Measuring Your Cyber Security Posture

The Huntsman Security Scorecard continuously measures your cyber security posture across a range of key security performance indicators. The eight controls identified are as a result of analysis of organisations that have succumbed to cyber attacks and malware.

The Security Scorecard focuses on the eight controls that have been found to have the highest impact on preventing a cyber attack and improving your ability to recover from one.

Measuring control effectiveness is a key element of any risk management process.

“ You cannot manage what you cannot measure ”

The 8 essential controls

<table>
<thead>
<tr>
<th>Top 4</th>
<th>Application white listing</th>
<th>Patching applications</th>
<th>Patch operating systems</th>
<th>Restrict administrative privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>These 4 controls alone have been assessed to reduce the likelihood of suffering a cyber attack by up to 85%</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+</td>
<td>Daily back up of data</td>
<td>Multifactor authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>++</td>
<td>Disable untrusted Microsoft Office macros</td>
<td>User application hardening</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Security Posture at a glance

To help mitigate cyber security risks the Security Scorecard is a powerful toolset that provides:

- Executive Summary Report and detailed control reports
- Clear Visibility of current security posture
- Guidance on where vulnerabilities exist

The Security Scorecard gives you a measure of the efficiency and effectiveness of your security controls and reveals the direction your cyber security posture is moving.

For more information: https://www.huntsmansecurity.com/products/security-scorecard/
The 8 essential controls

Each of the controls is reported in detail on a weekly basis and is automatically compared to the previous week so you can see if your security posture is going in the right direction. The controls fit into two categories:

Controls to mitigate against cyber threats:
- Application Whitelisting – running in enforcement mode.
- Patching Applications – for extreme risk security vulnerabilities in Adobe Flash, web browsers etc.
- Disable untrusted Microsoft Office Macros
- User Application Hardening

Controls to limit the extent of incidents and recover data:
- Patch operating systems – patch for extreme risk security vulnerabilities with 48 hours.
- Restrict administrative privileges – duties-based restrictions on privileged accounts.
- Daily back-up of data
- Multi-factor authentication – for users performing privileged actions, accessing important data, remote access etc.

Implementation of these eight controls improves cyber resilience, minimises the likelihood of an attack being successful and increases your ability to recover from one in real terms.

Status Dashboard

Monitoring of your environment including on-premise, cloud and hybrid.
Pre-defined alerts, dashboards, queries and reports.