Scorecard for
Explaineverything

SecurityScorecard

Generated **August 17, 2020**
by Anna Borowska (anna.borowska@explaineverything.com), Explaineverything

A 97

Threat Indicators

A 98 **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Out of date company assets which may contain vulnerabilities or risks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**
Measuring security level of employee workstations

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

B 83 **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:
Technology

● explaineverything.com
● industry average
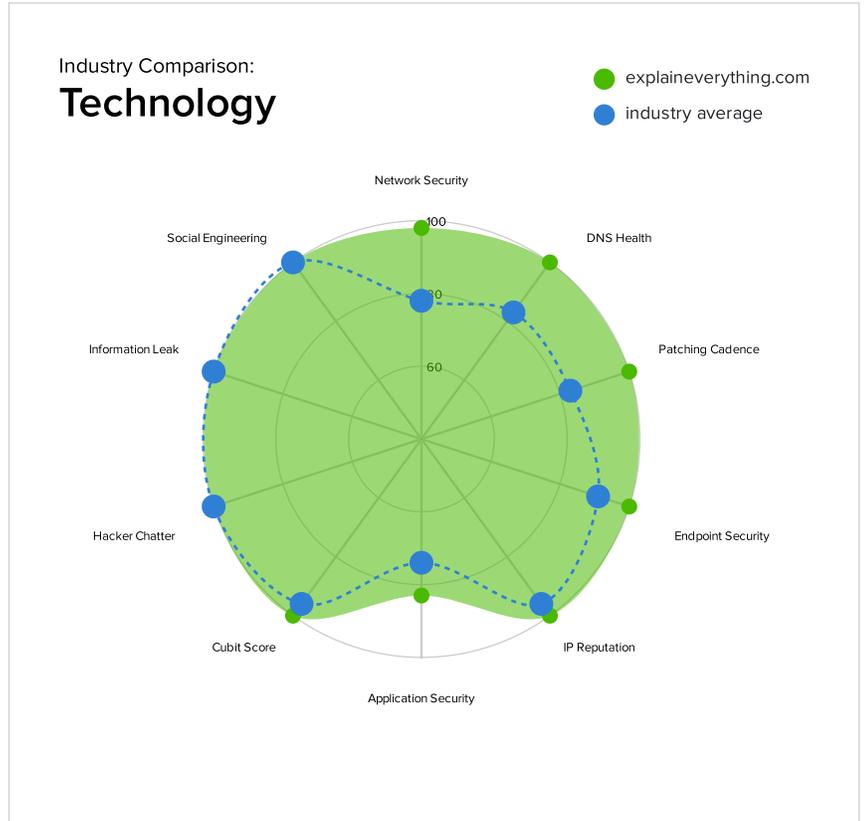
VULNERABILITIES	MEASURE
Open Ports	0
Site Vulnerabilities	15
Malware Discovered	0
Leaked Information	0