Security+ SY0-601 Review

A STRUCTURED REVIEW

BRIAN FORD, COMPTIA SECURITY+, CYSA+, CASP+

Your Instructor: Brian Ford

Brian@fordsnotes.com

bford@comptia.global

https://linkedin.com/in/brford

@ccie2106

CompTIA Security+, CySA+, CASP+, and others…

CCIE #2106 (expired)

Certified Novell Instructor (CNI) Novell expired

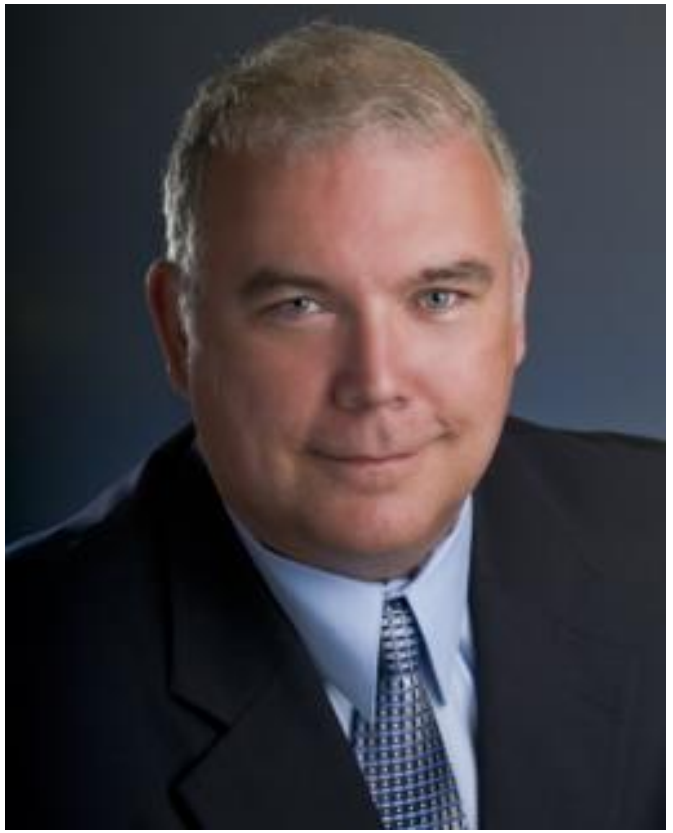
B.S. Computer Science, SUNY Stony Brook

M.S. Information Assurance, Norwich University

30+ years in IT, Networking, Internet Security

NIST National Initiative on Cybersecurity Education (NICE) Contributor

Member of the Cybersecurity Workforce Alliance



Agenda

- Introduction to Certification Exams
- SY0-601 Exam Objectives & Weighting
- Review of Objectives
  - Course Mapping Content from CertMaster
- Testing Tips
- What's Next

Introduction to Certification Exams

Who creates these exams?

- "CompTIA exams are built by the industry, for the industry."
- Who creates and maintains these exams:
  - Subject matter experts (SMEs)
    - Are used in focus groups, item writing sessions, and item review sessions.
    - CompTIA estimates that 5,000 subject matter expert hours are required to develop one exam.
  - Psychologist/Psychometrician
    - Assists the development, review and maintenance of the exam.
- CompTIA compiles data about each exam and each question

How are CompTIA exams scored?

- From the exam objectives we know that for the SY0-601 exam…
  - Number of questions: Maximum of 90
  - Type of Questions: Multiple-choice and performance-based
  - Length of test: 90 minutes
  - Passing score: 750 (on a scale of 100-900)
- The exam scoring system is not publicly disclosed anywhere.
- Exam score is insignificant.
  - Candidates should care whether they **passed** or **failed**.
  - Pass or fail the printed exam report provides detailed information on topics they got wrong.

Keywords from the Objectives

- Directly from the SY0-601 Exam Outline…
- Compare and contrast …
  - These questions are used to elicit a comparison or contrast response demonstrating an understanding of subtle differences or unexpected similarities between two subjects.
- Explain …
  - These questions are used to test understanding of concepts.
- Given a scenario …
  - Given a scenario, analyze
  - Given an incident, apply
  - Given an incident, utilize
  - These questions are used to describe how to respond or answer to a supposed situation.
- Summarize …
  - These questions test your understanding of main ideas and concepts.

Keywords: Compare and contrast

- Compare and contrast …
  - These questions are used to elicit a comparison or contrast response demonstrating an understanding of subtle differences or unexpected similarities between two subjects.
- Example:

Which of the following statements accurately compares and contrasts symmetric encryption and asymmetric encryption?

A) Symmetric encryption uses a single key for both encryption and decryption, while asymmetric encryption uses different keys for encryption and decryption.

B) Symmetric encryption is more secure than asymmetric encryption because it uses longer key lengths.

C) Symmetric encryption is suitable for secure key exchange, while asymmetric encryption is more efficient for bulk data encryption.

Keywords: Explain

- Explain …
  - These questions are used to test understanding of concepts.
- Example

Which of the following best explains the concept of a Security Information and Event Management (SIEM) system?

A) SIEM is a software tool used for vulnerability scanning and penetration testing.

B) SIEM is a network device that provides secure remote access to resources.

C) SIEM is a centralized platform that collects, correlates, and analyzes security events and logs from various sources.

Keywords: Given a scenario

- Given a scenario …
  - Given a scenario, analyze
  - Given an incident, apply
  - Given an incident, utilize
- These questions are used to describe how to respond or answer to a supposed situation.
  - Often there is a scenario presented.

Example Scenario

"Imagine you are a security analyst working for a financial institution. One of the employees received an email from what appears to be a trusted source, requesting sensitive financial information. The email includes a link that directs to a website asking for login credentials. Describe the steps you would take to analyze this situation, identify potential risks, and recommend appropriate actions to mitigate the threat.“

- This is an ‘analyze’ question.
- The subject is “a link that directs to a website asking for login credentials”.
- This question could be rephrased :Describe the steps to investigate this suspect website.

Given a scenario, analyze…

You are a security analyst conducting a risk assessment for a small company. During your assessment, you discover that the company's servers are located in an open and easily accessible area with no physical access controls. Which of the following risks is the company most vulnerable to?

A. Data exfiltration through network attacks
B. Insider threats and unauthorized access
C. Social engineering attacks targeting employees

Answer to ‘Given a scenario, analyze…’

Correct answer: B) Insider threats and unauthorized access

Option B, *insider threats and unauthorized access* is the most appropriate and specific risk associated with the given scenario. Unauthorized individuals could gain physical access to the servers, potentially compromising sensitive data, altering configurations, or performing other malicious activities.

Option A, *data exfiltration through network attacks* could be a risk if the servers were accessible remotely, but the scenario specifically mentions that the vulnerability lies in the physical access controls.

Option C, *social engineering attacks* targeting employees may be a concern but is not directly related to the lack of physical access controls to the servers.

Keywords: Summarize

- Summarize …
  - These questions test your understanding of main ideas and concepts.
- Example

Which of the following best summarizes the concept of social engineering?

A) Social engineering involves the unauthorized access and exploitation of computer networks and systems.

B) Social engineering refers to the use of psychological manipulation to deceive individuals and gain unauthorized access to sensitive information.

C) Social engineering is the practice of implementing security controls and measures to protect against unauthorized access attempts.

Exams use multiple choice questions

- **Multiple choice questions** are composed of one question with multiple possible answers, including the correct answer and several incorrect answers (**distractors**).
  - Multiple choice questions are often used to test student's knowledge of a broad range of content.
- A type of multiple-choice question might involve matching. Matching questions pair a definition with one of the choices provided.
  - These questions are often used to **assess recognition and recall** and so are most often used where acquisition of detailed knowledge is an important goal.

The “best answer”

- Nobody likes ‘trick questions’.
  - Questions are developed so that students who know the material can find the correct answer.
- Questions instruct students to select the “best answer” rather than the “correct answer.”
  - The idea is that there may be more than one ‘correct’ answer to the multiple-choice question, but one correct answer is better than the others.

Distractors

- Distractors are plausible but incorrect answers.
  - Some distractors are statements based on common student misconceptions
  - Distractors draw the test takers attention
- Example

Question: Which of the following is NOT a common type of authentication factor?

A) Something you know

B) Something you have

C) Something you are

D) Something you need

Note that these are correct answers if not for the NOT

This is the correct answer to the question.

Tips for answering scenario-based questions

- Read each question carefully to make sure you understand what the scenario is presenting and process all important information.
- Do not try to answer the questions prior to reading and understand the scenario.
- **Read all the choices before selecting your answer** and be sure to notice if it is asking you to choose one, two or three.
- Answer all of the questions.
  - If you don't know the answer (given 4 choices) you have a 25% chance of guessing correctly, and no points are deducted for incorrect answers.

Tips for answering scenario-based questions

- **Skip any questions you have difficulty answering and come back to them after reviewing** the other questions.
  - Sometimes completing other questions or re-reading the challenging question may give you a different perspective and help you to answer it.
- **Trust your instincts**. Once you have answered a question, don't change your answer unless you are certain that your first choice is wrong. *Research shows that most changed answers go from the correct choice to an incorrect one.*

Performance Based Questions (PBQs)

- PBQs are designed to test a candidate's ability to solve problems in real-world settings.
- PBQ Types
  - **Simulations** "are an approximation of an environment or tool, such as a firewall, network diagram, terminal window, or operating system. They typically have restricted system functionality but are designed to allow for multiple possible responses or paths."
  - **Virtual environments** "are virtual machines/systems running select operating systems and software in a production environment. Because they are full versions of the technology assessed by the exam item, all manner of incorrect steps or paths may be pursued."
  - Virtual PBQs require you use a **reset** to change answers. The **reset** takes the question back to starting state, erasing any selected or entered answers.

Performance Based Questions (PBQs)

- Simulation PBQs use multiple windows.
  - At the start of the question the top window will not cover the entire screen area.
  - There will be a larger, full screen window below.
- Simulation questions have a reset button, virtual PBQs do not.
  - Reset erases all the answers you selected for that question, going back to the starting state.
- You can skip simulation PBQs and return to them later, you cannot do the same with virtual PBQs!
- There can be multiple ways to solve a question or challenge posed in a PBQ.
- Partial credit may be given for answers in any PBQ.

SY0-601 Exam Objectives & Weighting

Security+ SY0-601 Exam Domains

1. Threats, Attacks, and Vulnerabilities
2. Architecture and Design
3. Implementation
4. Operations and Incident Response
5. Governance, Risk, and Compliance

SY0-601 Domain Weighting (% of Exam)

#	Domain	% of Exam
1	Threats, Attacks, and Vulnerabilities	24%
2	Architecture and Design	21%
3	Implementation	25%
4	Operations and Incident Response	16%
5	Governance, Risk, and Compliance	14%
	Total	100%

Review of Objectives

LINKING THE EXAM OBJECTIVES TO COMPTIA CERTMASTER CONTENT

1.0 Threats, Attacks, and Vulnerabilities (24%)

- Compare and contrast different types of social engineering techniques.
- Given a scenario, analyze potential indicators to determine the type of attack.
- Given a scenario, analyze potential indicators associated with application attacks.
- Given a scenario, analyze potential indicators associated with network attacks.
- Explain different threat actors, vectors, and intelligence sources.
- Explain the security concerns associated with various types of vulnerabilities.
- Summarize the techniques used in security assessments.
- Explain the techniques used in penetration testing.

Topics 1.1 – 1.3

- Compare and contrast different types of social engineering techniques.
  - Lesson 4 – Topic A
  - Lesson 4 – Social Engineering
- Given a scenario, analyze potential indicators to determine the type of attack.
  - Lesson 4 - Malware
  - Lesson 7 – Password attacks
  - Lesson 12 – Supply chain attacks and malicious USB
  - Lesson 21 - Card cloning & skimming
- Given a scenario, analyze potential indicators associated with application attacks.
  - Lesson 14 – Topics A & B
  - Lesson 14 – Cross site scripting, Request Forgery, Injection Attacks, Overflows

Question:

You are a security analyst monitoring the network of a large organization. After reviewing the logs, you notice the following activities:

1. An employee's account has multiple failed login attempts from different IP addresses within a short time frame.
2. The web server is receiving a significant number of requests from various IP addresses, all targeting the same URL.
3. A sudden spike in outbound network traffic is observed from a user's workstation to an unknown IP address.

Based on these observations, which of the following attacks are most likely occurring? Select all that apply.

A. Brute force attack on the employee's account
B. Distributed Denial of Service (DDoS) attack on the web server
C. Malware infection on the user's workstation
D. Phishing attack targeting the organization's employees
E. Man-in-the-Middle (MitM) attack on the network

The correct answers are:

A) Brute force attack on the employee's account,

B) Distributed Denial of Service (DDoS) attack on the web server, and

C) Malware infection on the user's workstation.

Explanation:

A brute force attack on the employee's account is indicated by multiple failed login attempts from different IP addresses. Attackers are trying to gain unauthorized access by systematically trying different login credentials.

A significant number of requests targeting the same URL from various IP addresses suggests a DDoS attack on the web server. The goal is to overwhelm the server with traffic, making it unavailable to legitimate users.

A sudden spike in outbound network traffic from a user's workstation to an unknown IP address indicates a potential malware infection. The workstation may be compromised and communicating with a command-and-control server or participating in malicious activities.

The wrong answers are:

D) Phishing attack targeting the organization's employees

E) Man-in-the-Middle (MitM) attack on the network are not supported by the given scenario. Although these attacks can occur, they are not specifically indicated by the provided activities.

Topics 1.4 – 1.6

- Given a scenario, analyze potential indicators associated with network attacks.
  - Lesson 9 – Layer 2 attacks (ARP, MAC attacks), Evil Twin Rogue Access Point
  - Lesson 11 - DoS, DDoS, DNS,
  - Lesson 13 – Bluetooth, RFID, Jamming
  - Lesson 14 – Bash shell & Powershell
- Explain different threat actors, vectors, and intelligence sources.
  - Lesson 2 - Topics A & B
  - Lesson 2 – Actors & threats, Attributes of Actors, Threat Vectors, Threat Intel Sources
- Explain the security concerns associated with various types of vulnerabilities.
  - Lesson 3 – Topic B
  - Lesson 3 – Threat Hunting & Vulnerability scans
  - Lesson 10 - Syslog

Question:

In a network environment, which of the following can be potential indicators of a Distributed Denial of Service (DDoS) attack? Select all that apply.

A. Sudden increase in network traffic volume
B. Unusual patterns of incoming and outgoing network connections
C. Inability to access critical network services or resources
D. Unauthorized modification or deletion of critical files
E. Presence of unfamiliar system processes or services consuming excessive resources

A DDoS attack aims to overwhelm a network, system, or service with a flood of traffic, resulting in disruption or denial of service. Several indicators can help identify a potential DDoS attack:

The correct answers:

A) Sudden increase in network traffic volume,

B) Unusual patterns of incoming and outgoing network connections, and

C) Inability to access critical network services or resources.

And the wrong answers are:

D) Unauthorized modification or deletion of critical files is not typically associated with DDoS attacks. Instead, it may indicate a different type of attack, such as a breach or data manipulation.

E) The presence of unfamiliar system processes or services consuming excessive resources may suggest a different type of attack or malware infection, but it is not directly indicative of a DDoS attack.

Topics 1.7 – 1.8

- Summarize the techniques used in security assessments.
  - Lesson 3 – Topic C
  - Lesson 3 – Threat Hunting, Vulnerability scans
  - Lesson 3 – CVSS, CVE
  - Lesson 10 – Syslog, SOAR
- Explain the techniques used in penetration testing.
  - Lesson 3 – Topic D
  - Lesson 3 – Known versus unknown environment, Rules of engagement, Privilege escalation
  - Lesson 3 – Footprinting, OSINT, Pivoting
  - Lesson 3 – Penetration testing, Reconnaissance, Red / Blue Teams, Exercise types

2.0 Architecture and Design (21%)

- Explain the importance of security concepts in an enterprise environment.
- Summarize virtualization and cloud computing concepts.
- Summarize secure application development, deployment, and automation concepts.
- Summarize authentication and authorization design concepts.
- Given a scenario, implement cybersecurity resilience.
- Explain the security implications of embedded and specialized systems.
- Explain the importance of physical security controls.
- Summarize the basics of cryptographic concepts.

Topics 2.1 - 2.3

- Explain the importance of security concepts in an enterprise environment.
  - Lesson 5 – Hashing
  - Lesson 11 – SSL / TLS, APIs
  - Lesson 16 – Data Protection & Sovereignty, Geographic considerations
  - Lesson 20 - Deception & Disruption, Site resiliency
- Summarize virtualization and cloud computing concepts.
  - Lesson 15 – Cloud models, Containers, Edge/Fog, SDN/SDV, Serverless, Virtualization
- Summarize secure application development, deployment, and automation concepts.
  - Lesson 14 – Automation/Scripting, Secure Coding, Agile/Waterfall, SDKs, Software diversity

Topics 2.4 – 2.6

- Summarize authentication and authorization design concepts.
  - Lesson 7 – Topics A, C, D
  - Lesson 7 – Authentication, Attestation, Federation, Smart Cards, MFA, AAA
- Given a scenario, implement cybersecurity resilience.
  - Lesson 20 - Topic A, B, C
  - Lesson 20 – RAID, multipath, NIC teaming, PDU
  - Lesson 20 – Backup types
  - Lesson 20 – Redundancy, Replication, Backups, Diversity
- Explain the security implications of embedded and specialized systems.
  - Lesson 12 – Topic C
  - Lesson 12 – Embedded Systems, SCADA and ICS, IoT, HVAC, SoC/RTOS, Constraints

Topics 2.7 – 2.8

- Explain the importance of physical security controls.
  - Lesson 21 topics A & B
  - Lesson 21 – Faraday cage, Bollards, Badges, Mantraps, Air Gap, Hot/Cold Aisles, Data Destruction
- Summarize the basics of cryptographic concepts.
  - Lesson 5 – Topics A, B, C, D
  - Lesson 5 - Ciphers, Keys, Asymmetric/Symmetric, Block/Stream, PFS, Nonce/Salting, Homomorphic & Lightweight crypto

3.0 Implementation (25%)

- Given a scenario, implement secure protocols.
- Given a scenario, implement host or application security solutions.
- Given a scenario, implement secure network designs.
- Given a scenario, install and configure wireless security settings.
- Given a scenario, implement secure mobile solutions.
- Given a scenario, apply cybersecurity solutions to the cloud.
- Given a scenario, implement identity and account management controls.
- Given a scenario, implement authentication and authorization solutions.
- Given a scenario, implement public key infrastructure.

Topics 3.1 – 3.3

- Given a scenario, implement secure protocols.
  - Lesson 9 – Routing & Switching
  - Lesson 11 – Protocols, DHCP, DNS/DNSSEC, SFTP/FTPS, POP3/IMAP/SMTP, SSL/TLS, IPSEC ESP/AH
- Given a scenario, implement host or application security solutions.
  - Lesson12 –Boot & Endpoint integrity, Hardening, FDE/SED, TPM, Sandboxing
  - Lesson 14 – Application security, HTTP Headers
  - Lesson 16 – Hashing, Salting, Tokenization
- Given a scenario, implement secure network designs.
  - Lesson 7 – Network Appliances
  - Lesson 9 – DNS, NAC,. Load balancing, Route security, Implications of IPv6
  - Lesson 10 – Firewalls, Proxy servers (forward/reverse)
  - Lesson 11 – VPNs, Jump Servers

Topics 3.4 – 3.6

- Given a scenario, install and configure wireless security settings.
  - Lesson 9 – Topic C
  - Lesson 9 – Wireless, Authentication, Crypto, Methods, Installation
- Given a scenario, implement secure mobile solutions.
  - Lesson 13 – Topics A & B
  - Lesson 13 – Mobile Devices, Deployment, Management, Policies, Monitoring, SEAndroid
- Given a scenario, apply cybersecurity solutions to the cloud.
  - Lesson 15 – Topic B
  - Lesson 15 –Cloud Security Controls, Compute, Storage, Network, CASB, Cloud native

Topics 3.7 – 3.9

- Given a scenario, implement identity and account management controls.
  - Lesson 8 - Topics A & B
  - Lesson 8 –Identity, IdP, Tokens, Accounts, Permissions, Lockout, Geofencing
- Given a scenario, implement authentication and authorization solutions.
  - Lesson 7 – Authentication management, Knowledge-based auth, , PAP/CHAP, SSO, SAML, OAuth/OpenID
  - Lesson 8 -MAC, DAC, ABAC, Role based Access, Rule-based Access
- Given a scenario, implement public key infrastructure.
  - Lesson 6 – Topics A & B
  - Lesson 6 – PKI, Certificates, Formats, CA/RA, Online/Offline, Stapling, Pinning, Escrow, Wildcards, OCSP/CRL

4.0 Operations and Incident Response (16%)

- Given a scenario, use the appropriate tool to assess organizational security.
- Summarize the importance of policies, processes, and procedures for incident response.
- Given an incident, utilize appropriate data sources to support an investigation.
- Given an incident, apply mitigation techniques or controls to secure an environment.
- Explain the key aspects of digital forensics.

Topic 4.1

- Given a scenario, use the appropriate tool to assess organizational security.
  - Lessons 3,4,6,7,8,10,11,14,18,21
  - Lesson 3 – Network Reconnaissance, arp, nslookup/dig, tracert/traceroute, ping/pathping, netstat, netcat, nmap
  - Lesson 3 (continues) – tcpdump, tcpreplay, Wireshark, pcap, Metasploit, Nessus, curl
  - Lesson 4 – Network Reconnaissance, Cuckoo sandbox
  - Lesson 6 – OpenSSL, Shells & scripts
  - Lesson 7 – Cain & Abel, Hashcat
  - Lesson 8 – chmod
  - Lesson 10 – cat, head, tail, grep
  - Lesson 11 – ssh
  - Lesson 18 – dd, .mem files, Autopsy, FTK imager
  - Lesson 21 - reidentification

Topic 4.2 – 4.3

- Summarize the importance of policies, processes, and procedures for incident response.
  - Lesson 17 – Topic A
  - Lesson 17 - Incident response plans, Disaster recovery plan, Business continuity plan, COOP, Stakeholder management
  - Lesson 17 – Cyber Kill Chain, MITRE ATT&CK, Diamond Model
- Given an incident, utilize appropriate data sources to support an investigation.
  - Lesson 17 – Topic B
  - Lesson 17- log files, vulnerability scans, dump files, SIEM, SIP,
  - Lesson 17 - syslog/Journalctl, Netflow//IPFIX/Sflow, metadata

Topics 4.4 – 4.5

- Given an incident, apply mitigation techniques or controls to secure an environment.
  - Lesson 17 – Topic C
  - Lesson 17 – SOAR, runbook, segmentation, containment, Firewall rules, ACLS/ACEs
  - Lesson 17 - Approved app list, blocklist, quarantine, tombstone
- Explain the key aspects of digital forensics.
  - Lesson 18 – Topics A & B
  - Lesson 18 – Evidence, chain of custody, Legal hold, Order of volatility, e-discovery

5.0 Governance, Risk, and Compliance (14%)

- Compare and contrast various types of controls.
- Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.
- Explain the importance of policies to organizational security.
- Summarize risk management processes and concepts.
- Explain privacy and sensitive data concepts in relation to security.

Topics 5.1 – 5.3

- Compare and contrast various types of controls.
  - Lesson 1 – Topic B
  - Lesson 1 – Control Categories, Control Types
- Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.
  - Lesson 1 –Topic B
  - Lesson 1 - Regulations, Standards, Benchmarks/Secure Config Guides
- Explain the importance of policies to organizational security.
  - Lesson 8 – Personnel, Job rotation, Separation of duties, Mandatory vacations
  - Lesson 12 – third party vendors, supply chain, SLA, MOU, BPA, EOL, EOS, EOSL
  - Lesson 16 – Secret, Top Secret, Governance, Retention
  - Lesson 20 – Change Control. Asset Management

Topics 5.4 – 5.5

- Summarize risk management processes and concepts.
  - Lesson 19 – Topics A & B
  - Lesson 19 – Risk, Risk Acceptance, Risk Avoidance, Risk Transference, Risk Register, Risk Appetite
  - Lesson 19 – Asset Value, SLE, ALE, ARO, Likelihood of Occurrence
  - Lesson 19 –Business Impact Analysis, RTO, RPO, MTTR, MTBF
- Explain privacy and sensitive data concepts in relation to security.
  - Lesson 16 – Topics A & B
  - Lesson 16 – Reputational damage, IP theft
  - Lesson 16 – Public, Confidential, Secret, Top Secret, Proprietary
  - Lesson 16 - Privacy Enhancing Technology, Masking, Tokenization, Anonymization

Scenario:

You are a security analyst working for a large corporation. An employee reports receiving an email with an attachment that claims to be an important document from the company's CEO. The email is unexpected, and the employee is unsure whether it is legitimate. The attachment is a Microsoft Word document named "Important_Message.docx." What should the employee do to ensure the security of the company's network and systems?

A. Immediately open the attachment to verify its contents and report any suspicious activity.
B. Forward the email to the IT department and wait for further instructions.
C. Open the attachment on a separate, isolated computer to assess its content.
D. Reply to the email, asking for additional verification or clarification before taking any further action.

Testing Tips

Scheduling your exam

- ✓Schedule your exam 10 days to 2 weeks before you plan to test.
  - ✓You can re-schedule up to the day before the exam
  - ✓You can change your exam date and time up to 24 hours before the appointment.
  - ✓You are allowed to change the appointment one time at no charge.
- ✓Take a day off after you schedule your exam. Relax.
- ✓The day after your day off spend time reviewing your notes.
  - ✓I suggest doing your own ‘structured review’.
- ✓Don’t take too many practice exams.
  - ✓If you continue taking the practice exam time after time you will memorize those questions and answers.
  - ✓This is a common test taker mistake. Don’t do that.

Where to Test?

Test at Testing Center

Find a Pearson Authorized Testing Center
- These are operated by other companies.
- Pearson and CompTIA define rules.

Plan your travel.
- Late due to traffic is not a valid excuse.
- There is a test window. If you are too late you forfeit.

Arrive 15-30 minutes early.
- There may be many other people testing.
- You may need to wait to sign in
- You may need to wait for a station to be available.

Test at home via On Vue

Before you schedule your exam:

Read the On Vue requirements carefully.

Test your system.
- Make sure your computer and peripherals meets all requirements.

Follow the On Vue instructions to the letter.
- Plan to install the software up to a day early.

Follow all Proctors' instructions.

At the Testing Center

- ✓Print out your Test Appointment confirmation email before you leave for the testing center.
  - ✓Or make sure that you can pull it up on your mobile device.
  - ✓Bring that with you.
- ✓At the testing center you need 2 forms of ID.
  - ✓One should be a government issued ID (Drivers License).
  - ✓One with a picture.
  - ✓The Admin will ask for your signature and take your picture.
- ✓Don’t bring anything else with you to a testing center.
  - ✓If you plan to arrive early leave your books / notes in your car (or don’t bring them).
- ✓Lock up your keys and phone.
  - ✓Lockers should be provided by the Testing Center.
- ✓Before going into the testing room, <u>always ask for a white board and marker for notes.</u>
  - ✓Or paper and pencil for notes
  - ✓You will need to erase / throw away when test completes
  - ✓Don’t try to smuggle anything out!

The Test Begins …

- ✓The test begins after you have sat down at a station and reviewed the CompTIA testing agreement.
  - ✓Sit down and relax.
  - ✓Be quiet.
  - ✓Get comfortable.
  - ✓Don’t look around the room.
  - ✓Before you touch the computer make sure that no one / no thing around you will distract you during the exam.
    - ✓If so, ask for a different seat.
  - ✓Review the testing agreement.
    - ✓The exam begins after you agree to the testing agreement.

What to do next?

If you passed the test…

Congratulations!

- You will receive an email from CompTIA usually with 48-72 hours at the email address you used to schedule the exam.
- Update your resume or profile at LinkedIn with your new certification.
- Register / Sign-in at Credy (https://credly.com) and download your certification badge.
  - Credly is now part of Pearson Vue
- Share the news with family, friends, and your employer.

If you didn’t pass the test…

Don’t Panic!

Your score report is very valuable.
- Don’t abuse or lose that report.

The score report will tell you what objectives & topics you scored poorly on.
- That should be an important part of your revised study plan.

Don’t re-test right away.
- I suggest giving yourself 7-10 days to review and study.
- Recall that you have CertMaster access for 1 year from date of purchase.
- More CertMaster Practice, More CertMaster PBQs, More CertMaster Labs

Maintaining your certification

Important: You maintain the highest certification in a stack!

Continuing Education Units (CEUs)

- You enter CEUs at the Certmetrics portal.
- CEUs are earned at a rate of 1 CEU for each hour spent on some activity.
- Activities can be learning, educating others (teaching), or mentoring.
- CEUs are audited
  - My experience has been that the audits are tough.
  - You must demonstrate how the activity relates back to specific topics in the objectives.
- CEUs can only be entered after you have paid your CE fee.

CertMaster CE

- You buy the CertMaster CE version of the course.
- You complete the exercises, labs and exam for the CertMaster CE course.
- Upon completion of the CertMaster CE course you are re-certified.
  - Download and print out your course completion certificate.
  - The CertMaster CE course records your completion.
  - You don't have to do anything else.
- This is the 'easy button'.

Other CompTIA Security Certifications

Will expand on what you learned in Security+. Think Security Analyst or SOC position. CySA+ stacks on top of Security+.

Updates your Security+, Net+, A+

Penetration tester or security consultant certification.

Updates your Security+, Net+, A+

Will expand on what you learned in Security+. Think SOC or Security Manager or leadership position. CASP+ stacks on CySA+, Pentest+, and Security+.

Updates your CySA+, Pentest+, Net+, A+

Vendor neutral Cloud and virtualization focused certifications. Cloud Essentials Introduces concepts used in AWS, Azure, and GCP. Cloud+ extends and deepens that knowledge and that includes (but is not all about) Security.

Does not update your Security+

Thanks for joining this webinar!

Keep in touch. Visit my website https://fordsnotes.com. Follow me on LinkedIn.