xstormlive

Online vulnerability scanning

Without regular vulnerability scanning you can never be sure your network is secure. Regular scanning is a critical security control and can provide early detection of vulnerabilities before they can be exploited. Hackers accessing your network through insecure ports or weaknesses can result in significant security breaches.

How can xstormlive help?

NCC Group's xstormlive service provides you with an external vulnerability scanning platform and the capability to perform ad hoc and scheduled scans of your Internet perimeter.

It provides users with a self-contained platform enabling them to perform network and web application vulnerability scanning themselves.

If vulnerabilities are discovered with xstormlive you are notified immediately via an alert email, enabling you to start the process of remediation as soon as possible.

xstormlive has the ability to perform:

- Authenticated & unauthenticated vulnerability scanning of public facing network infrastructure
- Unauthenticated web application scanning

Scanning can be executed instantly or scheduled to be run out of hours on a daily, weekly, monthly or quarterly basis. This means a scanning regime can be created in line with organisational or operational constraints.

xstormlive is powered by multiple commercial and open source vulnerability scanning engines. This approach means that xstormlive can harness the strengths of various scanners in order to identify the broadest range of vulnerabilities.

No new hardware or software required

xstormlive is accessed and controlled through an easy to use online platform. It is located outside of your network in an NCC Group data centre, providing users with vulnerability scanning as a service. NCC Group maintain the data centre along with the underlying hardware, software and scanners required to run your scanning activities.

Users simply schedule scans via their browser while xstormlive handles the scanning and produces an automated security assessment report after each scan. We will alert you if a high severity issue is detected and also inform you when scans start, stop and even if they fail.

The service is deployed as a secure, available and scalable web application.

How is xstormlive licensed?

xstormlive has a flexible licensing model which allows users to perform an unlimited number of scans against a defined set of assets. Unlimited scanning means that any remedial actions can be tested as often as needed without incurring additional costs.

Unlimited scanning of defined assets

- **IP Address -** Unlimited scanning on a defined number of IP addresses (one licence per IP address)
- **Web URLs -** Unlimited scanning on a defined number of web URLs (one licence per web URL)

Benefits

- **High fidelity scans:** The platform utilses multiple scanners to greatly reduce the likelihood of undetected weaknesses.
- **Simple user interface:** Not every organisation has an army of security experts who know how to use complicated security tools. The xstormlive portal features clear, well laid out controls that anyone can use. Every effort has been made to ensure the portal is as accessible as possible.
- **Track improvement:** Good security hygiene isn't just about checking for vulnerabilities, it's about fixing them too. xstormlive allows you to perform unlimited follow up scans to ensure your remedial actions are effective.

Why should you undertake vulnerability scanning?

Software patches

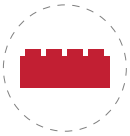
The software and operating systems used in your organisation may not be updated with the latest release or version, leaving them vulnerable to exploitation.

Old vulnerabilities

Known vulnerabilities are an easy target for cyber criminals, so it's important to ensure that all systems are checked regularly and patched to avoid exploitation.

New vulnerabilities

Previously unknown vulnerabilities are discovered every day, so systems and networks must be analysed frequently to ensure new risks are identified as quickly as possible before any damage is done.



Poor configuration

Best practices are often not followed when setting up new systems. This may be due a lack of time, awareness, knowledge or resources, but it can leave systems open to attack.

Unplanned change

The nature of business and IT is that it changes regularly and quickly. These changes can unintentionally introduce services or vulnerabilities which can be used by an attacker.

Human error

System operators may, often with good intentions, reconfigure settings. Without testing, changes can unknowingly introduce insecure services which can lead to a compromise.

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate & respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.

For more information from NCC Group, please contact:

+44 (0) 161 209 5200 response@nccgroup.trust www.nccgroup.trust

NCCGMSSXSLV11117