Cyber

Hygiene Report

DOMAINNAME.COM

Last Scan Date: 16/09/2022

Report Generated: 19/09/2022

Powered by
cygienic.com

Table **of Contents**

Report
Introduction

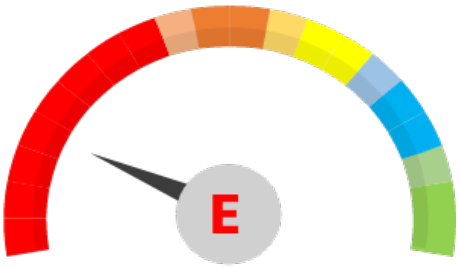
Inside this report you will find a comprehensive set of Cyber Hygiene tests, that have be carefully constructed and Meticulously delivered to determine the cyber security posture of a domain.

Cygienic's Cyber Hygiene tests are diligently crafted to ensure that no domain is impacted during a scan and there are no illegal missteps. Essentially, Cyber Hygiene tests are passive, non-intrusive scans, tailored to analyse Habitual, best practice domain security.

Just like a doctor awards a patient with a Clean bill of health, or not. Cyber Hygiene Scanners, similarly, provide an indicator of health, by awarding a domain with a rating.

Like personal hygiene, where you develop a routine of basic daily health checks, Cyber Hygiene, comparably, inspects basic routine security checks that are essential to the safeguard of a domain

Executive **Summary**



E DOMAINNAME.COM

Critical

Total Check Points	38.0	105.0

The Domain has attained less than 40% of the Cyber Hygiene Checkpoints

Domain Hygiene Checkpoints

Cyber Hygiene Rating

Email Security	10.0	15.0	Average -The Domain has attained 62-69% of the Cyber Hygiene Checkpoints
Webpage Security	4.0	25.0	Critical -The Domain has attained less than 40% of the Cyber Hygiene Checkpoints
IP Reputation	24.0	24.0	Leader -The Domain has attained more than 92% of the Cyber Hygiene Checkpoints
Domain Vulnerability	0.0	28.0	Critical -The Domain has attained less than 40% of the Cyber Hygiene Checkpoints
Data Privacy	0.0	13.0	Critical -The Domain has attained less than 40% of the Cyber Hygiene Checkpoints

A Excellent B Good C Average D Poor E Critical

Cyber Hygiene
Scan Result

E

DOMAINNAME.COM

Critical 38.0 105.0

Email Security 10.0 | 15.0

Probe	Result	Result Message	Recommendation
Email SPF Secure [HIGH]	PASS	[SEVERITY] HIGH ..... [THREAT] Spoof emails that are not detected and appropriately managed by notifying users can be targets for phishing attack campaigns [PROTECTION] ON	N/A
Email SPF Treatment [MEDIUM]	PASS	[SEVERITY] MEDIUM ..... [THREAT] Spoof emails that are not detected and appropriately managed by notifying users can be targets for phishing attack campaigns [PROTECTION] ON	N/A
DMARC Authentication [MEDIUM]	FAIL	[SEVERITY] MEDIUM ..... [THREAT] The Authentication of the senders email domain and IP address can stop attackers hijacking domains and send fake emails [PROTECTION] OFF	[FIX SUMMARY] Configure DMARC authentication in DNS server [OWNER] System Admin [EXAMPLE] Configure DNS TXT RECORD v=DMARC1; p=quarantine; pct=25; rua=mailto:postmaster@branddomain.com Alt set p=none to test processes. [REFERENCE] https://tools.ietf.org/html/rfc7489

DMARC Treatment [MEDIUM]	FAIL	[SEVERITY] MEDIUM ..... [THREAT] The Authentication of the senders email domain and IP address can stop attackers hijacking domains and send fake emails [PROTECTION] OFF	[FIX SUMMARY] Configure DMARC authentication in DNS server [OWNER] System Admin [EXAMPLE] Configure DNS TXT RECORD v=DMARC1; p=quarantine; pct=25; rua=mailto:postmaster@branddomain.com Alt set p=none to test processes. [REFERENCE] https://tools.ietf.org/html/rfc7489
Company Email Banner [LOW]	FAIL	[SEVERITY] LOW ..... [THREAT] An SMTP banner displaying the company name helps other system identify the authenticity of the source - This is less important today, but one that should still be considered for good hygiene [PROTECTION] OFF	[FIX SUMMARY] Configure email Banner with Company Name [OWNER[Email Admin [EXAMPLE] Changes to the SMTP Banner Connector. (this may not be permitted for shared email service providers) Open an Exchange Management Shell session & Run this cmdlet, Get ReceiveConnector [enter] Set-ReceiveConnector -Identity ConnectorName -Banner 220 YourTextGoesHere [REFERENCE] https://docs.microsoft.com/en-us/exchange/mail-flow/connectors/modify-smtp
Open Relay Security [MEDIUM}	PASS	[SEVERITY] MEDIUM ..... [THREAT] Email server can be hijacked if the the Email Relay configuration is bad. This is known as an open relay attack where your email server will be hijacked to send out large volume of spam and phishing emails [PROTECTION] ON	N/A
Email Encryption-STARTTLS [MEDIUM]	PASS	[SEVERITY] MEDIUM ..... [THREAT] The email server can be forced at the initial handshake with another email server to downgrade to a weak encryption standard and allow the attack to decrypt your messages. [PROTECTION] ON	N/A

Probe	Result	Result Message	Recommendation
Browser Trusted Site[HIGH]	FAIL	[SEVERITY] HIGH ..... [THREAT] A website NOT trusted by one or more of the following Website Browsers: Mozilla, Chrome, Internet Explorer or Safari has an impact on your sites trustworthiness [PROTECTION] OFF	[FIX SUMMARY] The web server is not trusted by browser standard and maybe registered as a site of concern. [OWNER] System Admin [EXAMPLE] if you have a bad IP Reputation or Data Privacy TLS certs are not valid you will be listed as untruted by browsers. Any changes to your domain may need up to 7 days to reflected in the this probe. [REFERENCE] Browser Trust
HTTPS Only [HIGH]	FAIL	[SEVERITY] HIGH ..... [THREAT] By only allowing browsers to communicate with HTTPS encrypted web pages protects the user from being diverted to fake website or using unencrypted data communications [PROTECTION] OFF	[FIX SUMMARY] Configure HSTP in security headers [OWNER] System Admin [EXAMPLE] Configure Apache server /etc/apache2/httpd.conf file add the header "set Strict-Transport-Security 'max-age=31536000; includeSubDomains; preload' always [REFERENCE] https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
Clickjack Protection [MEDIUM]	FAIL	[SEVERITY] MEDIUM ..... [THREAT]A Click-jack exploit allows the hacker inject hidden malicious code into the website pages and iframes. [PROTECTION] OFF	[FIX SUMMARY] Configure Xframe protection in security header [OWNER] System Admin [EXAMPLE] Configure Apache server /etc/apache2/httpd.conf file add the header Header always set X-Frame-Options ""SAMEORIGIN", Header set X-Frame-Options ""DENY", [REFERENCE] Https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
Malicious XSS Code Injection [MEDIUM}	FAIL	The web pages are NOT protected from malicious code injections between the server and the users browser	The web server is not protected for XSS code injection attacks. Please contact your website administrator to make changes to the security header files. As example Apache server /etc/apache2/httpd.conf file add the ""header set 'X-XSS-Protection: 1; mode=block' "" Refer to the sites for more details on XSS protection https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection"

MIME X-Content type [LOW]	FAIL	[SEVERITY] LOW ..... [THREAT] Servers without standard MIME file format policy fail to protect attackers from uploading malicious executable programmes within a different file type, also known as MIME Sniffing. [PROTECTION] OFF	[FIX SUMMARY] Configure x content to no sniff [OWNER] System Admin [EXAMPLE] configure Apache server /etc/apache2/httpd.conf file add the ""X-Content-Type-Options: nosniff"" [REFERENCE] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options"
Content Security Policy [MEDIUM]	FAIL	[SEVERITY] MEDIUM ..... [THREAT] Webpages that DO NOT restrict its content delivery to users browser can be compromised and receive content from unknown malicious websites. [PROTECTION] OFF	[FIX SUMMARY] Configure CSP in Security Header [OWNER] System Admin [EXAMPLE] Configure Apache server /etc/apache2/httpd.conf file add the ""Header set Content-Security-Policy ""default-src 'self';"" [REFERENE] https://content-security-policy.com/"
Referrer Policy [LOW]	FAIL	[SEVERITY] LOW ..... [THREAT] Webpages that DO NOT secure with a referrer policy fail to protect the users identity and data when being redirected to another website [PROTECTION] OFF	[FIX SUMMARY] Configure Content Referrer in Security Headers [OWNER] System Admin [EXAMPLE] Configure Apache server /etc/apache2/httpd.conf file add the ""Header set Content-Referrer-Policy""default-src 'self';"" [REFEREENCE] Content Referrer policy
Server Cache-Control [MEDIUM]	FAIL	[SEVERITY] MEDIUM ..... [THREAT] Webpages that DO NOT use data storage management policies are exposed to cyber attacks leading to data loss from server memory [PROTECTION] OFF	[FIX SUMMARY] Configure Cache Control in Security Headers [OWNER] System Admin [EXAMPLE] Configure Apache server /etc/apache2/httpd.conf file add the Header Set Cache-Control: max-age=<seconds> or Cache-Control: max-stale[=<seconds> [REFERENCE] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
Cross Domain permission [LOW]	FAIL	[SEVERITY] LOW ..... [THREAT] Webpages that DO NOT use approved whitelists to control content from other domains and web services are exposed to fake malicious website data [PROTECTION] OFF	[FIX SUMMARY] Configure X permission cross domain in security headers [OWNER] System Admin [EXAMPLE] Configure Apache server /etc/apache2/httpd.conf file add the Header set 'X-Permitted-Cross-Domain-Policies' 'none' - blocks other sites from loading content to browser. [REFERENCE] https://owasp.org/www-project-secure-headers/#x-permitted-cross-domain-policies"

Except-CT TLS [LOW]	FAIL	[SEVERITY] LOW ..... [THREAT] Website encryption certificates should be verified by the CT Public Log - a trusted public database subscription service. [PROTECTION] OFF	[FIX SUMMARY] Configure Expect -CT verify in security Header [OWNER] System Admin [EXAMPLE] Configure Apache server /etc/apache2/httpd.conf file add the 'Expect-CT: max-age=86400, enforce, report-uri= 'https://foo.example/report' [REFERENCE] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Expect-CT" Please note Except-CT is being redacted in 2022.
Server-Service Displayed [MEDIUM}	PASS	[SEVERITY] MEDIUM ..... [THREAT] Webpages displaying service information can be useful for hackers during their reconnaissance stage. [PROTECTION] ON	N/A
Hide X Powered Services [MEDIUM]	PASS	[SEVERITY] MEDIUM ..... [THREAT] Servers that display service & version are exposing critical system information that the attacker can use against them [PROTECTION] ON	N/A
Cookie Notification [LOW]	FAIL	[SEVERITY] LOW ..... [THREAT] Website cookie notification page provides trust that user data is appropriately managed [PROTECTION] OFF Disclaimer: The server may use a plug cookie program which allows the user to select their cookie preferences. Currently our scanners don't detect the plugins. We are working on a solution for this and will update you soon. Therefore this control maybe regarded as a false positive finding. Please contact support to override this probe to pass	[FIX SUMMARY] Add a webpage notifying users how site cookies are managed [OWNER] System Admin [EXAMPLE] The cookie statement should explain to the user how cookies and any identifiable are being managed on the site. [REFERENCE] https://www.cookielaw.org/the-cookie-law/
Privacy Notification [LOW]	FAIL	[SEVERITY] LOW ..... [THREAT] Website privacy notification page provides trust that a users privacy data is appropriately managed [PROTECTION] OFF	[FIX SUMMARY] Add a webpage notifying users how data privacy is managed [OWNER] System Admin [EXAMPLE] Privacy statement should explain to the user how privacy data is being managed on the site. [REFERENCE] https://en.wikipedia.org/wiki/Privacy_policy"

Probe	Result	Result Message	Recommendation
Internet Proxy Services [HIGH]	PASS	[SEVERITY] HIGH ..... [THREAT] Attackers can use Proxy Servers to protect their identity and shield themselves from their attack methods. Servers can be hijacked and used to divert malicious code and attack methods [PROTECTION] ON	N/A
Tor Darkweb Node Services [MEDIUM]	PASS	[SEVERITY] MEDIUM ..... [THREAT] Servers that are not secure can be hijacked as a TOR relay service to host and stream illegal data to other internet users. Immediately, there will be a noticeable impact on resources for legitimate services and eventually the server will be blacklisted along with any hosted websites. [PROTECTION] ON	N/A
VPN Services [HIGH]	PASS	[SEVERITY] HIGH ..... [THREAT] Servers that are not secure can be hijacked as a VPN Service to hide the identity of attackers from cyber attacks. [PROTECTION] ON	N/A
Malware Hosting [HIGH]	PASS	[SEVERITY] HIGH ..... [THREAT] Servers that are not secure can be hijacked to host and distribute Malware or have been breached with known malware [PROTECTION] ON	N/A
Spyware Hosting [MEDIUM]	PASS	[SEVERITY] HIGH ..... [THREAT] Servers that are not secure can be hijacked to host and distribute Spyware [PROTECTION] ON	N/A
Dshield Compromised Domains [HIGH]	PASS	[SEVERITY] HIGH ..... [THREAT] Dshield.org monitor check for compromised servers. Unsecure servers will be listed here. [PROTECTION] ON	N/A

IP Netblock Hijack [MEDIUM]	PASS	[SEVERITY] MEDIUM ..... [THREAT] Unsecure IP Netblock address management can be hijacked and used by attackers to hide their cyber attacks [PROTECTION] ON	N/A
Malicious Bot site [HIGH]	PASS	[SEVERITY] HIGH ..... [THREAT] Servers that are not secure can be hijacked to host and distribute Botnet CR services [PROTECTION] ON The domain's IP address has NOT been flagged for running a Malicious Botnet Service or is part of a Botnet CR network	N/A
Spam Host [HIGH]	PASS	[SEVERITY] HIGH ..... [THREAT] Servers that are not secure can be hijacked to host and distribute Spam emails [PROTECTION] ON	N/A

Domain Vulnerability 0.0 | 28.0

Probe	Result	Result Message	Recommendation
Port Exposure [HIGH]	FAIL	[SEVERITY] HIGH ..... [THREAT] The web server maybe running malicious port services OR displaying unnecessary port services & versions. The attacker can use the information to find a known vulnerabilities to gain access the server. [PROTECTION] OFF	[FIX SUMMARY] Check all Port Numbers listed as found for any unauthorized services. Hide all server ports from the internet. [OWNER] System Admin [EXAMPLE]Display only ports 80 and 443 - Avoid displaying Ports 993, 2082, 2083, 2086, 208, 2079, 3306, 587, 465, 995, 21, 22, 2096, 139, 44531,1170, 1234,1243,1981, 2001, 2023,2140, 2989, 3024, 3150, 3700, 4950, 6346, 6400, 6667, 6670, 12345, 12346, 16660, 18753, 20034, 20432, 20433, 27374, 27444, 27665, 30100, 31335, 31337, 33270, 33567, 33568, 40421, 60008, 65000 [REFERENCE] https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml 110, 21, 22
Critical Risk Vulnerabilities [CRITICAL]	FAIL	[SEVERITY] CRITICAL ..... [THREAT] Known CVE Vulnerabilities can be exploited by an cyber attack to access the website and steal confidential data [PROTECTION] OFF	[FIX SUMMARY] Review the CVE codes provided below and use the NIST reference link to review the recommended remediation [OWNER] Security Team [EXAMPLE]' CVE 2021 4356: CVE Code example [REFERFENCE] https://nvd.nist.gov/vuln/search CVE-2002-0640, CVE-2002-0639, CVE-2003-0693, CVE-2006-5051, CVE-2003-0789, CVE-2004-0492
High Risk Vulnerabilities [HIGH]	FAIL	[SEVERITY] HIGH ..... [THREAT] Known CVE Vulnerabilities can be exploited by a cyber attack to access the website and steal confidential data [PROTECTION] OFF	[FIX SUMMARY] Review the CVE codes provided below and use the NIST reference link to review the recommended remediation [OWNER] Security Team [EXAMPLE]' CVE 2021 4356 ' :CVE code example [REFERFENCE] https://nvd.nist.gov/vuln/search CVE-2006-4924, CVE-2003-1562, CVE-2015-5600, CVE-2006-5794, CVE-2014-1692, CVE-2003-0695, CVE-2007-4752, CVE-2016-10009, CVE-2016-1908, CVE-2010-4478, CVE-2016-10012, CVE-2003-0682, CVE-2013-5697, CVE-2004-1082, CVE-2003-0987, CVE-2004-0488, CVE-2022-22720, CVE-2009-1891, CVE-2022-31813, CVE-2021-44790, CVE-2009-1890, CVE-2013-2249, CVE-2003-0542, CVE-2004-2343, CVE-2003-0993, CVE-2002-2272, CVE-2021-39275, CVE-2011-3192

Medium Risk Vulnerabilities [MEDIUM]	FAIL	[SEVERITY] MEDIUM ..... [THREAT] Known CVE Vulnerabilities can be exploited by a cyber attack to access the website and steal confidential data [PROTECTION] OFF	[FIX SUMMARY] Review the CVE codes provided below and use the NIST reference link to review the recommended remediation [OWNER] Security Team [EXAMPLE] CVE 2021 4356: CVE code example [REFERFENCE] https://nvd.nist.gov/vuln/search CVE-2004-1653, CVE-2017-15906, CVE-2015-6564, CVE-2007-2243, CVE-2006-5052, CVE-2006-0225, CVE-2015-5352, CVE-2004-0175, CVE-2014-2653, CVE-2014-2532, CVE-2005-2798, CVE-2019-6110, CVE-2010-5107, CVE-2018-15473, CVE-2020-15778, CVE-2016-10708, CVE-2010-4755, CVE-2016-20012, CVE-2019-6111, CVE-2016-10010, CVE-2008-4109, CVE-2019-6109, CVE-2008-2939, CVE-2003-1418, CVE-2002-1658, CVE-2014-0118, CVE-2017-9798, CVE-2001-1556, CVE-2007-5000, CVE-2015-3183, CVE-2005-3352, CVE-2004-0174, CVE-2011-3368, CVE-2009-2699, CVE-2011-3348, CVE-2022-28330, CVE-2013-1896, CVE-2014-0226, CVE-2022-22721, CVE-2011-4317, CVE-2007-6750, CVE-2013-6438, CVE-2004-0263, CVE-2021-40438, CVE-2021-34798, CVE-2012-0031, CVE-2022-30522, CVE-2008-0455, CVE-2017-9788, CVE-2009-3555, CVE-2018-1301, CVE-2018-1302, CVE-2018-1303, CVE-2016-5387, CVE-2003-0460, CVE-2012-0883, CVE-2004-0940, CVE-2004-0942, CVE-2015-0228, CVE-2011-0419, CVE-2014-0231, CVE-2022-29404, CVE-2010-0010, CVE-2003-0020, CVE-2014-0098, CVE-2022-30556, CVE-2007-6388, CVE-2009-1195, CVE-2022-28615, CVE-2022-28614, CVE-2022-22719
SSL Cert Heartbleed Vulnerability [MEDIUM]	FAIL	[SEVERITY] MEDIUM ..... [THREAT]OpenSSL below version 1.0.1g does not properly handle Heartbleed Extension packets, allowing remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-reads [PROTECTION] OFF	[FIX SUMMARY] Upgrade OPENSSL to the latest version [OWNER] Website Admin [EXAMPLE] Openssl version 3.0 [REFERENE] https://nvd.nist.gov/vuln/detail/cve-2014-0160 (Risk Cat Med High)

TLS CCS Injection Vulnerability [MEDIUM]	FAIL	The SSL certificate is vulnerable to the CCS INJECTION attack. SSL certificate 'OpenSSL' before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of Change Cipher Spec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability	Upgrade OpenSSL to the latest version. SSL certificate 'OpenSSL' before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of Change Cipher Spec messages. Refer for more details: https://nvd.nist.gov/vuln/detail/cve-2014-022
SSL Ticketbleed Vulnerability [MEDIUM]	FAIL	The SSL certificate is vulnerable to the TICKETBLEED attack A virtual server configured with a Client SSL profile that has the non-default Session Tickets option enabled may leak up to 31 bytes of uninitialized memory. A remote attacker may exploit this vulnerability to obtain Secure Sockets Layer (SSL) session IDs from other sessions. It is possible that other data from uninitialized memory may be returned as well.	You will need to update the configuration of the 'Ticket Session' on F5 appliances and refer to vendor upgrade guidance. Refer for more details: https://nvd.nist.gov/vuln/detail/CVE-2016-9244
SSL BREACH Vulnerability [LOW]	FAIL	[SEVERITY] LOW ..... [THREAT] A BREACH method decrypts communications between server and user via the 'CSRF' man in the middle technique [PROTECTION] OFF	[FIX SUMMARY] There are a number of things to consider 1. disable HTTP compression 2. enable CSRF protection on web pages 3. install latest SSL cert. [OWNER] System Admin [EXAMPLE] The HTTPS protocol, as used in unspecified web applications, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which makes it easier for man-in-the-middle attackers to obtain plaintext secret values by observing length differences during a series of guesses in which a string in an HTTP request URL potentially matches an unknown string in an HTTP response body, aka a "BREACH" attack, a different issue than CVE-2012-4929. [REFERENCE] https://nvd.nist.gov/vuln/detail/CVE-2013-3587

SSL POODLE Vulnerability [LOW]	FAIL	[SEVERITY] LOW ..... [THREAT] A POODLE method decrypts communications between server and user via a man in the middle technique [PROTECTION] OFF	[FIX SUMMARY] Upgrade your SSL cert or openssl version to the latest [OWNER] System Admin [EXAMPLE] SSL 3.0 or Openessl 1.0.1i are no longer secure. As a result, it makes it easier for man-in-the-middle attacker to obtain cleartext data via the "POODLE" attack method. [REFERENCE] Https://nvd.nist.gov/vuln/detail/cve-2014-3566
SSL DROWN Vulnerability [LOW]	FAIL	[SEVERITY] LOW ..... [THREAT] A DROWN method decrypts communications between server and user via a SSLv2 communications technique [PROTECTION] OFF	[FIX SUMMARY] Disable SSL2 communications and upgrade your SSL cert. [OWNER] System Admin [EXAMPLE] The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack. [REFERENCE] https://nvd.nist.gov/vuln/detail/CVE-2016-0800
SSL Renegotiation Vulnerability [MEDIUM]	FAIL	[SEVERITY] MEDIUM ..... [THREAT] A SSL RENEGOTIATION method performs a denial of service and a man in the middle cyber attack to steal user credentials [PROTECTION] OFF	[FIX SUMMARY] Configure SSL communication to protect against the Secure Renegotiation attack method by [OWNER] System Admin {EXAMPLE] Upgrade webserver services to latest version e,g, apache, nginx donâ€™t allow client initiation of ssl renegotiation attack [REFERENCE]
TLS Fallback Vul [HIGH]	FAIL	[SEVERITY] HIGH ..... [THREAT] A TLS FALLBACK / DOWNGRADE method allows the attacker to downgrade the SSL communication to an unsecure standard e.g. SSL 3.0, and then allows the attacker to decrypt all communication and inject malicious code into the website. [PROTECTION] OFF	[FIX SUMMARY] Ensure all website SSL protocol communications are ONLY allowed with secure protocols SSL v.1.2 or 1.3. ALL other SSL protocol comms should be disabled. [OWNER] System Admin [EXAMPLE] You should ensure the TLS protocol has the Cipher Suite Value (SCSV) that is used to guard against protocol downgrade attacks. You must upgrade to the latest version of Openssl or ensure your TLS protocol is running â€œFallback SCVCâ€•. [REFERENCE] https://www.ietf.org/archive/id/draft-bmoeller-tls-downgrade-scsv-02.txt

Probe	Result	Result Message	Recommendation
SSL Cert Date Valid [MEDIUM]	FAIL	[SEVERITY] MEDIUM..... [THREAT] Failure to renew the SSL certification with a CA authority will flag to the user that the website is no longer secured by a valid encryption cert, supported by CA Authority, and therefore cant be TRUSTED for secure communications [PROTECTION] OFF	[FIX SUMMARY] Renew the SSL Certificate [ONWNER] Website administrator [EXAMPLE] Refer to Reference [REFERENCE] Https://tools.ietf.org/html/rfc5246
SSL Cert Cipher Suite [MEDIUM]	FAIL	[SEVERITY] MEDIUM..... [THREAT] Older encryption standards can be broken and the data communication can be decrypted between the server and user by a man in the middle cyber attack. This may results in revealing confidential information such as user credentials and other sensitive data [PROTECTION] OFF	[FIX SUMMARY] Purchase SSL cert with a Cipher Suite standard in EXAMPLE below [OWNER] Website administrator A stronger cipher suite will be available [EXAMPLE} SSL CERT with following configuration from any registered CA certified authority that can generate a CSR and private key for your domain "TLS_AES_128_GCM_SHA256" "TLS_AES_256_GCM_SHA384 " "TLS_CHACHA20_POLY1305_SHA256" [REFERENCE] https://tools.ietf.org
SSL Cert Secure [HIGH}	FAIL	[SEVERITY] HIGH..... [THREAT] Older encryption standards can be broken and the data communication can be decrypted between the server and user by a man in the middle cyber attack. This may results in revealing confidential information such as user credentials and other sensitive data [PROTECTION] OFF	[FIX SUMMARY] Install latest SSL cert encryption standard version 1.3 or 1.2. [OWNER[Website administrator [EXAMPLE]Install a SSL V.1.2 or 1.3. obtained from a registered CA to generate a CSR and private key for your domain [REFERENCE] Refer to site for more details: https://tools.ietf.org/html/rfc5246 , https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

Cookie Sucure Flag [MEDIUM]	FAIL	[SEVERITY] MEDIUM..... [THREAT] Unencrypted Cookie Data with user access credentials can be read by a man in the middle cyber attack [PROTECTION] OFF Disclaimer: Our scanners currently do not detect external cookie security plugin programmes. We are working on a solution for this and will update the system soon. Therefore this probe maybe regarded as a false positive if your domain uses a plugin cookie programme.	[FIX SUMMARY] Configure Secure Cookie in the security header [OWNER] Website Admin [EXAMPLE] Set javascript Set-Cookie: <cookie code> expires=Tue, 20-Apr-21 05:23:36 GMT; path=/; domain=.www.domain.com; <b>SECURE<b>/ [REFERENCE] https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies"
Cookie Samesite [LOW]	FAIL	[SEVERITY] LOW..... [THREAT] Unprotected Site Cookie Data can be stolen by a "Cross Site Request Forgery (CSRF)" cyber attack [PROTECTION] OFF Disclaimer: Our scanners currently do not detect external cookie security plugin programmes. We are working on a solution for this and will update the system soon. Therefore this probe maybe regarded as a false positive. Please contact support to change probe to PASS	[FIX SUMMARY] Configure Samesite Cookie in the security header [OWNER] Website Admin [EXAMPLE]Configure Security Header - Javascript Set-Cookie: <cookie code> expires=Tue, 20-Apr-21 05:23:36 GMT; path=/; domain=.www.domain.com; SameSite=LAX OR Strict: [REFERENCE] https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies"
Cookie HttpFlag Protection [LOW]	FAIL	[SEVERITY] LOW..... [THREAT] Unprotected HTTP Cookie Data can be stolen by a javascript (XSS) cross-site scripting cyber attack [PROTECTION] OFF	[FIX SUMMARY] Configure HTTPflag Cookie Protection in the security header. [OWNER] Website Admin [EXAMPLE] Configure Security header - javascript Set-Cookie: <cookie code> expires=Tue, 20-Apr-21 05:23:36 GMT; path=/; domain=.www.domain.com; HTTPONLY [REFERENCE] https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

Cookie Notification [LOW]	FAIL	[SEVERITY] LOW..... [THREAT] Failure to notify the user on how cookies are managed lowers the trustworthiness of the website [PROTECTION] OFF Disclaimer: The server may use a plug cookie program which allows the user to select their cookie preferences. Currently our scanners don't detect the plugins. We are working on a solution for this and will update you soon. We can override this probe to PASS - please contact support	[FIX SUMMARY] Add a cookie notification page or cookie plugin -Disclaimer our probes may not pick up site plugin cookie programmes - we can overide this failure in our system. please contact support. [OWNER] Website Admin [EXAMPLE] Refer to reference [REFERENCE] https://www.cookielaw.org/the-cookie-law/
Privacy Notification [LOW]	FAIL	[SEVERITY] LOW..... [THREAT] A website without a Data Privacy notification page is deemed as untrustworthy. The notification must explain how data is collected and managed. In many countries this is now a regulatory requirement and failure to do this will lower the trustworthiness of the website [PROTECTION] OFF	[FIX SUMMARY] Add a privacy notification page to your website [OWNER] Website administrator [EXAMPLE] refer to reference [REFERENCE] https://en.wikipedia.org/wiki/Privacy_policy"

Overview
Cyber Hygiene Scans

Cyber Hygiene Scans provide a quick and cost-effective way to review a company's cyber security posture. We do this by pointing Hygiene Probes at a domain's security entry points and collect publicly available data from open source feeds.

Cygienic Ratings guide the user in making risk-related decisions based on the security of a domain's data and communication posture. By providing the user with critical cyber security information, a user can ascertain the level of risk associated with the website. (For example, has it been compromised? How well is the website secured? What are its vulnerabilities?)

Scanners, passively probe the Domain with a non-intrusive cybersecurity assessment. By dispatching a collection of finely tuned probes, we can retrieve and dissect important data signals to reveal a domain's trustworthiness.

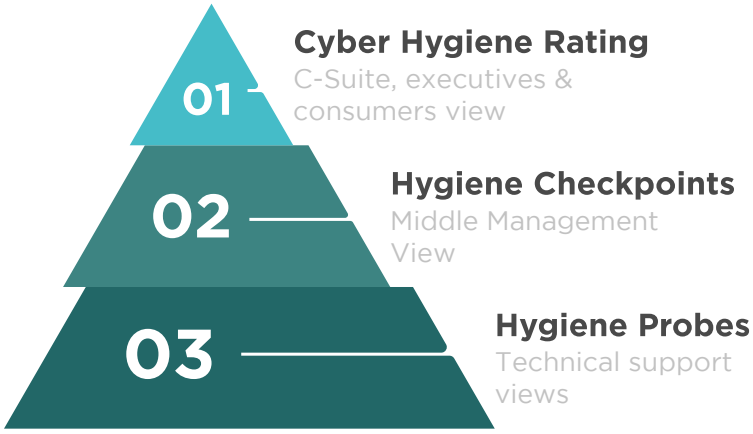
Cygienic
Hygiene Rating

A Cyber Hygiene Rating is a grade awarded to a domain based on the results from the Hygiene Scan. Hygiene Probes are dispatched and then reported back to the Hygiene Checkpoints to determine if a probe is a pass or fail. The scores are then calulated and consolidated as a final grade e.g.A-E.

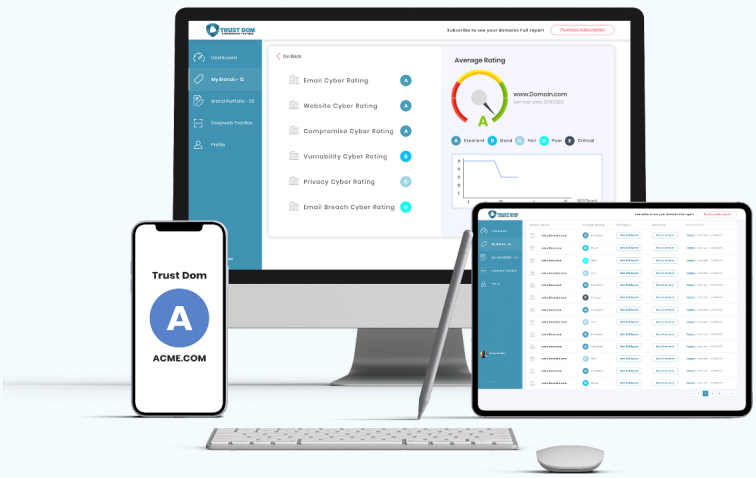
Hygiene Rating is a grade awarded to a domain or company

Hygiene Checkpoints Control the Hygiene Probes

Probes record technical details and remediation plans



A Hygiene Rating indicates an overarching cybersecurity profile of the Domain's services. All Ratings are available in real-time, providing the user with an immediate grade at their fingertips. Domain ratings provide the user with confidence that an 'A' grade domain exhibits an excellent level of cyber security and trustworthiness and is therefore safe to use.



Hygiene Checkpoint **Scores**

Hygiene Checkpoints are assessed across five categories. Each checkpoint consist of several probes that are designed to access the level of cybersecurity exposure and vulnerability. These five Checkpoints comprises a composite of over 50 probes which when scanned and scored, produce a Rating. A Grade is then assigned to the Domain for its overall Cyber Hygiene

As example, 2/8 for the Email security settings reflects very poor Communication security. This may potentially lead to emails being susceptible too malware, ransomware and spam.

Email security

Can we trust that the email communications has protected our privacy? Is it susceptible to email fraud and malware ? Does it protect, encrypt, and secure communications?

Webpage security

Can we trust the website to protect our privacy, data and access? Does the website protect us from malware and attempted data breaches?

IP Reputation

Can we trust that the domain has not been compromised by hackers? Is it safe to join the website or communicate with this domain?

Domain Vulnerability

Can we trust that the domain is not vulnerable to a cyber attack? Has the domain been regularly patched and fixed with the latest security service advisories?

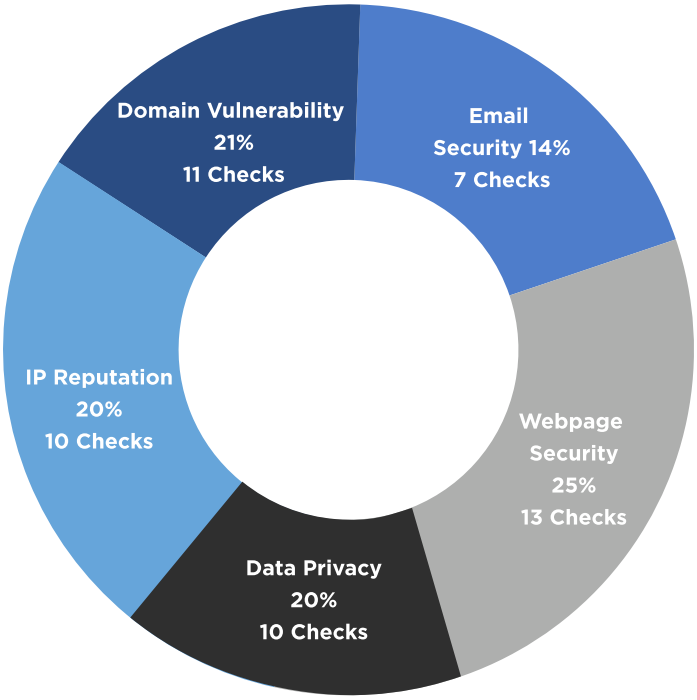
Data privacy

Can we trust that the website follows global privacy standards? Is the website secure in protecting personal information?

Cyber Hygiene **Weightings**

The risk weighting is managed by an algorithm that calculates each security checkpoint against a Hygiene probe before assigning a Rating.

Note: The algorithm may change from time to time as our experts adjust it to reflect new cyber risks. Please also note that we do not share details of our Probes values or our algorithms.



- Email Security 14%
- Domain Vulnerability 21%
- IP Reputation 20%
- Webpage Security 25%
- Data Privacy 20%

How accurate are **Cyber Hygiene ratings?**

We have taken every effort to ensure that our ratings are accurate and transparent. We have focused on assessing data points that are tangible and clearly quantifiable.

Our ratings explicitly indicate whether an organisation has sufficiently implemented security standards that allow us to trust their public security and trust profile and our email and web-based interactions with them.

Whilst these ratings can correlate to the internal security profile of an organisation, we should NOT assume that an “A” rating definitively means that an organisation is fully secure.

Cyber Stats

Cyber-attacks are on the rise

Let’s work together to stop your company becoming yet another cyber-attack statistic. As the world becomes increasingly connected and more businesses move online, cyber security will become everyones shared responsibility.

More Cyber Security Stats...

01. The global cybercrime economy generates approx USD 1.5 trillion yearly

02. The average cost of a data breach for a company in 2020 was US$3.86m

03. The average cost per stolen record is US$120