Dynamic Penetration Testing

DATASHEET

Putting Cyber Risk in Context

Actionable Reporting for Effective Risk Remediation

Dynamic Penetration Testing (DPT) brings actionable risk remediation back to Penetration Testing. It gives businesses a new way of continually managing cyber risks, through a proprietary framework and dedicated portal.

In global businesses where IT is spread across the world, modern Penetration Testing finds too much data and does not convert it into meaningful, trackable information. DPT has created a new way of working, a better way of tackling Penetration Testing, which gives organisations actionable cyber security information. Using this information and CNS Group's modelling, organisations are able to find the patterns and work out what to fix, attribute issues, assign remediation activity, check that fixes work and track the improvements to demonstrate return.

Service Elements

The DPT External Penetration Test is built up of a number of individual services packaged to provide a proactive service.

DPT Portal

A unique dedicated client portal which takes pen test reporting from static to dynamic, enabling you to:

- Survey the risk spread and level across the whole of your organisation
- Allocate issues to individuals for fixes
- Track the progress of fixes and the impact on the organisations risk levels
- Accept issues
- Request issues are retested
- Request clarification or more detail on issues
- Weight issues by adjusting the level of importance for specific host
- Weight issues by adjusting the level of importance for specific types of issues

Manual External Penetration Test

A full Manual External Penetration Test against the contracted IP address ranges as defined. This will include a full TCP and common UDP port scan, full vulnerability scan and manual investigation of any open ports or services against the full IP Range identified (including unused IPs). The output of this will be a formal PDF report and the results will be uploaded to the client portal.

Port Scan Diff Identification

A Network Mapper (NMAP) Differential (Diff) Scan against the contracted IP range, comparing it with the baseline established on a regular basis. Alerting you by email if:

- Any critical issues found
- If we detect a change or
- If we find any issues on customer notified changes to be checked

Key Features & Benefits

On-going risk management addressing risk issues at their root

- Creates joint priorities between business and IT
- Carries out a full, manual Penetration Test to establish a base line
- Presents Penetration Test results via an online client portal, so that risk can be viewed across whole of an organisation
- Creates risk scores, giving issues a business context
- Tracks and allocates issue remediation, including drilling down into technical detail
- Includes ability to upgrade or downgrade risk as the security landscape changes
- Provides continual retesting and updates on applications, systems, and or network changes
- Relieves CISOs and risk owners of the annual test stress
- Provides actionable information quickly
- Facilitates the clear tracking and reporting of risk reduction, thus providing demonstrable value to auditors and executives

Why Choose CNS Group?

UK based cyber security experts

- Penetration Testing experts
- All service delivery staff are SC cleared
- Clear reporting
- Deep understanding of regulatory and compliance implications of incidents
- To improved business continuity
- 24 x 7 service capability

What Clients are Saying About DPT

"For us the value of Dynamic Penetration Testing is in the management of risk. We can combine business input with the technical experience of the pen testers, by attributing risk scores to any issues. This means we can weight and prioritise the outcomes, pulling things up the list if needs be. Secondly, the job of resolving these issues can be assigned and tracked automatically, with fixes being retested by CNS Group once they're complete. It takes the legwork out of manually tracking resolutions, making it easier to monitor progress"

Information Security Officer
Global Law Firm

Port Scan Diff Identification

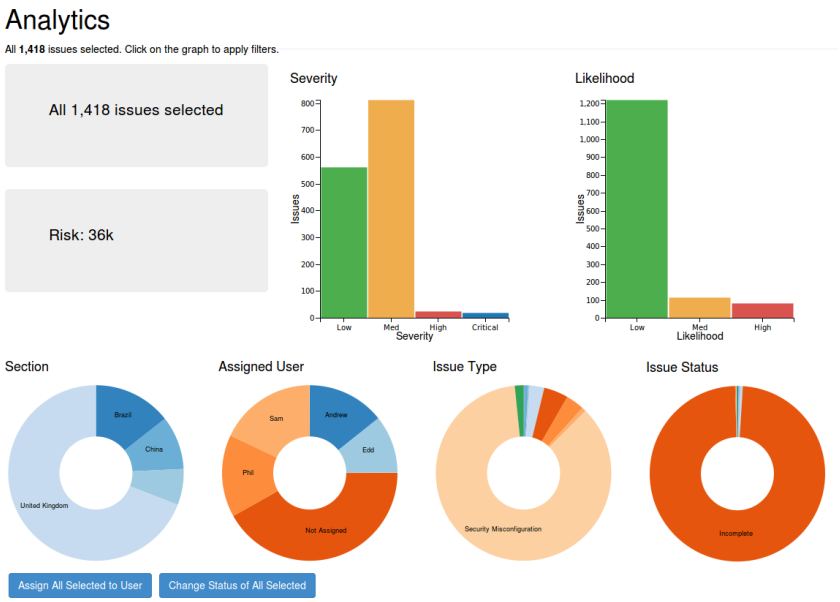
A Network Mapper (NMAP) Differential (Diff) Scan against the contracted IP range, comparing it with the baseline established on a regular basis. Alerting you by email if:

- Any critical issues found
- If we detect a change or
- If we find any issues our customer is notified changes to be checked

Manual Testing of Notified or Identified Changes

Regular manual testing of the below listed items with the results published in the DPT Portal:

- Any changes detected through the Port Scan Diff
- Any issues marked as fixed by the client in the portal
- Any changes notified by the client
- Any High or Critical Issues that already exist



View of DPT Portal Analytics Dashboard

Core Clients

Large corporations with global networks

CNS Group built the DPT service largely in response to client feedback and needs. DPT clients span the financial services, legal and exhibitions sectors. All of these initial clients are global organisations with IT remediation teams across the world.

Companies best positioned to benefit from DPT include:

- Financial services firms
- Legal firms
- Insurance agencies
- Exhibitions companies
- Logistics firms
- Travel sector companies

Our business is securing your data

As a government accredited company, we help UK organisations of all sizes build cyber security capabilities and maintain compliance through practical consulting and Managed Security Services. For more information on how our Managed Security Services can help protect your business, contact us now on:

info@cnsgroup.co.uk

020 7592 8800

@CNS_Security

www.cnsgroup.co.uk