**Empowered by:**

SecurityScorecard

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong

(852) 2788 5857

cybersec@hkpc.org

www.hkpc.org

# SecurityScorecard LITE

Know Your Company, **INSIDE OUT!**

*Evaluate an organisation's security profiles non-intrusively by collecting its digital footprints exposed*

## SECURITYSCORECARD LITE

**SecurityScorecard LITE** is empowered by SecurityScorecard. It offers an '**outside-in**' report card of the security risk posture of an organisation and continuously gathers security intelligence data and instantly grades companies from **A to F** across ten crucial security categories.

**SecurityScorecard LITE** evaluates an organisation's cyber security risk using **data-driven**, **objective**, and **continuously evolving** metrics that provide **visibility** into any organisation's information security control weaknesses as well as potential vulnerabilities throughout the supply chain ecosystem.

## SERVICE HIGHLIGHTS

Enables organisations to **rate**, **understand**, and **monitor** the security risk of their organisations

**Non-intrusively** and from an outside-in perspective (same as a third-party or attacker)

**Easy to understand** A to F rating scale used to provide visibility of organisation's digital footprints in the cyber world

Categorised into **10 Risk Factors** in order to understand the weakest link in their networks

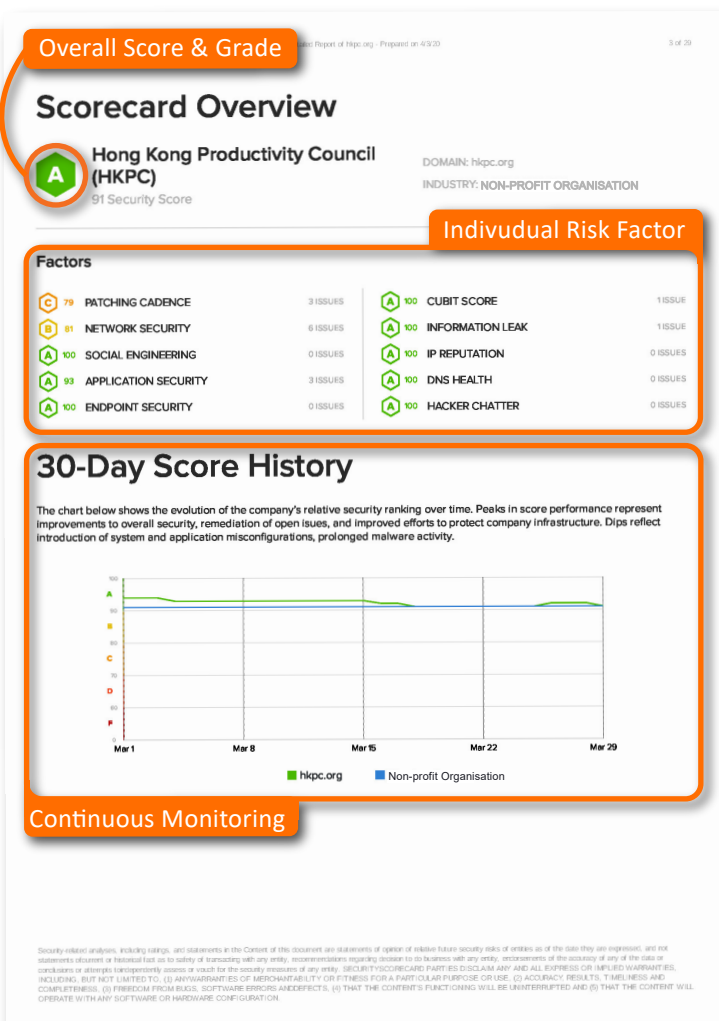**A** **B** **C** **D** **F**

## SERVICES INCLUDE

**SecurityScorecard LITE** includes the following services:

• **ONE (1) Full Report** per month

• **ONE (1) Hour Consultancy Service** per month to explain the findings and alerts from the report

• **Continuous** monitoring and alert

# SecurityScorecard LITE

## THE RISK FACTORS

**Network Security**
Detecting insecure network settings

**DNS Health**
Detecting DNS insecure configurations and vulnerabilities

**Patching Cadence**
Out of date company assets which may contain vulnerabilities or risks

**Endpoint Security**
Measuring security level of employee workstations

**IP Reputation**
Detecting suspicious activity, such as malware or spam, within your company network

**Application Security**
Detecting common website application vulnerabilities

**Hacker Chatter**
Monitoring hacker sites for chatter about your company

**Cubit Score**
Proprietary algorithms checking for implementation of common security best practices

**Information Leak**
Potentially confidential company information which may have been inadvertently leaked

**Social Engineering**
Measuring company awareness to a social engineering or phishing attacks

## REPORT INSIGHTS

*Overall Score & Grade*

### Scorecard Overview

**A**

Hong Kong Productivity Council (HKPC)
91 Security Score

DOMAIN: hkpc.org
INDUSTRY: NON-PROFIT ORGANISATION

*Indivudual Risk Factor*

**Factors**

| | | | | | | |
|---|---|---|---|---|---|---|
| C | 79 | PATCHING CADENCE | 3 ISSUES | A 100 | CUBIT SCORE | 1 ISSUE |
| B | 81 | NETWORK SECURITY | 6 ISSUES | A 100 | INFORMATION LEAK | 1 ISSUE |
| A | 100 | SOCIAL ENGINEERING | 0 ISSUES | A 100 | IP REPUTATION | 0 ISSUES |
| A | 93 | APPLICATION SECURITY | 3 ISSUES | A 100 | DNS HEALTH | 0 ISSUES |
| A | 100 | ENDPOINT SECURITY | 0 ISSUES | A 100 | HACKER CHATTER | 0 ISSUES |

### 30-Day Score History

The chart below shows the evolution of the company's relative security ranking over time. Peaks in score performance represent improvements to overall security, remediation of open issues, and improved efforts to protect company infrastructure. Dips reflect introduction of system and application misconfigurations, prolonged malware activity.

Mar 1 | Mar 8 | Mar 15 | Mar 22 | Mar 29

■ hkpc.org  ■ Non-profit Organisation

*Continuous Monitoring*

---

**C 79 PATCHING CADENCE**

The Patching Cadence module analyzes how quickly a company reacts to vulnerabilities to measure patching practices. We look at the time to remediate and apply patches compared to peers.

*Severity Level*

| HIGH SEVERITY | MEDIUM SEVERITY | | LOW SEVERITY | POSITIVE |
|---|---|---|---|---|
| There are no High Severity Issues for Patching Cadence | End-of-Service Product | 2 | There are no Low Severity Issues for Patching Cadence | There are no Positive Signals for Patching Cadence |
| | Medium-Severity Vulnerability in Last Observation | 6 | | |
| | Medium Severity CVEs Patching Cadence | 3 | | |

**INFORMATIONAL**
There are no Informational Signals for Patching Cadence

**End-of-Service Product**          **-1.9** SCORE IMPACT

We observed an end-of-service product, one that is no longer supported by the manufacturer, publicly exposed.

**Description**
A product that has been declared as end-of-service (EOS) by the manufacturer has been detected. An EOS product is no longer eligible for any support, security patches, or replacement parts. Products at this stage in their life cycle are more likely to have vulnerabilities that need to be patched, but without service support those vulnerabilities will persist until the product is replaced. Using EOS products also violates several compliance frameworks, including PCI DSS and HIPAA.

**Recommendation**
Replace or upgrade the affected product. Review the vendor's statement of EOS guidelines for replacement products or contact the vendor. In some cases, it may be possible to negotiate a custom support plan for the EOS product.

*Technical Advice Given*

*Detailed Issues Found*

| PRODUCT VERSION | IP ADDRESS | PORT | END OF LIFE DATE | PRODUCT MANUFACTURER | PRODUCT NAME | MANUFACTURER STATEMENT | LAST OBSERVED |
|---|---|---|---|---|---|---|---|
| 6.0 | XXX.XXX.XXX.XXX | 80 | 7/14/2015, 12:00:00 AM | Microsoft | Internet Information Services 6.0 | https://support.microsoft.com/en-us/lifecycle?p1=2097 | 3/10/2020, 3:04:52 AM |
| | XXX.XXX.XXX.XXX | 443 | 3/31/2016, 12:00:00 AM | Juniper | Netscreen SSL Hardware SA2000 | http://www.juniper.net/support/eol/ssl_hw.html | 2/16/2020, 11:11:28 AM |

**Medium-Severity Vulnerability in Last Observation**          **-1.6** SCORE IMPACT

We observed a medium-severity vulnerability during our last scan, which may still be publicly exposed.

**Description**
Common vulnerabilities and exposures (CVE) is a list of publicly-known vulnerabilities in software and hardware. Each CVE contains an ID, a description of the vulnerability, and the product names and versions which are affected by the vulnerability. Software and hardware frequently self-report

**Recommendation**
Update or patch affected software and hardware. Enable automatic updates if available from your software vendor and permitted in your environment. Monitor CVE lists and vulnerability repositories for exploit code that may affect your infrastructure. Subscribe to the Bugtraq mailing list to be alerted to new exploits

---

**Interested? Scan the QR code now and we will get back to you shortly!**

For enquiry, please contact **Mr Summ Chan** at **+852 2788 5857** or email to **cybersec@hkpc.org**