The Essential Guide to Cyber Security

Following the NCSC's 10 Steps to Cyber Security

Huntsman®
Defence-Grade Cyber Security

Following the NCSC's 10 Steps to Cyber Security

The UK Government's 10 Steps to Cyber Security framework[1] is guidance designed for organisations looking to protect themselves in cyberspace. It defines the fundamental controls which all organisations should implement.

The 10 Steps put in place capabilities to mitigate the risk from common cyber threats. They provide a broad set of competencies to measure your current cyber capabilities, and define a sound footing for a business to implement more complete cyber protection.

In this document we lay out a measured approach to implementing the 10 steps. We recognise that you will already have some of these areas covered, and that other parts you will know about and have plans to protect.

The order of steps is our plan to allow progression by setting up the basics first, like secure configurations and monitoring, then adding more complex items, such as removable media controls, which can be added incrementally and monitored and managed.

If you already have some level of protection against most, if not all, of the steps, then this guide can provide you with a way of checking for completeness and planning to enhance.

Take a look at the NCSC's 10 Steps to Cyber Security and our progressive order in which to assess them.

LOOK AT THE 10 STEPS ▶

Huntsman®
Defence-Grade Cyber Security

1 - NCSC 10 Steps to Cyber Security ©Crown copyright, subject to Open Goverment Licence ncsc.gov.uk/terms-and-conditions

National Cyber Security Centre

10 Steps to Cyber Security

Approach each step as part of a structured plan, building in complexity. Create a phased plan to assess and implement against each step.

SEE THE PLAN OVERVIEW ▶

1 Set up your Risk Management Regime

Assess the risks to your business's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

2 Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

3 Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

4 Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

5 Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

6 Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

7 Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

8 Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

9 User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

10 Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to **www.ncsc.gov.uk**

Huntsman®
Defence-Grade Cyber Security

- Establish Risk Management regime
- Three main phases building in sophistication
- In parallel, deliver user education and working policies

Each phase builds in complexity, recognising you will already have good solutions in place in some areas. User awareness and working policies can be created in parallel.

READ MORE OVER ▶

Establish

2 Secure configuration

3 Monitoring

4 Incident management

Manage

5 Managing user privilege

6 Network Security

Enhance

7 Malware prevention

8 Removable media controls

Deliver

9 User education and awareness

10 Home and mobile working

1 Risk Management Regime

Assess the risks to your business's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Huntsman®
Defence-Grade Cyber Security

Establish the foundations of solid cyber security.

The core requirements for strong cyber security are an up to date (patched) infrastructure with minimal vulnerabilities, an efficient monitoring regime to watch over the activities of users and systems across the entire corporate infrastructure, and a well practised approach to managing and resolving any incidents.

Establishing this baseline allows you to maximise the use of existing cyber defence measures, and to extend and strengthen the capability in a controlled manner.

LOOK AT THE NEXT STEPS OVER ▶

2 Secure configuration

What

Establish baseline IT measures across the corporate infrastructure to greatly improve the security of systems. Quickly fix known vulnerabilities and remove or disable unnecessary functionality from systems.

Why

- Stop exploitation of known bugs and insecure system configurations
- Prevent unauthorised changes to systems

How

- Use supported software
- Update and patch systems regularly
- Implement secure baseline builds
- Conduct regular vulnerability scans
- Establish configuration control
- Disable unnecessary peripheral devices
- Limit user ability to change configuration
- Limit privileged user functionality

3 Monitoring

What

Capability to detect attacks across all systems and business services, covering external attacks and both malicious and accidental internal breaches.

Why

- Inadequate monitoring can lead to attacks going unnoticed and/or non-compliance with legal/regulation (eg GDPR)
- Your business will be exposed to risk if you are unable to quickly investigate and resolve an incident

How

- Establish a sound monitoring strategy
- Implement a SIEM to monitor across all systems and security controls, and centralise log collection and analysis
- Correlate security events to eliminate false positives and give context to alerts
- Monitor for unusual behaviours across systems, networks and users
- Monitor user privilege changes

4 Incident management

What

An established and practiced corporate process to deal with security incidents. Backed by systems to detect, manage and investigate the cyber security incident and efficiently manage the analysis and communication process.

Why

- Minimise actual business impact (system outage/customer confidence/financial loss)
- Complying with legal/regulatory reporting

How

- Establish and test an incident response capability
- Establish a data recovery capability
- Create an incident investigation and analysis platform
- Automatically collate pre- and post-incident data
- Conduct a lessons learned review

Huntsman®
Defence-Grade Cyber Security

Manage your cyber security across users and networks

Managing the access users have to data and systems is a core cyber security requirement, protecting against both malicious insider activities and also the more commonly undetected misappropriation of a user's account by external attackers. Similarly, having robust defence against ingress by external hackers built in to your network's architecture is a solid part of a well managed cyber security stance.

Manging user privileges and creating a protective network will build a broad and robust platform of cyber security which can then be enhanced with more specific tools.

SEE ENHANCE STEPS OVER ▶

5 Managing user privilege

What

Consistent restriction of granting unnecessary user privileges and the timely removal of user privileges no longer needed. Preventing administrator and privileged user accounts being forgotten and compromised.

Why

- Prevent deliberate misuse of privilege
- Stop unauthorised access to information
- Prevent unauthorised system changes
- Halt attackers increasing their capability

How

- Limit privileges and access to level employees need to do their job
- Monitor access to sensitive information
- Limit the number of privileged accounts
- Monitor for privilege escalations
- Manage user accounts from creation, through life and to deletion
- Monitor use of privileged account actions
- Establish robust user authentication and access control

6 Network Security

What

Network connections to the Internet and to partner networks expose you to attack. Create a robust network architecture to reduce their chance of success. Networks often span several sites, the use of mobile / remote working, and cloud services, which makes defining a fixed boundary difficult, so as well as physical connections, monitor and protect where data is processed and stored.

Why

- Poor network architecture can give an attacker access to systems hosting sensitive information
- A compromised network could allow damage to internal and externally facing systems and data
- Attackers can intercept poorly protected information whilst in transit (such as between your end user devices and a cloud service)
- Internet-facing networks may be vulnerable to Denial Of Service (DOS) attacks

How

Manage the network perimeter:

- Firewall rules should deny traffic by default
- Prevent malicious content: Deploy malware checking solutions and reputation-based scanning services to examine both inbound and outbound data in addition to protection deployed internally
- Monitor network traffic to detect and react to attempted network intrusions

Protect the internal network:

- Ensure there is no direct routing between internal and external networks
- Segregate networks as sets
- Secure wireless access
- Enable secure administration
- Configure the exception handling processes
- Conduct regular penetration tests and simulated cyber attack exercises

Huntsman®
Defence-Grade Cyber Security

Enhance your cyber security defences.

You undoubtedly already deploy antivirus protection as a minimum. Enhancing these protections to cover broader malware and removable media is aimed at many of the vulnerabilities particularly associated with the behaviour of a business's own users. These measures are an essential backbone to protect users and the business and they should be complemented with ongoing user awareness training and use policies.

7 Malware prevention

What

Malware can attack any system, process or function so a technical architecture that provides multiple defensive layers (defence in depth) should be considered. Routes of attack can include email, web browsing, web services, removable media and personally owned devices (e.g. mobile phones)

Why

- Any data exchange carries a risk of malware infection. Implementing security controls can reduce the risk

How

- Scan all data at the network perimeter
- Blacklist malicious web sites
- Establish malware defences
- End user device protection (antivirus)
- Content filtering on external gateways
- Disable the Windows AutoRun function
- Automatically scan removable media for malicious content

8 Removable media controls

What

Removable media is a common way of introducing malware and the accidental or deliberate exporting of sensitive data. You should be clear of the business need to use it and apply appropriate security controls.

Why

- Removable media is easily lost and can result in the loss of vast amounts of sensitive data, with repercussions of reputational damage and huge fines
- Uncontrolled use of removable media increases the risk of introducing malware

How

- Do not use removable media as a default mechanism to store or transfer information
- Limit the use of removable media
- The secure baseline build should deny access to media ports by default
- Scan all media for malware
- Sensitive data should be encrypted at rest
- Actively manage the reuse and disposal

Enhancing your cyber defences with malware prevention and removable media controls will create an extremely robust level of protection. All these measures are reliant on user awareness - learn next about user awareness and mobile working policies.

LOOK AT THE NEXT STEPS OVER ▶

Huntsman®
Defence-Grade Cyber Security

Deliver training and policies to guide and protect users

Users have a vital role to play in their organisation's security and so it's important that security rules and the technology provided enables users to do their job as well as help keep the organisation secure. This is especially important when users are working remotely and accessing sensitive corporate information and systems in public places and from networks you don't control.

User education is a never ending task as new users join and old users forget. Managing home and mobile working must also evolve with the pace technology changes. A broad but flexible cyber security platform is needed to underpin the 10 steps.

ANATOMY OF A CYBER PLATFORM ▶

9 User education and awareness

What

Users have a critical role to play in helping to keep an organisation secure. Train them to work safely and be aware of security, and test and reinforce their awareness regularly.

Why

- Users are a primary focus for external attackers, acquiring credentials or running malicious code via phishing and social engineering attacks
- Untrained users can inadvertently misuse data, breaching legal / regulatory controls

How

- Produce a user security policy, with consideration to different business roles
- All users should receive security training with regular refreshers
- Establish a staff induction process for new users, contractors and 3rd party users
- Encourage staff in security roles to develop and formally validate their security skills
- Test the effectiveness of security training
- Promote an incident reporting culture

10 Home and mobile working

What

Mobile working and remote access extends the transit and storage of data outside the corporate infrastructure, typically over the Internet. It offers great business benefits but exposes new risks that need to be managed.

Why

- Lost or stolen mobile devices risk being used to access sensitive data and systems
- Working in public spaces can be observed, compromising sensitive information
- User credentials on a lost or stolen device could access and compromise services
- An unattended device could be subverted to allow monitoring of user activity

How

- Assess the risks and create a mobile working policy
- Determine the processes for authorising users to work off-site
- Increase level of monitoring on all remote connections and systems being accessed
- Train all users on the use of their mobile device, including direction on:
  - secure storage and use of user credentials
  - incident reporting
  - environmental awareness (the risks from being overlooked, etc.)
- Develop a secure baseline build and configuration for all types of mobile devices
- Minimise the data stored on mobile devices and if possible encrypt the data at rest
- Encrypt all data exchanged over remote connections
- Update the corporate incident management plans to deal with a range of incidents, including loss or compromise of a device
- Put technical processes in place to remotely disable a lost device and deny it access to the corporate network

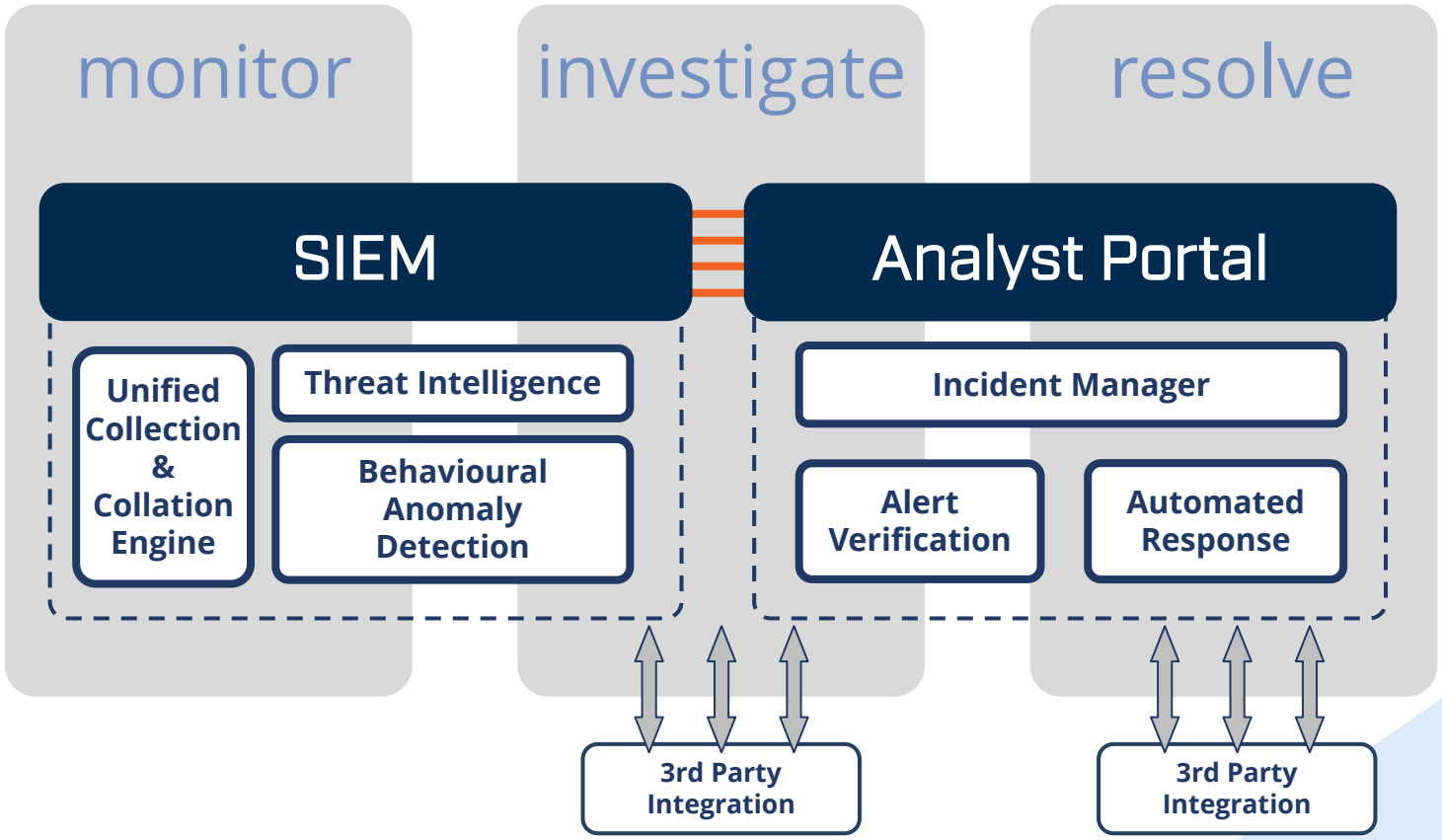
Huntsman®
Defence-Grade Cyber Security

The anatomy of a cyber security monitoring platform

Throughout the 10 Steps to Cyber Security there are numerous areas which need monitoring, from spotting user privilege escalations, through identifying unexpected network behaviour, to knowing when removable media are being used. These cases should all raise alerts which must then be investigated and resolved. Providing a robust and flexible cyber security platform to monitor, investigate and resolve issues is the foundation on which to build your forward looking cyber defences.

Cyber security defences should never stop evolving, just as the threats faced are constantly evolving. Having world class cyber defences that are able to easily expand and grow over time is critical.

TALK TO HUNTSMAN ABOUT BUILDING WORLD CLASS CYBER DEFENCES ▶



Huntsman®
Defence-Grade Cyber Security

Achieving confidence with Huntsman

Huntsman Enterprise SIEM is at the core of the Huntsman Cyber Security Platform. The product delivers an intelligent security log, event and incident management solution that analyses and correlates events in real–time to provide early detection of security threats and regulatory compliance issues.

Huntsman® offers a single console view of all alerts, notifications and reports. Its drill-down dashboards permit rapid investigation for triage of issues that can then be fully analysed in conjunction with related events using the in-built incident management system or exported to a ticketing solution.

Huntsman Security is part of Tier-3 Pty Ltd. The technology's heritage lies in delivering a key foundation stone of the cyber security risk management, monitoring and response capability in some of the most secure and sensitive environments within intelligence, defence and criminal justice networks across the five eyes community of Australia, Canada, New Zealand, United Kingdom and United States. Huntsman® solutions are deployed and accredited within this community to the highest security levels.

Huntsman | Tier-3 Pty Ltd

Asia Pacific
t: +61 2 9419 3200
e: info@huntsmansecurity.com
Level 2, 11 Help Street
Chatswood NSW 2067

EMEA
t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com
7 Adam Street, Covent Garden,
London, WC2N 6AA

North Asia
t: +81 3 5953 8430
e: info@huntsmansecurity.com
Awajicho Ekimae Building 5F
1-2-7 Kanda Sudacho
Chiyodaku, Tokyo 101-0041

Americas
toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com
Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com
linkedin.com/company/tier-3-pty-ltd
twitter.com/Tier3huntsman

Huntsman®
Defence-Grade Cyber Security