GROUP-IB

CYBERSECURITY ULTIMATE ASSESSMENT GUIDE

PART 2. HUMAN-CENTRIC ASSESSMENTS

GROUP-IB.COM

E-GUIDE

Table of contents

Introduction

Cybersecurity has long focused on technology: firewalls, endpoint detection systems, threat intelligence platforms... Yet despite all the advancements made in recent years, the same weakest link remains — people. According to Verizon's 2025 Data Breach Investigations Report, the human element was involved in 60% of data breaches.

As organizations continue to adopt cloud infrastructure and promote remote work, their attack surface becomes wider. Each user, device, and third-party connection increases the risk of human-related incidents. Meanwhile, generative AI is reshaping the threat landscape. Attackers now use AI to craft convincing phishing emails, generate deepfakes, and conduct more targeted social engineering. The 2025 Identity Fraud Report by the Entrust Cybersecurity Institute revealed that deepfakes accounted for 40% of all biometric fraud in 2024.

To keep up with such evolving threats, organizations must strengthen the human side of their cybersecurity defences. One of the most effective ways to do so is through human-centric cybersecurity assessments. They help evaluate and improve both the knowledge and response capabilities of employees, from junior analysts to senior leadership.

This guide, crafted by Group-IB Education Practice and Academic Alliances, is the second chapter in our e-book series dedicated to cybersecurity assessments. The first chapter introduced different types of assessments and featured the Cybersecurity Assessment Compass, a practical matrix for navigating them. In this chapter, we take a closer look at two core types of human-centric assessments:

Knowledge-based evaluations

which assess awareness of, attitudes to, and theoretical understanding of cybersecurity matters

Technical simulations and exercises

which test practical skills, decision-making, and incident response under realistic conditions

This guide provides practical strategies for implementing such assessments and offers clear use cases, with benefits for various teams and organizations. Our goal is to help you build a resilient security culture that combines informed awareness with hands-on competence.

Whether you're a **CISO, DFIR lead, HR manager, or head of team training**, this chapter will help you assess and strengthen the cybersecurity capabilities of your people. By the end of this chapter, you will understand how to apply the right human-based assessments for different roles, use them to uncover knowledge and skill gaps, and lay the groundwork for stronger, more security-aware behavior across your organization.

Written by Group-IB specialists

Svetlana Ostrovskaya
Head of Education Practice

Anastasia Barinova
Head of Academic Alliances

About Group-IB Education Practice

Group-IB Education Practice was established in 2018. With our mission to fight against cybercrime, our practice is dedicated to training technical specialists in various areas of cybersecurity. This helps companies create effective information security departments and enhances the skills of law enforcement specialists.

6,000+
students
have taken part in our training courses

50+
countries
where we deliver training programs

15+
expert trainers
with hands-on experience

Multi-disciplinary expertise
in fraud prevention, investigations, DFIR, consulting, and red teaming

90%
satisfaction rate
among participants

15+
training programs
for both technical professionals and non-technical audiences

Knowledge-based assessments

01 Objectives and scope

Leaders who are focused on organizational development and risk management face critical questions on a daily basis that shape their teams' resilience and the organization's security posture:

- Do employees have the knowledge to recognize basic security threats and respond to them?
- Are they familiar with, and adhering to, our organization's security policies?
- How well do managers understand evolving threats and security best practices?
- What additional training or awareness programmes are needed to enhance the organization's security posture?

These questions are not theoretical — they determine whether an organization can withstand sophisticated cyberthreats. A well-structured human-centric assessment provides clear, data-driven answers, ensuring that security teams are not merely compliant but truly prepared for the challenges ahead.

Human-centric cybersecurity assessments benefit the organization as a whole, as well as individual teams directly involved in incident response. In the former case, the primary objectives of **knowledge-based assessment** are:

Identifying knowledge gaps

Pinpoint areas where employees lack a critical understanding of cybersecurity principles and common threats.

Measuring general awareness

Evaluate how well employees recognize everyday cybersecurity risks and adhere to basic protective measures.

Evaluating attitudes towards security

Assess employees' general attitudes towards security practices to reveal potential complacency or resistance.

Measuring training effectiveness

Understand the effectiveness of training and workshops through pre- and post-assessment comparisons.

For technical teams involved in incident response, the objectives also include:

Policy and procedure mastery

Evaluate the detailed understanding of, and adherence to, complex security policies, guidelines and regulatory compliance.

Supporting career development

Determine the depth of technical and theoretical knowledge, and assess its relevance to specific roles. Align the assessment with the grading system and plan relevant certifications or training.

Overall, knowledge-based assessments evaluate employees' theoretical understanding and awareness of cybersecurity concepts. These assessments are designed to identify knowledge gaps, misconceptions and attitudes about cyber security, and form the basis for effective training and awareness programmes.

The scope of knowledge-based assessments will vary depending on the organisation's industry, regulatory obligations and risk exposure. One or more of the following areas will usually be covered:

01 Cybersecurity awareness and best practices

Testing employees' ability to recognize phishing, social engineering attacks, and other digital hygiene gaps.

02 Compliance and regulatory knowledge

Ensuring employees understand legal and industry-specific security requirements (e.g., GDPR, PCI DSS, ISO 27001) as well as internal security policies.

03 Technical knowledge for security teams

Assessing SOC analysts, incident responders, and security engineers on threat detection, malware analysis, and forensic procedures.

Lastly, a knowledge check could help the organisation identify skills gaps and ensure alignment with policies and frameworks before and after the technical simulations and exercises. Such an approach can greatly optimize training resources by providing hands-on training to those who need it most.

Once these areas are defined, the next step is to determine who should be assessed and at what priority level.

02 Who needs knowledge-based assessments?

Ultimately, any organization could benefit from such assessments as they are fairly straightforward and can be flexible. Nevertheless, the following types of companies might benefit the most:

- Organizations that have ongoing and consistent training plans for their cybersecurity teams
- Companies expanding their SOC teams or areas of expertise
- Companies subject to new external regulations or internal policies that require in-house training
- Organizations going through a merger or acquisition process
- Companies adopting new technologies and tools that require greater cybersecurity awareness

Another factor to consider are the different priorities of different teams and the various roles within cybersecurity department:

high priority

01 Cybersecurity teams

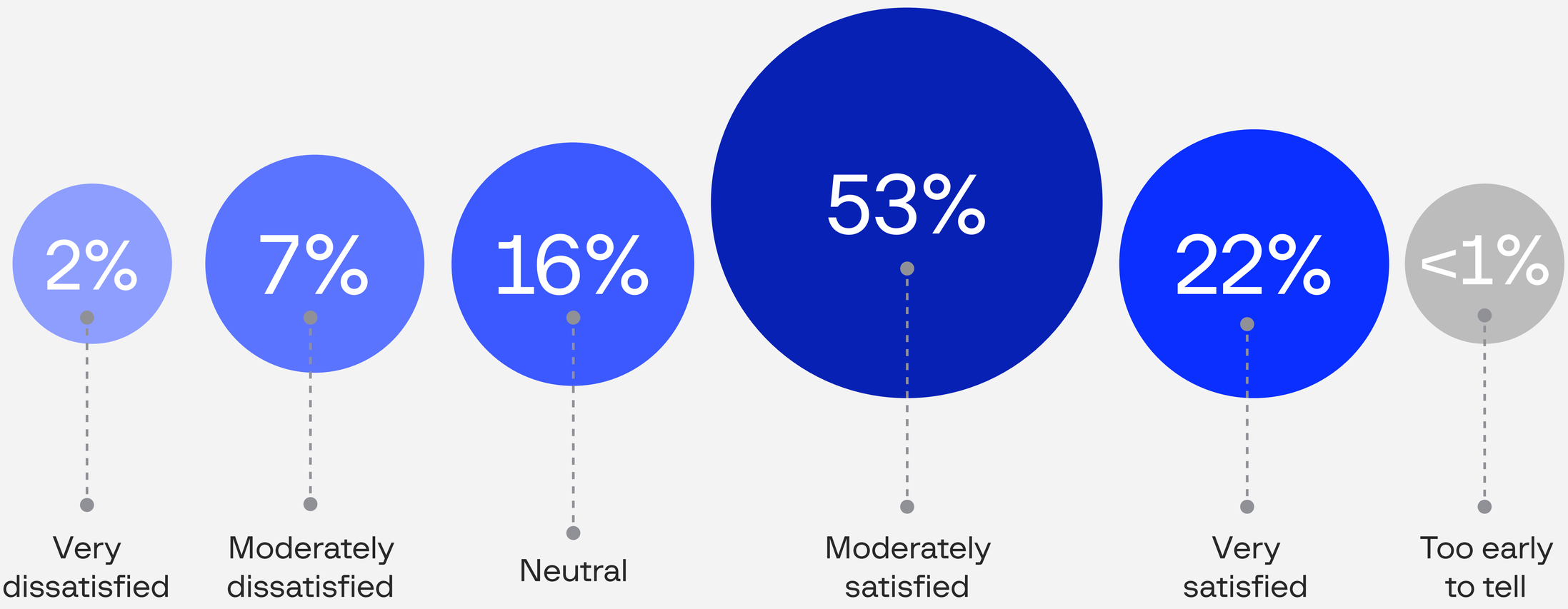
- **Security Operations Center (SOC) analysts:** To check their knowledge of threat detection, malware analysis, and incident response protocols.
- **Incident responders:** To check their ability to triage security events, implement containment strategies, and preserve forensic evidence.
- **Threat intelligence analysts:** To check their understanding of adversary tactics, techniques, and procedures (TTPs) to anticipate and mitigate potential threats.

Use case

A multinational organization conducts semiannual knowledge-based assessments for its SOC: L1 analysts, incorporating real-world questions to evaluate their proficiency in identifying and responding to advanced persistent threats (APTs).

According to Gartner Insights, 53% of SOC leaders are moderately satisfied with the current skills level of their employees, while 16% of responders have neutral feelings about it. These “average” survey results may mean that companies lack structured approaches and techniques to assess the skills of professionals.

How satisfied are you with your SOC team’s skills?



Gartner Insights

high priority

02 Wide audience: Employees requiring general cybersecurity awareness

- **All employees (non-security staff):** Any employee with access to company networks, email, and sensitive data.
- **HR, finance, and legal teams**: Departments handling confidential personal, financial, and legal data that are prime targets for cyberattacks.

Use case

Assessing knowledge of key security rules and best practices in digital hygiene: “When should you change the passwords for your critical corporate services?” The results of the assessment will be used for training purposes later.

high priority

03 IT and engineering teams

- **Developers:** To evaluate skills in secure coding practices and the ability to prevent vulnerabilities in software applications.
- **System administrators:** To evaluate competencies in managing system configurations securely, overseeing patch management, and ensuring robust network defenses.
- **Cloud and DevOps engineers:** To evaluate understanding of cloud security principles and the ability to spot misconfigurations that could expose the organization to risks.

Use case

A leading technology firm integrates secure coding assessments into its developer onboarding process, thereby ensuring that all new hires demonstrate their ability to identify and mitigate common security weaknesses.

medium priority

04 Executives and decision-makers

- **Chief Information Security Officers (CISOs) and security managers:** To evaluate understanding of cybersecurity frameworks, risk management strategies, and compliance obligations.
- **C-level executives (CEOs, COOs, CFOs):** To evaluate familiarity with the broader implications of cybersecurity, including business continuity planning and the financial impact of potential breaches.

Who does not need knowledge-based assessments?

Not every organization will benefit from conducting **knowledge-based cybersecurity assessments**. While such assessments help to evaluate skills, identify knowledge gaps, and align training strategies, in some cases where they may be unnecessary — or even counterproductive.

When adopting assessment methodologies, companies should be **strategic** about their choices rather than blindly following industry trends. Below, we highlight key parameters that determine when knowledge-based assessments are **unnecessary** or **ineffective**.

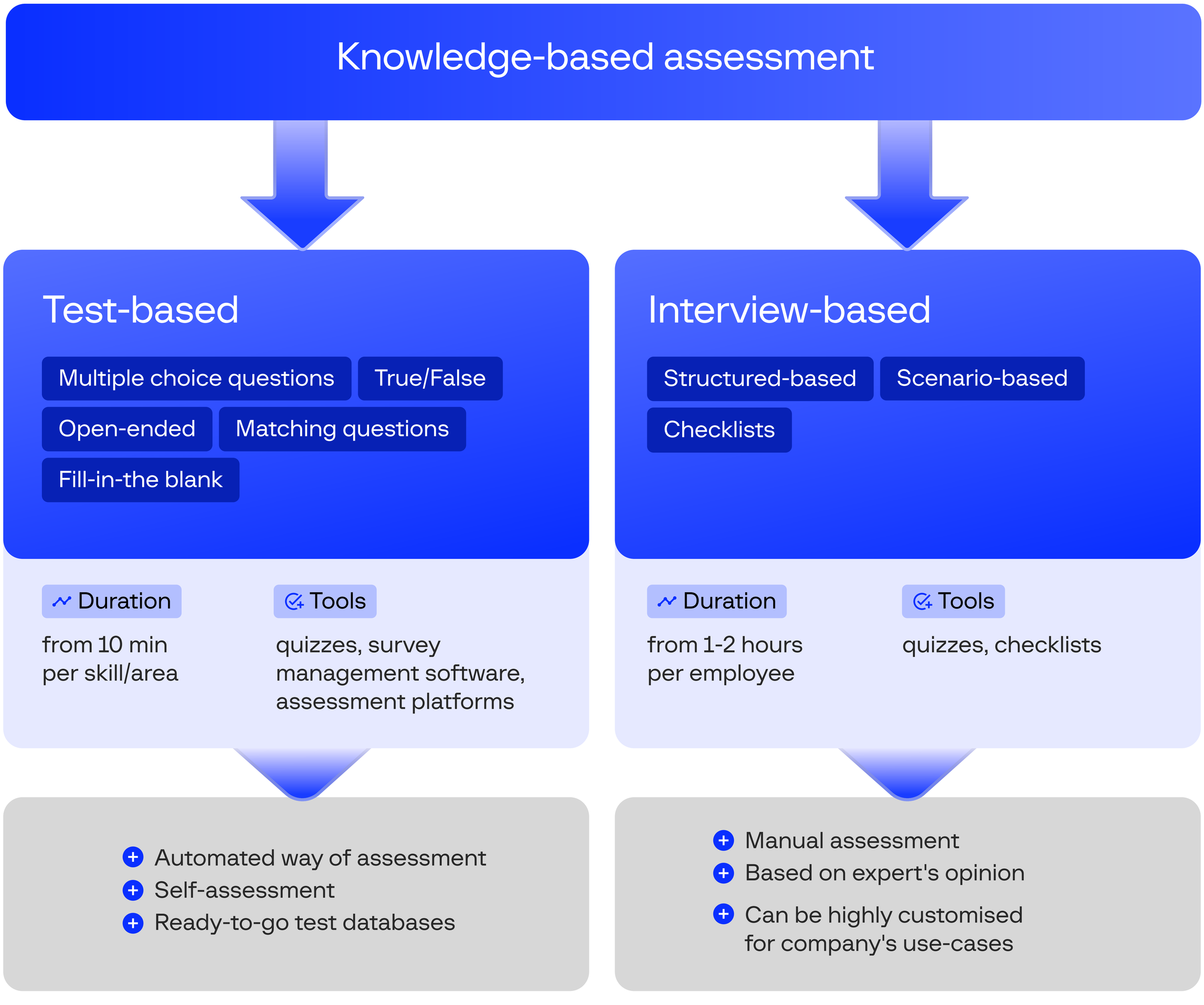
Companies without a learning strategy or training capabilities	A knowledge assessment is only valuable when there is a clear plan to act on the results. Organizations that lack a structured training roadmap or learning strategy and budgets often struggle to apply the findings from such assessments. Without predefined learning paths, upskilling programs, or career progression plans, assessment results become meaningless numbers rather than actionable insights.
Small businesses with simple IT needs, currently without dedicated cybersecurity roles and goals	Small businesses, especially ones without dedicated cybersecurity teams, often have limited attack surfaces and basic security needs (e.g., endpoint protection, firewall, strong passwords). Running detailed knowledge assessments in such environments might be overkill if there is no team to apply that knowledge in practice. In the case of small businesses, practical security measures (like strong policies, automated security tools, and regular security awareness training for employees) are often more effective than formal knowledge assessments.

Use case

Small businesses in the retail sector surveyed their employees on their knowledge of cybersecurity. It turned out that only 10% of employees are aware of the key security measures in their workplace. The company does not have a budget for professional training as well as a dedicated role for cybersecurity, however.

03 Types of knowledge-based assessment

The following diagram explains the main categories of assessments that are useful for improving cybersecurity knowledge:



Test-based assessments

Tests and quizzes are one of the most common methods for assessing theoretical knowledge in cybersecurity. They come in various forms, each designed to measure different aspects of a professional's knowledge. It can often be helpful to check general not-specific knowledge from various cybersecurity domains such as network security, operating systems, risk management, and security operations.

Common test types include multiple choice questions (MCQ), true or false, matching questions, and open-ended questions.

In some cases, tests can be the most useful assessment method:

- **Validating a SOC analyst's knowledge:** After onboarding, SOC analysts (L1/L2) can be tested on fundamental security concepts, such as SIEM rules, log analysis, malware classification and vulnerabilities.
- **Ensuring compliance awareness:** Tests can assess whether employees understand regulations such as the GDPR, ISO 27001, or internal security policies.
- **Evaluating executive-level security awareness:** Security managers and executives can be tested on risk management principles, governance models, and compliance requirements.

Best practices

- Avoid simplistic or obvious answers. Crafting questions with realistic distractors forces test-takers to think critically.
- Use scenario-based MCQs. Instead of asking “What is a phishing attack?”, ask “A user receives an email claiming to be from IT support, requesting password confirmation. What type of attack is this?”
- Limit the number of answer choices to 4 or 5. Too many options increase confusion (but too few make the test too easy!).
- Incorporate weighted scoring. Some questions can carry more weight based on how relevant they are to the role.

The table below shows a few options of how each of the test types can be applied:

Test type	Best for
MCQs	Broad knowledge check, compliance, quick evaluations
True/false	Basic awareness, policy training, rapid assessment
Fill-in-the-blank	Memorization of technical terms, regulatory compliance
Matching	Terminology association, attack vectors vs. defenses
Open-ended	Critical thinking, management roles, incident response

Interview-based assessments

While tests provide a structured way to assess theoretical knowledge, interviews offer a more **personalized** approach to assessing theoretical knowledge. This type of evaluation involves structured conversations with team members to assess their understanding of security principles and decision-making capabilities. Interviews can come in various forms, but they are particularly useful when you need to evaluate **complex problem-solving abilities** or **understanding of abstract concepts.**

When crafting interview-based assessments, an appropriate approach is to use previous cases as a reference as well as to add details related to the organization's **current network, policies, and business processes.**

It's also a good idea **to standardize hiring evaluations** for cybersecurity roles.

Interview types can be classified as follows:

Structured interviews

Structured interviews follow a predefined set of **consistent** questions, ensuring **objectivity** and **comparability** between the answers of different employees.

Use cases

- **Assessing SOC analysts:** An interviewer could ask, "What steps would you take after receiving an alert about suspected malware?"
- **Assessing SOC analysts:** "Your CISO asks you to evaluate the effectiveness of your SIEM rules. How do you measure whether your detection capabilities are sufficient?"
- **Assessing GRC team members:** "Your company is expanding to a new region and must comply with the GDPR and other local regulations. What steps do you take to ensure compliance?"

Checklist-based interviews

Checklist-based interviews involve predefined topics, **security controls or procedures** that need to be verified against an individual's knowledge and responsibilities. The interviewer systematically checks the participant's **awareness of, adherence to, and proficiency** in specific cybersecurity issues.

Use case

Verifying incident response readiness

"Do you know where to find our company's disaster recovery plan and how to execute it?"

Scenario-based interviews

Scenario-based interviews present **real-world cybersecurity situations** and ask candidates or employees how they would respond. Such interviews test **critical thinking, adaptability, and problem-solving skills** rather than just memorized knowledge.

Use case	**Simulating an ongoing attack**
Question 1	“Your organization's SIEM has triggered an alert: multiple failed login attempts from an unusual IP address (XXX.XXX.XXX.XXX) targeting several corporate accounts within a short timeframe. The login attempts originate from a country where your company has no operations. What do you do?”
Example of response	Check event logs and SIEM alerts for patterns and correlate with threat intelligence.
Question 2	“If you determine that this is a brute-force attempt, how would you mitigate it immediately?”
Example of response	Block IP addresses, enforce MFA, implement account lockout policies, review IAM policies.
Question 3	“Further investigation reveals that one of the targeted accounts has successfully logged in after several failed attempts. What is the best course of action?”
Example of response	Force a password reset, terminate active sessions, and block the suspicious IP. Escalate for further forensic analysis.

Use case	**Phishing response evaluation**
Question	“An employee from the finance department reports receiving an email from their manager. The email contains a ZIP attachment named 'Invoice_0325.zip.' The employee found the email suspicious and forwarded it to the security team. What do you do?”
Example of response	Instruct the employee not to open the attachment, scan the attachment, search for similar emails.

04 Pros and cons

Let’s outline the strengths and weaknesses of knowledge-based assessments:

Advantages of knowledge-based assessments

Knowledge-based assessments play a crucial role in identifying gaps in cybersecurity expertise and ensuring that teams stay aligned with the organization’s security standards.

First of all, the results of such an assessment help to **pinpoint** specific **training needs** by highlighting areas where employees require additional education or skill development. Knowledge-based assessments also ensure compliance with internal security policies and regulatory requirements, confirming that team members understand and follow established procedures.

In addition, they support **career development** by serving as a foundation for progression, training plans, and certification pathways. For **large organizations**, knowledge-based assessments provide a scalable way to evaluate distributed teams, ensuring consistent skill levels across different regions and departments.

Challenges and limitations

Knowledge-based assessments require strong management skills	Without clear communication, frequent assessments can demotivate employees. Some employees may feel uncomfortable or pressured, so the program leaders should transparently communicate the goals, reasons, and criteria during the assessment.
Time-consuming preparation	Significant time and effort are required to design and update custom assessments.
AI and LLM circumvention risks	Unless they are well structured, traditional exams can be “hacked” by AI-generated answers. One of the biggest challenges with using knowledge-based assessments is ensuring that they accurately measure an individual’s true understanding and that they **cannot be easily bypassed using AI models (e.g., ChatGPT, Bard, or Copilot).**

AI tools like ChatGPT are powerful, but they should assist learning, **not replace critical thinking**. Some key strategies exist that help to **prevent “hacking”** the test’s standard forms.

First, try to use real-world scenarios with as much detail as possible, combined with past cases and reference to your internal policies and guidelines.

Use case

Questions should be phrased as follows

“Your organization, ACME Corp, enforces VPN access with MFA for remote employees. The European SOC team detects multiple failed login attempts from an IP address originating in São Paulo, Brazil, followed by a successful login using the corporate VPN. The login belongs to Daniel R., a senior system administrator based in the London office, who is currently on vacation and unreachable. How would you determine whether this is a credential theft incident, a malware compromise, or an insider threat?”

Second, randomizing and rotating question sets and using time limits reduces an employee or candidate’s ability to use chatbots effectively.

Another approach is to include open-ended and peer-reviewed questions or linked questions, which allows for fewer opportunities to use AI assistants.

Overall, knowledge-based assessments should be combined with practical exercises and simulation-based evaluations to provide a comprehensive, multi-dimensional approach to assessing cybersecurity skills. While theoretical assessments help gauge an individual's understanding of concepts, frameworks, and policies, practical simulations (such as c**yber drills, hands-on labs and cyber ranges, purple teaming activities, and table-top exercises**) test a person’s ability to **apply that knowledge in high-pressure, real-time situations.**

Technical simulations and exercises

01 Objectives and scope

In contrast with knowledge-based assessments, technical simulations and exercises provide a practical evaluation of employees' cybersecurity capabilities, focusing on their ability to apply knowledge in real-world scenarios. These assessments help organizations identify weaknesses in their operational security practices and incident response capabilities, helping to develop targeted skills and build resilience.

The main objectives of **technical simulations and exercises** include:

Assessing response capabilities

Measure how effectively employees respond to cyberthreats in real time.

Validating decision-making under pressure

Assess whether employees are able to make informed and safe decisions under pressure and stress.

Validating the application of policies and procedures

Ensure that employees know how to implement cybersecurity policies and protocols correctly.

Pinpointing gaps in practical skills

Identify areas where additional training or practice is needed to improve an employee’s cybersecurity posture.

The following table helps to better understand the core differences between knowledge-based assessments and technical simulations and exercises you can use the following table:

Key objective	Knowledge-based assessments	Technical simulations and exercises
Knowledge gaps	Identify gaps in an employee's theoretical understanding of cybersecurity concepts.	Evaluate how an employee applies cybersecurity skills in practice.
Awareness levels	Assess an employee's general level of understanding and whether they are able to recognize threats.	Measure an employee's ability to detect and manage cybersecurity incidents.
Attitudes towards security	Assess an employee's attitudes, beliefs and perceptions relating to cybersecurity practices.	Evaluate an employee's behaviour, decision-making processes and adherence to established protocols.
Policy familiarity	Evaluate how familiar an employee is with cybersecurity policies and procedures.	Test whether an employee is able to apply policies in threat scenarios in an effective way.
Incident response	Assess an employee's theoretical knowledge of incident response plans and communication and coordination strategies.	Test whether an employee is able to respond to incidents effectively through practical simulations and exercises.

The scope of technical simulations and exercises is determined by various factors, including the organization's threat landscape, the maturity of its cyber security programme, and the operational roles of the participants being assessed. These elements usually include:

Incident response and crisis management

Individuals and teams are assessed as regards their ability to detect, escalate and respond to cybersecurity incidents through simulations and scenario-based exercises.

Technical problem solving and analysis

Employees are tested in terms of their practical capabilities such as incident response, forensic investigation, malware analysis, threat hunting and the use of threat intelligence.

Cross-functional collaboration

The coordination of business, information security, IT, legal and other roles is evaluated during cyber crisis simulations in tabletop exercises involving internal teams or in collaboration with external stakeholders.

Technical simulations and exercises provide valuable insights into how employees perform under pressure and work as a team in real-world cybersecurity scenarios. As a result, organizations are able to test whether their employees are adequately prepared and, if needed, strengthen and improve their incident response and decision-making processes.

02 Who needs technical simulations and exercises?

Although all organizations can benefit from technical simulations and exercises, practical, immersive evaluations will be a higher priority and more useful to some. Entities that would benefit the most include:

- Companies often exposed to incidents and cyberthreats.
- Digital enterprises or businesses transitioning to cloud infrastructure.
- Organizations with complex environments and cross-functional responsibilities.
- Regulated organizations required to demonstrate robust incident response capabilities (e.g., entities working in finance, healthcare or critical infrastructure).
- Distributed companies with multiple offices and decentralized cybersecurity functions.

When conducting a human-centered cybersecurity evaluation,teams requiring technical simulations and exercises should be prioritized in a strategic way. Doing so involves carefully identifying and ranking teams based on their roles, their responsibilities, and the potential impact of their actions on the organization's security posture. It’s key to prioritize high-risk teams — ones that handle sensitive data, manage critical infrastructure, or respond to incidents.

high priority

01 Cybersecurity teams

- **SOC analysts:** To check their ability to detect, analyze and respond to threats in real time using logs, SIEM and detection tools.
- **Incident response specialists:** To check the ability to analyze raw data, reconstruct incidents, contain threats, communicate effectively and carry out all necessary post-incident actions.
- **Threat intelligence analysts:** To check that they understand their role in the incident response and adversarial threat hunting processes; and that they are able to enrich data, attribute detected activity, and provide actionable insights.
- **Threat hunters:** To check that they understand their role in the incident response and threat hunting processes; and that they have necessary logic and skills in detecting hidden threats in a simulated hostile environment.
- **Security engineers:** To check that they can apply secure configurations and remediate system vulnerabilities through simulated scenarios.

Use case

A global manufacturing firm runs quarterly cyber drills for its blue team, simulating ransomware attacks and measuring time-to-containment across regions.

The percentage of organizations with formalized threat-hunting methodologies have increased to 51%, according to the SANS 2024 Threat Hunting Survey. The increase is a significant jump from the 35% reported in the previous year. By including threat hunters and intelligence analysts in simulations, organizations can test their ability to proactively identify hidden threats and translate threat intelligence into effective mitigation strategies.

high priority

02 IT and engineering teams

- **System administrators:** To check their proficiency in identifying and resolving misconfigurations, patching vulnerabilities, and understanding their role in supporting the incident response process.
- **Cloud and DevOps engineers:** To check that they understand their role in responding to simulated cloud breaches, preventing privilege escalation, and remediating security gaps.

Use case A fintech company uses red/blue team simulations during its CI/CD pipeline reviews to test its defensive procedures and incident handling capabilities.

high priority

03 Executive leadership and risk owners

- **CISOs and security managers:** To check their leadership skills in crisis situations as well as their ability to communicate with boards and prioritize risks.
- **C-level executives:** To help understand the crucial role of leadership in navigating the implications of cyber incidents and shaping their business impact.

Use case A regional bank conducts annual tabletop exercises for senior leadership, simulating regulatory breach disclosures and media response.

According to Corporate Compliance Insights and Directors & Boards, almost half of Fortune 100 companies are estimated to engage in simulations and tabletop exercises as a way of preparing for cybersecurity challenges.

medium priority

04 Cross-functional teams

- **Legal, compliance, PR, HR:** To assess understanding of their role in responding to coordinated breaches, reporting, and managing internal and external stakeholders.
- **External stakeholders and partners (context-specific):** To evaluate escalation and communication workflows and cooperative response planning.

Use case A healthcare entity includes a cloud service provider and regulatory body observers in a joint tabletop exercise to test coordination during a breach involving leaks of patient data.

“Third-party breaches caused 38% of healthcare-related incidents, highlighting weak vendor risk management,” according to GlobeNewsWire.

Who does not need knowledge-based assessments?

Although technical simulations and exercises can provide valuable insights, they are not always a prerequisite. In some situations, they could divert resources from core priorities or establish unrealistic expectations.

Such assessments should only be used when they align with an organization's operational maturity, staffing, and incident response needs. In the two scenarios below, technical simulations and exercises may not be beneficial.

Organizations lacking cybersecurity capabilities	Technical simulations and exercises depend on participating in active simulations. If a company does not have dedicated cybersecurity or IT response teams, it will probably find that it is unable to effectively act on the results of the simulation. If there are no clearly defined incident response roles, escalation procedures, and technical readiness, technical simulations risk being purely theoretical and unproductive. It is much more effective to prioritize foundational capabilities such as automated protections, awareness training, and clear incident response plans.
Early-stage or small businesses with outsourced security	Technical simulation-based assessments may not accurately reflect real-world responses for startups and small businesses that rely solely on managed service providers (MSPs). Vendor-led reviews, service-level testing, and tabletop exercises covering roles and expectations would be more beneficial.

Use case

A small real-estate firm without an in-house IT team carried out a simulated phishing drill. The team expressed confusion regarding their roles, an issue with response coordination was identified, the MSP was unaware that the test was being carried out, and follow-up actions were unclear. The exercise resulted in more anxiety than improvement.

In such cases, focusing on vendor coordination, awareness training, and clear escalation procedures is more impactful until in-house readiness justifies simulation-based testing.

03 Types of technical simulations and exercises

Although different in style and scope, technical simulations and exercises all aim to evaluate how well individuals and teams are able to put their knowledge into practice within realistic or modeled situations. The main focus of such assessments is on actions, choices, and whether the team can work effectively under pressure. The following points outline typical technical simulations and exercises that are used to determine cybersecurity preparedness.

Cyber drills

Cyber drills simulate specific cyber threats (such as DDoS attacks, malware infections and phishing campaigns) in order to test the response capabilities of technical teams and, occasionally, end users. Such exercises might include the coordinated modelling of fraudulent emails, attempts at stealing credentials, and internal escalation workflows.

Best for

- SOC analysts
- incident responders
- threat hunters
- threat intelligence analysts
- system administrators
- DevSecOps specialists
- end users
- high-risk departments

Use case

A major company with a significant number of employees, whether in retail, e-commerce, or another industry, conducts phishing simulations on a quarterly or biannual basis for all staff. The goal is to assess compliance with internal cybersecurity policies and to monitor metrics such as MTTR (Mean Time to Report). These metrics reflect how quickly employees report phishing attempts to the appropriate teams.

Best practices

- Use threat intelligence to design realistic scenarios
- Incorporate simulated logs and alerts to replicate the functionality of detection systems for technical teams
- Monitor efficiency in terms of detection, reporting, escalation and containment effectiveness (e.g. MTTD (Mean Time to Detect), MTTR)
- Vary simulated scenarios to prevent them from being anticipated

Tabletop exercises

Interactive, scenario-driven discussions are used to evaluate the roles, decisions, and communication skills of senior leadership and support personnel in crisis situations. Such assessments are designed to simulate real-world challenges and test organizational readiness.

Best for

executive leadership | boards of directors | compliance teams | risk officers | communication leads and external teams

Use case

A regional bank conducts annual tabletop exercises for top management to raise awareness of current threats and their potential impact on the business. These exercises serve to test executive decision-making and crisis management in the context of cybersecurity incidents, while also supporting compliance with regulatory requirements, as many central banks recommend conducting such exercises annually.

Best practices

- Develop realistic, business-driven scenarios based on the relevant threat landscape
- Ensure that key decision-makers take part
- Conclude with debriefings that result in actionable plans and clearly defined responsibilities

Purple teaming

Purple teaming fosters collaboration between offensive (red) and defensive (blue) teams, allowing for comprehensive testing of detection logic, incident response procedures, and threat visibility.

Best for

mature SOCs | detection engineers | threat hunters

Use case

A state-owned oil pipeline operator conducts purple teaming exercises every six to twelve months. The goal is to identify potential vulnerabilities and weaknesses in the infrastructure, detection logic, and security tool coverage. These exercises also assess the blue team's capabilities, including in-house SOC and incident response teams, in detecting, analyzing, and effectively responding to actions that simulate real-world attackers.

Best practices

- Design purple teaming activities focusing on potential gaps, relevant threat landscape, or newly discovered attack techniques
- Use industry-recognized frameworks such as MITRE ATT&CK to structure purple teaming activities and enhance collaboration between red and blue teams
- Collect and analyze telemetry to make detection and validation more accurate

Hands-on labs and cyber ranges

Technical teams can gain invaluable experience in threat detection, investigation and remediation by working in realistic, immersive environments. Cyber ranges provide such safe, sandboxed infrastructures that effectively mimic enterprise environments.

Best for

security engineers | SOC analysts | system administrators | cloud/DevOps teams

Use case

A telecommunications company runs quarterly cyber range exercises to assess and strengthen the technical team's ability to coordinate response efforts, contain threats, and harden systems.

Best practices

- Organize sessions that focus on modern cybersecurity threats
- Incorporate telemetry monitoring and detailed post-activity analysis
- Use telemetry for onboarding, developing advanced skills, and validating playbooks

The following diagram summarizes the main characteristics of the technical simulations and exercises described.

Technical simulations and exercises

Cyber Drills

Test detection, response, and recovery to mock cyberattacks

Best for

SOC, IR, Engineers

Focus on

real-time incident response containment, coordination

Periodicity

Monthly or quarterly

Tabletop Exercises

Walk through cyber crisis scenarios to discuss roles and decisions

Best for

Executives, Legal, Risk, Compliance, IT, Cybersecurity

Focus on

planning, decision making, communication and coordination

Periodicity

Annually

Purple Teaming

Align red and blue team activities to find and remediate gaps

Best for

Detection Engineering, Blue & Red Teams

Focus on

detection validation, real threat actor simulation

Periodicity

Annually or semiannually

Hands-On Labs

Test and practice using tools in controlled environments

Best for

Security Engineers, Admins, DevOps

Focus on

secure configuration, vulnerability remediation

Periodicity

Continuous or on-demand

Cyber Ranges

Train and validate technical skills in realistic, isolated environments

Best for

Advanced SOC, Threat Hunters, IR Teams

Focus on

high-fidelity attack simulation and remediation

Periodicity

Quarterly or semiannually

04 Pros and cons

Let's delve into the advantages and limitations of technical simulations and exercises.

Advantages of technical simulations and exercises

Technical simulations and exercises are essential for thoroughly evaluating an organization’s preparedness and for refining its incident response tactics. The main advantage of technical simulations is that they assess practical skills in realistic, high-pressure scenarios, providing a valuable opportunity to observe how individuals and teams perform under the inevitable stresses of cyber incidents.

Such exercises serve many purposes

They bridge the gap between theoretical knowledge and practical application

They do more than simply test whether information has been retained — they provide a way to confirm whether employees are able to translate their understanding into tangible actions. This crucial step ensures that knowledge is not just passively absorbed but actively deployed when required.

They foster synergy and communication excellence

Exercises such as tabletop exercises (which involve guided discussions of hypothetical scenarios) and purple teaming (which involves both offensive and defensive security teams working together) are instrumental in identifying communication bottlenecks and fostering seamless cooperation between different departments and stakeholders. The resulting enhanced communication is vital for ensuring coordinated and effective responses to threats.

They uncover weaknesses and vulnerabilities

Drills (which involve practicing specific procedures) and cyber ranges (simulated environments that mimic real-world networks) expose concrete deficiencies in an organization’s detection, response and recovery plans that often remain concealed in standard audits or theoretical evaluations. Such exercises show where improvements are needed.

They cultivate instinctive and rapid reactions

Consistent, meticulously designed and realistic simulations play a critical role in helping teams develop ingrained reflexes and automatic rapid responses during high-intensity incidents. The resulting muscle memory means that employees are able to act swiftly and decisively under pressure and minimize potential damage.

They deepen and reinforce a robust security mindset

Taking part in simulation exercises greatly increases awareness of potential threats, reinforces established best practices, and demonstrates management's commitment to proactive cybersecurity measures. The collective effort fosters a security-conscious culture throughout the organization, involving everyone in the defense strategy.

The above practical advantages make technical simulations and exercises indispensable for enhancing cybersecurity preparedness. The inherent challenges and limitations associated with their implementation should also be acknowledged, however.

Challenges and limitations

Significant demand on resources	Developing, organizing, and conducting effective simulations is time-consuming and requires substantial preparation and specific tools.
Dependent on organizational readiness	Simulation exercises yield optimal results when organizations have established incident response plans, clearly defined roles, and well-structured coordination mechanisms.
Risk of overwhelming unprepared teams	If teams are not sufficiently prepared or if clear objectives are not communicated, simulations may lead to confusion or decreased confidence.
Limited scope per exercise	Limited scope per exercise: Each drill or scenario usually focuses on a specific threat vector or procedure, which makes it difficult to assess overall capability unless the exercises are carefully integrated.
Reliance on tools and data	Reliance on tools and data: Whether simulations are effective often depends on the quality and accessibility of threat intelligence, telemetry, logs, and systems that emulate real-world production conditions.

Recommendation

Human-centric cybersecurity assessments require combining technical simulations and knowledge-based evaluations in order to measure staff's theoretical understanding and practical application of defensive strategies. Exercises should mimic real-world cyber threats and include a detailed analysis after each exercise to identify weaknesses and improve performance.

Clear, measurable goals help to refine cybersecurity postures on an ongoing basis, which enhances the organization's ability to proactively defend against evolving risks by understanding human factors and ensuring that technical defenses are supported by capable individuals.

Roadmap to a genuine behavior change

Successfully assessing human-centric cybersecurity risk involves more than just identifying weaknesses — the idea is to foster tangible, measurable improvements in behavior and decision-making across the organization. Conducting knowledge-based assessments and technical simulations is about embedding security awareness and best practices into every employee's daily routine and operational fabric. Such an integration ensures that security becomes an ingrained habit rather than an afterthought.

Seamless integration and meaningful change require a multifaceted approach. The following key strategies provide a roadmap for successful implementation.

Immediate and actionable feedback	It is crucial to provide prompt, personalized and role-specific feedback immediately following simulations or assessments. Immediate feedback strengthens the learning process by connecting actions with consequences in real time and fostering accountability. The feedback should be constructive, identify specific areas for improvement, and offer practical steps to address them.
Tailored and adaptive training programs	Insights gained from assessments should be used to develop highly customized training paths. Rather than taking a one-size-fits-all approach, training should be targeted in order to address identified skill gaps and awareness deficiencies within specific teams or roles. Doing so ensures that training resources are used efficiently and that employees receive the most relevant and helpful training.
Lessons learned integrated into daily workflows	Move beyond isolated training sessions by embedding microlearning modules and just-in-time prompts in the tools and workflows that employees use daily. Secure email prompts, workflow reminders, and quick-reference guides embedded within familiar interfaces transform learning into an ongoing, seamless experience. Such an approach maximizes retention and ensures that security knowledge is readily accessible when it is needed most.

Leadership engagement and visible support	Securing visible and sustained leadership commitment is paramount. When executives take part in exercises and simulations, it sends a powerful message about the importance of security. By actively promoting security priorities, leaders foster a culture in which security is valued and practiced at all levels of the organization. Such an endorsement by leadership acts as a catalyst for broader behavioral change.
Dynamic engagement and motivation strategies	Creative engagement techniques should be used to maintain motivation and ongoing participation. Gamification (such as leaderboards and friendly competition) can make learning more enjoyable. It is usually helpful to implement incentive programs such as recognizing exceptional security practices or awarding certifications for advanced security knowledge. Such techniques ensure that employees remain actively involved in and invested in improving their security behaviors.

Ultimately, fostering true behavioral change is not a one-off event but a sustained, continuous journey. It requires consistent reinforcement of positive practices, a proactive approach to building a security-focused culture, and an unwavering commitment to continuous improvement. Rather than treating security as a series of isolated tests or training sessions, it must be integrated into the organization's culture. Doing so ensures that security becomes an integral, natural part of daily operations, making the organization more resilient and protected.

Assess your team's readiness and prepare for modern threats with Group-IB

The Group-IB team offers various human-centric assessments designed to uncover vulnerabilities within the most critical element of your cybersecurity defenses — your people.

One example is our Tabletop Exercises, a scenario-driven simulation that tests your organization's crisis response, coordination, and leadership under pressure. By immersing stakeholders in lifelike incidents, tabletop sessions strengthen decision-making, highlight communication bottlenecks, and prepare teams to manage real-world cyber threats — before they strike.

How the exercise works

Set goals

Select a scenario type

Take part in real-time crisis simulation

Receive a report

Interactive tools

Each team uses a control panel with access to incident data, timers, and resource simulations for direct communication with Group-IB's facilitator.

Clear exercise structure

The game unfolds over 1.5 to 2 hours, challenging teams to make key decisions that will determine their ability to effectively handle real-world cybersecurity incidents.

Guided experience

The game is led by an experienced Group-IB facilitator assessing the team responses, coordination, and decision-making while under pressure.

Invaluable lessons

The final stage involves a detailed assessment of your team's performance and expert recommendations for implementing improvements.

If any gaps in your current processes or response capabilities are identified, our Education Practice is here to address them with tailored training programs designed to align with your industry, threat landscape, infrastructure, and specific needs.

Talk to our experts →

Contact us to learn more about our tabletop exercises and training programs

Bonus

Employee security awareness check — Is your team ready?

Human-centric cybersecurity starts with everyday behavior. This test offers a quick yet valuable reflection on your employees' personal security habits. It can be used to assess cybersecurity awareness across your organization and identify areas that require additional training.

Each of the 10 questions includes three answer options. Your team members can choose the one that best matches their current habits.

01. Updates

How do you manage system and application updates?

- I always install updates promptly and ensure all software is current. (2)
- I install updates occasionally but sometimes delay or miss them. (1)
- I rarely install updates. (0)

02. Applications

Where do you typically download software and mobile apps?

- Only from official sources, such as verified app stores. (2)
- Sometimes from other websites, but I check reviews and the source. (1)
- From any source, including unverified sites. (0)

03. Passwords

How would you describe your approach to passwords?

- I use strong, unique passwords for every account and store them securely. (2)
- I use strong passwords but occasionally reuse them. (1)
- I try to use complex passwords but often fall back on simpler options. (0)

04. Device locking

What do you do when leaving your phone or computer unattended?

- I always lock both devices, even if stepping away briefly. (2)
- I lock my phone consistently and my computer when leaving for longer periods. (1)
- I rarely lock my devices, relying on auto-lock or trusting my environment. (0)

05. Tracking and data permissions

How do you manage app tracking and data permissions?

- I disable unnecessary location tracking, microphone access, and activity logging. (2)
- I limit permissions on mobile apps but leave browser settings unchanged. (1)
- I allow all permissions by default. (0)

06. Browser security

What are your habits regarding browser settings and stored data?

- I disable autofill and regularly clear browsing history. (2)
- I disable autofill but forget to clear history. (1)
- I use autofill and rarely clear browser history. (0)

07. Encryption

Do you use encryption for your data?

- Yes, for all storage types, including cloud files, drives, and removable media. (2)
- Only when sharing files externally or storing sensitive data. (1)
- I do not use encryption. (0)

08. Public Wi-Fi

How do you behave when using public wireless networks?

- I avoid public Wi-Fi or use a VPN if I must connect. (2)
- I use public Wi-Fi cautiously and avoid entering personal information. (1)
- I use public Wi-Fi without precautions. (0)

09. Removable devices

Do you connect unfamiliar USB devices or external hardware?

- Never — I only connect devices I fully trust. (2)
- Occasionally — if I recognize the source. (1)
- Frequently — I do not consider it a significant risk. (0)

10. Cybersecurity awareness

Do you follow cybersecurity news or updates?

- Yes — I actively stay informed about cyber risks and best practices. (2)
- Occasionally — I rely on general news or colleagues for updates. (1)
- No — I do not follow cybersecurity-related news. (0)

Scoring and interpretation

Total score: _____ / 20

16-20 points: High personal security awareness

You consistently follow best practices and demonstrate strong cybersecurity habits. Continue reinforcing your behavior and helping others do the same.

10-15 points: Moderate security posture

You have a generally good awareness but may benefit from refining a few key areas. Revisit the questions where you scored 0 or 1 and consider adjusting your behavior.

0-9 points: Low security posture

Your current practices may expose you to significant risk. Improving your approach to updates, passwords, and application sources can significantly strengthen your digital hygiene.

GROUP-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,550+
Successful investigations of high-tech crime cases

500+
Employees

60
Countries

$1 bln+
Saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

*According to Cybersecurity Excellence Awards

11
Unique Digital Crime Resistance Centers

Global partnerships

- INTERPOL
- EUROPOL
- AFRIPOL

Recognized by top industry experts

- Forrester®
- Aité Novarica
- kuppingercole ANALYSTS
- Gartner®
- IDC
- Frost & Sullivan

Fight against cybercrime

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785