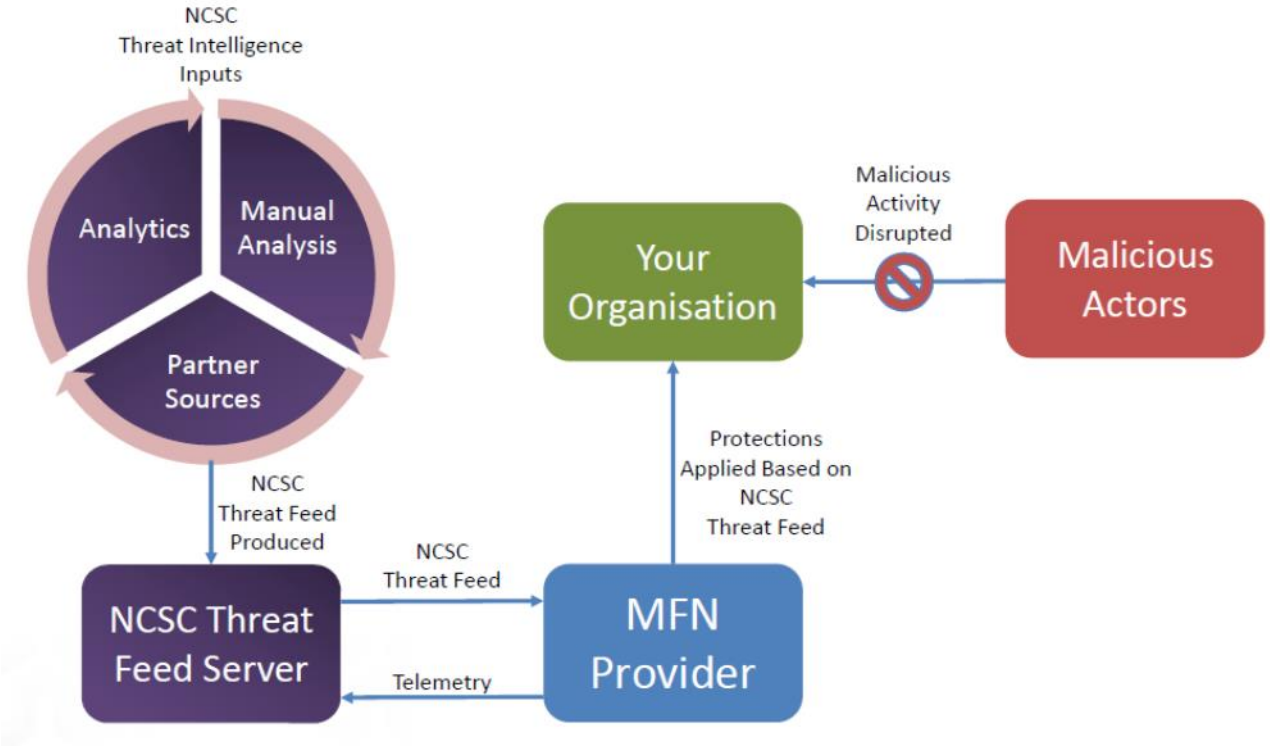
SERVICE DESCRIPTION: MALWARE FREE NETWORKS (MFN)

DESCRIPTION

The purpose of Malware Free Networks (MFN) is to provide a service-based Cyber Threat Intelligence (CTI) feed consolidation platform (based on STIX2/TAXII) to New Zealand small to medium enterprises, large corporates, and government to enhance the overall security posture of each subscribed organisation. The vision of MFN is to "Deliver a scalable, future-proof cyber security service to New Zealand through collaborative partnership".

The One New Zealand service is designed to consume CTI feeds from several sources, however, most significantly is the use of the Malware Free Networks (MFN) threat feed provided by the NCSC and the Phishing Disruption Service threat feed provided by NZ CERT.

The indicators of compromise (IoCs) derived from these CTI feeds are used to deploy a detection and disruption capability across various One New Zealand security services, with an initial focus on using DNS as the primary disruptor to malicious actors' threats.



NCSC MFN SERVICE

The NCSC gathers threat intelligence from partner sources and provides the information via the use of STIX2 & TAXII to One New Zealand's Threat Intelligence Service. One New Zealand then uses the threat intelligence to enhance the protection of services and solutions which integrate into our customers infrastructure.

Telemetry and sighting information for MFN derived indicators is reported back to the NCSC to aid in the ongoing awareness of the New Zealand cybersecurity landscape.

OPTIONS AND INCLUSIONS

INCLUSIONS	
NCSC MFN Threat Feed	Malware Free Networks IoC feed, provided by New Zealand's National Cyber Security Centre

CERT NZ Phishing Disruption Service Threat Feed	Phishing Disruption Service IoC feed, provided by CERT NZ
Tasking of DNS IoCs	One New Zealand integrates Fully Qualified Domain Names (FQDN) indicators from the threat feeds into special DNS resolvers, which are only accessible to subscribing customers. MFN integrates into the One New Zealand DNS servers using zone transfers which occur regularly at 60 second intervals. This ensures the most up to date MFN threat intelligence is available.
Blocking of customer DNS queries for threat indicators	When a customer DNS query is received for a FQDN threat indicator, the DNS resolvers will respond to the query with an unresolvable response (NXDOMAIN). Any connection attempts to the FQDN threat indicator are therefore blocked, protecting the customer from any malicious consequences due to the connection.
OPTIONS	
MFN Consenting Customer Agreement	Signing of the Malware Free Networks consent to the provision of Telemetry to GCSB authorising the collecting and passing of telemetry information to the GCSB which identifies your organisation
MFN Expanded Telemetry (Consenting customers only)	The Expanded telemetry integrates a customer identifier, which may be an IP address, with the IoC block, date and time. Depending on the service integration, this may include source and destination ports and protocols. Due to limitations in DNS, it is not possible to determine applications source and destination ports for this integration.
MFN Basic Telemetry (all other customers)	Basic telemetry does not identify a customer, just the IOC that was blocked, along with the date and time.
Monthly Reporting (consenting customers only)	One New Zealand will provide you a monthly report of all indicators blocked which identifies: • Feed (MFN or CERTNZ) • Indicator FQDN (malicious indicator) • Category (malware activity, phishing, unknown) • Source IP address (source of DNS query) • Time/Date stamp

SERVICE CONDITIONS

- The Malware Free Networks (MFN) service is based on a minimum 12-month term
- We make no guarantees or warranties that the service will correctly detect and identify all:
    - Security Events or Incidents:
    - Instances of unauthorised access to your network
    - Malware:
    - Exploits: or
    - Other types of attacks or issues
- You will need to make changes to your recursive DNS infrastructure to direct queries to the One New Zealand DNS servers which deliver the MFN service. If Microsoft AD or a Web Proxy are used for DNS resolution for outbound internet traffic, it is a simple change or addition to point to the One New Zealand DNS servers as a secondary resolver. If using other DNS resolvers such as cloud based DNS services, consultation may be required in order to ensure MFN is able to be used.
- The engagement will commence at a mutually convenient time

- You will provide the access required to establish and maintain the service
- You will make available any required system or information
- You will provide resources to support the discovery and onboarding phase and on-going improvement of the service
- You will provide access to the relevant resources and materials to enable completion of the deliverables of the service
- Travel and disbursements will be agreed prior and charged at cost if required.