Scorecard for
MITE3 Cybersecurity

Generated **September 21, 2022**
by Joram Teusink (joram@mite3.nl), MITE3 Cybersecurity
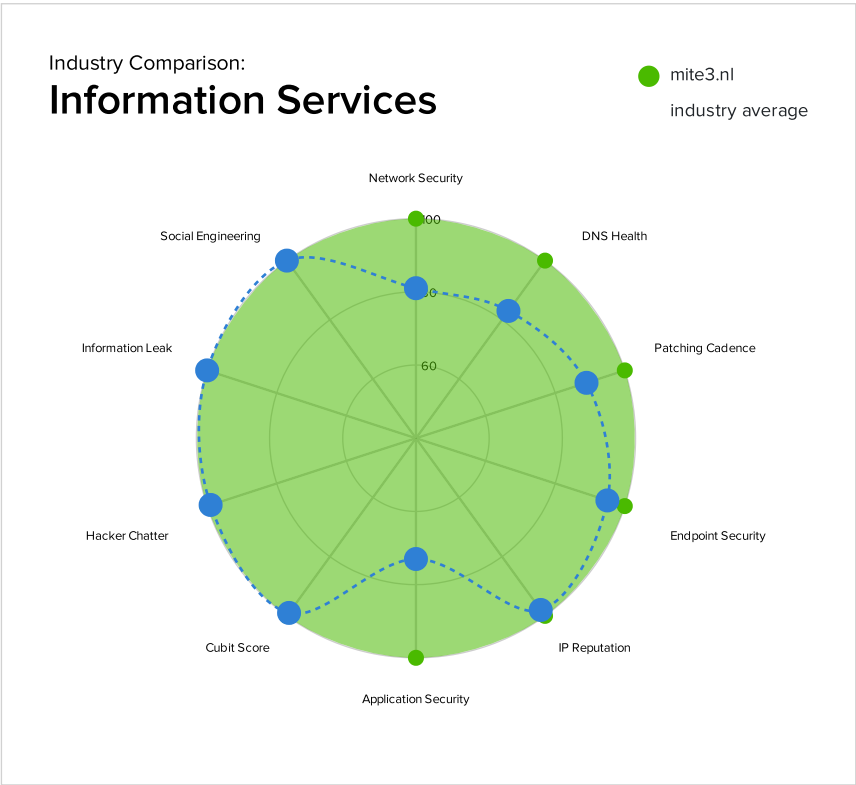
MITE3 CYBERSECURITY

powered by SecurityScorecard

A 100

Threat Indicators

A 100   **NETWORK SECURITY**
Detecting insecure network settings

A 100   **DNS HEALTH**
Detecting DNS insecure configurations and vulnerabilities

A 100   **PATCHING CADENCE**
Out of date company assets which may contain vulnerabilities or risks

A 100   **ENDPOINT SECURITY**
Detecting unprotected endpoints or entry points of user tools, such as desktops, laptops, mobile devices, and virtual desktops

A 100   **IP REPUTATION**
Detecting suspicious activity, such as malware or spam, within your company network

A 100   **APPLICATION SECURITY**
Detecting common website application vulnerabilities

A 100   **CUBIT SCORE**
Proprietary algorithms checking for implementation of common security best practices

A 100   **HACKER CHATTER**
Monitoring hacker sites for chatter about your company

A 100   **INFORMATION LEAK**
Potentially confidential company information which may have been inadvertently leaked

A 100   **SOCIAL ENGINEERING**
Measuring company awareness to a social engineering or phishing attack

Industry Comparison:
Information Services

- mite3.nl
- industry average

Network Security · DNS Health · Patching Cadence · Endpoint Security · IP Reputation · Application Security · Cubit Score · Hacker Chatter · Information Leak · Social Engineering

COMMENT BY MITE3 CYBERSECURITY

Our focus in regard to our Security Rating to have a rating as high as possible. Although we continuously aim for a rating of 100 (A), the practice is that it is slightly lower. Due to sometimes technical limitations or a different view on a security topic we diverge from some best practices. If there are any questions or remarks whatsoever, do not hesitate to contact us.

VULNERABILITIES	MEASURE
Open Ports	0
Site Vulnerabilities	14
Malware Discovered	0
Leaked Information	0