CIRCL
Computer Incident Response Center Luxembourg

Back-office environment, with a hundred machines & Web assets targeted for continuous internal and external scans.

The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg and aims to gather, review, report and respond to cyber threats in a systematic and prompt manner. CIRCL processes more than 2.6GB of compressed malware samples and honeypot network capture per day, with its MISP threat sharing platform servicing more than 400 organizations across the globe.

\\ Challenge

Maintenance-free & continuous internal & external surveillance The CIRCL needed to continuously search for potential vulnerabilities on their internal network and public-facing Websites containing a variety of devices and Web platforms. Their daily activities acting as a CERT providing rapid response to new cyber-threats and maintaining the MISP threat sharing platform dramatically reduced the available time to operate traditional VA solutions, often requiring constant maintenance and supervision.

" Warden is very easy to use and can easily be left to work on its own, only to be informed when new vulnerabilities are discovered without intruding our workflow. In a context of a team with limited resources, it is very useful to get a quick view of what needs to be addressed and updated"

– Raphaël Vinot
Incident Handling and CERT Operations at CIRCL

\\ Solution

The CIRCL effortlessly set up Warden and its integrated Edge Services, allowing them to immediately discover and scan both their internal and external assets in a continuous way.

The use of Warden not only allowed CIRCL to harden some devices configuration but it was also pivotal in identifying potential issues with specific networking equipment from a large manufacturer; the CIRCL was able to work with the manufacturer to correct detected vulnerabilities and release a new firmware version, enhancing the security for everyone.

\\ Benefits

The use of Warden at CIRCL helped them rapidly gain a continuous visibility on their external and internal back-office assets without spending time configuring scan schedules or templates and maintaining a resource-intensive VA solution. It provides a crucial helping hand to this CERT team to efficiently detect and address new vulnerabilities on all their assets, while they continue to help their customers in addressing new cyber threats.

Warden's SmartVA engine brings the first completely driverless experience to the traditional VA process, allowing teams to continuously scan all their machines and Web applications in a fully integrated manner, without the need to configure schedules, templates and filter through heaps of false-positives.

As corporate IT networks continue to expand in a context of security expertise scarcity, managers and experts are faced with an ever-increasing challenge to protect companies from cyber-attacks and data breaches. The growing complexity of modern enterprise networks puts pressure on security teams to scale their continuous vulnerability detection and remediation activities.

Recent advances in the field of Artificial Intelligence are at the heart of Warden, allowing companies to efficiently scale their security coverage via the first Smart VA engine in the industry. It provides well needed assistance to security teams, reduces their menial activities and helps them focus on mission critical tasks.

Try the First Smart VA Solution for the Enterprise

www.delve-labs.com/trial

DELVE LABS

602-3875 Saint-Urbain, Montréal, (QC) H2W 1V1

1 844 353-3583 • info@delvelabs.ca