examundo

Examen de práctica CompTIA CySA+ en español

40 preguntas con respuestas. Las guías y las traducciones las hizo y las revisó un software. Ninguna persona las ha revisado todavía.

Actualizado el 25 de noviembre de 2026 · examundo.tech/es/comptia-cysa-plus/

Operaciones de seguridad

1. Un analista de inteligencia de amenazas necesita automatizar el intercambio de datos de indicadores de compromiso entre el SIEM de la organización y una comunidad externa de intercambio de información, en un formato estructurado y legible por máquinas. ¿Qué combinación de tecnologías cumple MEJOR este requisito?

A threat intelligence analyst needs to automate the exchange of indicator of compromise data between the organization's SIEM and an external information sharing community in a structured, machine-readable format. Which combination of technologies BEST supports this requirement?

A. YARA para la estructura de los datos y Snort para el transporte

B. OpenIOC para la estructura de los datos y SMTP para el transporte

C. STIX para la estructura de los datos y TAXII para el transporte

D. CVE para la estructura de los datos y RSS para el transporte

---

2. Un analista que revisa los registros de seguridad de Windows encuentra el Event ID 4698: un usuario sin privilegios de administrador creó una tarea programada poco después de abrir un archivo adjunto sospechoso de un correo. ¿Cuál es la técnica de MITRE ATT&CK que MÁS probablemente representa esta actividad?

An analyst reviewing Windows Security logs finds Event ID 4698 indicating a new scheduled task was created by a non-administrative user account shortly after a suspicious email attachment was opened. Which MITRE ATT&CK technique does this activity MOST likely represent?

A. T1055 – Process Injection

B. T1071 – Application Layer Protocol

C. T1003 – OS Credential Dumping

D. T1053 – Scheduled Task/Job

---

3. Según la escala estándar de severidad de syslog, ¿qué nivel indica la condición MÁS grave, que exige una acción correctiva inmediata?

According to the standard syslog severity scale, which level indicates the MOST severe condition, requiring immediate corrective action?

A. Warning (advertencia)

B. Notice (aviso)

C. Informational (informativo)

D. Emergency (emergencia)

---

4. Un escaneo de vulnerabilidades arroja dos hallazgos: CVE-2024-1111 con un puntaje base CVSS de 7.2 y sin explotación conocida, y CVE-2024-2222 con un puntaje base CVSS de 6.1 que aparece en el catálogo Known Exploited Vulnerabilities (KEV) de CISA. ¿Cuál hallazgo debe priorizar el analista para corregir PRIMERO?

A vulnerability scan identifies two findings: CVE-2024-1111 with a CVSS base score of 7.2 and no known exploitation, and CVE-2024-2222 with a CVSS base score of 6.1 that is listed on the CISA Known Exploited Vulnerabilities catalog. Which finding should the analyst prioritize for remediation FIRST?

A. CVE-2024-2222, porque la explotación activa aumenta el riesgo real sin importar el puntaje CVSS
B. Ambos por igual, porque CVSS ya incluye la probabilidad de explotación
C. Ninguno, hasta que el proveedor publique oficialmente un parche
D. CVE-2024-1111, porque su puntaje CVSS es más alto

---

5. Un analista de seguridad revisa datos de NetFlow y nota que una estación de trabajo inicia conexiones salientes a la misma IP externa cada 60 segundos; cada sesión dura menos de 2 segundos y lleva una carga (payload) de exactamente 512 bytes. ¿Cuál es la técnica que MÁS probablemente está observando el analista?

A security analyst reviews NetFlow data and notices a workstation initiating outbound connections to the same external IP every 60 seconds, each session lasting under 2 seconds with a payload of exactly 512 bytes. Which technique is the analyst MOST likely observing?

A. Transferencia de zona DNS
B. Beaconing de comando y control
C. Balanceo de carga de una aplicación web
D. Sincronización NTP legítima

---

6. Un atacante crea una macro maliciosa de Excel dentro de un archivo adjunto de correo, pensada para darle un punto de apoyo (foothold) cuando se abra, pero la fase en la que se ejecuta la carga útil (payload) aún no ha ocurrido. ¿Qué fase de la Cyber Kill Chain representa el archivo adjunto creado en sí?

An attacker crafts a malicious Excel macro embedded in an email attachment designed to establish a foothold when opened, but the phase in which the payload actually executes has not yet occurred. Which Cyber Kill Chain phase does the crafted attachment itself represent?

A. Weaponization (preparación del arma)
B. Exploitation (explotación)
C. Delivery (entrega)
D. Reconnaissance (reconocimiento)

---

7. Una alerta del SIEM muestra que un atacante usó una cuenta de servicio comprometida para crear una tarea programada que ejecuta un script malicioso cada vez que el sistema se reinicia. Según el marco MITRE ATT&CK, ¿con qué táctica se alinea MÁS esta actividad?

A SIEM alert shows that an attacker used a compromised service account to create a new scheduled task that executes a malicious script every time the system reboots. According to the MITRE ATT&CK framework, this activity MOST closely aligns with which tactic?

A. Persistence (persistencia)
B. Initial Access (acceso inicial)
C. Exfiltration (exfiltración)
D. Discovery (descubrimiento)

---

8. Un analista confirma que un adversario extrajo hashes de contraseñas NTLM de la memoria de LSASS y luego reutilizó esos hashes para autenticarse en otros equipos sin crackearlos. ¿Cómo se debe clasificar el paso de extracción de hashes en MITRE ATT&CK, a diferencia del paso de reutilización?

An analyst confirms that an adversary extracted NTLM password hashes from LSASS memory and later reused those hashes to authenticate to additional hosts without cracking them. How should the hash extraction step be classified within MITRE ATT&CK, as distinct from the reuse step?

A. La extracción corresponde a Credential Access (TA0006); la reutilización, a Lateral Movement (TA0008)

B. Ambos pasos corresponden a Credential Access (TA0006)

C. Ambos pasos corresponden a Lateral Movement (TA0008)

D. La extracción corresponde a Discovery (TA0007); la reutilización, a Defense Evasion (TA0005)

---

9. Un analista de un SOC empieza a buscar activamente señales de compromiso en el entorno a partir de una hipótesis, sin esperar a que se dispare una alerta automática. ¿Cuál de las siguientes opciones describe MEJOR esta actividad?

A SOC analyst begins actively searching the environment for signs of compromise based on a formulated hypothesis, without waiting for an automated alert to trigger. This activity is BEST described as which of the following?

A. Respuesta a incidentes (incident response)

B. Pruebas de penetración (penetration testing)

C. Caza de amenazas (threat hunting)

D. Escaneo de vulnerabilidades (vulnerability scanning)

---

10. Un actor de amenazas crea una tarea programada que ejecuta en silencio un script malicioso cada vez que el equipo comprometido se reinicia. ¿Con qué táctica de MITRE ATT&CK se alinea MEJOR esta técnica?

A threat actor creates a new scheduled task that silently executes a malicious script each time the compromised host reboots. Which MITRE ATT&CK tactic does this technique BEST align with?

A. Persistence (persistencia)

B. Initial Access (acceso inicial)

C. Privilege Escalation (escalada de privilegios)

D. Execution (ejecución)

Gestión de vulnerabilidades

11. Un analista de seguridad escanea una granja de servidores Windows y quiere identificar parches faltantes a nivel del registro de Windows (registry), en lugar de depender de la captura de banners (banner grabbing). ¿Qué configuración de escaneo debe usar?

A security analyst is scanning a Windows server farm and wants to identify missing patches at the registry level rather than relying on banner grabbing. Which scan configuration should the analyst use?

A. Escaneo perimetral externo

B. Escaneo pasivo

C. Escaneo sin credenciales (uncredentialed)

D. Escaneo con credenciales (credentialed)

---

12. El informe trimestral de escaneo externo de un ASV (Approved Scanning Vendor, proveedor de escaneo aprobado) de PCI DSS muestra un resultado aprobatorio a pesar de varias vulnerabilidades abiertas. ¿Qué condición explica que el resultado sea aprobatorio pese a esos hallazgos?

An organization's PCI DSS ASV (Approved Scanning Vendor) quarterly external scan report shows a passing result despite several open vulnerabilities. Which condition explains a passing ASV scan result despite these open findings?

A. La organización presentó una hoja de trabajo de controles compensatorios que cubre todos los hallazgos

B. Las vulnerabilidades quedan fuera del alcance del ASV cuando se etiquetan con severidad 'media'

C. Por política, los escaneos ASV solo evalúan hallazgos de severidad crítica y alta

D. Las vulnerabilidades con puntaje CVSS inferior a 4.0 no hacen fallar automáticamente un escaneo ASV

---

13. Durante la revisión de un escaneo de vulnerabilidades, un analista ve que el escáner reportó una falla crítica de inyección SQL en un servidor, pero una prueba manual confirma que la entrada está correctamente sanitizada. Este resultado del escaneo es un ejemplo de:

During a vulnerability scan review, an analyst finds that the scanner reported a critical SQL injection flaw on a server, but manual testing confirms the input is properly sanitized. This scan result is an example of a:

A. Falso negativo (false negative)

B. Hallazgo de día cero (zero-day)

C. Verdadero positivo (true positive)

D. Falso positivo (false positive)

---

14. Según CVSS v3.1, ¿en qué rango numérico se encuentra el puntaje base (Base Score) asignado a una vulnerabilidad?

According to CVSS v3.1, the Base Score assigned to a vulnerability falls within which numeric range?

A. 0.0-5.0

B. 0-100

C. 1-5

D. 0.0-10.0

---

15. ¿Qué técnica de escaneo de vulnerabilidades identifica debilidades monitoreando el tráfico de red existente, sin enviar sondeos a los sistemas objetivo?

Which vulnerability scanning technique identifies weaknesses by monitoring existing network traffic without sending probes to target systems?

A. Escaneo activo (active scanning)

B. Escaneo de cumplimiento (compliance scanning)

C. Escaneo con credenciales (credentialed scanning)

D. Escaneo pasivo (passive scanning)

---

16. Un SOC instala software ligero en cada equipo que informa de forma continua los datos de configuración y parches a una consola central, incluso cuando el dispositivo está fuera de la red corporativa. Esto describe:

A SOC deploys lightweight software on each endpoint that continuously reports configuration and patch data to a central console, even when the device is off the corporate network. This describes:

A. Escaneo basado en red (network-based scanning)

B. Escaneo pasivo (passive scanning)

C. Escaneo basado en agente (agent-based scanning)

D. Escaneo sin credenciales (uncredentialed scanning)

---

17. Una vulnerabilidad exige que el atacante gane una condición de carrera (race condition) que ocurre solo en una ventana de tiempo muy estrecha, y además requiere reconocimiento adicional de la configuración del objetivo antes de poder explotarla. ¿Qué valor de Attack Complexity de CVSS v3.1 refleja MEJOR esta vulnerabilidad?

A vulnerability requires an attacker to win a race condition that occurs only within a very narrow timing window and requires additional reconnaissance of the target's configuration before exploitation can succeed. Which CVSS v3.1 Attack Complexity value BEST reflects this vulnerability?

A. Attack Complexity: Low
B. Attack Complexity: Medium
C. Attack Complexity: None
D. Attack Complexity: High

---

18. ¿Qué métrica temporal de CVSS v3.1 refleja el estado actual de la sofisticación de la técnica de explotación o la disponibilidad de código de explotación público para una vulnerabilidad?

Which CVSS v3.1 temporal metric reflects the current state of exploit technique sophistication or public exploit code availability for a given vulnerability?

A. Exploit Code Maturity (E)
B. Remediation Level (RL)
C. Report Confidence (RC)
D. Attack Complexity (AC)

---

19. Una organización tiene muchas laptops de empleados remotos que se conectan por VPN desde fuera de la red corporativa, con un horario irregular. ¿Qué enfoque de escaneo de vulnerabilidades daría la cobertura MÁS constante de estos equipos?

An organization has a large population of remote employee laptops that frequently connect from outside the corporate network via VPN on an inconsistent schedule. Which vulnerability scanning approach would provide the MOST consistent coverage of these endpoints?

A. Escaneos manuales trimestrales programados durante las reuniones generales
B. Análisis pasivo del tráfico de red en el firewall perimetral
C. Escaneo basado en red lanzado solo desde el centro de datos interno
D. Escaneo basado en agente instalado localmente en cada laptop

---

20. Un escaneo de vulnerabilidades identifica el mismo CVE en dos servidores: uno aloja un sitio web público de marketing y el otro aloja la base de datos principal de pagos de los clientes de la organización. Ambos tienen el mismo puntaje base CVSS. ¿Qué factor debe influir MÁS al decidir cuál servidor se corrige primero?

A vulnerability scan identifies the same CVE on two servers: one hosting a public marketing website and another hosting the organization's primary customer payment database. Both servers have identical CVSS base scores. Which factor should MOST heavily influence which server is remediated first?

A. El servidor que se analizó primero en orden cronológico
B. El calendario predeterminado de parches del proveedor del sistema operativo
C. El orden en que aparecen las vulnerabilidades en el informe del escaneo
D. La criticidad del activo y el impacto en el negocio de la base de datos de pagos

---

Informes y comunicación

21. Una organización de salud confirma que una parte no autorizada accedió a ePHI no asegurada (unsecured) de 750 pacientes durante un incidente de ransomware. Según la HIPAA Breach Notification Rule, ¿en cuántos días desde el descubrimiento se debe notificar a las personas afectadas?

A healthcare organization confirms that unsecured ePHI belonging to 750 patients was accessed by an unauthorized party during a ransomware incident. Per the HIPAA Breach Notification Rule, within how many days of discovery must affected individuals be notified?

A. 14 días
B. 72 horas
C. 60 días
D. 30 días

---

22. ¿Qué lenguaje estructurado está diseñado para representar inteligencia de amenazas cibernéticas, incluidos patrones de ataque, campañas y relaciones entre objetos de amenaza, en un formato estándar y legible por máquinas para intercambiarla entre organizaciones?

Which structured language is designed to represent cyber threat intelligence, including attack patterns, campaigns, and relationships between threat objects, in a standardized, machine-readable format for exchange between organizations?

A. TAXII
B. STIX
C. YARA
D. OpenIOC

---

23. Durante un incidente activo, un analista confirma que un atacante exfiltró una base de datos con números de Seguro Social de clientes. Antes de emitir cualquier declaración pública, ¿qué parte interesada (stakeholder) DEBE participar para determinar las obligaciones de notificación regulatoria?

During an active incident, an analyst confirms that an attacker exfiltrated a database containing customer Social Security numbers. Before any public statement is released, which stakeholder MUST be engaged to determine regulatory notification obligations?

A. El equipo legal y de cumplimiento (compliance)
B. El personal de la mesa de ayuda (help desk)
C. El departamento de marketing
D. Un proveedor externo de pruebas de penetración

---

24. En un informe de incidente, un analista clasifica el comportamiento observado del atacante con MITRE ATT&CK. El informe dice que el adversario usó PowerShell (T1059.001) para ejecutar una carga útil tras obtener acceso inicial mediante un correo de phishing (T1566.001). ¿Qué elemento de ATT&CK representa 'T1059.001'?

During an incident report, an analyst maps observed attacker behavior to MITRE ATT&CK. The report states the adversary used PowerShell (T1059.001) to execute a payload after gaining initial access via a phishing email (T1566.001). Which ATT&CK element does 'T1059.001' represent?

A. Una técnica con una subtécnica asociada
B. Una táctica que describe el objetivo del adversario
C. Un identificador de campaña
D. Una fuente de datos usada para detección

---

25. Al redactar el informe del incidente, un analista escribe que el atacante usó 'Persistence' para mantener el acceso mediante una tarea programada. En la terminología de MITRE ATT&CK, ¿qué elemento del marco representa 'Persistence' en esta frase?

While drafting the incident report, an analyst writes that the attacker used 'Persistence' to maintain access via a scheduled task. In MITRE ATT&CK terminology, which element of the framework does 'Persistence' represent in this statement?

A. Técnica (technique)
B. Procedimiento (procedure)
C. Subtécnica (sub-technique)
D. Táctica (tactic)

---

26. Un analista de un SOC identifica un hash de archivo malicioso y una dirección IP externa sospechosa vinculados a una campaña de phishing reciente. ¿Qué término describe MEJOR estos artefactos?

A SOC analyst identifies a malicious file hash and a suspicious external IP address linked to a recent phishing campaign. Which term BEST describes these artifacts?

A. Tácticas, técnicas y procedimientos (TTP)
B. Datos de atribución del actor de amenazas
C. Firmas de vulnerabilidades
D. Indicadores de compromiso (IoC)

---

27. Un analista de seguridad descubre evidencia de que una brecha de datos expuso información personal de clientes. Antes de redactar cualquier declaración pública, ¿a qué parte interesada (stakeholder) DEBE asegurarse el analista de involucrar PRIMERO, según las mejores prácticas de comunicación de incidentes?

A security analyst discovers evidence that a data breach has exposed customer personal information. Before drafting any public statement, which stakeholder MUST the analyst ensure is engaged FIRST, according to incident communication best practices?

A. El asesor legal y el equipo de cumplimiento
B. Un proveedor externo de inteligencia de amenazas
C. El equipo de marketing en redes sociales
D. Todos los empleados, por correo a toda la empresa

---

28. Durante la investigación de un incidente, un analista confirma que un atacante obtuvo un punto de apoyo mediante un archivo adjunto de correo malicioso que abrió un empleado. Según el marco MITRE ATT&CK, ¿a qué táctica se debe asignar esta técnica en el informe del incidente?

During an incident investigation, an analyst confirms that an attacker gained a foothold through a malicious email attachment opened by an employee. According to the MITRE ATT&CK framework, which tactic should this technique be mapped to in the incident report?

A. Persistence (persistencia)
B. Initial Access (acceso inicial)
C. Execution (ejecución)
D. Exfiltration (exfiltración)

---

29. El gerente de un SOC revisa las métricas trimestrales y nota que los analistas dedican demasiado tiempo a clasificar (triage) alertas que al final no requieren ninguna acción. ¿Qué métrica se debe medir y reportar para cuantificar esta ineficiencia operativa?

A SOC manager reviewing quarterly reporting metrics notices that analysts are spending excessive time triaging alerts that ultimately require no action. Which metric should be tracked and reported to quantify this operational inefficiency?

A. Dwell time (tiempo de permanencia)
B. Puntaje de superficie de ataque (attack surface score)
C. Tasa de falsos positivos (false positive rate)
D. Tiempo medio de detección (mean time to detect)

---

30. Tras implementar en el SIEM reglas de correlación automáticas que marcan el movimiento lateral a los pocos minutos de ocurrir, el informe trimestral de métricas de un SOC muestra una mejora significativa. ¿En qué medición específica se refleja esa mejora, independientemente de cualquier cambio en el proceso de contención?

After implementing automated SIEM correlation rules that flag lateral movement within minutes of occurrence, a SOC's quarterly metrics report shows significant improvement in which specific measurement, independent of any change to the containment process?

A. Tiempo medio entre fallas (MTBF)
B. Tiempo medio de remediación (MTTR)
C. Tiempo medio de detección (MTTD)
D. Objetivo de punto de recuperación (RPO)

Respuesta a incidentes

31. Tras erradicar una infección de ransomware, el equipo de respuesta a incidentes revisa los registros del firewall, de la puerta de enlace de correo y de los endpoints, y determina que el malware entró por un correo de phishing que aprovechó una vulnerabilidad sin parchar en un lector de PDF. ¿Qué actividad representa esta revisión?

After eradicating a ransomware infection, an incident response team reviews firewall, email gateway, and endpoint logs and determines the malware entered through a phishing email that exploited an unpatched vulnerability in a PDF reader. Which activity does this review represent?

A. Reunión de lecciones aprendidas (lessons learned)
B. Caza de amenazas (threat hunting)
C. Análisis de causa raíz (root-cause analysis)
D. Escaneo de vulnerabilidades (vulnerability scanning)

32. Una organización de salud en EE. UU. confirma que un incidente resultó en acceso no autorizado a información de salud protegida (PHI) no asegurada (unsecured) de 800 pacientes. Según la HIPAA Breach Notification Rule, ¿en cuántos días desde el descubrimiento debe la organización notificar a las personas afectadas?

A U.S.-based healthcare organization confirms that an incident resulted in unauthorized access to unsecured protected health information (PHI) affecting 800 patients. Under the HIPAA Breach Notification Rule, within how many days of discovery must the organization notify affected individuals?

A. 72 horas
B. 60 días
C. 24 horas
D. 30 días

33. Un analista desconecta de la red una estación de trabajo infectada para evitar que el malware se propague mientras continúa la investigación. ¿De qué actividad de respuesta a incidentes es un ejemplo esta acción?

An analyst disables network connectivity to an infected workstation to prevent malware from spreading while the investigation continues. This action is an example of which incident response activity?

A. Lecciones aprendidas (lessons learned)
B. Contención (containment)
C. Erradicación (eradication)
D. Recuperación (recovery)

34. Según la guía NIST SP 800-61r2, ¿cuándo es ideal hacer la reunión de 'lecciones aprendidas' (lessons learned) después de resolver un incidente mayor?

Per NIST SP 800-61r2 guidance, when should the post-incident 'lessons learned' meeting ideally be held after resolution of a major incident?

A. Después de que termine el año fiscal
B. En pocos días, mientras los detalles aún están frescos
C. Inmediatamente, durante la fase de contención
D. Solo si hay un litigio

---

35. Durante la recolección de evidencia forense en un servidor comprometido, un analista debe capturar los datos según el orden de volatilidad (order of volatility). ¿Cuál de los siguientes se debe recolectar PRIMERO?

During forensic evidence collection at a compromised server, an analyst must capture data in order of volatility. Which of the following should be collected FIRST?

A. Registros (logs) archivados en cinta de respaldo
B. Documentación impresa de la configuración del sistema
C. Contenido de la memoria RAM del sistema
D. Datos almacenados en el disco duro

---

36. Tras eliminar el malware de un servidor infectado, el equipo restaura el sistema desde una copia de seguridad confiable (known-good backup) y lo monitorea de cerca para detectar señales de reinfección. ¿Qué fase describe esto?

After malware has been removed from an infected server, the team restores the system from a known-good backup and monitors it closely for signs of reinfection. This describes which phase?

A. Contención (containment)
B. Identificación (identification)
C. Preparación (preparation)
D. Recuperación (recovery)

---

37. Durante un incidente activo, un analista deshabilita una cuenta de servicio comprometida y bloquea en el firewall el dominio de C2 del atacante, pero aún no ha eliminado la webshell que quedó en el servidor comprometido. ¿Qué fase del ciclo de vida del incidente está en curso ACTUALMENTE y cuál NO ha comenzado todavía?

During an active incident, an analyst disables a compromised service account and blocks the attacker's C2 domain at the firewall, but has not yet removed the webshell dropped on the compromised server. Which phase of the incident lifecycle is CURRENTLY underway, and which phase has NOT yet begun?

A. La recuperación está en curso; las lecciones aprendidas aún no han comenzado
B. La identificación está en curso; la contención aún no ha comenzado
C. La erradicación está en curso; la recuperación aún no ha comenzado
D. La contención está en curso; la erradicación aún no ha comenzado

---

38. Un analista quiere determinar el dominio exacto de comando y control con el que se comunica una muestra de malware, sin arriesgar su ejecución en una red de producción ni en una red de laboratorio conectada a internet. ¿Qué enfoque de análisis cumple MEJOR este requisito?

An analyst wants to determine the exact command-and-control domain a malware sample contacts without risking execution on a production or internet-connected lab network. Which analysis approach BEST meets this requirement?

A. Análisis estático con un desensamblador para inspeccionar cadenas, importaciones e indicadores de red incrustados en el código

B. Análisis dinámico ejecutado directamente en el equipo infectado original de producción

C. Análisis dinámico en un sandbox conectado a internet para observar el tráfico de C2 en vivo

D. Análisis estático limitado a consultar la reputación del hash en fuentes de inteligencia de amenazas

---

39. Un analista de CySA+ identifica que se exfiltró información personal identificable (PII) de clientes durante una brecha confirmada. Según un plan de comunicación de respuesta a incidentes bien estructurado, ¿qué grupo de partes interesadas debe participar TEMPRANO para determinar las obligaciones legales y regulatorias de notificación?

A CySA+ analyst identifies that customer PII has been exfiltrated during a confirmed breach. According to a well-structured incident response communication plan, which stakeholder group should be engaged EARLY to determine legal and regulatory notification obligations?

A. Una agencia externa de relaciones públicas

B. El equipo legal y de cumplimiento

C. El departamento de marketing

D. Los usuarios finales del sistema afectado

---

40. Una organización de salud confirma que un incidente de ransomware resultó en acceso no autorizado a historiales de pacientes sin cifrar. ¿Qué parte interesada DEBE participar PRIMERO para determinar las obligaciones regulatorias de notificación de la brecha antes de cualquier divulgación pública?

A healthcare organization confirms that a ransomware incident resulted in unauthorized access to unencrypted patient records. Which stakeholder MUST be engaged FIRST to determine regulatory breach-notification obligations before any public disclosure occurs?

A. Los pacientes afectados, directamente

B. El asesor legal o el oficial de cumplimiento

C. El equipo de relaciones públicas de la organización

D. La aseguradora de ciberseguridad

Respuesta correcta

1. C STIX define el esquema estándar para describir datos de amenazas (indicadores, TTP, campañas) y TAXII los comparte entre plataformas con un transporte basado en API. YARA detecta patrones de malware y Snort es un motor de reglas de IDS. OpenIOC es un formato de indicadores sin transporte propio, y SMTP no sirve para el intercambio automatizado. CVE nombra vulnerabilidades, no indicadores, y RSS es un formato genérico sin estructura de inteligencia.

2. D El Event ID 4698 registra la creación de una tarea programada (scheduled task), que corresponde a la técnica T1053, muy usada para persistencia o ejecución tras el acceso inicial. T1055 se vería en eventos de procesos o memoria. T1003 implica acceder a credenciales, por ejemplo la memoria de LSASS. T1071 describe comunicación de C2 en la red, no la creación de una tarea.

3. D Según la RFC 5424, el nivel 0, Emergency, significa que el sistema es inutilizable y requiere atención inmediata: es la prioridad más alta. Warning (nivel 4) avisa de una condición que podría volverse un error. Notice (nivel 5) marca eventos normales pero importantes. Informational (nivel 6) solo registra mensajes de operación rutinaria.

4. A Estar en el catálogo KEV de CISA confirma que la vulnerabilidad se explota activamente, un riesgo real e inmediato que el puntaje base de CVSS no refleja, porque es más bien teórico. Priorizar solo por número ignora ese contexto. El puntaje base no pondera la explotación confirmada; eso lo hacen las métricas temporales o herramientas como EPSS. Esperar al parche ignora los controles compensatorios disponibles.

5. B Una periodicidad constante de intervalo corto con tamaño de carga fijo es típica del beaconing de C2, sobre todo con poco jitter; conviene revisar la IP de destino en inteligencia de amenazas y el historial de resolución DNS. NTP también es periódico, pero usa UDP 123 con paquetes pequeños de unos 48 a 90 bytes. Las transferencias de zona DNS son grandes y van por TCP. El tráfico de un balanceador depende de la demanda de los clientes, no de un reloj.

6. A En Weaponization el adversario une una carga de acceso remoto con un exploit o señuelo, por ejemplo una macro maliciosa en un documento de Excel, para crear un archivo listo para entregar; ocurre antes de enviarlo. Reconnaissance es investigar al objetivo, anterior a crear el artefacto. Delivery es enviar la carga al objetivo. Exploitation es activar la vulnerabilidad cuando la víctima abre el archivo, una fase posterior.

7. A Crear una tarea programada que sobreviva a un reinicio es una técnica de Persistence (T1053, Scheduled Task/Job), porque permite al adversario mantener su punto de apoyo tras reiniciar el sistema. Initial Access es cómo entró el atacante al entorno, algo que la alerta no describe. Exfiltration es sacar datos robados de la red. Discovery es explorar el entorno, por ejemplo enumerar usuarios o sistemas.

8. A OS Credential Dumping: LSASS Memory (T1003.001) pertenece a Credential Access porque obtiene material de autenticación. Pass the Hash (T1550.002) pertenece a Lateral Movement porque usa ese material para llegar a más sistemas. ATT&CK separa la fase de obtención de la fase de uso. Pass the Hash también se asocia con Defense Evasion, pero Discovery no describe ninguna de las dos acciones.

9. C La caza de amenazas es un proceso proactivo basado en hipótesis, en el que el analista busca actividad adversaria no detectada en lugar de reaccionar a una alerta. La respuesta a incidentes es reactiva: empieza cuando el incidente ya fue detectado o reportado. El escaneo de vulnerabilidades identifica debilidades conocidas y no prueba hipótesis de compromiso. Las pruebas de penetración simulan un ataque con alcance y reglas definidos, no buscan amenazas reales existentes.

10. A Scheduled Task/Job (T1053) es una técnica de Persistence porque hace que el código del atacante siga ejecutándose tras un reinicio, sin tener que volver a explotar el sistema. Privilege Escalation busca obtener más permisos, no mantener el acceso. Execution es correr código del atacante, algo que ocurre, pero el propósito principal de esta tarea es sobrevivir a los reinicios. Initial Access es la entrada inicial, que ya ocurrió.

11. D Un escaneo con credenciales se autentica en el equipo con una cuenta de administrador, así que el escáner puede consultar el registro de Windows, WMI o las versiones de archivos en lugar de deducir el nivel de parches por los banners, y es mucho más preciso. Sin credenciales solo se ve lo expuesto a la red (puertos, banners) y hay falsos negativos. El escaneo pasivo solo observa tráfico. El externo prueba el perímetro desde fuera y normalmente tampoco usa credenciales.

12. D La guía del programa PCI ASV fija en general el umbral de reprobación en un puntaje base CVSS de 4.0 o más. Por eso, las vulnerabilidades por debajo de 4.0 no hacen fallar el escaneo automáticamente, aunque ciertas condiciones de falla automática se aplican sin importar el puntaje. La etiqueta 'media' no excluye nada. Las hojas de controles compensatorios son para excepciones de requisitos de PCI DSS. El ASV evalúa todas las vulnerabilidades, no solo críticas y altas.

13. D Un falso positivo ocurre cuando el escáner marca una vulnerabilidad que en realidad no existe, como aquí, donde la validación manual muestra que la entrada está bien sanitizada. Un falso negativo sería una vulnerabilidad real que el escáner no detectó, el caso contrario. Un verdadero positivo es una falla real bien identificada, y esta quedó descartada. Un día cero es una falla desconocida y sin parche, ajena a la precisión del escáner.

14. D Los puntajes base de CVSS v3.1 van de 0.0 a 10.0, con severidad None (0.0), Low (0.1-3.9), Medium (4.0-6.9), High (7.0-8.9) y Critical (9.0-10.0). Una escala de 0 a 100 la usan algunas herramientas propietarias de riesgo, no CVSS. Un rango de 1 a 5 se parece a una matriz de riesgo cualitativa genérica. Limitar a 0.0-5.0 dejaría fuera las vulnerabilidades High y Critical, que sí existen.

15. D El escaneo pasivo examina el tráfico existente, como los banners de servicios y el comportamiento de los protocolos, para inferir vulnerabilidades sin generar paquetes; es discreto y seguro para entornos frágiles, como las redes ICS/SCADA. El activo envía sondeos a los equipos y puede causar interrupciones. El escaneo con credenciales se refiere al nivel de autenticación. El de cumplimiento compara configuraciones con una línea base.

16. C El escaneo basado en agente instala un agente pequeño en cada equipo que recopila y reporta datos de vulnerabilidades de forma continua, incluso en dispositivos remotos o móviles fuera del perímetro corporativo. Los escáneres de red, en cambio, necesitan alcanzar el dispositivo por la red. El escaneo pasivo solo observa tráfico y no informa el estado local. El escaneo sin credenciales describe la falta de acceso, no la arquitectura de despliegue.

17. D Attack Complexity: High (AC:H) se aplica cuando el éxito de la explotación depende de condiciones fuera del control del atacante, como ganar una condición de carrera en una ventana estrecha o requerir mucho reconocimiento específico del objetivo, tal como se describe. Attack Complexity: Low (AC:L) se aplica cuando no hay condiciones especiales y el ataque se repite con fiabilidad. None y Medium no son valores válidos en CVSS v3.1: la métrica solo define Low y High.

18. A La métrica temporal Exploit Code Maturity (E) mide si la explotación es teórica, de prueba de concepto, funcional o alta (ampliamente disponible o automatizada), es decir, qué tan fácil es aprovechar hoy la vulnerabilidad. Report Confidence mide la fiabilidad del reporte, y Remediation Level indica si hay una solución oficial, temporal o ninguna. Attack Complexity es una métrica base, no temporal, y describe condiciones fuera del control del atacante.

19. D Los escáneres basados en agente se ejecutan en el propio equipo y pueden reportar cuando el dispositivo tenga cualquier conexión a internet, esté o no en la VPN, así que cubren de forma confiable los activos remotos y móviles. El escaneo de red desde el centro de datos solo llega a equipos conectados a la red corporativa y pierde los que están apagados o fuera de la VPN. El tráfico pasivo no evalúa el SO ni los parches. Los escaneos manuales trimestrales dan cobertura escasa.

20. D La gestión de vulnerabilidades basada en riesgo pondera el impacto en el negocio y la criticidad del activo junto con la severidad CVSS. Una base de datos de pagos con datos financieros sensibles implica mucho más riesgo si se compromete que un sitio público de marketing, por eso la criticidad del activo es la mejor respuesta aunque el CVSS sea igual. Las otras opciones son criterios arbitrarios que ignoran las consecuencias reales y no se pueden defender en un programa maduro.

21. C La HIPAA Breach Notification Rule exige que las entidades cubiertas notifiquen a las personas afectadas sin demora injustificada y a más tardar 60 días calendario después de descubrir la brecha. Los 30 y 14 días no son el estándar de HIPAA. Las 72 horas corresponden a otros marcos, como el GDPR (72 horas para avisar a la autoridad supervisora), que no rige en este caso de salud en EE. UU.

22. B STIX (Structured Threat Information eXpression) define un esquema estándar basado en JSON para describir objetos de inteligencia, como indicadores, malware y campañas, de modo que distintas herramientas los entiendan igual. TAXII es el protocolo que transporta los datos STIX, no el formato. YARA es un lenguaje de reglas para identificar malware por patrones. OpenIOC es un esquema XML más antiguo, en gran parte reemplazado por STIX.

23. A El equipo legal y de cumplimiento determina las leyes de notificación de brechas aplicables, como leyes estatales o normas de la industria, y los plazos, antes de emitir cualquier comunicación. Así se evitan sanciones y se informa con exactitud. Marketing redacta mensajes externos solo después de la guía legal. La mesa de ayuda atiende a usuarios, no decide cuestiones regulatorias. Un proveedor de pruebas de penetración evalúa la seguridad, pero no interviene en la notificación.

24. A Los ID de ATT&CK siguen una jerarquía: las tácticas llevan un ID con prefijo TA (como TA0002) y son el objetivo del adversario (por ejemplo, Execution); las técnicas llevan prefijo T (como T1059); y las subtécnicas añaden un decimal, como T1059.001, PowerShell dentro de Command and Scripting Interpreter. Una táctica tendría un ID TA y describe el 'por qué', no el 'cómo'. Las campañas y fuentes de datos usan otros formatos (C0001, DS0009).

25. D En MITRE ATT&CK, una táctica es el objetivo del adversario, el 'por qué' de una acción; 'Persistence' es una columna de tácticas en la matriz. La tarea programada corresponde a una técnica como T1053, que describe el 'cómo'. Una subtécnica precisa el mecanismo exacto, como T1053.005 Scheduled Task. El procedimiento es la implementación concreta observada, como el comando o binario exacto, y es más específico que una técnica.

26. D Los indicadores de compromiso (IoC) son artefactos forenses, como hashes, IP, dominios y nombres de archivo, que dan evidencia de que un sistema o una red fue comprometido. Las TTP describen el comportamiento del adversario, no artefactos sueltos. La atribución identifica al responsable y exige más investigación. Las firmas de vulnerabilidades describen debilidades explotables. Los IoC se comparten por STIX/TAXII para detectar y bloquear.

27. A El equipo legal y de cumplimiento (compliance) determina las obligaciones de notificación, el momento de la divulgación y la responsabilidad legal antes de cualquier comunicado externo. Un proveedor de inteligencia ayuda en lo técnico, pero no con esas obligaciones. Marketing solo debe comunicar tras la revisión legal. Un correo a toda la empresa arriesga una divulgación prematura y rompe el principio de necesidad de conocer (need to know).

28. B Spearphishing Attachment (T1566.001) es una técnica de la táctica Initial Access (TA0001), que describe cómo entró por primera vez el adversario al entorno. Execution es correr código malicioso después de entrar, no el vector de entrada. Persistence es mantener el acceso una vez establecido el punto de apoyo, y Exfiltration es una fase tardía de robo de datos. Ninguna describe el mecanismo de entrega usado aquí.

29. C La tasa de falsos positivos cuantifica con qué frecuencia las alertas clasificadas resultan no requerir acción, justo la ineficiencia que el gerente quiere medir y reportar para justificar el ajuste de reglas de detección o de personal. El tiempo medio de detección mide la velocidad, no la precisión de las alertas. El dwell time mide cuánto tiempo permanece sin ser detectado un adversario. El puntaje de superficie de ataque refleja la exposición, no la eficiencia del triage.

30. C Las reglas de correlación automáticas que marcan antes el movimiento lateral reducen el tiempo entre que ocurre un evento y se descubre, que es lo que mide el MTTD, sin importar los pasos de respuesta posteriores. El MTTR mide el tiempo para remediar o contener un incidente ya detectado, y este cambio no lo alteró. El MTBF es una métrica de confiabilidad de sistemas. El RPO es la pérdida de datos máxima tolerable en recuperación ante desastres.

31. C El análisis de causa raíz rastrea un incidente hasta la vulnerabilidad, la mala configuración o el factor humano que lo permitió, justo lo que hizo el equipo al identificar el correo de phishing y el lector de PDF sin parchar. La caza de amenazas busca amenazas no detectadas. El escaneo de vulnerabilidades es técnico y automatizado. La reunión de lecciones aprendidas es una revisión más amplia, cuando la causa raíz ya se conoce.

32. B La HIPAA Breach Notification Rule exige que las entidades cubiertas notifiquen a las personas afectadas sin demora injustificada y a más tardar 60 días calendario después de descubrir la brecha. Las ventanas de 24 y 72 horas se confunden con el GDPR, que pide avisar a la autoridad supervisora en 72 horas tras tener conocimiento de la brecha, otro marco regulatorio. Los 30 días no son un umbral de HIPAA y no aparecen en la norma.

33. B La contención busca detener la propagación de una amenaza activa, preservar la evidencia y dar tiempo a la investigación; aislar una estación de trabajo de la red es una acción clásica de contención a corto plazo. La erradicación sería eliminar el malware y la causa raíz, la recuperación restablece las operaciones cuando la amenaza ya no está, y las lecciones aprendidas son una revisión posterior. Aquí el malware sigue presente y solo está aislado, por eso es contención.

34. B NIST recomienda hacer la reunión de lecciones aprendidas pocos días después de resolver el incidente, para que los participantes aún recuerden con exactitud los detalles, decisiones y tiempos, lo que mejora las recomendaciones. Hacerla durante la contención es prematuro, porque el incidente no está resuelto. Esperar al fin del año fiscal deteriora la memoria y retrasa las mejoras. Limitarla a casos con litigio ignora el valor de mejorar de forma continua.

35. C La RAM es la fuente de datos más volátil: su contenido, como los procesos en ejecución y las claves de cifrado, se pierde de inmediato al cortar la energía, por eso se captura primero. Los datos del disco duro persisten tras el apagado y pueden esperar. Los archivos en cinta de respaldo ya son estáticos y no volátiles. La documentación impresa no es evidencia volátil. Seguir el orden de volatilidad preserva primero lo más perecedero.

36. D La recuperación se centra en devolver los sistemas afectados a una operación normal y validada, a menudo desde copias limpias, y en monitorear de cerca para confirmar que la amenaza fue eliminada y no vuelve. La contención ocurre antes, para limitar la propagación mientras la amenaza sigue activa. La preparación es dejar todo listo antes de cualquier incidente. La identificación (detección y análisis) es descubrir y delimitar el incidente, no restaurar el servicio.

37. D Deshabilitar la cuenta y bloquear el dominio de C2 son acciones de contención: impiden que el atacante se comunique o avance. La webshell sigue en el equipo, y quitarla es erradicación, que aún no ocurre. Que quede un artefacto no prueba por sí solo que la erradicación no empezó, pero esta opción es la que mejor describe el caso. No es identificación, porque ya hay contención. La recuperación llega cuando la amenaza ya se erradicó.

38. A El análisis estático con un desensamblador examina el binario sin ejecutarlo y permite extraer dominios, IP e importaciones de API del código y de las cadenas, sin riesgo de ejecución. En un sandbox con internet, el malware puede comunicarse y alertar al atacante. Ejecutarlo en producción agrava el compromiso y daña la evidencia. La reputación del hash suele fallar con malware nuevo y no revela un dominio de C2 sin catalogar.

39. B El equipo legal y de cumplimiento (compliance) debe participar pronto porque determina los plazos de notificación, las normas aplicables (leyes estatales de brechas o GDPR) y las divulgaciones requeridas, y eso define la respuesta y la comunicación. Marketing maneja el tono del mensaje, no las obligaciones legales. Los usuarios finales reciben el aviso, no deciden. Una agencia de relaciones públicas puede ayudar después de que legal evalúe el caso.

40. B Legal y cumplimiento deben determinar primero si el incidente cumple los umbrales regulatorios de brecha (por ejemplo, la regla de 60 días de HIPAA para PHI no asegurada) y qué obligaciones aplican según la jurisdicción. Relaciones públicas redacta mensajes solo después. Avisar antes a los pacientes arriesga datos inexactos o un aviso que no cumpla la norma. A la aseguradora se le avisa según la póliza, pero no decide las obligaciones.

Palabras clave en inglés

indicator of compromise (IoC)	indicador de compromiso	Hash, IP, dominio o archivo que da evidencia de una intrusión.
threat intelligence	inteligencia de amenazas	Información sobre atacantes, campañas e indicadores que ayuda a detectar y bloquear.
threat hunting	caza de amenazas	Buscar atacantes ocultos a partir de una hipótesis, sin esperar una alerta.
SIEM	gestión de información y eventos de seguridad	Sistema que reúne y correlaciona registros y genera alertas.
SOC (security operations center)	centro de operaciones de seguridad	Equipo que vigila, revisa alertas y responde a incidentes.
triage	clasificación de alertas	Revisar alertas y decidir cuáles importan y en qué orden.
STIX	formato de inteligencia de amenazas (STIX)	Esquema estándar para describir indicadores, campañas y otros datos de amenazas.
TAXII	protocolo de intercambio (TAXII)	Protocolo que transporta datos STIX entre plataformas.
MITRE ATT&CK	marco MITRE ATT&CK	Marco que clasifica lo que hacen los atacantes en tácticas y técnicas.
tactic	táctica	El objetivo del atacante, el porqué; su código empieza con TA.
technique / sub-technique	técnica / subtécnica	El cómo del ataque; la subtécnica agrega un decimal al código T.
procedure	procedimiento	La implementación exacta observada, por ejemplo el comando o programa usado.

Cyber Kill Chain	cadena de ataque	Modelo que divide un ataque en fases, desde reconocimiento hasta acciones finales.
weaponization	preparación del arma	Fase en que se crea el archivo malicioso, antes de enviarlo.
foothold	punto de apoyo inicial	Primer acceso que el atacante logra y quiere conservar.
persistence	persistencia	Táctica para mantener el acceso, por ejemplo después de un reinicio.
credential dumping	extracción de credenciales	Sacar contraseñas o hashes del sistema, por ejemplo de la memoria LSASS.
pass the hash	uso de hash robado	Entrar a otros equipos con un hash robado, sin crackearlo.
lateral movement	movimiento lateral	Pasar de un equipo comprometido a otros de la red.
command and control (C2)	comando y control	Canal con el que el atacante dirige equipos comprometidos.
beaconing	balizamiento	Conexiones repetidas a intervalos regulares hacia un servidor de C2.
exfiltration	exfiltración	Sacar datos robados fuera de la red.
NetFlow	registros de flujo de red (NetFlow)	Datos de conexiones: origen, destino, duración y tamaño, útiles para ver patrones.
credentialed scan	escaneo con credenciales	Escaneo que inicia sesión en el equipo para revisar parches y configuración.
passive scanning	escaneo pasivo	Busca debilidades observando el tráfico, sin enviar sondas.
agent-based scanning	escaneo con agentes	Un programa pequeño en cada equipo reporta su estado a una consola.
banner grabbing	captura de banners	Leer el texto que muestra un servicio para deducir su versión.
false positive	falso positivo	Alerta o hallazgo de algo que en realidad no existe.
false negative	falso negativo	Falla real que la herramienta no detectó.
CVSS base score	puntaje base CVSS	Severidad técnica de una vulnerabilidad, de 0.0 a 10.0.
Known Exploited Vulnerabilities (KEV)	vulnerabilidades explotadas conocidas	Catálogo de CISA con fallas cuya explotación está confirmada.
remediation	remediación	Corregir la vulnerabilidad y verificar que ya no está.
compensating control	control compensatorio	Medida que reduce el riesgo cuando no se puede aplicar la corrección.

asset criticality	criticidad del activo	Qué tan importante es un sistema o dato para el negocio.
containment	contención	Limitar el avance y el daño de un incidente activo.
eradication	erradicación	Quitar el malware y la causa del incidente.
order of volatility	orden de volatilidad	Recoger primero la evidencia que se pierde más rápido, como la RAM.
root-cause analysis	análisis de causa raíz	Rastrear un incidente hasta la falla o el error que lo permitió.
mean time to detect (MTTD)	tiempo medio de detección	Promedio entre que ocurre un evento y se descubre.
breach notification	notificación de brecha	Aviso que la ley exige a las personas afectadas o a una autoridad.

Examundo es independiente. No está afiliado con los organismos que hacen estos exámenes ni tiene su aprobación. Las preguntas son originales, no son del examen real. examundo.tech/es/comptia-cysa-plus/