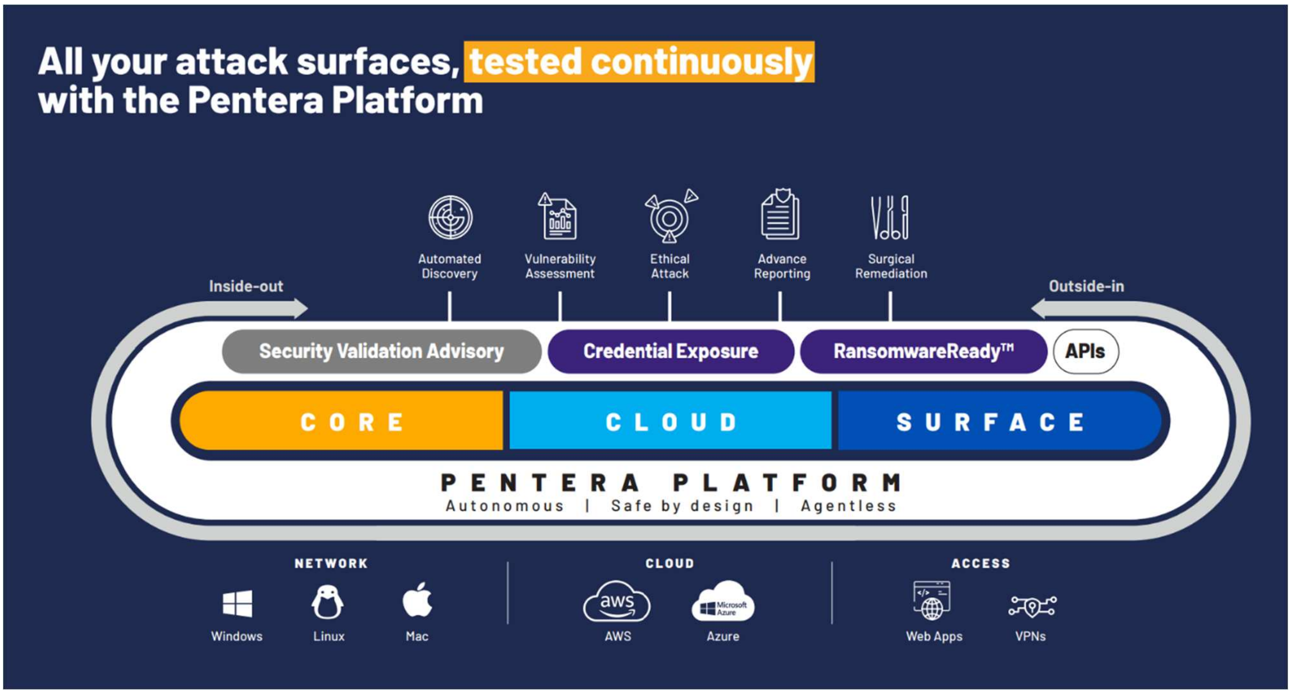
You have decided to work towards implementing CAF principles. Whether that's due to direction from above, or a conscientious decision for your Trust to achieve the level of cyber resilience the principles support, the first question is where do you start?

1. Understand the 4 main principles:
    - Manage Risk
    - Defend
    - Detect
    - Minimise impact
2. Implement the correct tools.
3. Create process and automation, which can be linked to your existing ISO27001 process.


Principles:
• A1 - Governance
• A2 - Risk Management
• A3 - Asset Management
• A4 - Supply Chain
Principles:
• B1. Service protection, policies and process
• B2. Identity and Access Control
• B3. Data Security
• B4. System Security
• B5. Staff Awareness and Training
A: Managing Security Risk
B: Defending against Cyber Attack
C: Detecting Cyber Security Events
D. Minimising the Impact of Incidents
Principles:
• C1. Security Monitoring
• C2. Proactive Security Event Discovery
Principles:
• D1. Response and Recovery Planning
• D2. Lessons Learned

Continuous threat exposure testing aligned with the Cyber Assessment Framework

To measure real-world cyber resilience there is a safer way to stress test your security controls across your organisation, and that aligns nicely with the CAF framework. Pentera together with Kubus Group Consultancy Services supports Trusts to implement the principles of CAF. While there is no silver bullet, towards achieving CAF adoption, continuous testing and validation provides you with the necessary proof that your security stack and processes are working as they should.



All your attack surfaces, tested continuously with the Pentera Platform

If you think one, or a few products and processes, have you covered, can you rest easily? Without continuous validation across your security system, there is really no way to be sure.

The Pentera Platform automatically uncovers real exposures in the organisation's environment. It challenges the entire IT attack surface (internal and external) by safely emulating the actions of an attacker, providing real-time security validation at scale.

Automation is at the heart of the Pentera platform.

With Pentera, trusts can continuously reduce cyber posture by performing validation tests as frequently as needed - daily, weekly, or monthly. Evidence-based test findings are prioritised based on their risk impact, giving trusts the ability to focus remediation efforts on the vulnerabilities that matter the most.

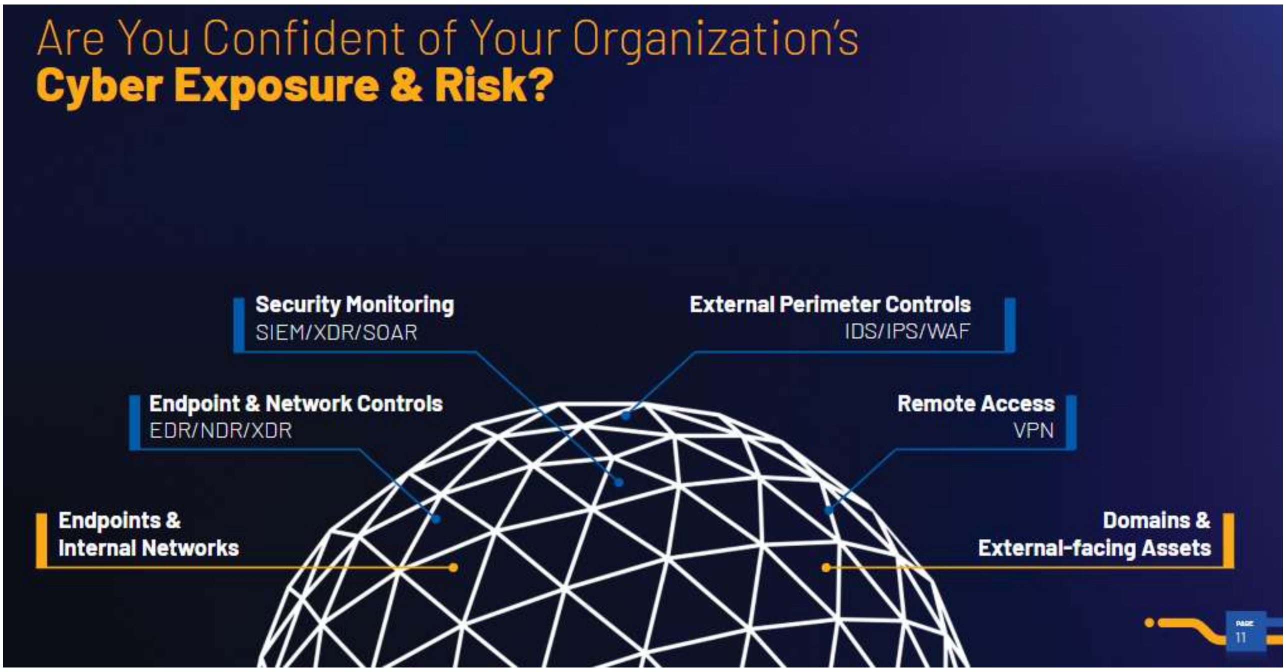
Step One - Understand the 4 Main Principles

Objective	Explanation	How Pentera Supports Adoption
Manage Risk	Ensure that the appropriate organisational structures, policies, processes, and procedures are in place to understand, assess, and systematically manage security risks to the network and information systems supporting essential functions.	You can combine Pentera with your existing processes (such as ISO) to cover this entire section. With Pentera in place, you can build a strong Risk Management platform, giving you real detail on where your exposures are and how to fix them.
Defend	Proportionate security measures are in place to protect the networks and information systems supporting essential functions from cyber-attacks.	As your cyber maturity evolves over time you want to ensure that you are getting continued value from new and existing cyber investments and identify controls that might need to be deprecated as they are no longer fit for purpose or overlap with other services. Pentera tests if your defenses are working, are there any misconfiguration problems that could be causing weaknesses in your defence? Has a recent update or policy change compromised defensive controls?
Detect	Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions.	Pentera allows you to validate if your existing security tools are detecting attacks, and that alerts are correctly identified locally and globally and trigger the correct response activities, as you make policy changes you want to test that the right outcomes are achieved.

Objective	Explanation	How Pentera Supports Adoption
Minimise impact	Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential function(s), including the restoration of those function(s) where necessary.	The lessons learned feature of CAF becomes quite interesting in this section, running automated security validation on a regular basis will detect if making changes to your environment has weakened any areas of your defence or improved upon them. This allows you to gather lessons learned without going through a real attack.

Step Two - Implementing the Correct Tools

Many organisations already have "Cyber Security" and "Network Security" products in place such as EDR/MDR/XDR, AV, SASE, NAC, NGFW, typically, the missing part is validation. Is your security system tested? Does it actually prevent attacks? Have your security investments successfully kept you protected?



Are You Confident of Your Organization's
Cyber Exposure & Risk?

Security Monitoring
SIEM/XDR/SOAR
External Perimeter Controls
IDS/IPS/WAF
Endpoint & Network Controls
EDR/NDR/XDR
Remote Access
VPN
Endpoints & Internal Networks
Domains & External-facing Assets

Manual pentesting has its place for certain use cases, however, a large part of testing can be automated at scale so it can be run regularly. We are all working in a constantly changing IT landscape which necessitates the need for continuous assessments to provide better visibility across the estate, at scale. A regular testing cadence supports the CAF framework which requires you to test your solution after making changes to your IT infrastructure.

Where running pentests manually is very cost-prohibitive for the average healthcare trust, running some pentests automatically, makes it far more feasible. The automated pentest run can also be used after implementing remediations, to check that those mitigations are indeed working and effective.

Pentesting generally selects a sample of your network or estate and focuses on finding weaknesses in a limited scope. We have found instances where the core organisation is in a good state but outliers, such as shadow IT, subdomains, and branch offices pose risks that were missed during a fixed pentesting engagement. Pentera can be used to run pentests across a distributed architecture, where multiple remote sites or networks can be scanned. These sites can be co-located within a single building (either part of or not part of the same LAN), or spread across different geographical areas. All sites are managed by a single management console.

Linking to Your Existing ISO27001 Process

Pentera can enhance and streamline ISO 27001 processes by directly addressing core aspects of ISO requirements through automated, adversarial-focused testing and comprehensive security validation capabilities.

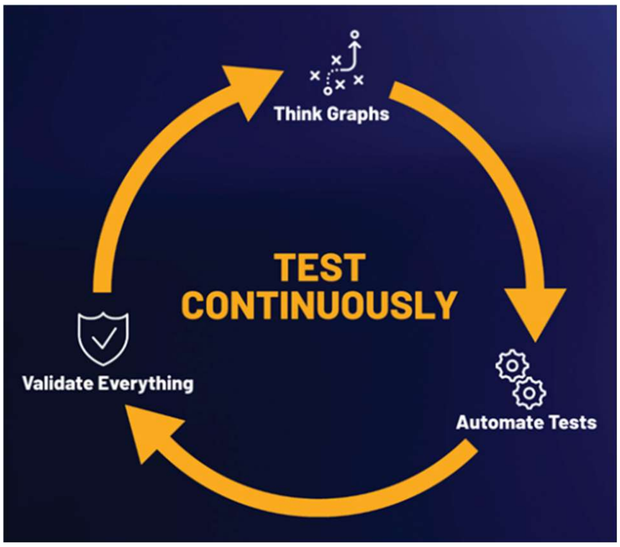
- Risk Assessment and Treatment (Clause 6.1.2)
- Information Security Objectives (Clause 6.2)
- Operational Security (Clause 8)
- Performance Evaluation and Reporting (Clause 9.1 & 9.2)
- Continuous Improvement (Clause 10)

By aligning Pentera with ISO 27001's structured approach to security management, organisations can achieve a higher level of compliance, reduce audit preparation time, and maintain a dynamic, robust security posture that is consistently validated against real-world threats.

Accelerate CAF Adoption with Pentera & Kubus

The combined partnership between Pentera and Kubus is equipped to provide access to named contacts who can advise on strategies using Pentera. Experts such as Solution Architects, who have a background in red teaming and cyber security, can be leveraged to advise on testing regimes and remediation advice that evolves with your cyber maturity journey through regular touchpoints and engagements.

With continuous automated validation software in place, your existing Risk Management Processes (with a little tweaking) will include everything you need. Providing you with insights as to how changes in your environment affect your security posture.



Framework Advisory Services

Pentera's Security Validation Advisory (SVA) program includes the consultancy services of UK-based advisors. Our experts have years of experience supporting UK enterprises and trusts with a wide-range of relevant compliance standards. They are equipped to provide crucial guidance on CAF adoption by offering expert-led, actionable insights into meeting alignment with its principles. They will assist with gap analysis related to CAF principles, and map critical attack paths - highlighting exposures that could hinder CAF compliance.

Agentless, Safe by design & Scalable platform

Pentera's platform is easy to deploy without needing intrusive agents on endpoints. This minimises operational disruptions and reduces setup complexity. The agentless deployment streamlines validation across diverse environments — whether cloud, on-premises, or hybrid — without the maintenance challenges of agent-based solutions.

Built-in safety controls ensure that Pentera's emulated attacks are conducted without risking data integrity or operational continuity. This allows organisations to rigorously test their defenses in production environments, gaining real-world insights without the potential for adverse impacts.

Pentera's platform easily scales to cover large, complex infrastructures, enabling consistent security validation across all network segments and attack surfaces. This scalability supports frequent and comprehensive testing, which is essential for maintaining a high level of cyber resilience as environments evolve.

Data stored where you want it, on-premises or the cloud

Pentera offers flexible data storage options—either on-premise or in the cloud—allowing organisations to balance regulatory compliance, scalability, and accessibility according to their unique needs. This dual storage approach enables organisations to choose the best fit for their security and operational requirements, enhancing the effectiveness of their security validation efforts while ensuring compliance and adaptability.

One-Day Proof of Value

Without any complex setup or deployment requirements, in a 1-day POV you can run real-world security validation tests across your environment to see Pentera's value. By the day's end, users receive an in-depth report that prioritises security gaps based on their impact, illustrating Pentera's ability to streamline remediation efforts and strengthen security posture through continuous, automated validation. This fast, hands-on assessment helps organisations immediately understand the tangible benefits and operational ease Pentera brings to their security programs.

Next Steps:

If you find this document useful and you would like a deeper dive into CAF, continuous testing, and meeting the framework principles, or if you would like to arrange a one-day challenge with Pentera at your premises, you can book a meeting with one of our security experts using the link below.

Get in touch

Links:

- www.pentera.io
- www.kubus.com
- www.ncsc.gov.uk/collection/cyber-assessment-framework/introduction-to-caf
- https://www.kubus.com/partners/pentera/achieving-caf-readiness/#book-meeting