



Department for Levelling Up,
Housing & Communities

NCSC Active Cyber Defence

 @LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

**LOCAL
DIGITAL**

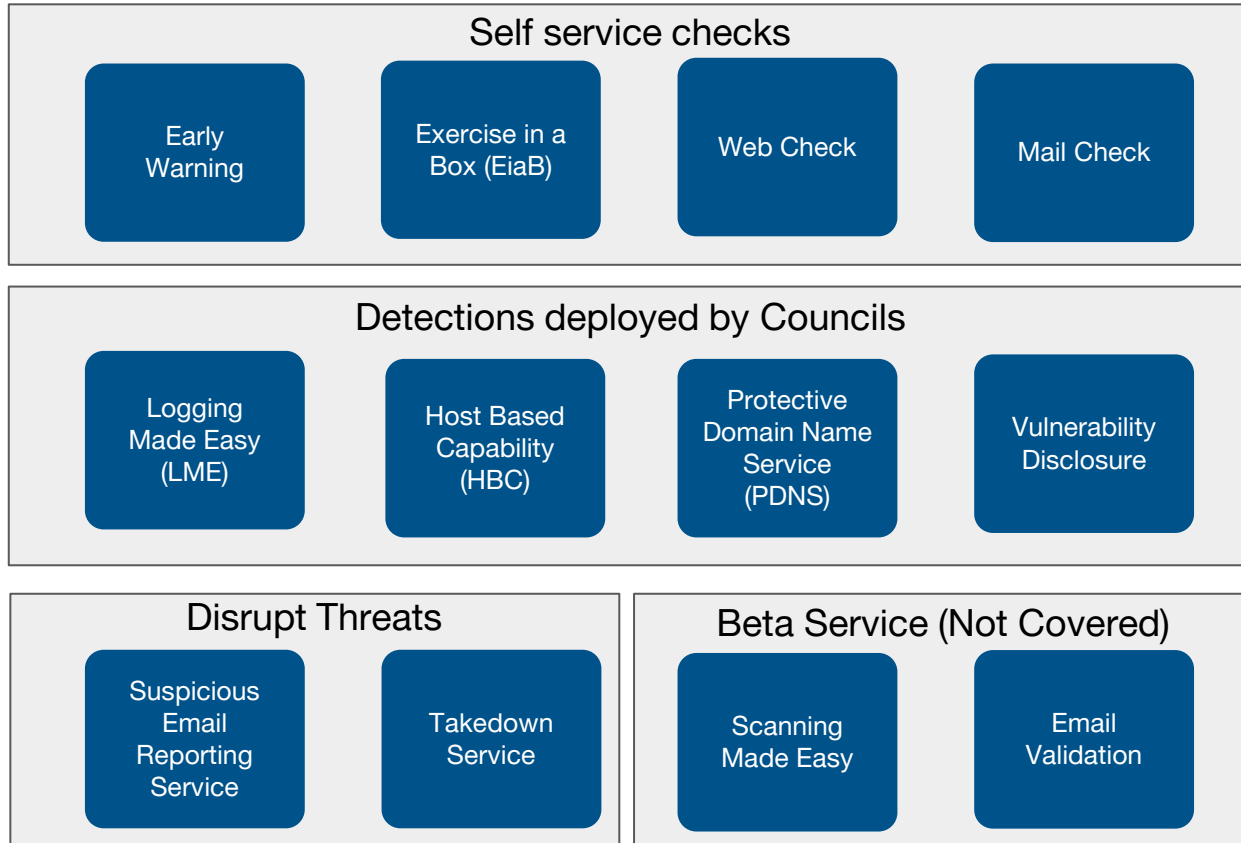
Cyber

Introduction to ACD

NCSC provides a range of free cyber security tools and services as follows:

- Self service checks - allow you to check and improve the security posture of your Council
- Detections deployed - integrate services into an environment to provide a protection or detection capability
- Disrupt threats – identification & response of phishing or malicious activity

Active Cyber Defence



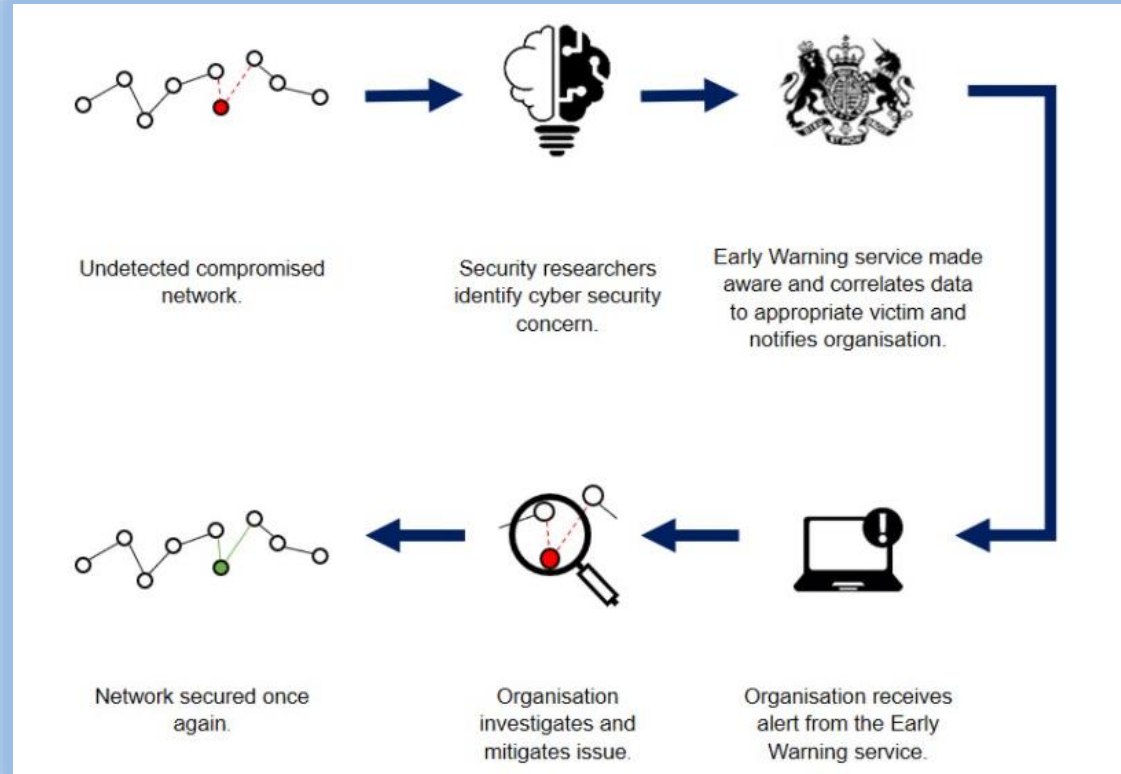
Introduction to Early Warning Service

Early Warning is a free NCSC service open to all UK Councils designed to inform your Council of potential cyber attacks on your network, as soon as possible.

Councils will receive the following high level types of alerts:

- Incident Notifications
- Network Abuse Events
- Vulnerability and Open Port Alerts

How Early Warning works



There are two types of alerts that will be sent when an alert is detected for your Council:

Daily Threat Alert - this includes Incident Notifications and Network Abuse Reports

Weekly Vulnerability Alert - this includes Vulnerability and Open Port Alerts

Benefits of Early Warning

- By signing up to Early Warning your Council will be alerted to the presence of malware and vulnerabilities affecting your network
- Early Warning enhances your Council's security by increasing your awareness of the low-grade incidents which could become much bigger issues, so you can act on them earlier
- Early Warning increases confidence in the security of your network

How to register for Early Warning - Continued...

Add First Contact

Individual Shared Inbox

First Name

Last Name

Email Address

The below fields are optional, but will help the NCSC to contact the right people in high priority situations.

Role (optional)

Phone Number (optional)

01245 234567 X12334

To add an extension, use format "X12345" after the primary phone number

Save Contact

- Receive notifications to the IP and domain names provided
- Review and confirm your selections
- Confirm & submit
- Your application will then be sent to NCSC for approval within 3-5 working days and will show as “Pending Approval” at this time

IP Addresses

Early Warning supports the following formats:

- Single IP (v4 or v6)
Example: 178.124.52.2, 2003:db8::
- IP ranges
Example: 178.124.52.2-178.124.52.10
- CIDR blocks
Example: 211.34.56.123/24
- IPv4 and/or IPv6 notation

Filter IP Assets

+ Add IP Upload Multiple

Domain Names

- Subdomains are captured by the system automatically.
Example: domain.com also checks for *.domain.com
- Please make sure to add domain names of websites and other online services, even if you have included their direct IP address already.

Filter Domain Assets

+ Add Domain Upload Multiple

Next >

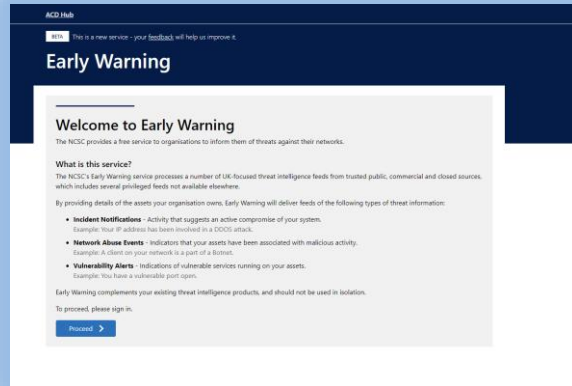
- Register a contact or department with a shared inbox
- Contact information will be saved, you then have the option to add additional contacts

How to register for Early Warning - Continued...

Upon receiving your email confirming approval and activation of your account, you can manage your enrolment through the dashboard found here:

<https://www.earlywarning.service.ncsc.gov.uk/?referrer=acdwebsite>

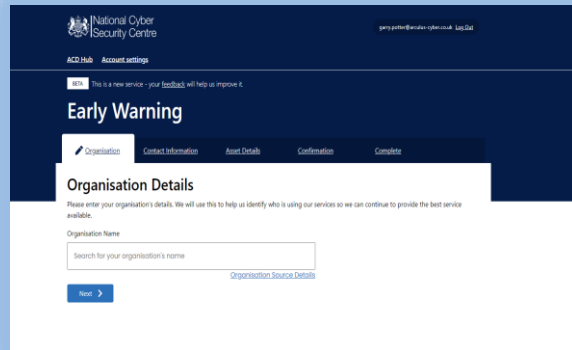
How to register for Early Warning



[Signup to Early Warning](#)

You will need the following details to sign up:

- NCSC Single Sign On details (if you don't yet have an account, follow the link on the Early Warning signup page to create an account)
- Council's name
- Council's public IP addresses and domain names
- The details of the contacts you wish alerts to go to (at least name and email address)

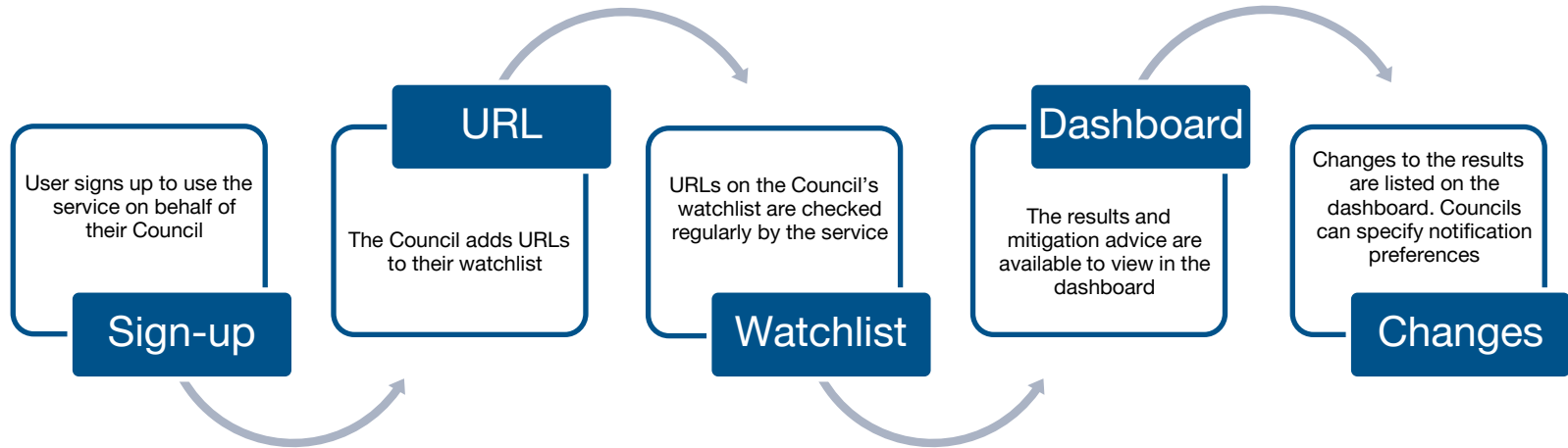


Introduction to Web Check

- All Council-owned websites should be included within the service
- Centralised alerting contact information should to be used
- Identified vulnerabilities should be triaged and where appropriate expedited through change control
- Website configuration and Vulnerability scanning service
- Checks for common vulnerability problems

NCSC IP addresses for whitelisting can be made available upon request

How Web Check works



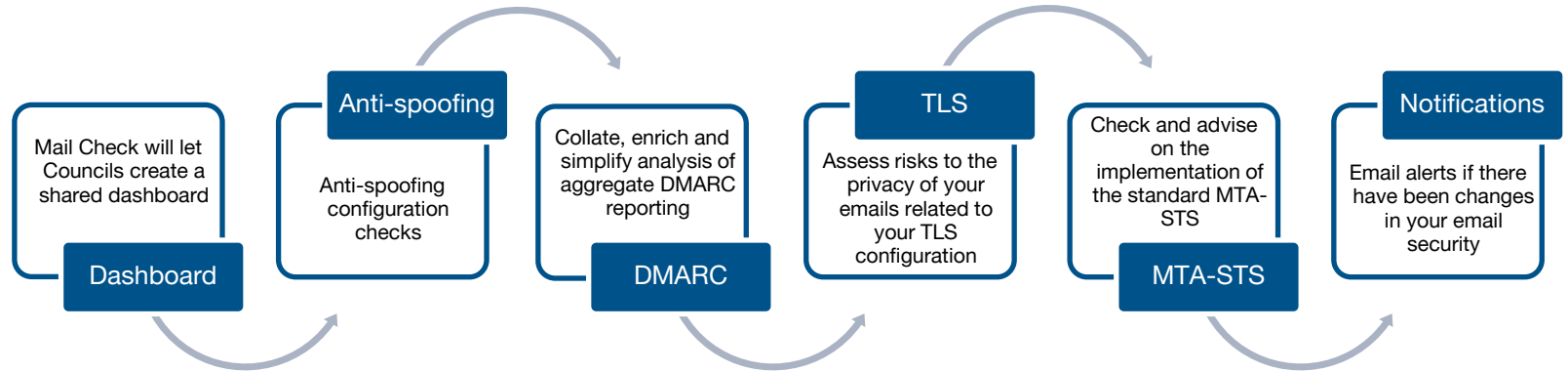
The benefits of Web Check

- Web Check alerts councils to the presence of a number of common website security issues and advises on how to fix these
- This in turn enables increased confidence in web-facing services and the reduced risk of damaging and costly cyber attacks
- Web Check is easy to use; it does not require a high level of technical skill
- Regular checking of websites has proved beneficial to Councils, even where there is already a good level of expertise and good practice

Introduction to Mail Check

- Email anti-spoofing controls (SPF, DKIM and DMARC)
 - Prevents attacks e.g. Phishing, Malware
- Email confidentiality (TLS)
 - Message encryption
- Mail Check is the NCSC's email security compliance platform
- Further information on Email security can be found here:
<https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing>

How Mail Check works



The benefits of Mail Check

- Assesses email security compliance by helping Councils identify, understand and prevent abuse of their email system
- Protect your council by making it difficult for cyber criminals to spoof your email address
- Protect the privacy of your information in transit
- Protect your brand and reputation
- Reducing the costs of service down-time
- Reducing risks of your email systems not being trusted

Introduction to Logging Made Easy (LME)

- Self-install tutorial for councils that do not have logging capability
- Report on patching status on enrolled devices
- Show where administrative commands are being run on enrolled devices
- See who is using which machine
- Using threat reports query for the presence of an attacker in the form of Tools, Techniques and Procedures (TTPs)

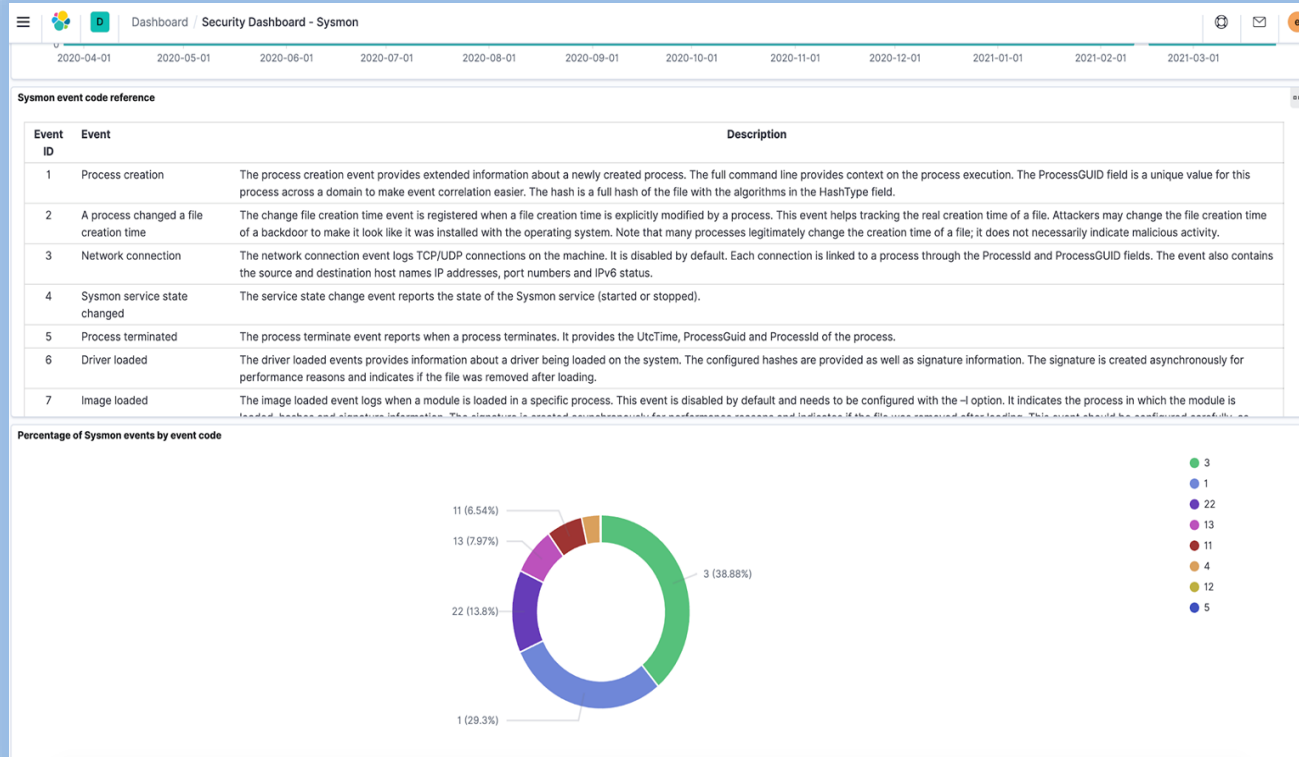
Who is LME for?

- Councils that don't have an Information Security Operations Centre (SOC) or Security Information and Event Management capability (SIEM)
- Councils with a lack of budget, time or understanding to set up their own logging system, or buy a professional solution
- Councils that recognise the need to begin gathering logs and monitoring their IT

Further information is available via the link below:

<https://www.ncsc.gov.uk/files/LME-Installation-Guide-October-2019.pdf>

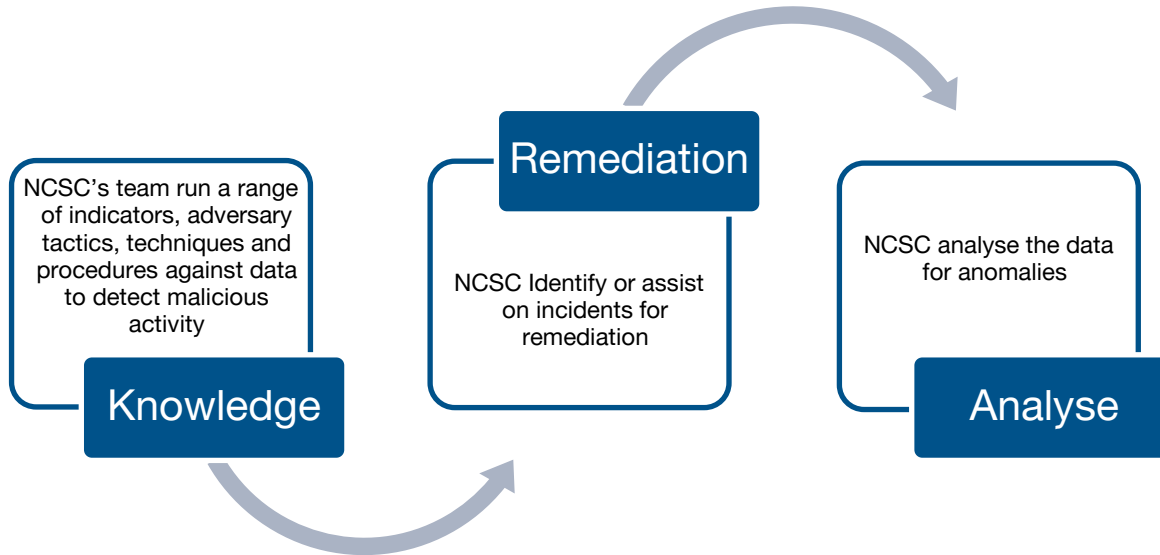
Example Dashboard



Introduction to Host Based Capability (HBC)

- Monitoring services to understand what is happening directly on IT endpoints
- High level of accuracy in detecting vulnerabilities via behaviour analysis and irregular data
- Collects metadata for analysis by the NCSC
- Only available to central government at the moment

How HBC works (Detect)



How HBC works (Threat Surface)

- Reporting Cyber Security metrics to Councils
- Example metrics:
 - Operating System versions
 - Admin accounts and unnecessarily processes
 - USBs
 - Network shares
- Feed into NCSC Assessments and Active Cyber Defence

How HBC works (Forewarn)

- Once HBC is rolled out it will warn Councils about major vulnerabilities
- Metadata is collected to understand each Council's exposure
- Councils will be informed of findings
- Councils are notified which devices have vulnerabilities

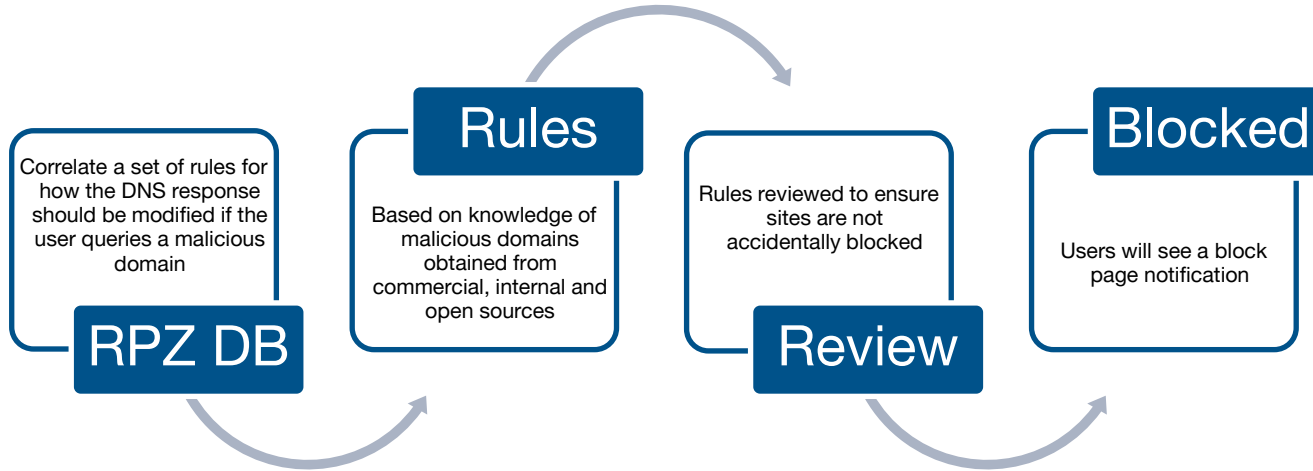
The benefits of HBC

- NCSC's expert analysts and knowledge
- Utilising NCSC's extensive coverage to better inform Councils IT departments
- Complementary tailored service to Councils
- Providing Councils with the information required to understand their IT strengths and opportunities to better secure their estate

Introduction to Protective DNS Service (PDNS)

- PDNS incorporated into council upstream recursive DNS resolution
- Where existing commercial-grade DNS filtering solutions are in place, councils may consider potential financial savings by migrating to PDNS
- Built to hamper the use of DNS for malware distribution
- Prevents access to domains known to be malicious
- Provides Councils with access to NCSC outreach support
- Used to inform and support LGA cyber incident response functions

How PDNS works



The benefits of PDNS

- Council remote users can benefit from the protection of PDNS (Core or Roaming https://www.ncsc.gov.uk/information/pdns#section_5)
- Prevents access to sites hosting malware, ransomware and spyware
- Dashboard and data logs are available to help Councils monitor their networks
- Subject matter expertise from the NCSC and Nominet

Introduction to Vulnerability Disclosure

- Vulnerability Disclosure Toolkit - contains the essential components Councils need to set up their own vulnerability disclosure process
https://www.ncsc.gov.uk/files/NCSC_Vulnerability_Toolkit.pdf
- Vulnerability Reporting Service - can be used by Councils to report vulnerabilities
<https://www.ncsc.gov.uk/information/vulnerability-reporting>
- Vulnerability Disclosure Pilot – aims to improve and adopt vulnerability disclosure best practices

Suspicious Email Reporting Service (SERS) & Takedown Service

- Enables the public to report suspicious emails by sending them to report@phishing.gov.uk
- Analyses emails and where found to contain links to malicious sites, seeks to remove those sites from the internet
- Takedown Service finds malicious sites and sends notifications to the owner to get them removed from the internet

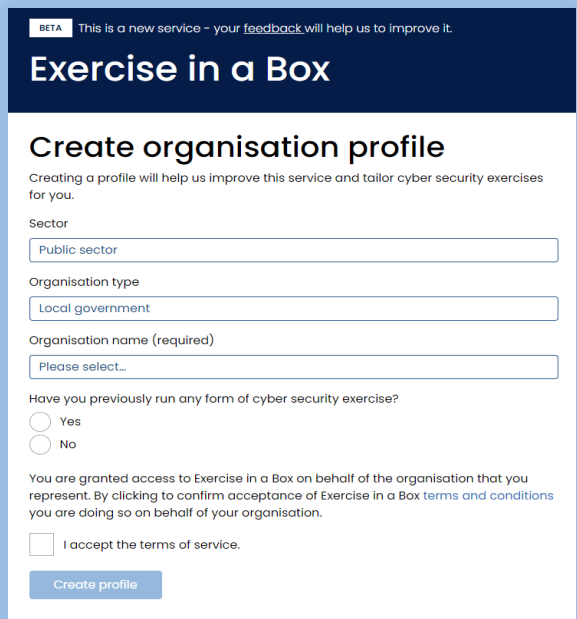
Introduction to Exercise in a Box (EiaB)

- Online tool which helps Councils test and practise their response to a cyber attack
- Based around the main cyber threats, which the Council can do in their own time, in a safe environment, as many times as they want
- Live tool which will keep evolving, based on user feedback, to ensure it stays current, relevant, and engaging
- Exercises tailored towards Local Government scenarios

The benefits of EiaB

- How effective the Council's current defence and response mechanisms are
- Test and check the Council's existing policies and procedures
- Improve your colleagues' internal relationships and skills (specifically their ability to deal with an actual cyber attack)
- Identify areas for further improvement

Profile Creation EiaB



BETA This is a new service – your [feedback](#) will help us to improve it.

Exercise in a Box

Create organisation profile

Creating a profile will help us improve this service and tailor cyber security exercises for you.

Sector

Organisation type

Organisation name (required)

Have you previously run any form of cyber security exercise?

☐ Yes
☐ No

You are granted access to Exercise in a Box on behalf of the organisation that you represent. By clicking to confirm acceptance of Exercise in a Box [terms and conditions](#) you are doing so on behalf of your organisation.

☐ I accept the terms of service.

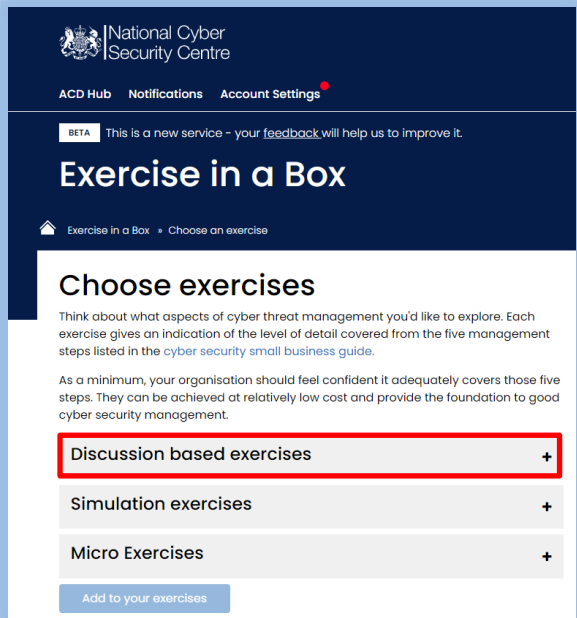
[Create profile](#)

- Create Council profile
- Sector – Public sector
- Organisation type – Local government
- Organisation name – Select Council name from the list

Discussion Based Exercises

Discussion based exercises topics:

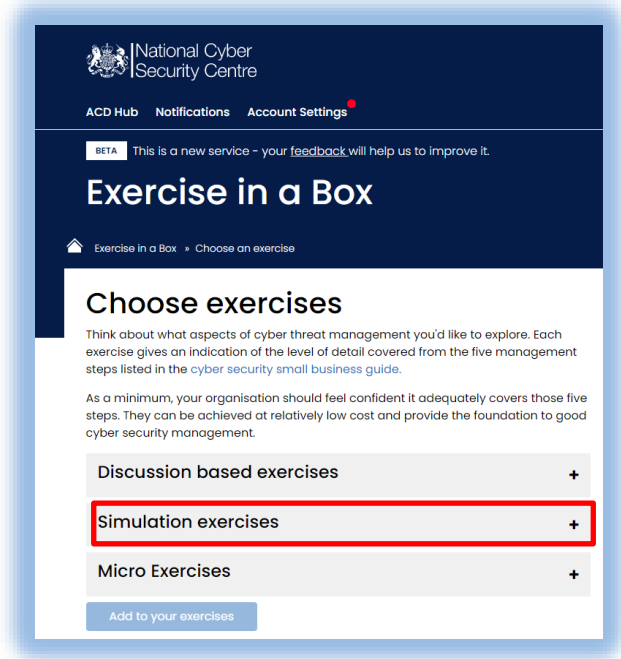
- A ransomware attack delivered by a phishing email
- Mobile phone theft and response
- Being attacked from an unknown Wi-Fi network
- Insider Threat resulting in a Data Breach
- Third Party Software Compromise
- Bring Your Own Device
- Threatened leak of sensitive data
- Supply Chain
- Home and Remote Working
- Managing a Vulnerability Disclosure
- Supply Chain Software
- Supply Chain Ransomware Attack



Discussion Based Resources

- Senior decision maker – someone who can make important decisions
- Senior IT stakeholder– someone who has overall responsibility for your IT
- Technical IT security adviser – someone who can provide technical advice
- Media/comms representative – someone who would manage your internal/external communications during an incident
- Council policy adviser – someone who has oversight of your Council policies, such as HR, business continuity, etc
- Scribe - someone to take notes during the exercise delivery

Simulation Exercise



Simulation exercise topic:

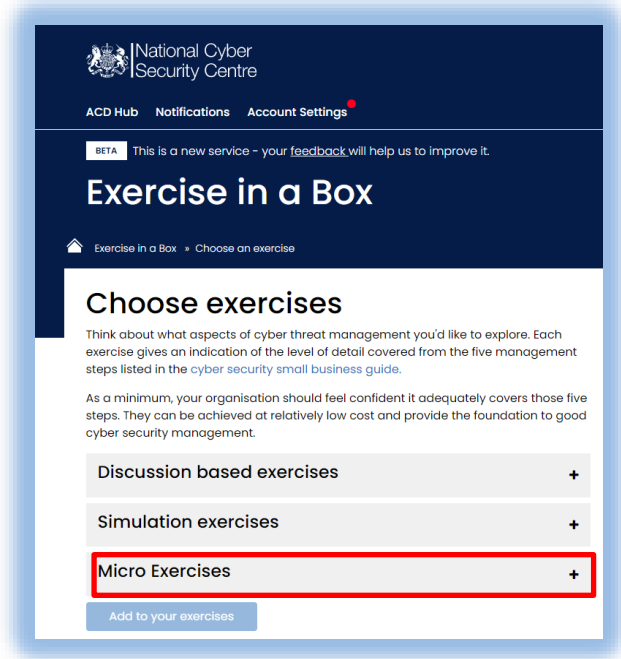
- Cyber threat simulation exercise –
A simulation to see if your Council can
locate and stop a mock threat

Simulation Based Resources

- Network defenders – Those with the knowledge and understanding of your network
- Technical administrators – Roles with more junior responsibilities but who would be essential in supporting an incident response
- Senior IT stakeholder (observer). Individuals with overall responsibility for your network may wish to observe this scenario
- Scribe/observer - someone to take notes during the exercise delivery

It is not recommended to bring in other Senior Decision Makers, allowing the technical teams to respond effectively

Micro Exercises



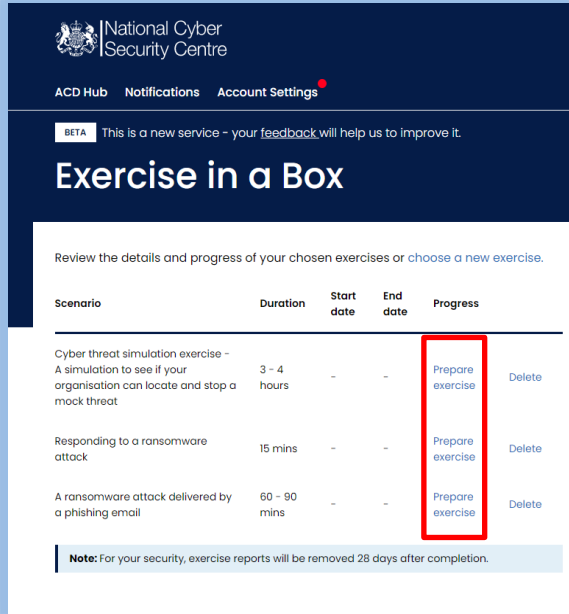
Micro exercises topics:

- Responding to a ransomware attack
- Identifying and reporting a suspected phishing email
- Using Passwords
- Connecting Securely
- Securing Cloud Productivity Suites
- Securing Video Conferencing Services

Micro Exercise Resources

- You can have as many or as few people involved as you like, and no one taking part in this exercise needs to be a cyber security expert
- NCSC recommend 3-5 people including a nominated facilitator to run the session

Prepare Exercise



National Cyber Security Centre

ACD Hub Notifications Account Settings

BETA This is a new service - your feedback will help us to improve it.

Exercise in a Box

Review the details and progress of your chosen exercises or [choose a new exercise](#).

Scenario	Duration	Start date	End date	Progress
Cyber threat simulation exercise - A simulation to see if your organisation can locate and stop a mock threat	3 - 4 hours	-	-	Prepare exercise Delete
Responding to a ransomware attack	15 mins	-	-	Prepare exercise Delete
A ransomware attack delivered by a phishing email	60 - 90 mins	-	-	Prepare exercise Delete

Note: For your security, exercise reports will be removed 28 days after completion.

- Once exercise have been chosen they will appear in your dashboard
- Select “**Prepare exercise**” to launch
- Follow the on screen instructions to run through the exercises

Registering with NCSC

Registration enables you to access all of your NCSC online services.

Information required:

- First name
- Last name
- Email address
- Organisation (Council name)
- Create password
- Agree with NCSC storing these details

Email confirmation will be sent after registration.

Eligibility to Register

Web Check	Mail Check	PDNS
<ul style="list-style-type: none">• Local Authorities• Central Government• Devolved Administrations• Emergency Services• NHS Organisations• Academia (universities, further education colleges, and all UK schools)	<ul style="list-style-type: none">• Local Authorities• Central Government• Devolved Administrations• Emergency Services• NHS Organisations• Academia (universities, further education colleges, and all UK schools)	<ul style="list-style-type: none">• Local Authorities• Central Government• Devolved Administrations• Emergency Services• NHS Organisations

Further Information

NCSC Active Cyber Defence Services:

<https://www.ncsc.gov.uk/section/active-cyber-defence/services>

NCSC Cybersecurity Information Sharing Partnership:

<https://www.ncsc.gov.uk/section/keep-up-to-date/cisp>



Department for Levelling Up,
Housing & Communities

Thank you

[We welcome feedback on our cyber support service](#)

 @LDgovUK

www.localdigital.gov.uk

#LocalDigital #FixThePlumbing

**LOCAL
DIGITAL**

Cyber