Compliance Guide

Cyber Essentials

How Huntsman Security supports continuous compliance

Huntsman®
Defence-Grade Cyber Security

Cyber Essentials

Mapping to the requirements with Huntsman Security technology

Cyber Essentials is a UK Government information assurance scheme operated by the National Cyber Security Centre (NCSC) that is intended to encourage organisations to adopt good practice in information security.

The scheme comprises a framework of five fundamental mitigation controls:

- **Secure your Internet connection**
- **Secure your devices and software**
- **Control access to your data and services**
- **Protect from viruses and other malware**
- **Keep your devices and software up to date**

The vast majority of successful cyber-attacks rely on the ready availability of simple methods and tools to exploit the basic vulnerabilities inherent in software and computer systems. The Cyber Essentials controls, when effectively deployed, will protect your organisation against the majority of these common threats.

Cyber Essentials assesses these five fundamental security controls and whether they are in place and working effectively. For an increasing number of organisations there is a distinct benefit for them to have Cyber Essentials assurance on a more continuous basis. However, for most organisations, they cannot justify a fully manned SOC (Security Operations Centre).

This compliance guide explains how Huntsman Security's solution continuously measures the effectiveness of the Cyber Essentials controls

Continuing its support for regional compliance standards Huntsman Security has developed a Cyber Essentials monitoring solution. The capability undertakes systematic, continuous monitoring of the controls listed in the assessment process and provides a single pane of glass dashboard and control reports that convey the ongoing efficacy of them. It also generates alerts if a priority event occurs, which can be emailed to an individual or service desk.

Huntsman Security's Cyber Essentials solution

The continuous nature of Huntsman Security's Cyber Essentials monitoring solution provides a number of advantages over scheduled scans and manual assessments:

Continuous Real-Time Monitoring and Full Assessment

Operating continuously and performing regular assessments of the whole monitored environment (rather than just a sample subset) ensures the quick detection of issues, wherever they are, and even intermittent issues that may not be present during quarterly assessments.

Through integration with software and patch management systems the solution generates clear and concise reports that show all critical patches not installed on any managed endpoints, as well as applications or operating systems that do not meet minimum required versions. The assessment of centralised policies, and the monitoring of policy deployment, also means Huntsman Security's Cyber Essentials solution can not only report on the quality of policies, but also whether they are failing to be enforced.


HUNTSMAN SECURITY CONTINUOUS MONITORING COMMERCIAL IN CONFIDENCE Huntsman

Patch Applications

<Insert Company Name>

Mitigation strategies to prevent malware from running

Time Period: 14 Mar 2018 14:10 - 21 Mar 2018 14:10

What does the control cover?

Ensure that application software has had all relevant vendor-supplied

Why is this control important?

Malicious software often gains access and propagates through the use of known software vulnerabilities. Application vulnerabilities are often used to gain unauthorised access to all data to which the user account would legitimately have access, and also for the execution and propagation of malicious software such as ransomware which impacts data to which the user has write access.

How does Huntsman Security's Executive Cyber Scorecard achieve the goal of this control?

For this control, the software monitors for inconsistencies between the patch state of installed applications and the published list of security-critical patches defined by the security administrator.

CYBER SECURITY MATURITY

Maturity Level 3 (Workstations)

- Patches for extreme risk security vulnerabilities in Adobe Flash, web browsers, Microsoft Office, Oracle Java and PDF viewers are applied and verified within 48 hours for all workstations.
- Only vendor-supported yet deprecated versions of the above applications are used.

Maturity Level 3 (Servers)

- Patches for extreme risk security vulnerabilities in web server software, other server applications that store important (sensitive or high-availability) data, and all other internet-accessible server applications, are applied and verified within 48 hours.
- Only vendor-supported yet deprecated versions of applications are used for web server software, other server applications that store important data and all other internet-accessible server applications.

Patch Applications Control	Control Failures			Vulnerable Unique Endpoints
	Workstations	Servers	Total	
Extreme Risk Security Patch not applied within 48 hours	75	24	99	4
Non-Supported Application Version Detected	0	0	0	0
Total	75	24	99	4

Indicators - last 2 weeks

Additional Data

	Total
Number of Monitored Endpoints	131
Number of new Critical Security Updates	1
Number of different non-compliant Applications	
Number of Monitored Endpoints that failed the Control	4

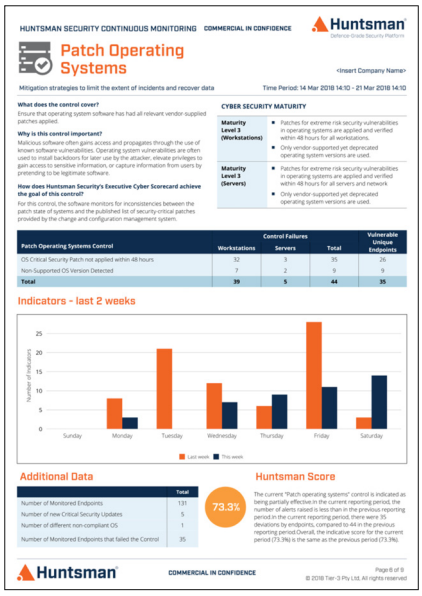
Huntsman Score

86.9%

The current "Patch applications" control is indicated as being generally effective in the current reporting period, the number of alerts raised is more than in the previous reporting period in the current reporting period, there were 4 deviations by endpoints, compared to 1 in the previous reporting period.Overall, the indicative score for the current period (96.9%) is the same as the previous period (96.9%).

Huntsman COMMERCIAL IN CONFIDENCE Page 3 of 9

© 2018 Tier-3 Pty Ltd. All rights reserved


HUNTSMAN SECURITY CONTINUOUS MONITORING COMMERCIAL IN CONFIDENCE Huntsman

Patch Operating Systems

<Insert Company Name>

Mitigation strategies to limit the extent of incidents and recover data

Time Period: 14 Mar 2018 14:10 - 21 Mar 2018 14:10

What does the control cover?

Ensure that operating system software has had all relevant vendor-supplied patches applied.

Why is this control important?

Malicious software often gains access and propagates through the use of known software vulnerabilities. Operating system vulnerabilities are often used to install backdoors for later use by the attacker, elevate privileges to gain access to sensitive information, or capture information from users by pretending to be legitimate software.

How does Huntsman Security's Executive Cyber Scorecard achieve the goal of this control?

For this control, the software monitors for inconsistencies between the patch state of systems and the published list of security-critical patches provided by the change and configuration management system.

CYBER SECURITY MATURITY

Maturity Level 3 (Workstations)

- Patches for extreme risk security vulnerabilities in operating systems are applied and verified within 48 hours for all workstations.
- Only vendor-supported yet deprecated operating system versions are used.

Maturity Level 3 (Servers)

- Patches for extreme risk security vulnerabilities in operating systems are applied and verified within 48 hours for all servers and network
- Only vendor-supported yet deprecated operating system versions are used.

Patch Operating Systems Control	Control Failures			Vulnerable Unique Endpoints
	Workstations	Servers	Total	
OS Critical Security Patch not applied within 48 hours	32	3	35	26
Non-Supported OS Version Detected	7	2	9	9
Total	39	5	44	35

Indicators - last 2 weeks

Additional Data

	Total
Number of Monitored Endpoints	131
Number of new Critical Security Updates	5
Number of different non-compliant OS	1
Number of Monitored Endpoints that failed the Control	35

Huntsman Score

73.3%

The current "Patch operating systems" control is indicated as being partially effective in the current reporting period, the number of alerts raised is less than in the previous reporting period in the current reporting period, there were 35 deviations by endpoints, compared to 44 in the previous reporting period.Overall, the indicative score for the current period (73.3%) is the same as the previous period (73.3%).

Huntsman COMMERCIAL IN CONFIDENCE Page 8 of 9

© 2018 Tier-3 Pty Ltd. All rights reserved

Alerting Workflow and Reduced Remediation Time

Huntsman Security's Cyber Essentials monitoring ensures that upon detecting an issue, an alert is raised and a notification is sent to nominated personnel for remediation. When integrated with an organisation's ticketing system, this enables the solution to automatically identify issues and breaches of compliance, which can then be forwarded to the technical team for quicker response and remediation. This automation improves the security process of the organisation by adding efficiency, reducing its time at risk, and ensures Cyber Essentials standards are being maintained at all times.

Management Reporting

Visibility of compliance performance and the identification of emerging issues is critical. Huntsman Security's Cyber Essentials monitoring solution provides reports to meet a wide range of requirements, from board executives, security and risk managers through to technical teams. Summaries provide a clear and easy to understand overview of status of the Cyber Essentials controls and their trending, whilst details of remediation items are available for technical personnel, broken down by system, patch, policy, etc. These reports demonstrate to external stakeholders that Cyber Essentials standards are being maintained over time, and that detected issues are appropriately dealt with.

HUNTSMAN SECURITY:
Cyber Essentials

Huntsman
Defence-Grade Cyber Security

FIREWALLS

Alerts	24 hr	7 days
High	1	1
Medium	0	0
Low	2	4

SECURE CONFIGURATION

Alerts	24 hr	7 days
High	0	0
Medium	2	2
Low	1	3

ACCESS CONTROL

Alerts	24 hr	7 days
High	1	2
Medium	1	1
Low	3	5

MALWARE PROTECTION

Alerts	24 hr	7 days
High	3	4
Medium	1	5
Low	2	3

PATCH MANAGEMENT

Alerts	24 hr	7 days
High	0	1
Medium	1	1
Low	1	3

INCIDENT SUMMARY

Open	15
Closed	12
New	3
Updated	2

File and Directory Monitoring

Agents deployed on key systems monitor critical and sensitive files and directories for any changes. Huntsman Security's solution alerts upon these changes and can also take a copy of the changed file for use in investigations or remediation. This provides protection of sensitive data, even from authorised users, and easy recovery in the event of data loss or destruction by malicious users or malware.

Huntsman

Mapping to the Cyber Essentials controls

The following pages outline the requirements of each Cyber Essentials control and explain how Huntsman Security's solution evidences each of the sub-controls within the assessment questionnaire.

The solution monitors logs from key devices, collects information from **Software Management** systems such as Microsoft WSUS, SCCM or Redhat Satellite and assesses policies within **Active Directory**. Importantly, the installation of these solutions are pre-requisites for the automated and continuous measurement of Cyber Essentials compliance levels.

Firewalls

Use a firewall to secure your Internet connection

You should protect your Internet connection with a firewall. This effectively creates a 'buffer zone' between your IT network and other, external networks.

Huntsman Security's Cyber Essentials solution identifies and reports upon:

- The use of vulnerable services passing through firewalls
- Firewall policy changes which could indicate prior "good" settings needing reconfirmation and allow a regular review
- Admin logons from the Internet

Secure configuration

Choose the most secure settings for your devices and software

Manufacturers often set the default configurations of new software and devices to be as open and multi-functional as possible. They come with 'everything on' to make them easily connectable and usable. Unfortunately, these settings can also provide cyber attackers with opportunities to gain unauthorised access to your data, often with ease.

Huntsman Security's Cyber Essentials solution identifies and reports upon:

- Any use or access from guest/default user accounts;
- Microsoft GPO policy on password strength, complexity, frequency of change, longevity of history, etc.;
- Microsoft GPO policy on browser and Microsoft Office security settings and the deployment of these across the Windows environment;
- Use of removable media (and alerts when it occurs)
- Use and deployment of application whitelisting provided by Microsoft AppLocker within Windows environments;
- Key events from security controls including proxy servers, host based firewalls, authentication and access logs for key systems, network and remote access VPNs, and backup operations;
- Events from MDM solutions and alerts when the MDM solution detects a device has breached policy or been placed into a locked mode.

All log information is managed and retained centrally and then archived according to a retention policy.

Access control

Control who has access to your data and services

To minimise the potential damage that could be done if an account is misused or stolen, staff accounts should have just enough access to software, settings, online services and device connectivity functions for them to perform their role. Extra permissions should only be given to those who need them.

Huntsman Security's Cyber Essentials solution identifies and reports upon:

- Account addition, modification and management activities;
- Privileged account addition, modification and management activities including non-administrative settings being applied to administrative accounts;
- Use of "generic" accounts that are shared;
- Admin accounts that have additional facilities that introduce risk such as email addresses (exposing the holder to phishing attacks) or web browser Internet access (to avoid drive by downloads);
- Microsoft GPO policy on password strength, complexity, frequency of change, longevity of history, etc.;
- Accounts that have seen no access or are inactive over a defined timeframe.

Malware protection

Protect yourself from viruses and other malware

Malware is short for 'malicious software'. One specific example is ransomware, which you may have heard mentioned in the news. This form of malware makes data or systems it has infected unusable - until the victim makes a payment.

Viruses are another well-known form of malware. These programs are designed to infect legitimate software, passing unnoticed between machines, whenever they can.

Huntsman Security's Cyber Essentials solution identifies and reports upon:

- Anti-virus events such as malware detection, signature updates, whether success or failure;
- Use and changes to application whitelists and execution of software that is disallowed;
- Events and alerts from common sandboxing platforms e.g. FireEye / Check Point / Bluecoat;
- Successful and failed backup jobs.

Patch management

Keep your devices and software up to date

No matter which phones, tablets, laptops or computers your organisation is using, it's important they are kept up to date at all times. This is true for both Operating Systems and installed apps or software. Happily, doing so is quick, easy, and free.

Huntsman Security's Cyber Essentials solution identifies and reports upon:

- Missing critical patches that have not been applied to operating systems within a specified number of days since their release;
- Missing critical patches that have not been applied to applications within a specified number of days since their release;
- Applications that fall below minimum software versions for known/ used packages;
- Issues and alerts raised by MDM solutions that control mobile platforms;
- Critical events and findings from vulnerability scanning solutions.

Want to find out more?

For a more detailed discussion on Huntsman Security's Cyber Essentials solution, please contact the appropriate office listed on the last page.

About Huntsman Security

Huntsman Security is the trading name 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 the intelligence, defence and criminal justice networks across the world, where Huntsman Security solutions are deployed and accredited 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**

7-10 Adam Street, Strand
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

huntsmansecurity.com

linkedin.com/company/tier-3-pty-ltd

© 2020 Tier-3 Pty Ltd, All rights reserved