The UK National Cyber Security Centre Cyber Assessment Framework

An Approach to a Successful Implementation

Executive Summary

Since the release of the Cyber Assessment Framework (CAF) by the UK National Cyber Security Centre (NCSC), many UK Critical National Infrastructure (CNI) organisations have implemented the CAF to better understand and manage cyber risk.

The CAF provides guidance for organisations responsible for vitally important services and activities and can be applied by businesses of any size within any industry. Currently, its application is required in certain sectors of the UK economy covered under the UK Network and Information Systems (NIS) Regulations of 2018[1]. With the publication of the Government Cyber Security Strategy in January 2022, the UK Government has shown it intends to place greater emphasis on the CAF as a mechanism for government departments to assess their cyber maturity.

The CAF defines four top-level objectives consisting of 14 principles with guidance on how to apply them. The principles are designed to help organisations make their digital services cyber resilient and demonstrate the level of resilience achieved. Critically, the principles are outcome-focused and describe good cybersecurity practices, ultimately describing the steps organisations need to take to prevent/minimise the impact of incidents.

Palo Alto Networks aligns with the CAF's primary directive of enabling CNI operations to effectively manage security risks, protect against cyberattacks, detect cybersecurity events, and minimise the impact of cybersecurity incidents. Palo Alto Networks is natively integrated to counter cyberattacks before they manifest in an organisation's environment. With full visibility into traffic – across the network, endpoints, and the cloud – organisations can mitigate and minimise cyberattacks regardless of how or where applications and data reside or are being used. This allows CNI and other organisations to identify the most serious ongoing threats to key business operations and reduce overall cybersecurity risk.

This white paper explores the benefits of the CAF and how Palo Alto Networks capabilities and products map to and fulfil CAF guidance.

[1] "The Network and Information Systems Regulations 2018" Legislation.gov.uk, May 2018, https://www.legislation.gov.uk/uksi/2018/506/made

Objectives	Principles
A: Managing security risk	A1: Governance
	A2: Risk management
	A3: Asset management
	A4: Supply chain
B: Protecting against cyber attack	B1: Service protection policies & processes
	B2: Identity & access control
	B3: Data security
	B4: System security
	B5: Resilient networks & systems
	B6: Staff awareness & training
C: Detecting cyber security events	C1: Security monitoring
	C2: Proactive security event discovery
D: Minimising the impact of cyber security incidents	D1: Response & recovery planning
	D2: Lessons learned

Source: National Cyber Security Centre, The Cyber Assessment Framework 3.0

This section further explores the practicalities in delivering the principles laid out in the CAF and highlights some of the key outcomes and additional guidance from the NCSC to ensure successful adoption and maximise the return of effort.

Objective A: Managing Security Risk – An enduring and effective managed risk approach must work dynamically in every tier of the organisation.

The approach should begin with an understanding of what 'good' looks like for the organisation and its business processes and objectives. It will then be possible to detect and react to any anomalies or divergences. This is best achieved by establishing an accurate and real-time understanding of the organisation's digital estate, including an inventory of its assets (hardware, software, virtual, and services) and their locations, connectivity, and interactions. It is this understanding of the cyber-estate, combined with an authoritative register of services, data criticality, and owners that will put the organisation in an excellent position to commence its CAF-aligned transformation.

Objective B: Protecting against Cyberattack – Once an organisation has identified and classified the 'cyber-estate' with the 'sanctioned', 'tolerated', and 'unsanctioned' classifications – for all applications, workflows, services, users and privileges – the next step to effective zero trust implementation is to segment and deploy as 'actionable' and 'enforced' policies throughout the architecture. This will effectively reduce an organisation's exposed attack surface whilst having no impact on its day-to-day operations. NCSC's secure-by-design[2] and zero trust principles[3] can provide further support during this phase.

[2] "Secure design principles," National Cyber Security Centre, https://www.ncsc.gov.uk/collection/cyber-security-design-principles
[3] "Zero trust architecture design principles," National Cyber Security Centre, https://www.ncsc.gov.uk/collection/zero-trust-architecture

Objective C: Detecting Cybersecurity Events – Once the digital estate has been defined and the attack vectors minimised, it is essential that the resultant business interactions are proactively protected to not only detect attacks and anomalous behaviour but also to prevent exploits as close to the point of origin as possible. Given the level of complexity, it is essential that cyber events are detected, correlated, and mitigated automatically to ensure the most responsive model and free up the scarce human resources to focus on the edge-case analyses. This prevention model should leverage the best in Machine Learning (ML) and Artificial Intelligence (AI) to prevent anomalous bad behaviours effectively and automatically.

Finally, effective detection of cyber events needs to be augmented by threat intelligence, using high-powered data analytics to spot anomalies in real-time and enabling the prevention technology (deployed for Objective B) to apply the alerting and automated mitigations in a seamlessly integrated approach. This should include integration of third-party and supply chain feeds.

Objective D: Minimising the impact of Cybersecurity Incidents – Once an organisation has been impacted by a security event, it is imperative that it reacts swiftly and decisively to minimise the disruption and potential losses.

If the above objectives have been completed successfully then an organisation will:

- Know key decision-makers and service owners for Critical Services.
- Segment the services so surgical isolation can be promptly achieved and recovery commenced.

Thus, it will be able to deliver an effective, timely, and measured response to any security event.

Another key measure to help minimise the impact of cybersecurity incidents is the adoption of incident response planning and exercises. Initiatives such as the NCSC Exercise in a Box[4] and other Cyber-Range-type activities will allow staff to practise response drills.

Key Enablers for Success

Cybersecurity adversaries are perpetually changing techniques, and organisations need to update and modify their processes – which means continually changing the configurations of systems. This places additional burdens on organisations striving to achieve and maintain the required security posture. People and processes are not always as agile or scalable enough to meet the challenges.

Therefore, it is essential that organisations leverage automated integrated intelligence and prevention-focused tool sets that can help protect systems, users, and devices – irrespective of their locations. Palo Alto Networks believes there are six cardinal enablers that will assist in achieving a successful implementation aligned with the CAF's four objectives. These are mapped below.

[4] "Exercise in a Box," National Cyber Security Centre, https://www.ncsc.gov.uk/information/exercise-in-a-box

Objectives	Principles	Enablers					
		Visibility	Reduce attack surface	Prevent exploits	Threat intel & exposure	Vulnerability management	Config, ops & training
A: Managing security risk	A1: Governance	●					●
	A2: Risk management	●	●	●	●	●	●
	A3: Asset management	●	●	●	●		
	A4: Supply chain	●	●	●	●	●	
B: Protecting against cyber attack	B1: Service protection policies & processes	●	●	●			
	B2: Identity & access control	●	●	●	●		
	B3: Data security	●	●	●	●		
	B4: System security	●	●	●	●	●	
	B5: Resilient networks & systems	●	●	●	●	●	
	B6: Staff awareness & training	●					●
C: Detecting cyber security events	C1: Security monitoring	●	●	●	●	●	
	C2: Proactive security event discovery	●	●	●	●	●	
D: Minimising the impact of cyber security incidents	D1: Response & recovery planning	●	●	●		●	●
	D2: Lessons learned	●					●

Figure 1: The six enablers mapped against the CAFs objectives

Palo Alto Networks Can Support These Six Enablers by Helping Organisations To:

Have Complete Visibility – The key to any successful implementation will be the ability of an organisation to have full visibility of its assets and associated risks by focusing on workflows, devices, locations, and services, including custom applications. Moreover, it must be deployed consistently across an organisation's entire digital estate (public/private clouds and on-prem) for all users and services.

Palo Alto Networks capabilities can help organisations to visualise their network, cloud, and endpoint dataflows spanning all protected ingress and egress points, whilst accurately identifying thousands of different applications and services across all of the digital estate. For those custom or bespoke protocols not automatically categorised, there is an ability to set specific/tailored definitions. This enables accurate mapping of all existing traffic and starts the process of defining corporate 'sanctioned', 'tolerated', and 'unsanctioned' policies.

Reduce the Attack Surface – Having defined these policies and identified the residual risks, the same technologies can be used to enforce these policies across the key axes of network and location, and persona and device hygiene. All policies need centralised management and reporting across the organisation. This approach will not only assist in maintaining the minimum attack surface but also reduce the resources required to maintain this posture whilst providing a real-time compliance view across the entire digital estate.

Palo Alto Networks can also provide a scalable, remote access solution for organisations' hybrid working needs that leverage all of the above capabilities.

Prevent Known and Unknown Exploits – Once an organisation has minimised its attack surface from both a zero trust and hygiene axis using the same technologies, it is now possible to ensure that all traffic is inspected to ensure it does not contain any known or unknown exploits or threats.

Palo Alto Networks detection engines use classical signature-based patterns, behavioural analytics, machine learning, and artificial intelligence techniques to help ensure that all aspects of your environment have the optimum automated prevention delivered in-depth at all critical points within your digital estate – not just at the network level.

Leverage Threat Intelligence and Visualisation – In the dispersed digital environment, it is also important to ensure that organisations will implement protection profiles and continually challenge that posture by actively looking from all viewpoints to ensure no accidental or unplanned changes have been made resulting in exposing weaknesses.

Palo Alto Networks products and consulting services include dedicated specialist resources that can provide impact reports to assist with this continual analysis – as well as specific security posture reports and advice, assistance with monitoring any third-party capabilities, and the provision of compliance views that can be designed to be dynamically presented in dashboards and consumed by all levels of an organisation.

Undertake Vulnerability Management – In considering vulnerability management two key factors should be addressed:

- **Operational Vulnerabilities** – Those vulnerabilities that an organisation inherits through the consumption of third-party services and software.
- **Development Vulnerabilities** – Those vulnerabilities that an organisation introduces during internal development cycles of specific capabilities and workflows. NCSC provide guidance on this in their Secure Design Principles[5] and Secure Development and Deployment Principles[6].

Palo Alto Networks technologies will support real-time auditing and vulnerability analysis across the complete DevSecOps cycle. These technologies are suitable from dynamic container-based environments to more traditional server deployments.

Configuration, Management and Operations, Training and Exercises – An organisation can deploy the most capable technologies and services, but these must be optimised and maintained to ensure they continue to provide the required effects. This includes ensuring staff are suitably equipped and trained to fully leverage these preventative capabilities.

Palo Alto Networks supports this continual service management and improvement. Palo Alto Networks training and education programme has a range of consulting and professional services that can assist an organisation at all levels and stages of its journey. It is essential that training is dynamic and reflective of the shifting business operations, threat landscape, and best practices at all levels of the organisation. NCSC has a good online resource[7] to start this activity.

[5] "Secure design principles," National Cyber Security Centre, https://www.ncsc.gov.uk/collection/cyber-security-design-principles

[6] "Secure development and deployment guidance," National Cyber Security Centre, https://www.ncsc.gov.uk/collection/developers-collection

[7] "NCSC's cyber security training for staff now available, National Cyber Security Centre, https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

How Can the Palo Alto Networks Platform Help?

Palo Alto Networks has developed disruptive and effective cybersecurity solutions that reflect the real needs of organisations and their users. Our extensive portfolio maps across multiple disciplines and technology areas, which align with the key enablers discussed. Figure 2 below maps solutions and services that can contribute to comply with the CAF and the other key derived principles, as well as reducing present and future risk.

Principles	Network security	SASE	Cloud native security	SECOPS	Threat intel & consulting	Education & pro services
Visibility	●	●	●	●	●	
Reduce attack surface	●	●	●	●	●	◖
Prevent known & unknown exploits	●	●	●	●	●	
Threat intelligence	●	●	●	●	●	
Vulnerability management	●	●	●	●	◖	
Configuration, management, operations & training					●	●

Figure 2: Palo Alto Networks solutions and services to contributre to comply with the CAF

For further information about how Palo Alto Networks capabilities can assist organisations' CAF implementation as identified in the table above, see:

paloalto NETWORKS

140 Leadenhall Street
London, EC3V 4QT
United Kingdom

0800 028 3904

www.paloaltonetworks.com

The UK National Cyber Security Centre Cyber Assessment Framework