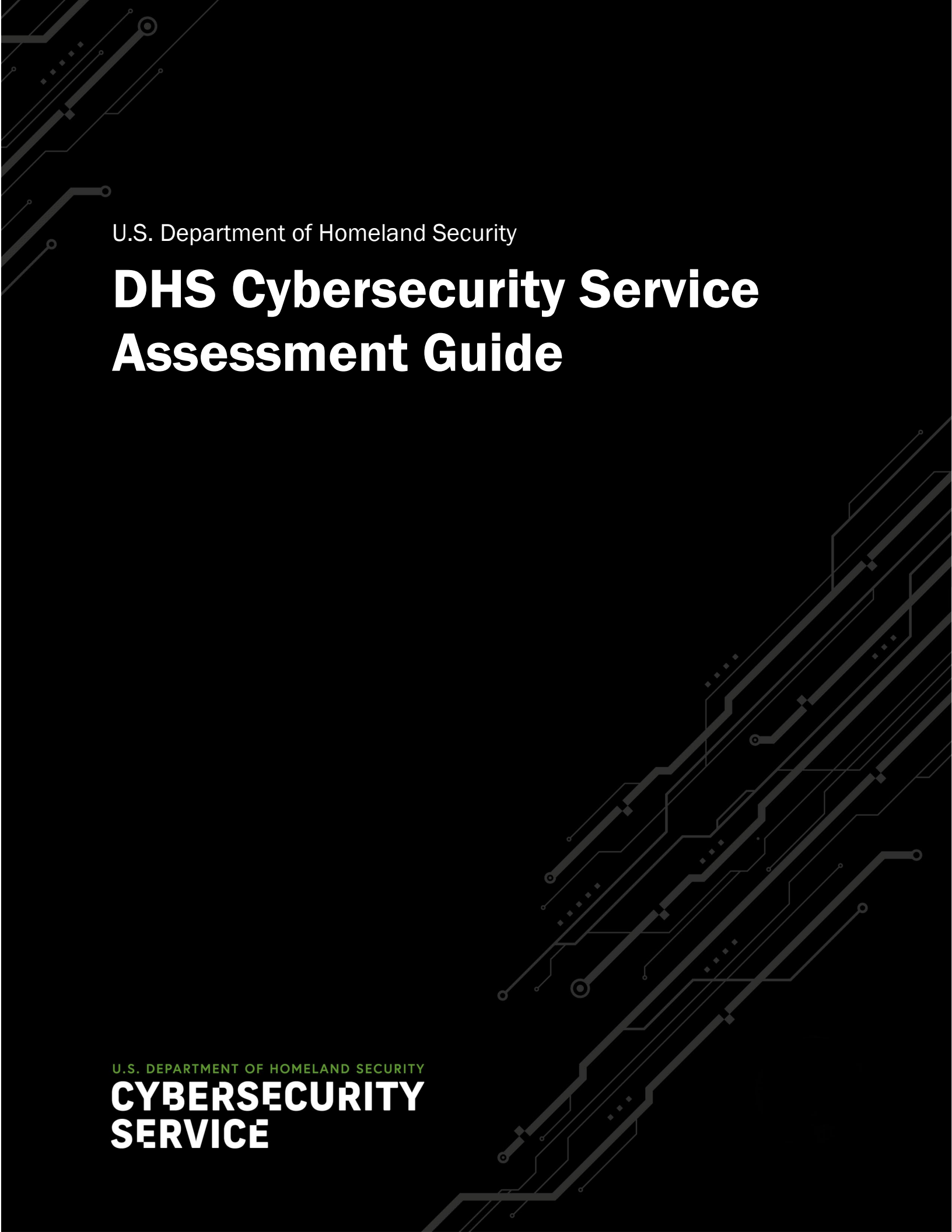
U.S. Department of Homeland Security

DHS Cybersecurity Service Assessment Guide



U.S. DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY SERVICE

DHS Cybersecurity Service Assessment Guide

Version: June 2023

The DHS Cybersecurity Service Assessment Guide provides information concerning what to expect during the assessment process and answers to common questions.

We encourage you to visit other pages and resources on the application portal to help you determine which track best reflects your expertise and experience. The career track that you apply for will inform the assessment process (noted in the guide below) that you will undergo.

If you are applying for a specific opportunity, a career track and associated assessment process will be noted in the opportunity announcement.

Contents

DHS Cybersecurity Service Assessment Guide

Overview: Cybersecurity Service Assessment Process

The DHS Cybersecurity Service uses a **multi-phase assessment process** that is designed to measure an applicant's expertise and qualifications. Applicants must successfully complete each phase to advance in the application process. As you prepare for the assessment process, please review the Career Level Guide, as individuals whose experience closely matches what is outlined for a particular career level are more likely to be successful and considered for jobs at that career level. We also encourage you to review the Capabilities guide to learn more about the capabilities on which you will be assessed.

Types of Assessments

Throughout the assessment process you may be asked to complete one or multiple types of assessments. These vary based on the career track for which you are applying. *Note: Applicants in the Executive Track will also have a Structured Resume Review (see the Executive Track section for more information).*

Online Assessments

You choose the time and location! Measure non-technical areas important for success in the DHS Cybersecurity Service. No knowledge of DHS or cybersecurity is required.

Proctored Assessments

Scheduled in advance and completed at a designated assessment center. Cybersecurity knowledge is assessed, no knowledge of DHS is required.

Capability-based Interviews

Scheduled individually, will be completed online (live or recorded video).

Before any assessment, DHS will email you with instructions and information to help you prepare. Assessments are time sensitive, so please monitor your email to ensure you have plenty of time to complete them prior to any deadlines!

Note: You may be contacted about scheduling by our contracting partner, PSI (USAHIRE_Support@panpowered.com). Please check your spam or junk mail folder for any email notifications.

DHS Cybersecurity Service Assessment Guide

Entry Track

An entry-level cybersecurity professional who is primarily a learner participating in a formal development program to gain technical expertise.

Applicants in the **Entry Track** will participate in a **one-phase assessment process.** This assessment requires a computer with audio (speakers or headphones) and a reliable internet connection.

Online Assessment

Includes three assessments to assess your professional capabilities.

- **Work styles** inventory presents you with questions about your work-related interests and preferences.
- **Reasoning assessment** asks you to draw logical conclusions, analyze scenarios, and evaluate arguments based on information provided
- **Writing assessment** asks you to provide a written response to an open-ended prompt; grammar/spelling, organization, and content will be evaluated

The total time commitment is approximately **2 hours** (many applicants require less time!). After you complete the online assessment you will be contacted by DHS with information on any next steps.

DHS Cybersecurity Service Assessment Guide

Developmental Track

A cybersecurity professional with some experience who applies still-burgeoning technical expertise to perform routine work with significant supervision and clear guidance

Applicants in the **Developmental Track** will participate in a **two-phase assessment process**.

Phase I: Online Assessment

Includes two assessments to evaluate your professional capabilities:

- **Work styles** inventory presents you with questions about your work-related interests and preferences.
- **Work simulation** presents you with realistic, work-related scenarios and asks you to respond to them.

No knowledge of DHS or cybersecurity is required for these assessments.

Remember! Assessments require a computer with audio and reliable internet connection.

Phase II: Proctored Assessment

DHS Cybersecurity jobs are structured around cybersecurity specializations – called technical capabilities. There is a different assessment for each technical capability.

- In Phase II you will complete a Technical Capability Assessment which presents realistic, work-related cybersecurity scenarios and questions to assess your technical skills in the technical capability you have selected.
- See the Appendix for more details and specific preparation tips.

The average commitment is approximately **3 hours** (many applicants require less time!). You will have up to 2.5 hours to complete Phase I and up to 2.5 hours to complete Phase II.

DHS Cybersecurity Service Assessment Guide

Technical Track

A cybersecurity professional who has worked in progressively difficult cybersecurity roles, contributed to efforts to address cybersecurity challenges and/or to cybersecurity projects, programs, and teams, and has a primary technical capability

The Technical Track covers four career levels ranging from full-working level to various expert levels. Please review the Career Level Guide for more information on the various career levels.

Applicants in the **Technical Track** will participate in a **three-phase assessment process**.

Phase I: Online Assessment

Includes two assessments to evaluate your professional capabilities:

- **Work styles** inventory presents you with questions about your work-related interests and preferences.
- **Work simulation** presents you with realistic, work-related scenarios and asks you to respond to them.

No knowledge of DHS or cybersecurity is required for these assessments.

Remember! Assessment requires a computer with audio and reliable internet connection.

Phase II: Proctored Assessment

DHS Cybersecurity jobs are structured around cybersecurity specializations –called technical capabilities. There is a different assessment for each technical capability.

- In Phase II you will complete a Technical Capability Assessments which presents realistic, work-related cybersecurity scenarios and questions to assess your technical skills
- See the Appendix for more details and specific preparation tips.

Phase III: Advanced Technical Interview

- In Phase III you will complete an interview evaluated by DHS subject matter experts, designed to measure your level of deep technical expertise in your selected technical capability
- You will respond to a series of questions focused on your previous experience and hypothetical work situations or scenarios.
- Remember! Interview requires a computer, phone, or table with audio and reliable internet connection.

The average commitment is approximately **4 hours** (many applicants require less time!). You will have up to 2.5 hours to complete Phase I, 2.5 hours to complete Phase II, and 1 hour to complete Phase III.

DHS Cybersecurity Service Assessment Guide

Leadership Track

A cybersecurity professional who is interested in enhancing your management expertise and/or managing cybersecurity employees/organizations.

The Leadership Track covers three career levels ranging from full-working level to various expert levels. Please review the Career Level Guide for more information on the various career levels.

Applicants in the **Leadership Track** will participate in a **three-phase assessment process**.

Phase I: Online Assessment

Includes three assessments to evaluate your professional and leadership capabilities:

- **Work styles** inventory presents you with questions about your work-related interests and preferences.
- **Work simulation** presents you with realistic, work-related scenarios and asks you to respond to them.
- **Leadership simulation** presents you with realistic, work-related leadership scenarios and asks you to respond to them.

No knowledge of DHS or cybersecurity is required for these assessments.

Remember! Assessment requires a computer with audio and reliable internet connection.

Phase II: Proctored Assessment

DHS Cybersecurity jobs are structured around cybersecurity specializations –called technical capabilities. There is a different assessment for each technical capability.

- In Phase II you will complete a Technical Capability Assessments which presents realistic, work-related cybersecurity scenarios and questions to assess your technical skills
- See the Appendix for more details and specific preparation tips.

Phase III: Advanced Technical Interview

- In Phase III you will complete an interview evaluated by DHS subject matter experts, designed to measure your level of deep technical expertise in your selected technical capability
- You will respond to a series of questions focused on your previous experience and hypothetical work situations or scenarios.
- Interview requires a computer, phone, or table with audio and reliable internet connection.

The average commitment is approximately **4.5 hours** (many applicants require less time!). You will have up to 5 hours to complete Phase I, 2.5 hours to complete Phase II, and 1 hour to complete Phase III.

DHS Cybersecurity Service Assessment Guide

Executive Track

A cybersecurity executive with experience performing and leading work associated with a primary technical capability. Is interested in providing strategic mission leadership, guiding specific organizations—or all of DHS or groups of stakeholders—to deliver results.

The Executive Track covers two career levels. Please review the Career Level Guide for more information on the various career levels.

Applicants in the **Executive Track** will participate in a **three-phase assessment process**.

Phase I: Resume Review

- Phase I focuses on your cybersecurity work experience and leadership experience, including in the two positions you identify that most closely match the level of responsibility individuals have in Executive Track positions.
- You will answer initial questions and submit your resume.
- DHS will review your answers to initial questions about your expertise and experience as well as the resume you submit.

Phase II: Online Assessments

Phase II includes two assessments to evaluate your leadership capabilities:

- **Executive work simulation** presents you with realistic, work-related scenarios and asks you to respond to them.
- **Executive Situational Judgement Test** presents you with typical on-the-job scenarios and you evaluate viable options for handling them.

No knowledge of DHS or cybersecurity is required for these assessments. Remember! Assessment requires a computer with audio and reliable internet connection.

Phase III: Structured Interview

- Phase III includes an in person or online, live video interview with DHS subject matter expert(s) to discuss your cybersecurity career journey, including technical capability
- You will respond to work-related scenarios to assess your capability to lead technical cybersecurity talent and cybersecurity-focused organizations.

The average commitment is approximately **4 hours** (many applicants require less time!). Phase I takes approximately 10 minutes to complete, you have up to 3.5 hours to complete Phase II, and 1 hour to complete Phase III.

DHS Cybersecurity Service Assessment Guide

Frequently Asked Questions

1. **Can I complete all assessments for a career track at one time?**
   No - You must successfully complete each assessment in a phase to advance to the next phase.

2. **How will I know if I am moving on to the next phase?**
   After each phase, you will receive an email from DHS about the status of your application and any steps you need to take.

3. **What if I am unable to begin an online or proctored assessment or interview on time or need to reschedule?**
   Before starting each phase, you will receive instructions about the assessment for that phase and information about what to do if you need to reschedule or if something comes up. Please follow the instructions provided in the email.

4. **What should I do if I have a technical problem during an assessment?**
   In the event of a technical problem, please follow the instructions provided in the email for the assessment you are taking.

5. **How are the assessments scored? Who scores the assessments?**
   All assessments are scored using a standard set of scoring procedures. Most are scored by computer; interviews are scored by trained evaluators.

6. **Will I receive performance feedback on specific assessments, such as the online assessments, technical capability simulation, or interviews?**
   No – the only feedback you will receive will be concerning the status of your application, along with information about progression to the next phase and any required steps.

7. **Whom can I contact with questions about assessments (e.g., process, resources, trouble reserving space for a proctored assessment)?**
   Contact our talent team with questions.

DHS Cybersecurity Service Assessment Guide

Appendix

For Developmental, Technical, and Leadership Track Applicants

Technical Capability Assessments

The DHS Cybersecurity Service **Technical Capability Assessments** are proctored, online assessments designed to measure an applicant's technical expertise in one of the 16 CTMS technical capabilities. These assessments are designed to be highly challenging and were developed, reviewed, and tested by industry and DHS cybersecurity experts and are used to support hiring and selection decisions.

Content

- Applicants are presented with approximately 4-7 realistic, scenario-based modules that require application of cybersecurity knowledge and skills to core concepts and principles.
- Approximately 65-75 questions are asked, with some easy questions, some moderately challenging questions, and some very difficult questions.
- You may be asked to select the one best option, select multiple correct responses, rate the effectiveness of various actions, rank order information/solutions, and/or sort response options into different categories (see Sample Questions).

Duration

- Assessment times vary depending on the number of modules and questions within the assessment. Applicants have up to 2.5 hours and average 90 minutes to complete.

Scoring

- Points are given for each correct and partially correct answer. No points are deducted for incorrect responses. Overall scores determine advancement to the next phase of the assessment process.

DHS Cybersecurity Service Assessment Guide

How to Prepare for the Technical Capability Assessment

Preparation is key. Use the following steps to help develop a strategy to prepare for the Technical Capability Assessment.

1 Review

Review the definitions of the technical capability and underlying technical competencies.

2 Refresh

Look at **terms**, **concepts**, **processes**, **principles**, **standards**, and other information associated with the technical capability. Even easy items may be challenging if you have not reviewed this foundational information in a while.

- Identify other terms or concepts that you may have learned through your education or experience that are aligned to the technical capability.
- Think through how you may **apply** of the concepts, processes, principles, and standards associated with these terms.
  - What does the term mean when applied?
  - Are there different versions of that technical term?
  - How do they differ?
  - Are there any associated standards or industry guidelines for effective management of common situations involving that term?

3 Familiarize

Be prepared for different types of questions (see Sample Questions).

Note: actual Technical Capability Assessment questions may differ in content and in level of difficulty.

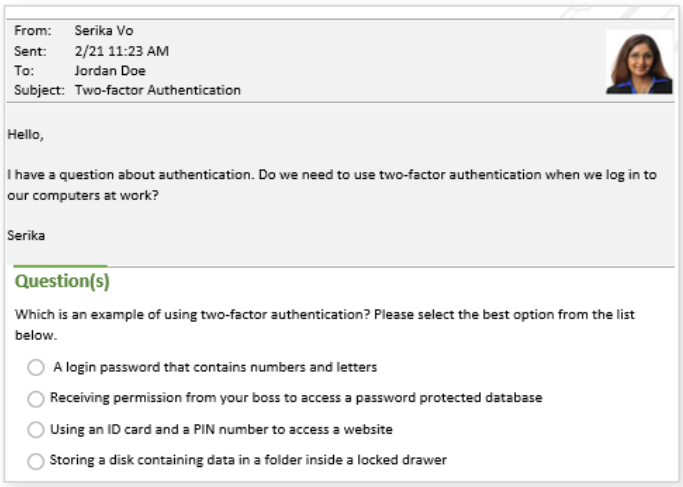
DHS Cybersecurity Service Assessment Guide

Technical Capability Assessment: Sample Questions

For each module, applicants are placed in a realistic, fictitious setting and asked to review emails, voicemails, texts, outputs, documents, etc. related to the scenario and apply their knowledge to answer the questions.

The screenshots below show a few of the types of questions that you may encounter in the Technical Capability Assessment.

Question Type: Select a Response



From: Serika Vo
Sent: 2/21 11:23 AM
To: Jordan Doe
Subject: Two-factor Authentication

Hello,

I have a question about authentication. Do we need to use two-factor authentication when we log in to our computers at work?

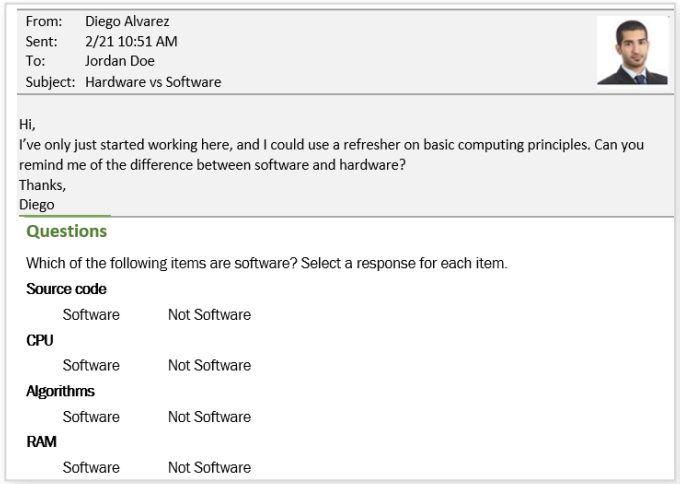
Serika

Question(s)

Which is an example of using two-factor authentication? Please select the best option from the list below.

- A login password that contains numbers and letters
- Receiving permission from your boss to access a password protected database
- Using an ID card and a PIN number to access a website
- Storing a disk containing data in a folder inside a locked drawer

Question Type: Select a Response



From: Diego Alvarez
Sent: 2/21 10:51 AM
To: Jordan Doe
Subject: Hardware vs Software

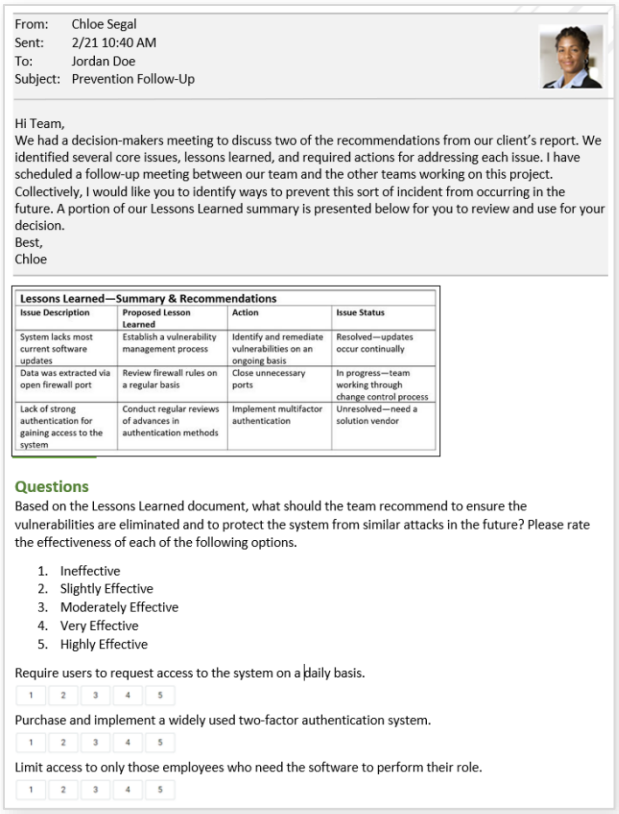
Hi,
I've only just started working here, and I could use a refresher on basic computing principles. Can you remind me of the difference between software and hardware?
Thanks,
Diego

Questions

Which of the following items are software? Select a response for each item.

Source code		
	Software	Not Software
CPU		
	Software	Not Software
Algorithms		
	Software	Not Software
RAM		
	Software	Not Software

Question Type: Rating Effectiveness



From: Chloe Segal
Sent: 2/21 10:40 AM
To: Jordan Doe
Subject: Prevention Follow-Up

Hi Team,
We had a decision-makers meeting to discuss two of the recommendations from our client's report. We identified several core issues, lessons learned, and required actions for addressing each issue. I have scheduled a follow-up meeting between our team and the other teams working on this project. Collectively, I would like you to identify ways to prevent this sort of incident from occurring in the future. A portion of our Lessons Learned summary is presented below for you to review and use for your decision.
Best,
Chloe

Lessons Learned—Summary & Recommendations

Issue Description	Proposed Lesson Learned	Action	Issue Status
System lacks most current software updates	Establish a vulnerability management process	Identify and remediate vulnerabilities on an ongoing basis	Resolved—updates occur continually
Data was extracted via open firewall port	Review firewall rules on a regular basis	Close unnecessary ports	In progress—team working through change control process
Lack of strong authentication for gaining access to the system	Conduct regular reviews of advances in authentication methods	Implement multifactor authentication	Unresolved—need a solution vendor

Questions

Based on the Lessons Learned document, what should the team recommend to ensure the vulnerabilities are eliminated and to protect the system from similar attacks in the future? Please rate the effectiveness of each of the following options.

1. Ineffective
2. Slightly Effective
3. Moderately Effective
4. Very Effective
5. Highly Effective

Require users to request access to the system on a daily basis.

1 2 3 4 5

Purchase and implement a widely used two-factor authentication system.

1 2 3 4 5

Limit access to only those employees who need the software to perform their role.

1 2 3 4 5

Example: Cybersecurity Threat Analysis

The following outlines how an applicant may apply the preparation tips for the Cybersecurity Threat Analysis Assessment. The steps outlined below are not an exhaustive representation of the full preparation required.

1 **Review** the capability and competency definitions (a partial definition of Cybersecurity Threat Analysis definition is below):

- Provides tactical/operational analysis, including attribution of **cyber actors** using a variety **of analytic techniques and tools**

2 **Refresh** your knowledge using the capability and competency definitions as a general guide, along with other knowledge you have gained from your technical education or experiences. For example, for Cybersecurity Threat Analysis, you might:

- Review the terms presented in the definition (e.g., cyber actor).
- Review the concepts presented in the definitions (e.g., analytic techniques and tools related to cybersecurity threat analysis).
- Review other terms, standards, concepts, and processes specific to the technical capability (e.g., industry standards or guidelines).
- Be ready to apply the terms, concepts, standards, and processes to a given situation.

3 **Familiarize** yourself with the sample questions provided in this Appendix to get a sense of the types of questions to expect. *Note: the sample questions are not specific to Cybersecurity Threat Analysis.*