Cybersecurity Assessment

Helping businesses protect themselves against rapidly evolving cyberthreats.

More threats, more Insight

Digital technologies are transforming businesses. Most companies are moving towards digital transformation which presents a range of opportunities, but also brings challenges. As more applications, data and processes move into the digital realm, our reliance on software increases, which makes topics such as securing networks, hardening systems and protecting data from cyberthreats become more important than ever.

The current cybersecurity landscape is complex. Attackers develop new and ingenious methods of compromising systems on a daily basis. With the use of intrusion tools, ransomware attackers are looking for vulnerabilities and/or monetizing their activities. Therefore, companies are in urgent need for ways to test their security status and infrastructure quickly and simply.

At Insight we work together with companies to develop solutions that encompass the latest skills, tools and methodologies to mitigate the risk of cyberthreats. Through our Cybersecurity Assessment we are able to help your organization to gain more insights in vulnerabilities based on information provided from your organizational infrastructure and Office 365 through our scanning tool. In addition we will gather the soft data and information through by means of a questionnaire.

Urgent and high priority actions are identified in the assessment.

Insight's Cybersecurity Assessment

The objective of a Cybersecurity Assessment is to provide an independent and in-depth review of your ability to protect information assets against relevant threats. During the assessment we will define the current situation of your deployed software to identify the maturity of current information security capabilities and vulnerable areas.

This gives us the information to provide recommendations and guidance on cybersecurity programs and policies, which will help your company to enable effective IT software asset management.

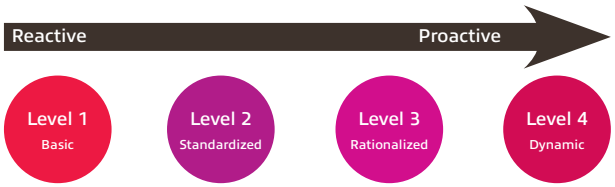
How does it work?

Intake & Installation	Scanning
• Check endpoint and network access • Installation tool on a (Virtual) Machine • Configuration of the tool	• Scan endpoints • Scan Active Directory and Azure Active Directory • Scan Office 365, SharePoint sites and Intune
Reporting & Recommendation	**Presenting Results**
• Answer questionnaire based on CIS-model • Analysis on the collected data • Creating report	• Presentation and discussion of findings • Conclusion and recommendation

What we deliver

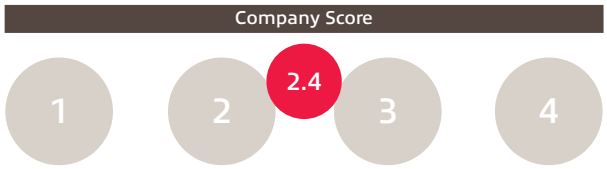
The outcome of the Assessment will provide you with a comprehensive report containing the following key topics:

1. Security maturity level.



Based on CIS Controls™ (v7) and ISO/IEC 27001 additions. The assessment of your cybersecurity program and practices will show a global maturity rating.

2. Score.



The average score is also calculated and can be used to track progress in future security scans.

3. Action plan to improve Cybersecurity.

Urgent and high priority actions are identified in the Assessment. Below you will find an example of an action plan:

Action	Priority	Action	Associated Software Products
All devices and servers, including Domain Controllers, firewalls, network-based IPS, and inbound and outbound proxies, have been implemented and configured to verbosely log all traffic (both allowed and blocked) and failed login attempts. Logs are collected centrally, protected against tampering, and used for continuously to detect and report (CIS 6)	**Urgent**	Setup a logging platform and point the logging configuration of the boundary devices to the central logging platform.	Security information and event management solution, Advanced Threat Analytics
Assessments are performed on data to identify sensitive information that requires the application of encryption and integrity controls. Labeling and classification is performed on all sensitive documents (CIS 13)	**Urgent**	Identify sensitive information on the organization's main data sources. Apply labeling and classification.	Azure Information Protection
Software whitelisting tools are implemented that only allow authorized software programs to be executed on all of the organization's systems (CIS 3)	**High**	Configure whitelisting to restrict the usage of unwanted and malicious software	AppLocker
Ensure that every administrator has a dedicated personal admin account, separated from their normal user account. The organization implemented multi-factor authentication (MFA) for all administrative access (CIS 4)	**High**	Setup personal admin accounts and enable multi-factor authentication for all external administrative access	Multi-Factor Authentication (Azure Active Directory)

Your path to better security

Collaborate with us to build a comprehensive security road map you can rely on. Focusing on people, process and technology, we are certified professionals with security expertise committed to propelling your organization forward in the new digital era.

Use the Insight Cybersecurity Assessment and discover where you can improve your security.
Please contact your Insight Account Manager.

+31 (0)20 355 1662 | solutions.nl@insight.com | nl.insight.com
Insight Enterprises Netherlands B.V. Fauststraat 3, 7323 BA, Apeldoorn Nederland