NIPPER OmniSight
BY TITANIA

Automation Capabilities | NCSC CAF

# NCSC Cyber Assessment Framework Automation Summary

Your guide to the Contributing Outcome and Indicator of Good Practice evidence automated by Nipper OmniSight

titania.com

# Nipper OmniSight CAF Automation Capabilities

This summary explains the resilience risk and exposure visibility that Nipper OmniSight automates for routers, switches and firewalls in your essential functions (EFs), mapped to the National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF). The CAF has 4 objectives (rows A-D) divided into 14 Principles with which organizations must comply. NCSC has identified 39 Contributing Outcomes (CO) that demonstrate a company is acting on the CAF Principles, along with Indicators of Good Practice (IGPs) that evidence compliance. The 24 COs that Nipper OmniSight supports are listed in the table below, along with the details of the IGPs for routers, switches and firewalls, that Nipper OmniSight can automate evidence for.

| **A** | **CAF Objective: Managing Security Risk** | |
|---|---|---|
| | **Contributing Outcomes (CO)** | **Contributing Outcomes (CO)** |
| **A2.a** | **Risk Management Process:**<br>Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of the essential function(s) (EFs) and communicating associated activities | **Nipper OmniSight continuously monitors the "readiness and resilience" of essential function segmentation ensuring your risk assessments are:**<br>• Based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your EFs and your sector; and<br>• Informed by an understanding of the vulnerabilities in the network and information systems supporting EFs. |
| **A2.b** | **Assurance:**<br>You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to EFs. | **Nipper OmniSight continuously reports pentestaccurate visibility of EF exposure posture trends against (i) sector specific exploited attack vectors and (ii) macro segmentation Indicators of Compromise (IOCs), showing:**<br>• Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way. |

| A | CAF Objective: Managing Security Risk (Continued) | |
|---|---|---|
| | **Contributing Outcomes (CO)** | **Contributing Outcomes (CO)** |
| **A3.a** | **Asset Management (AM):**<br>Whichever risk management method your organization uses, AM will play a key role as you cannot effectively manage risks without understanding what assets are part of the EF. | **Nipper OmniSight provides near real-time visibility of configuration changes, proactively detecting,collecting and updating Configuration Management Databases (CMDBs), to assure that:**<br>• All assets relevant to the secure operation of EFs are identified and inventoried (at a suitable level of detail), and the inventory is kept up-to-date. |

| B | CAF Objective: Defending against Cyber Attack | |
|---|---|---|
| | **Contributing Outcomes (CO)** | **IGP evidence that can be automated** |
| **B1.b** | **Policy and Process Implementation:**<br>You have successfully implemented your security policies, processes and procedures and can demonstrate the security benefits achieved. | **Nipper OmniSight automates proactive near real-time security policy enforcement with monitoring of configuration benchmarks and known exploited vulnerabilities (KEVs) to demonstrate:**<br>• Appropriate action is taken to address all breaches of policies, processes and procedures with potential to adversely impact EFs including aggregated breaches |
| **B2.b/c** | **Device and Privileged User Management:**<br>b) You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential function(s).<br>b) You closely manage privileged user access to network and information systems supporting the essential function(s). | **Nipper OmniSight automates near real-time assessment of all indicators of Privilege Escalation in EFs - specifically blacklisted IPs with unauthorized access and blacklisted local accounts with privileged access, assuring that:**<br>b) All privileged operations performed on your network and information systems supporting your EFs are conducted from highly trusted devices, such as Privileged Access Workstations, dedicated solely to those operations.<br>c) Privileged user access to your EF systems is carried out from dedicated separate accounts that are closely monitored and managed. |

| B | CAF Objective: Defending against Cyber Attack (Continued) | |
|---|---|---|
| | **Contributing Outcomes (CO)** | **IGP evidence that can be automated** |
| **B3.a/ b/c** | **Understanding Data:**<br>a) You have a good understanding of data important to the operation of the essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would adversely impact the EFs.<br>b) You have protected the transit of data important to the operation of the EFs. This includes the transfer of data to third parties<br>c) You have protected stored soft and hard copy data important to the operation of the EFs | **Nipper OmniSight uses labelling in the CMDB and accurate posture reporting of every router, switch and firewall protecting EFs, to show you have:**<br>a) Current understanding of the data links used to transmit data;<br>b) Identified and protected (effectively and proportionately) all the data links that carry data important to the operation of the EF; and<br>c) Suitable, secured backups of data to allow the operation of the EFs to continue should the original data not be available. This may include off-line or segregated backups, or appropriate alternative forms such as paper copies. And that necessary historic or archive data is suitably secured in storage. |
| **B4.a** | **Secure by Design:**<br>You design security into the network and information systems that support the operation of the EFs. You minimise their attack surface and ensure that the operation of the EFs should not be impacted by the exploitation of any single vulnerability. | **Set-up and monitor macro segmentation whitelists in Nipper OmniSight to continuously update the CMDB and ensure network readiness and resilience by enabling effective Attack Surface Management (ASM) and disaster recovery, to assure your:**<br>• Network and information systems are segregated into appropriate security zones and that EFs have been designed with simple data flows and are easy to recover. |

| B | CAF Objective: Defending against Cyber Attack (Continued) | |
|---|---|---|
| | **Contributing Outcomes (CO)** | **IGP evidence that can be automated** |
| **B4.b** | **Secure Configuration:**<br>You securely configure the network and information systems that support the operation of EFs | **Nipper OmniSight enables you to manage "configuration as code" in line with NIST 800-160 Developing Cyber Resilient Systems principles by using a CMDB as a "digital network twin" to assess pre-and post-deployment policy, segmentation and ASM exposure impact of EF config changes, demonstrating:**<br>• You have identified, documented and actively manage (e.g. maintain security configurations, patching, updating according to good practice) assets that need to be carefully configured to maintain the security of the EFs;<br>• All platforms conform to your secure, defined baseline build, or the latest known good configuration version for that environment;<br>• You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented;<br>• You regularly review and validate your network and information systems have the expected, secure settings and configuration;<br>• Standard users are not able to change settings that would impact security or the business operation; and<br>• Generic, shared, default name and built in accounts have been removed or disabled. Where this is not possible, credentials to these accounts have been changed |
| **B4.c** | **Secure Management:**<br>You manage your organisation's network and information systems that support the operation of the EFs to enable and maintain security | **Nipper OmniSight automates macro segmentation whitelist validation and blacklist reporting by IP, port and account, demonstrating your:**<br>• Systems and devices supporting the operation of the EFs are only administered or maintained by authorised privileged users from highly trusted devices, such as Privileged Access Workstations, dedicated solely to those operations. |

| B | CAF Objective: Defending against Cyber Attack (Continued) | |
|---|---|---|
| | **Contributing Outcomes (CO)** | **IGP evidence that can be automated** |
| **B4.d** | **Vulnerability Management:**<br>You manage known vulnerabilities in your network and information systems to prevent adverse impact on the EFs | **Nipper OmniSight automatically prioritises remediation of misconfigurations and CISA KEVs by segment criticality and ATT&CK tactics, techniques and procedures (TTPs) exposure to demonstrate:**<br>• Announced vulnerabilities for all software packages, network and information systems used to support your EFs are tracked, prioritised and mitigated (e.g. by patching) promptly; and<br>• Regular testing to fully understand vulnerabilities of the network and information systems that support the operation of your EFs and verify this understanding with third-party testing. |
| **B5.a** | **Resilience Preparation and Design:**<br>You are prepared to restore the operation of your EFs following adverse impact. | **Nipper OmniSight allows you to set-up, test and continuously monitor segmentation whitelists and identification of segmentation blacklists by IP, port, and account, to enable:**<br>• Security awareness and threat intelligence sources to identify new or heightened levels of risk, which result in immediate and potentially temporary security measures to enhance the security of your network and information systems (e.g. in response to a widespread outbreak of very damaging malware). |

| B | CAF Objective: Defending against Cyber Attack (Continued) | |
|---|---|---|
| | **Contributing Outcomes (CO)** | **IGP evidence that can be automated** |
| **B4.c** | **Backups:**<br>You hold accessible and secured current backups of data and information needed to recover operation of your EFs. | **Nipper OmniSight enables you to maintain a complete and up to date CMDB and digital twin back-up (complete with change history for each config file) allowing (i) EF disaster recovery testing by restoring from CMDB and (ii) forensic post-incident recovery root cause analysis, assuring that:**<br>• You have appropriately secured configuration information backups (including data, configuration information, software, equipment, processes and knowledge);<br>• Backups are accessible to recover from an extreme event;<br>• Your comprehensive, automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event; and<br>• Backups of all important data and information needed to recover the EFs are made, tested, documented and routinely reviewed. |

| C | CAF Objective: Detecting Cyber Security Events | |
|---|---|---|
| | **Contributing Outcomes (CO)** | **IGP evidence that can be automated** |
| **C1.a** | **Monitoring Coverage:**<br>The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your EFs. | **Nipper OmniSight automatically assesses configs for IP connection changes between your network and the internet and between EF segments to identify access, privilege escalation or lateral movement exposure and IOCs where there is no traffic, demonstrating that:**<br>• Monitoring is based on an understanding of your networks, common cyber attack methods and what you need awareness of in order to detect potential security incidents; and<br>• Detecting the presence or absence of IOCs on your EFs is easy. |

| C | CAF Objective: Detecting Cyber Security Events (Continued) | |
|---|---|---|
| | **Contributing Outcomes (CO)** | **IGP evidence that can be automated** |
| **C1.c/d** | **Generating Alerts & Identifying Security Incidents:**<br>c) Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts<br>d) You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response. | **Nipper OmniSight automatically prioritises near realtime alerts by risk, helping expedite EF remediation and response by sector specific attack vectors, TTPs and IOCs, demonstrating that:**<br>c) Log data is enriched with other network knowledge and data when investigating certain suspicious activity and alerts can be easily resolved to network assets using knowledge of networks and systems. The resolution of these alerts is performed in almost real time; and<br>d) Threat intelligence sources or services you have selected use risk-based and threat-informed decisions based on your business needs and sector. |
| **C1.e** | **Monitoring Tools and Skills:**<br>Monitoring staff skills, tools and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have knowledge of the EFs they need to protect. | **Nipper OmniSight delivers proactive continuous (near real-time) "readiness and resilience" monitoring and visibility, frees up people and focuses them on EF risk-prioritized remediation and response, demonstrating:**<br>• Monitoring tools make use of all log data collected to pinpoint activity within an incident and monitoring staff and tools drive and shape new log data collection and can make wide use of it; and<br>• Monitoring staff are aware of the operation of EFs and related assets and can identify and prioritise alerts or investigations that relate to them. |
| **C2.a** | **System Abnormalities for Attack:**<br>You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify. | **Nipper OmniSight leverages "normal" EF segmentation whitelists (IPs, Ports, Accounts) to identify "abnormal" blacklists/IOCs, assuring that:**<br>• Normal system behaviour is fully understood to such an extent that searching for system abnormalities is a potentially effective way of detecting malicious activity and the system abnormalities you search for consider the nature of attacks likely to impact on the network and information systems supporting the operation of your EFs. |

| C | CAF Objective: Detecting Cyber Security Events (Continued) | |
|---|---|---|
| | **Contributing Outcomes (CO)** | **IGP evidence that can be automated** |
| **C1.c/d** | **Generating Alerts & Identifying Security Incidents:**<br>c) Evidence of potential security incidents contained in your monitoring data is reliably identified and triggers alerts.<br>d) You contextualise alerts with knowledge of the threat and your systems, to identify those security incidents that require some form of response. | **Nipper OmniSight automatically prioritises near realtime alerts by risk, helping expedite EF remediation and response by sector specific attack vectors, TTPs and IOCs, demonstrating that:**<br>c) Log data is enriched with other network knowledge and data when investigating certain suspicious activity and alerts can be easily resolved to network assets using knowledge of networks and systems. The resolution of these alerts is performed in almost real time; and<br>d) Threat intelligence sources or services you have selected use risk-based and threat-informed decisions based on your business needs and sector. |
| **C2.b** | **Proactive Attack Discovery:**<br>Monitoring staff skills, tools and roles, including You use an informed understanding of more sophisticated attack methods and of normal system behaviour tomonitor proactively for malicious activity. | **Nipper OmniSight's proactive near real-time network change detection and monitoring alerts you to (i) unauthorized network changes; and (ii) IOCs such as blacklisted IPs, ports, and accounts, demonstrating that you:**<br>• Routinely search for system abnormalities indicative of malicious activity on the network and information systems supporting the operation of your EFs, generating alerts based on the results of such searches; and<br>• Have justified confidence in the effectiveness of your searches for system abnormalities indicative of malicious activity. |

| D | CAF Objective: Minimising Impact of Cyber Security Incidents | |
|---|---|---|
| | **Contributing Outcomes (CO)** | **IGP evidence that can be automated** |
| **D1.a** | **Response Plan:**<br>You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your EFs and covers a range of incident scenarios. | **Nipper OmniSight uses labels of assets associated with each EF in the CMDB, to assess attack surface TTP and IOC exposure by segment, focusing remediation and response teams on quick and effective incident mitigation and/or recovery plans,ensuring they are:**<br>• Based on a clear understanding of the security risks to the network and information systems supporting your essential function(s); and<br>• Comprehensive (i.e. covers the complete lifecycle of an incident, roles and responsibilities, and reporting) and covers likely impacts of both known attack patterns and of possible attacks, previously unseen. |
| **D1.b** | **Response and Recovery Capability:**<br>You have the capability to enact you incident response plan, including effective limitation of impact on the operation of your EFs. During an incident, you have access to timely information on which to base your response decisions. | **Nipper OmniSight continuously updates the CMDB, providing a digital network twin of each EF, enabling "configuration as code" approach to minimizing risk of network issues through predeployment testing and ensuring Disaster Recovery and subsequent root cause analysis is effective, so:**<br>• Nipper OmniSight continuously updates the CMDB, providing a digital network twin of each EF, enabling "configuration as code" approach to minimizing risk of network issues through predeployment testing and ensuring Disaster Recovery and subsequent root cause analysis is effective, so: |
| **D1.c** | **Testing and Exercising:**<br>Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment. | **Nipper OmniSight enables the use of CMDB configuration files to (i) enable EF disaster recovery tests run by EFs and (ii) minimise risk of such cyber incidents from planned production changes through pre-deployment testing of config changes in the digital twin, to ensure:**<br>• Exercise scenarios are based on incidents experienced by your and other organisations or are composed using experience or threat intelligence.<br>• All parts of your response cycle relating to your essential function(s) (e.g. restoration of normal function(s) levels) are exercised and tested. |

**The NCSC Cyber Assessment Framework (CAF), which underpins many regulatory standards in the UK and beyond, including NIS2 and EU DORA, recognizes that not all essential functions and not all networks are critical. This CAF advocates for a truly risk-focused approach to developing the readiness and resilience of critical functions and segments. Highlighting that in a rapidly changing threat environment, NOC, SOC and Incident Response need visibility of fundamental information detailed in the CAF, to proactively secure their networks, including:**

Exploitable vulnerabilities introduced by planned and/or unauthorized network changes

Overall attack surface posture by mission critical segments

Exposure to specific APT TTPs as a consequence of network misconfigurations and software vulnerabilities

Indicators of compromise, including macro segmentation violations (IPs, Ports and Users)

**Nipper OmniSight is designed precisely to address this, proactively and at scale.**

TITANIA

Get in touch to arrange a demonstration of how to automate evidence of Indicators of Good Practice, to demonstrate compliance with the Cyber Assessment Framework.

Learn more at titania.com

**USA**
Suite 600,
2451 Crystal Dr, 6th Floor,
Arlington, VA 22202

**UK**
167-169 Great Portland Street,
London, England,
W1W 5PF