F-Secure

CYBER SECURITY STRESS TEST

SUMMARY REPORT

CYBER SECURITY STRESS TEST

FINAL SCORE

PREDICT:
High

PREVENT:
High

RESPOND:
High

DETECT:
High

BRILLIANT!

You got a **100/100**. That's as good as it gets. So take a second to give yourself a high five...and then get back to work. Because, as you already know, cyber security is a process. And if you aren't constantly improving your protocols and knowledge, you're regressing. So if you're looking for ways to protect your infrastructure against the latest threats, we should talk.

Your demographics' comparison is based on the following values:

Company size:
1-20
Industry:
Aviation
Your role in the organization:
CEO/COO/CFO

Your demographics' final score based on their answers is:
Medium-low

F-Secure

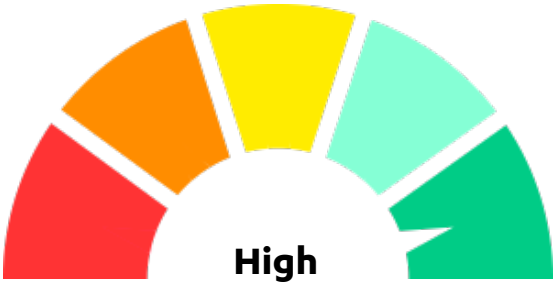
CYBER SECURITY STRESS TEST

PREDICT: Threat assessment

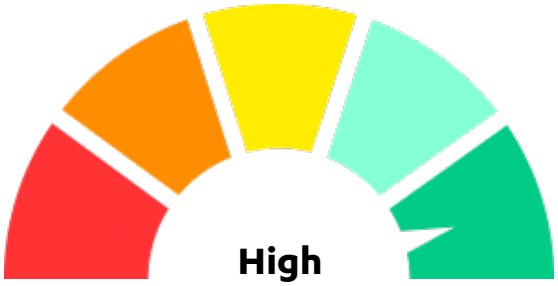
How good are your threat assessment practices?

YOUR ANSWERS

Estimated:

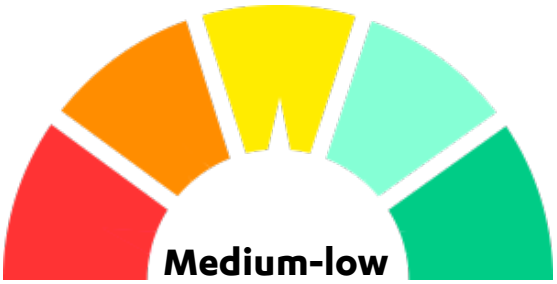


Actual score:

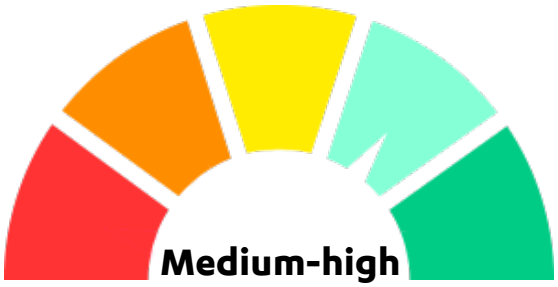


YOUR DEMOGRAPHICS' ANSWERS

Estimated:



Actual score:



Tip: Criminals and sophisticated attackers use known and zero-day exploits to breach corporate defenses and spread malware. So threat assessment and vulnerability management go hand-in-hand. By performing threat assessments and following best practices, you'll reduce your organization's attack surface. But it takes vulnerability management to make sure your nodes are configured and hardened correctly. Remember: vulnerability management is about a lot more than patches.

F-Secure

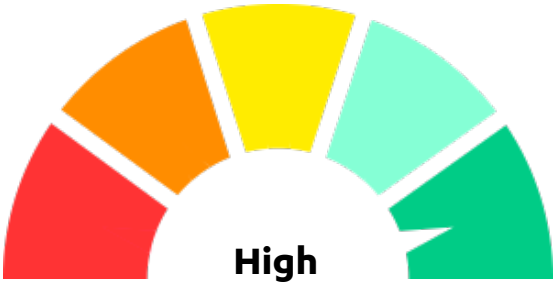
CYBER SECURITY STRESS TEST

PREDICT: InfoSec practices

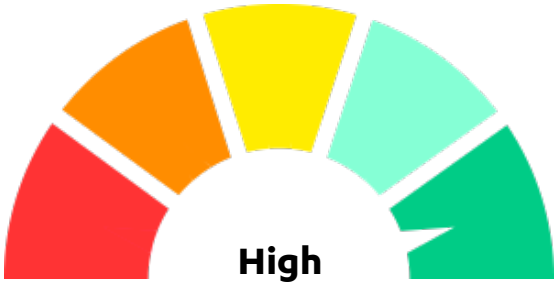
How good do you think your organization's InfoSec practices are?

YOUR ANSWERS

Estimated:

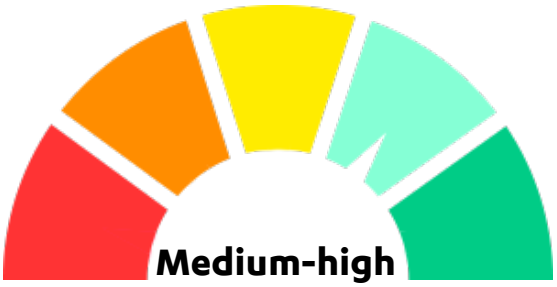


Actual score:

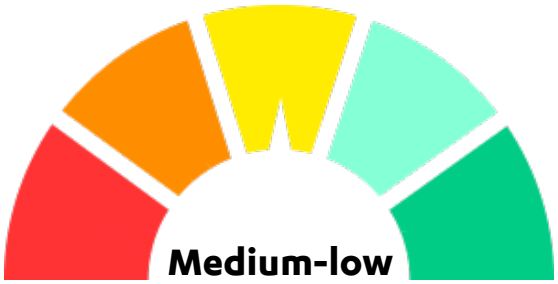


YOUR DEMOGRAPHICS' ANSWERS

Estimated:



Actual score:



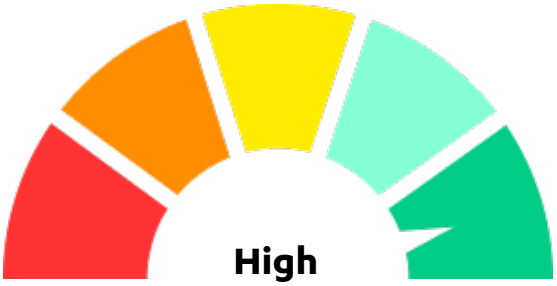
Tip: The best information security personnel are constantly following the news, social media, forums and other tactical threat intelligence feeds to improve their organization's security practices and infrastructure. The threat landscape is fluid and threat actors become more and more sophisticated every day. Keeping up is keeps you secure.

PREDICT: Compliance and Regulations

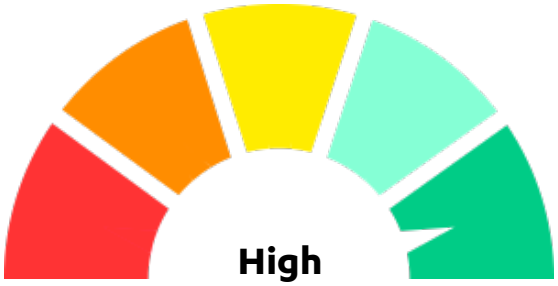
How well is your organization addressing industry compliance and regulations?

YOUR ANSWERS

Estimated:

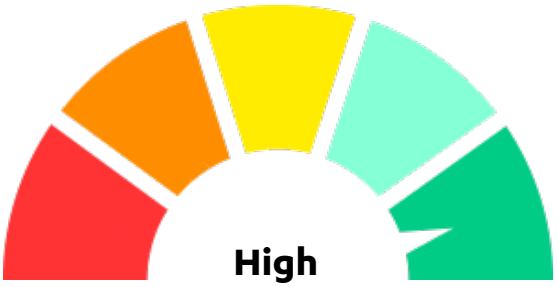


Actual score:

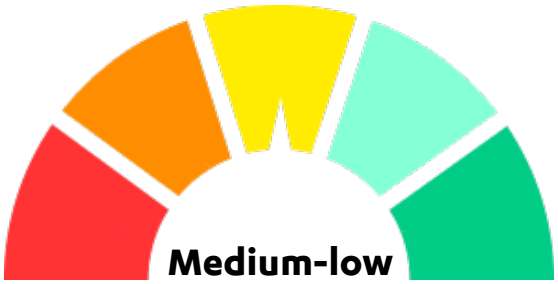


YOUR DEMOGRAPHICS' ANSWERS

Estimated:



Actual score:



Tip: Compliance guidelines like PCI-DSS provide a useful framework for building security practices in your organization. But following these guidelines won't guarantee your organization is immune to breaches, even though they certainly help. The good news is that in the event of a breach, being fully compliant means you'll have the practices and infrastructure in place to respond quickly and efficiently.

F-Secure

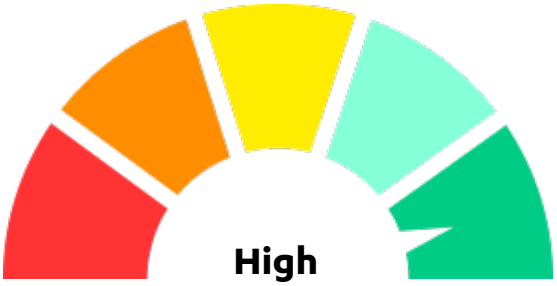
CYBER SECURITY STRESS TEST

PREVENT: Security Awareness

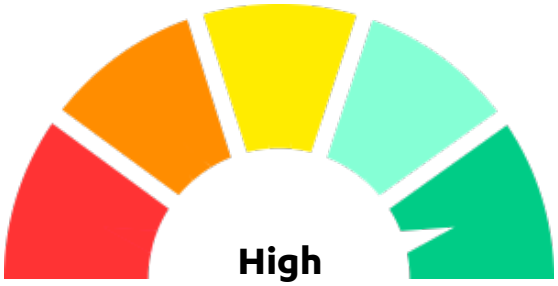
How security-aware are the people in your company?

YOUR ANSWERS

Estimated:

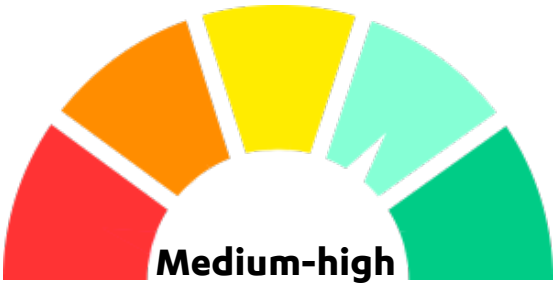


Actual score:

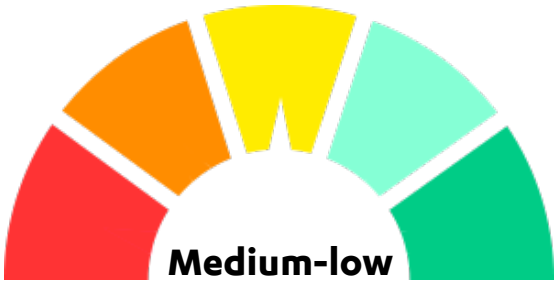


YOUR DEMOGRAPHICS' ANSWERS

Estimated:



Actual score:



Tip: Educating your staff about common security threats is an important part of cyber security. We recommend sending out frequent bulletins about good security practices that warn everyone about phishing campaigns and email scams. The key to getting this right is sharing clear instructions on what to do if someone thinks their machine has been compromised.

F-Secure

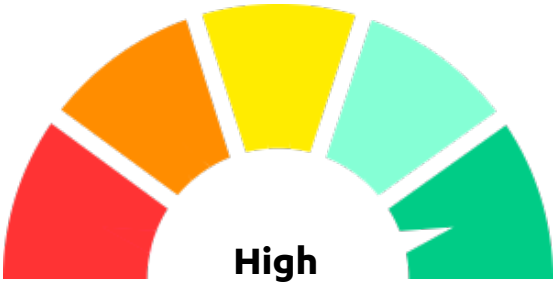
CYBER SECURITY STRESS TEST

PREVENT: Threat prevention

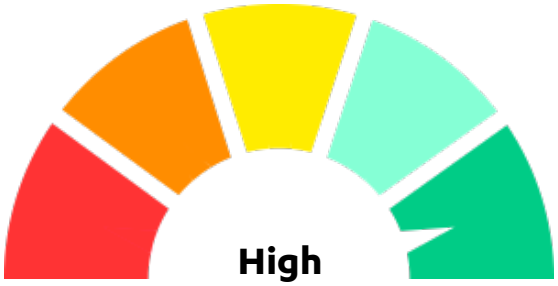
How well are your organization's endpoint devices (computers, tablets and phones) protected against common cyber attack vectors?

YOUR ANSWERS

Estimated:



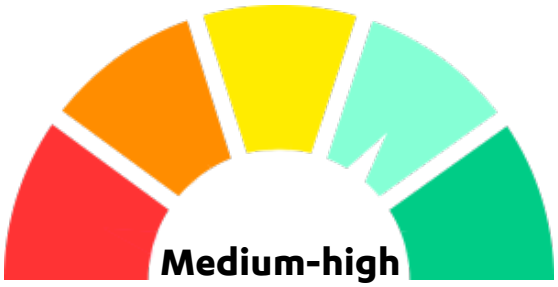
Actual score:



YOUR DEMOGRAPHICS' ANSWERS

Estimated:

Actual score:



Tip: By installing solid threat prevention solutions in your organization, you'll limit your employees' exposure to harmful content. It's impossible to completely eliminate all threats to your infrastructure. But running software that can detect and block common attacks will reduce your network's viable attack surface. In addition to deploying anti-malware software, content filtering gateways and firewall solutions, it's worth configuring all your machines to protect against common attack vectors.

F-Secure

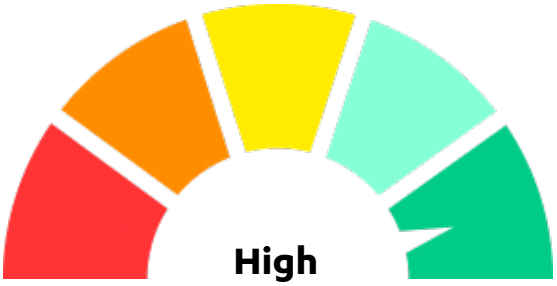
CYBER SECURITY STRESS TEST

DETECT: Intrusion detection

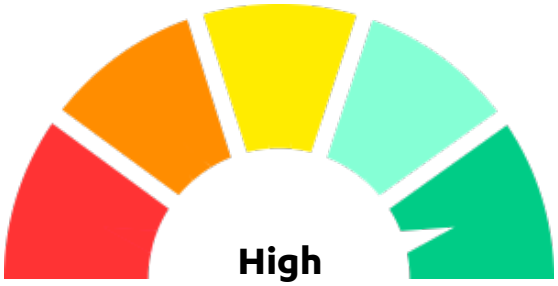
How easy would it be for you to detect the presence of an intruder in your internal network?

YOUR ANSWERS

Estimated:

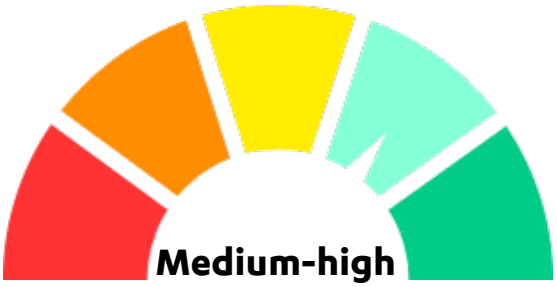


Actual score:

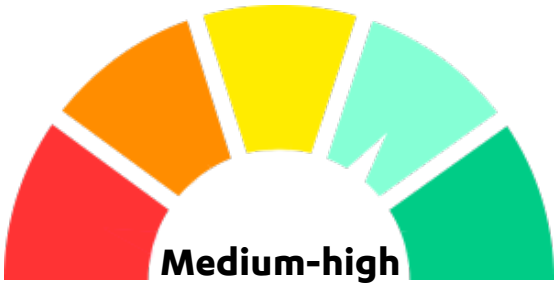


YOUR DEMOGRAPHICS' ANSWERS

Estimated:



Actual score:



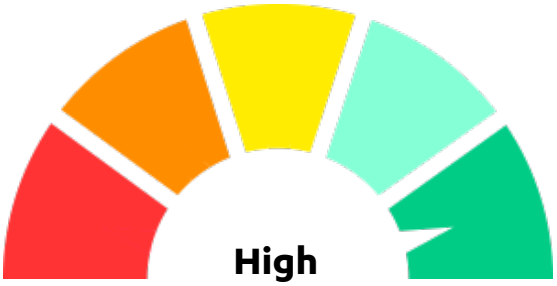
Tip: There are only two types of companies - those that have been hacked and know it - and those that have been hacked and don't know it. Advanced threats are increasingly common. They're designed to circumvent traditional measures. And they hit companies, large and small, every day. The only way to react is to catch them while they're happening.

DETECT: Insider threats

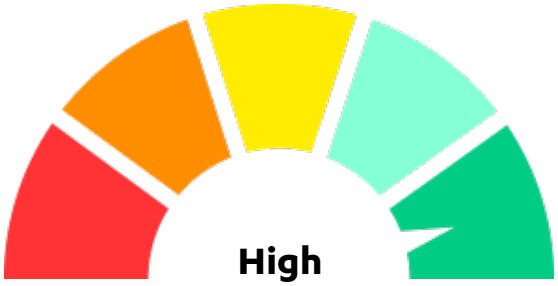
How easily could your organization detect an insider threat?

YOUR ANSWERS

Estimated:

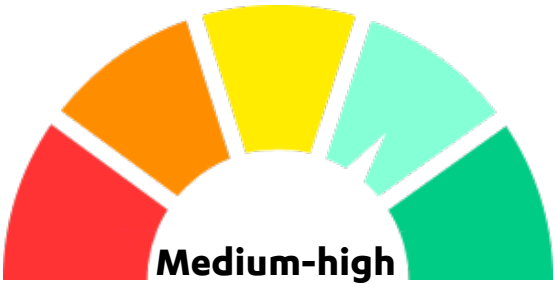


Actual score:

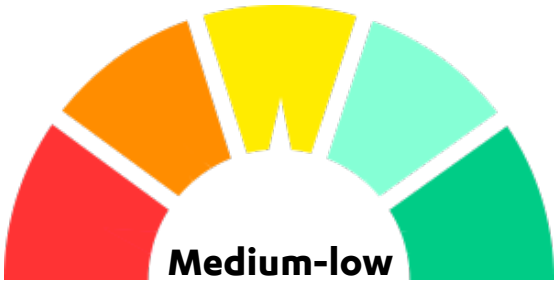


YOUR DEMOGRAPHICS' ANSWERS

Estimated:



Actual score:



Tip: We recently ran a poll asking people if they would sell their company password for the right price. 15% of respondents answered that they would. Insider threats can come in many shapes and forms - disgruntled employees, individuals paid or coerced into performing industrial espionage and external contractors. In too many companies, it's far too easy for strangers to use simple â social engineering' to enter and walk around the premises.

F-Secure

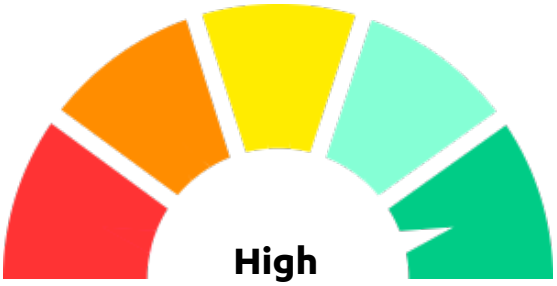
CYBER SECURITY STRESS TEST

RESPOND: Crisis management

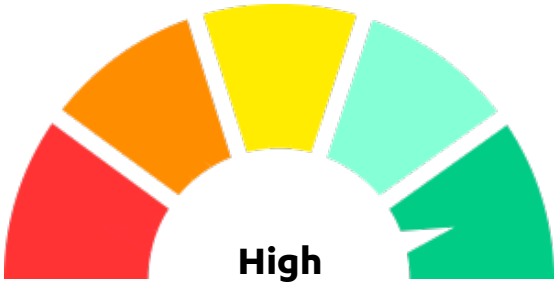
How well does your organization's crisis management plan cover cyber security incidents?

YOUR ANSWERS

Estimated:

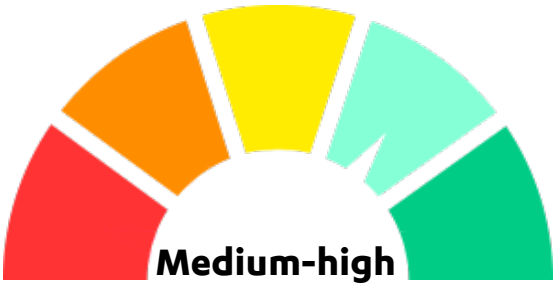


Actual score:

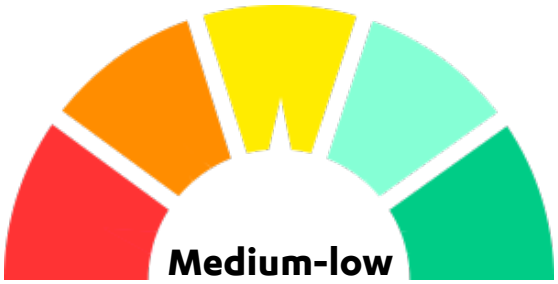


YOUR DEMOGRAPHICS' ANSWERS

Estimated:



Actual score:



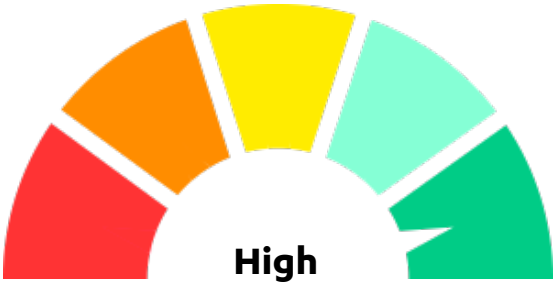
Tip: When it comes to cyber security, most companies just don't know what to do when something goes wrong. By defining a clear plan for crisis management you ensure everyone - from the top down - knows what to do to ensure safety and get back to work as soon as possible. Once you have a clear plan in place, rehearse it so you can learn from your mistakes.

RESPOND: Forensic evidence

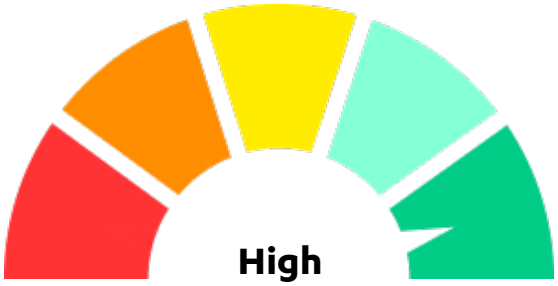
In the event of a breach, how good would your forensic evidence be?

YOUR ANSWERS

Estimated:

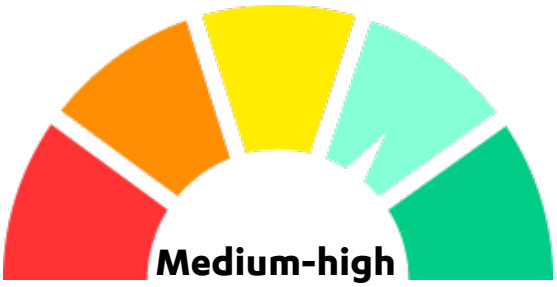


Actual score:

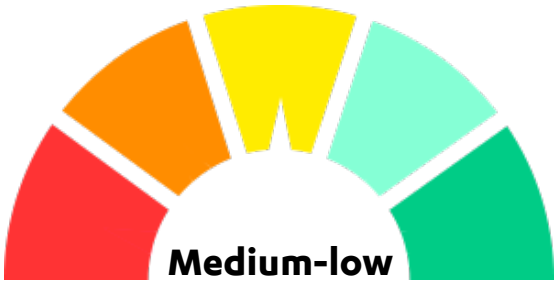


YOUR DEMOGRAPHICS' ANSWERS

Estimated:



Actual score:



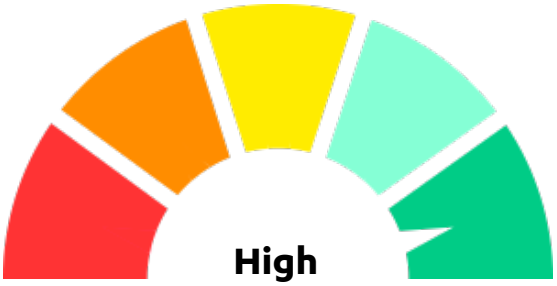
Tip: If you're not collecting and storing logs, events and other forensic evidence in a central, secure location, you're going to have a hard time responding to a breach. A good log collection strategy determines what's relevant and what isn't based on the type of threats your organization is likeliest to face. It also includes a solid data retention policy, with frequent backups. We recommend storing logs, events and other forensic evidence for at least two years.

RESPOND: Incident response

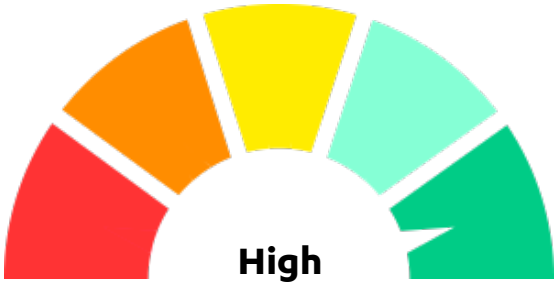
In the event of a major security incident, how clear is your incident response plan?

YOUR ANSWERS

Estimated:

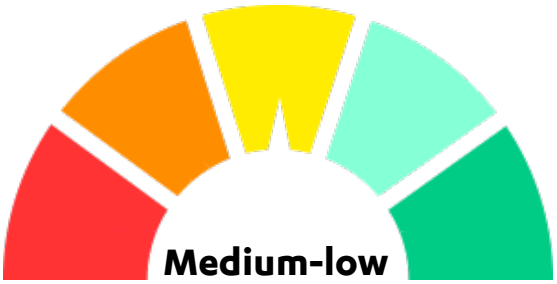


Actual score:

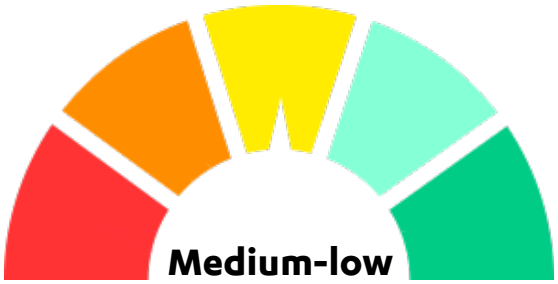


YOUR DEMOGRAPHICS' ANSWERS

Estimated:



Actual score:



Tip: Incident response has become an important part of crisis and risk management. But in order to get it right, you're going to need C-level buy-in. Because preparing well invariably comes down to having the right resources. We estimate that, for most organizations, it would take a team of ten trained in-house experts to deal with complex incidents. Since most organizations aren't likely to resource that, it makes sense to turn to external security experts to handle incident escalations.