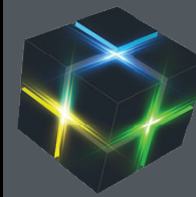


HAKWARE



XGRC[®]
SOFTWARE

IDENTIFY VULNERABILITIES BEFORE CYBER CRIMINALS DO

Hakware Archangel

Hakware Archangel is an Artificial Intelligence based vulnerability scanner and pentesting tool.

Archangel scanner enables organizations to monitor their networks, systems, and applications for security vulnerabilities with advanced Artificial intelligence continuously testing your environment.

Why use Archangel?

Our vulnerability scanning mitigates the risks of a data breach, which will come with a range of costs, including remediation, the loss of customers as a result of reputational damage and fines

GDPR AND POPI

Vulnerability scanning is not explicitly required by the GDPR (General Data Protection Regulation) or POPI (Protection Of Personal Information Act)

Although the Regulation does require organisations that process personal data to ensure that they have implemented appropriate technical and organisational security measures – which includes identifying vulnerabilities

ISO 27001

- Timely identification of vulnerabilities.
- Assessment of your organization's exposure to a vulnerability.
- Proper measures considering the associated risks.

HAKWARE

ARCHANGEL

WWW.HAKWARE.COM

WHAT IS HAKWARE ARCHANGEL?

Archangel scanner enables organizations to monitor their networks, systems, and applications for security vulnerabilities with advanced Artificial Intelligence continuously testing your environment.

As part of a wider security strategy, organisations should be running continuous vulnerability scans to pick up on new and emerging cyber threats.

THE COST OF CYBERCRIME

The global cost of cybercrime was estimated at some 8.4 trillion U.S. dollars in 2022. The cost of incidents caused by illegal activities on the internet are set to surpass the 11 trillion U.S. dollar mark in 2023

By 2026, annual cybercrime costs worldwide could exceed 20 trillion, an increase of almost 150 percent compared to 2022.



Cybercrime is up 600%
Due to COVID-19
Pandemic



Security Driven AI had best cost
mitigation, saving up to \$3.81
million (80% cost difference).



It is estimated that, worldwide, cyber
crimes will cost \$10.5 trillion
annually by 2025.



Global volume of cyberattacks
reached an all-time high in Q4
with an average of 1168 weekly
attacks per organization

ARTIFICIAL INTELLIGENCE

We used Artificial Intelligence to build an Information security monitoring solution that learns and hacks like a real hacker would.



RISK MANAGEMENT

IDENTIFY VULNERABILITIES BEFORE CYBER CRIMINALS DO. STAY ON TOP OF VULNERABILITIES AND AVOID HUMAN ERROR.

Mitigates the risks of a data breach,

which will come with a range of costs, including remediation, the loss of customers as a result of reputational damage and fines.



WHAT WE SCAN

-  NMAP Port scanning
-  Deep web password monitoring
-  HTTP Headers
-  SQL Injection
-  XSS - Cross site scripting
-  Whois
-  Directory Discovery
-  DNS scans
-  SSL Validation
-  Domain Impersonation
-  Brand Spoofing
-  Banner Grabbing
-  Footprinting
-  Local/Remote File Inclusion
-  Remote command execution
-  Log4j
-  Brute Force Attacks
-  FTP Sniffing



HACKWARE