WHY PEOPLE CHOOSE TRUSTISCAN

Fed up of waiting weeks for a pentest report?

We know that penetration testing has a reputation for being complicated and time consuming. That's why TrustiScan was built by penetration testers to disrupt the offensive security industry and deliver better results.

With decades of combined experience, we offer a **timely, accurate and professional** penetration service to all of our cunstomers.

We offer:

- **Scan**
- **Radar**
- **CREST-approved pentesting**

> *A straightforward, comprehensive and complete solution for security testing.*
>
> **Daniel S, Head of DevOps & Performance at YuLife**

38% more cost-effective

Precise, hourly billing with no padding out

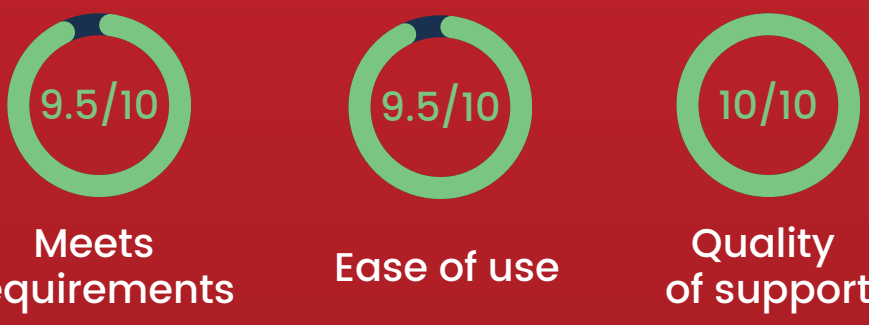
Instant communication

Real-time reporting, free retesting and enterprise integrations.

4x faster

Instant quoting, online booking and on-demand scheduling

As rated by our customers on G2



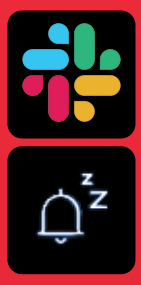
TrustiScan

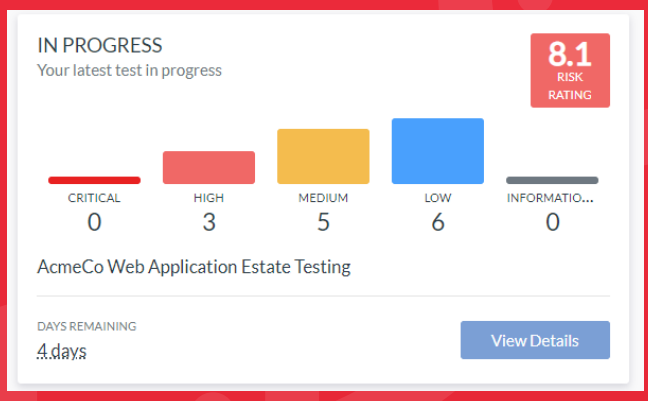
trust365.com

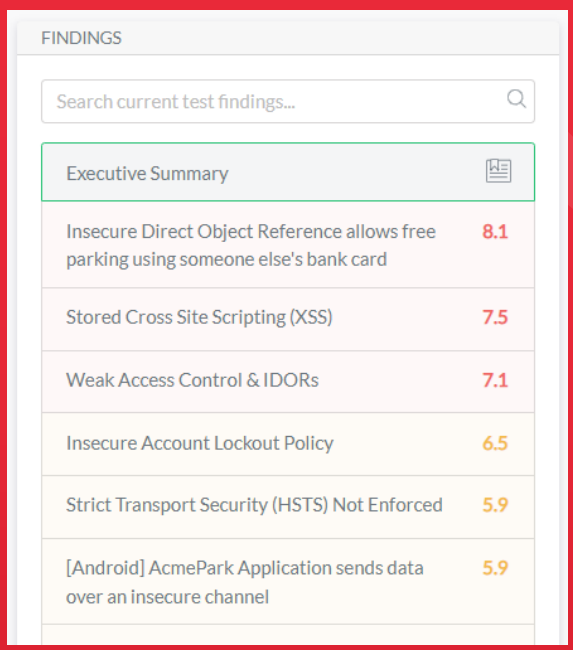
PORTAL BY TRUSTISCAN

What happens during a Penetration Test?

While your test is running, a summary of your results will be displayed on the home screen.







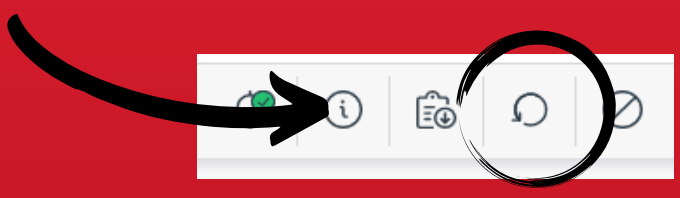
As your tester discovers findings, they will appear in the portal **in real time.**

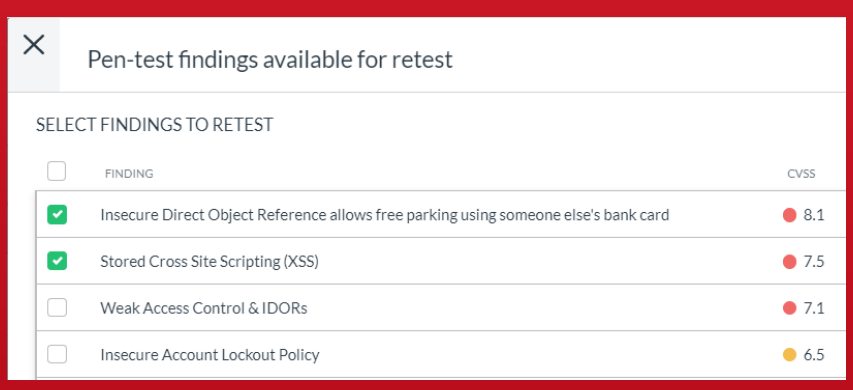
Each finding has a full technical overview, CVSS-based risk rating and recommendation.

You'll be notified within the platform, via email or SMS.

You can communicate directly with your testers as they test, via Slack.

Use the **Retest a Finding** button to see all your findings available for retest.





Tick the findings you would like to retest.

If you book these within 7 days of your test completion date, OnSecurity will retest your findings for **free.**

Your retests will be booked in by your Operations Team.

You can download a full report of your results using the **Download Report button.**

TrustiScan

trust365.com

G2 High Performer SPRING 2023

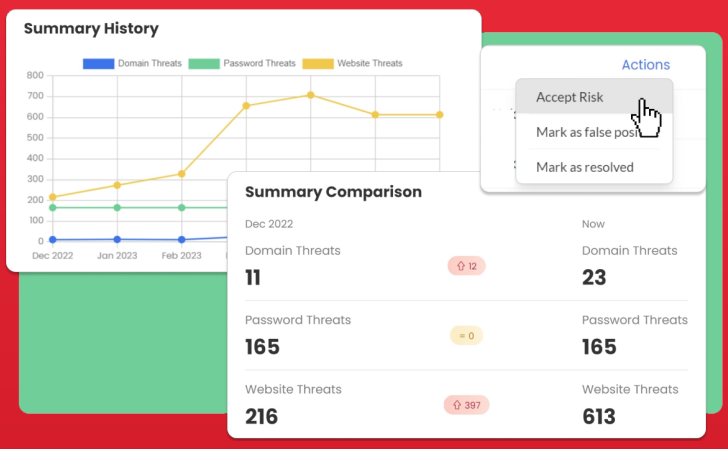
RADAR BY TRUSTISCAN

The attack surface has moved. Move with it.

Stay a step ahead of the criminals

80% of breaches are caused by hackers finding and exploiting known vulnerabilities. Radar watches your back 24/7 - giving you the power to find vulnerabilities before the bad guys do.

Radar was built from years of combined industry expertise.



Stay secure with scan

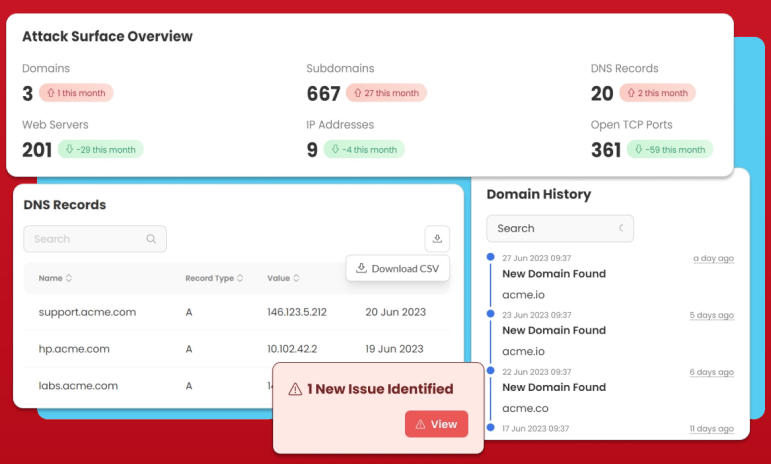
By processing over 14 billion breached credentials, motoring over 20,000 sites and over two million domains a year, Radar ensures your business, brand and customers are protected.

See what the bad guys see and understand potential attack vectors.

Threats at a glance

Use our Summary Page to get an instant update on your key threat areas. Rapidly triage your vulnerabilities via the findings change feature.

Our simple, functional design is suitable for everyone and quickly shows you what we've found and what it means for you and your business.



TrustiScan

trust365.com

High Performer SPRING 2023

SCAN BY TRUSTISCAN

Unpatched systems are a hacker's best friend.

Why do we use scan?

Scan monitors your external estate, finding and reporting vulnerabilities in your internet-facing infrastructure before the baddies do.

Stay secure with scan

Scan will identify any missing patches, security misconfigurations, default passwords, dangerous services or otherwise potentially harmful security vulnerabilities.

Carrying out 40,000 different checks on your systems, Scan makes sure your safe and secure, giving you peace of mind to get on with what you do best!

Prevent breaches with scan

Hackers specifically write tools to mass-scan the Internet to identify vulnerabilities that they can exploit. Scan will spot these vulnerabilities and rapidly report any potential dangers so you can take immediate action and close down any risk.

40,000

different checks on your system

TrustiScan

trust365.com

High Performer SPRING 2023

Are you an easy target for hackers?

PENTEST WITH TRUSTISCAN

But what is a pentest?

Our CREST-approved pentesters use the same techniques as cyber-criminals to try to break into your network and 'steal' your data.

The Pentest is carried out in a safe and controlled environment. We will report any found security problems in real time so that you can fix them before the cyber-criminals can exploit them.

How secure are you, really?

Even the most security-forward organisations need to ensure they stay ahead of the latest threats and keep businesses, brands and customers safe. **Regular pentesting is the best way to achieve this.**

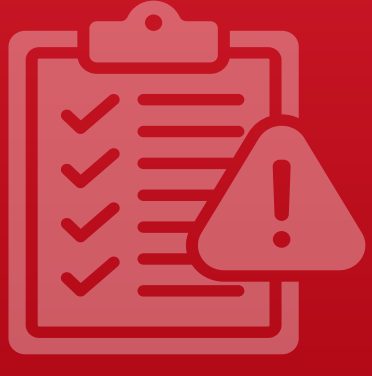
5 benefits of regular pentesting

- Get a 'hackers eye view' of your business
- Prevent breaches and associated recovery costs and fines
- Confidence in your IT security
- Compliance and regulation certification
- Prioritise and document your risk

Stay Compliant

Pentesting is required for ISO 27001 and PCI/DSS

To stay compliant, you are required to complete regular pentests, especially if you are planning to work with any **UK Government** organisations, including the NHS.



TrustiScan

trust365.com

High Performer SUMMER 2023 | Best Support SUMMER 2023 | High Performer Small Business SPRING 2023

OFFICE365 BY TRUSTISCAN

Auditing the security practices of Microsoft 365 usage as aligned to Microsoft recommendations and relevant 365 benchmarks.

What does it achieve?

Auditing the security configuration of your container images and runtime configuration as aligned to industry recommendations and benchmarks.

What do we access?

Depending on services in use on your tenant, this includes the assessment of:

- Authorisation and authentication configuration.
- Exchange configuration, including:
- General email client security configuration.
- Anti-spam, anti-phishing and anti-malware practices.
- DKIM, DMARC and SPF
- Microsoft Teams configuration.
- SharePoint configuration.
- General privilege management.
- Data protection overview, including data loss prevention and data lifecycle.

As rated by our customers on G2

Meets requirements

Ease of use

Quality of support

TrustiScan

trust365.com

WEB APPLICATION PENTESTING

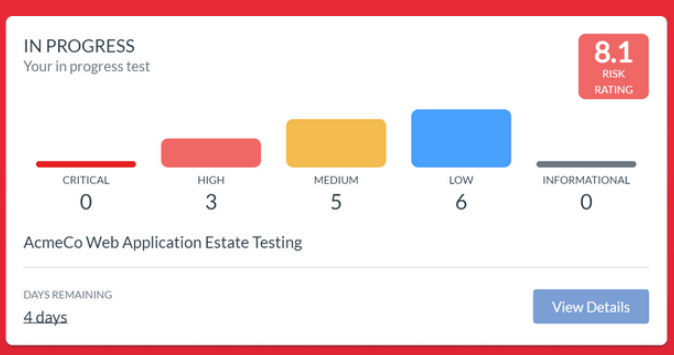
TrustiScan web application penetration testing follows a comprehensive testing methodology and involves the following activities

Discovery Phase

The discovery phase is used to gather useful information about the application and environment under assessment. It is divided into the following areas:

Target Identification & Information Gathering

Using the scope and target details provided in the scheduling process the tester/s will identify the target, and attempt to gather any publicly available information related to the target. This includes, but is not limited to, the interrogation of search engines, DNS records, SSL certificates etc. to gather information which may assist the team in identifying and exploiting vulnerabilities in the application or its environment



Target Enumeration

There is a huge array of technology choices available to organisations when developing and deploying web applications. It is vital for the tester to have an understanding of the front and back end technologies, data processing and storage, frameworks and hosting environment involved in an assessment. During this phase, the team uses a number of methods to identify the technologies, interfaces, protocols and frameworks in use in the target application. This allows the team to customise attacks with the aim of ensuring higher numbers of vulnerabilities and security issues are uncovered.

Attack Surface Enumeration

Using the scope provided for the assessment, we shall identify the size of the attack surface of the application. This includes but is not limited to:

- Manual crawling of the application (from unauthenticated and authenticated testing perspectives where applicable)
- Network traffic monitoring

Core Assessment Phase

The core assessment phase is where the tester/s identifies and exploits vulnerabilities. The tester/s will attempt to replicate as closely as possible real-life 'hacker' behaviour.

Activities that will be conducted as part of this phase are as follows

- Web server and supporting infrastructure configuration review
- Application Mapping
- Encryption/Cryptography Review
- Authentication Review
- Session Handling Review
- Access Control Review
- Input Validation Review
- Information Leakage Review
- Application Logic Review
- Overall application code quality
- Environmental/configuration /integration web server issues
- Web services testing
- Client Side Control Review

WHY PEOPLE CHOOSE TRUSTISCAN

38% more cost-effective

Precise, hourly billing with no padding out

4x faster

Instant quoting, online booking and on-demand scheduling

Instant communication

Real-time reporting, free retesting and enterprise integrations

Customers love us!

80% of our customers come back year on year!

TrustiScan

trust365.com

High Performer EMEA FALL 2023 · Momentum Leader WINTER 2024 · Best Support SUMMER 2023 · Best Meets Requirements WINTER 2024 · High Performer Europe WINTER 2024

MOBILE APPLICATION PENTESTING

TrustiScan penetration testing follows a comprehensive testing methodology and involves the following activities.

Discovery Phase

The discovery phase is used to gather useful information about the application and environment under assessment. It is divided into the following areas:

Target Identification & Information Gathering

Using the scope and target details provided in the scheduling process the tester/s will identify the target, and attempt to gather any publicly available information related to the target. This includes, but is not limited to, the interrogation of search engines, DNS records, SSL certificates etc. to gather information which may assist the team in identifying and exploiting vulnerabilities in the application or its environment.

Attack Surface Enumeration

Using the scope provided for the assessment, we shall identify the size of the application's attack surface.

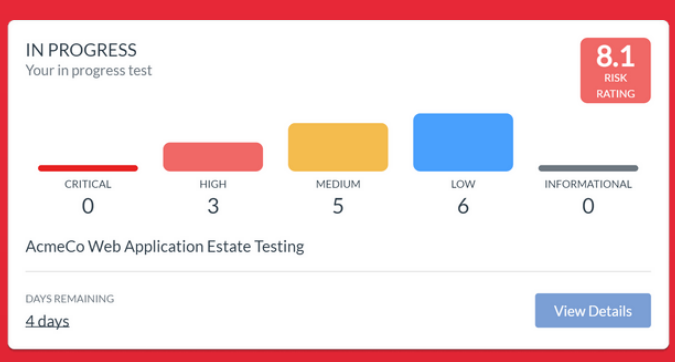
This includes but is not limited to;

- Manual crawling of the application
- Application package inspection
- Source code analysis through de-compilation
- Network traffic monitoring
- Identification of advanced security controls in use (rooting/jailbreak detection, etc.
- Enumeration of entry points and interaction with other applications, analysis of data stored on the device (databases, plist files, properties files, etc.), in order to ensure the complete attack surface is enumerated.

Target Enumeration

There is a huge array of technology choices available to organisations when developing and deploying a native mobile application. It is vital for the assessment team to have an understanding of the front and back end technologies, data processing and storage, frameworks and hosting environment involved in an assessment.

During this phase, the team uses a number of methods to identify the technologies, interfaces, protocols and frameworks in use in the target application. This allows the team to customise attacks with the aim of ensuring higher numbers of vulnerabilities and security issues are uncovered.



Attack Phase

Attack Phase - The attack phase is where the tester/s identifies and exploits vulnerabilities. The tester/s will attempt to replicate as closely as possible real-life 'hacker' behaviour.

Input Enumeration

All local and remote input vectors throughout the in-scope application are identified and enumerated. Normal (expected) input is submitted throughout the application to determine standard behaviour. A map of application behaviour is created, as well as a list of interesting and/or potentially unsafe functions. An exhaustive list of input vectors is used, including but not limited to GET and POST parameters, URLs, local files and databases, inter-app communication systems, inbound SMS, etc.

Business Logic Bypass

The testers/s will attempt to bypass any business logic rules in place in the application. These tests are not possible to automate and can only be performed by an experienced security consultant who can quickly ascertain how the application business logic functions. This phase is carried out using manual testing supported by ad-hoc tools such as proxies, debuggers and platform specific software and includes techniques such as intercepting and tampering network traffic and local OS calls, interacting with the application's exposed interfaces, etc.

Application Configuration Assessment

- Lack of code obfuscation
- Verbose logging,
- Broken cryptography to secure data at rest and in transit and appropriate protection mechanisms in the communication protocol with the back-end server.

End Point Assessment

Network communication is commonly found in native mobile applications. A security assessment of the application end-point hosting environment complements each evaluation. This assessment aims to identify weaknesses in the infrastructure or the transport layer which may allow attackers to compromise the host or application data via means other than native mobile application vulnerabilities.

Output Analysis

All output from the application is enumerated and analysed to identify potential attack egress points in the application. This will make subsequent tests easier to perform and classify. Output can take a number of forms, such as the return of requested information, encrypted or unencrypted data written on local files and\or databases, error messages, system logs, redirects and time delays.

Fuzzing

Unexpected input is submitted to input vectors throughout the application, to cause unexpected behaviour, error conditions, unexpected system logs, or causing the application to carry out functionality outside that intended by the application developers.

Vulnerability Identification

Application vulnerabilities are identified using a combination of the four steps above. Depending on the type of vulnerability and the potential impact, the team will decide whether to exploit further. To ensure consistency across engagements, the team use four industry standard classification methods to identify and classify vulnerabilities, namely OWASP Top Ten Mobile 2014, SANS Top 25, Mitre CAPEC and Mitre CWE.

Vulnerability Exploitation

Exploiting a vulnerability to its full extent allows the team to replicate what real-life attackers would do when 'hacking' an application. The team will attempt to compromise application data, subvert application logic, gain unauthorised access to the application or its accounts, or compromise the application server in line with agreed terms of reference for the engagement.