



The iStorm PVM appliance is a fully configurable vulnerability scanning and management tool designed for network security professionals by network security professionals. Positioned inside the network perimeter, iStorm provides detailed vulnerability assessments of all or selected parts of the network topology, together with a professional evaluation of the potential seriousness of the threat, if left unremediated.

Part of the RandomStorm range of Proactive Vulnerability Management (PVM) applications and services, iStorm has been developed to enable valuable network management resources to be focused on critical vulnerabilities; fixing weaknesses that could lead to serious breaches of the corporate security posture and enabling work on lower level vulnerabilities to be scheduled as part of a routine maintenance programme.

Combined with RandomStorm's online perimeter scanning service, xStorm, and plug-ins to a range of proprietary IDS/IPS systems, iStorm's unique management dashboard provides an at-a-glance picture of the current and historic threat levels across the entire network. iStorm enables continuous protection from exploitations of the numerous vulnerabilities that exist in any complex network environment.

Why iStorm?

- ✓ Supports a proactive approach to vulnerability management
- ✓ Universal Threat Management interface combines data from multiple sources
- ✓ Ensures compliance with the latest industry security regulations
- ✓ Enables prioritisation of remediation activity
- ✓ Generates cost and time saving by focusing on the most serious threats
- ✓ Advanced management reports demonstrate RoI and support budget requests
- ✓ Designed by security professionals for security professionals

System Features

- ✓ Unique user dashboard provides an 'at-a-glance' overview of system status
- ✓ Intuitive management interface to quickly configure scans as required
- ✓ Complete flexibility in user defined scan intervals: Hourly; daily; weekly; or as required
- ✓ Detailed reporting options including PCI DSS and SANS Top 20 formats
- ✓ Vulnerability Alerts and professional remediation advice





IDS/IPS Integration

RandomStorm's vulnerability scanning platform includes the optional plug-in capability to enable integration of management information from SNORT and other leading IPS/IDS solutions. By combining accurate vulnerability data with information relating to actual current attack traffic, iStorm minimises the number of false positives and brings an added layer of intelligence to the analysis of the potential security threat level, across the entire network topology. Accessed via a common management dashboard, the system's information enables remediation resources to be focused on critical vulnerabilities rather than wasting time and money resolving low priority issues.

Advanced Reporting

iStorm delivers technical and summary data in a concise report format. Graphical reports can be generated in HTML or PDF format utilising the easy-to-use web interface. Not all vulnerabilities carry the same level of urgency or security threat; iStorm reports summarise the security posture of each network device, including information about the scan, specific host information, and a list of detected vulnerabilities. These reports present a description of each security risk detected, the severity level of the threat, the potential consequences of exposure, regulatory compliance information and links to validated patches and fixes. Armed with this information, security managers can prioritise where, when and how to best implement corrective action.



Management Dashboard

At login, iStorm users are presented with a unique GUI dashboard that provides an 'at-a-glance' overview of their organisation's current security threat status.



Presented in clear graphical format, the network administrator can see immediately if there are any critical security issues that require urgent attention and drill down to obtain more detailed information on the exact nature of the threat together with professional remediation advice.

PCI Compliance



Government and industry regulations are an increasing issue for network security managers, particularly for organisations that store large amounts of personal customer information. This particularly applies to companies that process credit card transactions as part of their business operations and are subject to the PCI Data Security Standard regulations.

iStorm's PCI DSS approved reports and remediation workflow features are designed to help ensure full compliance between quarterly PCI audit periods.

Contact Us

RandomStorm Ltd
The Round Foundry Media Centre
Foundry Lane
Leeds LS11 5QP

Tel: 0845 6430995

sales@randomstorm.com

www.randomstorm.com

