SCS-C03 · CHEAT SHEET · CERTIFYDECK

# AWS Certified Security - Specialty

Dominios, pesos oficiales y habilidades clave del temario de SCS-C03, para repasar antes del examen.

Nivel: Advanced (Professional) Duración: 170 min Nota de corte: 750/1000 Fuente: guía de estudio oficial de Microsoft Learn

## 1. Detection

16–16%

### Design and implement monitoring and alerting solutions for an AWS account or organization

- Los requisitos de supervisión dependen del tipo de carga: GuardDuty analiza sin configuración adicional CloudTrail, los registros de flujo de VPC y DNS, y se amplía con planes de protección según el recurso (RDS Protection para inicios de sesión en Aurora y RDS, Lambda Protection, EKS Protection y Runtime Monitoring para contenedores e instancias). Inspector, Macie y Security Hub CSPM cubren vulnerabilidades, datos confidenciales y controles.
- Route 53 ofrece comprobaciones de punto de enlace (HTTP, HTTPS, TCP y coincidencia de cadena), calculadas y basadas en alarmas de CloudWatch, útiles para instancias con solo IP privadas. El grupo de seguridad debe permitir los comprobadores con la lista de prefijos administrada, y las alarmas sobre su estado se crean en EE. UU. Este (Norte de Virginia). Los canaries de Synthetics simulan al cliente y detectan cambios no autorizados.
- Para centralizar eventos, Security Hub CSPM replica hallazgos y estados de controles a una región de origen, GuardDuty usa la misma cuenta de administrador delegado en cada región, un agregador de Config basado en la organización da una vista de solo lectura sin autorizaciones por cuenta y CloudWatch enlaza cuentas de origen con una de supervisión. EventBridge no reenvía a una tercera cuenta eventos recibidos de otra.
- Los filtros de métricas sobre los registros de CloudTrail en CloudWatch Logs, con alarmas y SNS, alertan de eventos como el uso del usuario raíz; los controles CIS exigen el patrón exacto. GuardDuty, Macie y Security Hub CSPM publican hallazgos en EventBridge, y una regla en la cuenta de administrador cubre a los miembros. La detección de anomalías de CloudWatch aprende patrones diarios y semanales.
- Un conjunto de conformidad agrupa reglas de AWS Config y acciones de corrección; desplegado para la organización llega a las cuentas nuevas y los miembros no pueden modificarlo, pero exige tener activa la grabación de Config. Config corrige con documentos de Automation, State Manager mantiene el estado de los nodos según una programación y la configuración central de Security Hub CSPM impone estándares en cuentas y regiones.

### Design and implement logging solutions

- Cada necesidad tiene su origen: los eventos de datos de CloudTrail (no activos por defecto) registran Invoke de Lambda y operaciones de objetos de S3, pero no las solicitudes con credenciales no válidas, que sí guardan los registros de acceso al servidor de S3. Los registros de consultas de Resolver guardan el DNS, los de flujo de Transit Gateway el tráfico de la puerta de enlace y AWS WAF exige destinos con prefijo aws-waf-logs-.
- Un trail de la organización, creado por la cuenta de administración o el administrador delegado, registra todas las cuentas sin que los miembros lo cambien; el aws:SourceArn de la política del bucket usa el ID de la cuenta de administración. El agente de CloudWatch necesita CloudWatchAgentServerPolicy y parámetros con prefijo AmazonCloudWatch-, API Gateway un cloudWatchRoleArn por región y la centralización de CloudWatch Logs copia lo nuevo.
- Security Lake centraliza en buckets de S3 de tu cuenta datos de AWS, SaaS, locales y de terceros, normalizados a OCSF en Apache Parquet. Los orígenes nativos no requieren configurar registros, salvo los eventos de administración, que exigen un trail de la organización multirregión. Los orígenes personalizados deben entregar OCSF en Parquet, y los suscriptores tienen acceso a datos (notificaciones) o de consulta (Athena) por origen.
- CloudWatch Logs Insights analiza registros en CloudWatch Logs con su lenguaje de consultas, OpenSearch PPL o SQL (con JOIN entre grupos de registros) y acelera las búsquedas con índices de campo. Athena consulta con SQL los registros de CloudTrail o de flujo en S3, y la proyección de particiones evita añadirlas a mano. Las conclusiones de Security Hub CSPM agrupan hallazgos de varios proveedores por atributo.
- Los transformadores de CloudWatch Logs normalizan los eventos durante la ingesta con plantillas para registros de AWS o analizadores Grok. Security Lake normaliza datos a OCSF en Parquet, OpenSearch Ingestion los indexa sin servidores y Security Analytics de OpenSearch aplica reglas Sigma con alertas. Managed Grafana combina varios orígenes de datos en un panel.

### Troubleshoot security monitoring, logging, and alerting solutions

- Lambda solo escribe registros si su rol de ejecución tiene logs:CreateLogGroup, CreateLogStream y PutLogEvents. API Gateway necesita un rol en cloudWatchRoleArn en cada región. Las comprobaciones de Route 53 requieren permitir la lista de prefijos route53-healthchecks, y el registro heredado de CloudFront necesita ACL habilitadas y una clave administrada por el cliente si se usa SSE-KMS.
- Si faltan registros del agente de CloudWatch: un i/o timeout en subredes privadas pide puntos de enlace de interfaz con DNS privado; tras editar la configuración hay que ejecutar fetch-config; sin log_group_name, el grupo se nombra con file_path. Los registros de flujo necesitan un rol que confíe en vpc-flow-logs.amazonaws.com, y CloudTrail necesita permisos en la política del bucket y de la clave KMS.

## 2. Incident Response

14–14%

### Design and test an incident response plan

- OpsCenter crea OpsItems a partir de eventos de EventBridge y alarmas de CloudWatch, evita duplicados con /aws/dedup y permite ejecutar runbooks de Automation desde cada OpsItem, también entre cuentas con un administrador delegado. Los manuales siguen las fases analizar, contener, erradicar y recuperar, y los cuadernos Jupyter de SageMaker AI sirven para investigar con acceso raíz desactivado y sin internet directo.
- Las cuentas forenses por región se crean antes del incidente. La integración proactiva de Shield Advanced exige comprobaciones de Route 53, y el SPET no lee buckets cifrados con KMS.
- AWS Config corrige automáticamente con runbooks de Systems Manager Automation y mientras AWSSupport-ContainEC2Instance contiene instancias de forma reversible, también en grupos de Auto Scaling. Revocar sesiones de un rol usa aws:TokenIssueTime. Step Functions orquesta respuestas con Retry y Catch, Automated Forensics Orchestrator captura memoria y disco, y el despliegue fuera de la zona de A. a aparta tráfico de una zona.

### Respond to security events

- En una instancia EC2 comprometida se adquiere, por este orden, los metadatos, las protecciones y etiquetas, las instantáneas de EBS y la memoria, siempre antes de aislarla o apagarla. Las pruebas se guardan en una cuenta forense. Instantáneas cifradas con clave administrada por el cliente, S3 Object Lock en modo de cumplimiento y registros de CloudTrail con validación de integridad.
- Para buscar en registros de S3 se usa Athena con proyección de particiones, para CloudWatch Logs, Logs Insights, que con la observabilidad entre cuentas consulta grupos de varias cuentas de una región. Security Lake normaliza orígenes de AWS y externos a OCSF en Parquet y los suscriptores con acceso de consulta usan Athena. La identidad de origen de STS permite atribuir acciones de roles compartidos.
- El análisis empieza por validar la alerta, sigue con el alcance y termina con el impacto en el negocio. En GuardDuty, Resource.role indica si se reutiliza el objeto, actor, los falsos positivos confirmados se archivan con reglas de supresión, que Extended Threat Detection no usa como señales. Los hallazgos de exposición de AWS Security Hub correlacionan señales y accesibilidad de red.
- La contención puede ser de origen, de técnicas y accesos o de destino. Cambiar un grupo de seguridad no corta las conexiones establecidas; una ACL de red sí, pero afecta a toda la subred. Las sesiones de un rol se revocan con AWSRevokeOlderSessions y AWSSupportContainEC2Instance aísla de forma reversible. La recuperación usa copias limpias anteriores al primer evento y se prueba.
- Amazon Detective crea un gráfico de comportamiento con CloudTrail, registros de flujo de VPC y hallazgos de GuardDuty mediante flujos propios, sin cambiar la configuración existente. Los grupos de hallazgos son el punto de partida del análisis de la causa raíz y Detective Investigation analiza roles y usuarios de IAM con indicadores de compromiso. La Resource Timeline de AWS Config muestra qué cambió y quién lo cambió.

## 3. Infrastructure Security

18–18%

### Design, implement, and troubleshoot security controls for network edge services

- Shield Advanced solo protege los recursos especificados (CloudFront, Route 53, Global Accelerator, IP elásticas, ALB y NLB mediante IP elásticas) y añade el SRT y protección de costes; Firewall Manager aplica la protección en toda la organización. Las comprobaciones de estado de Route 53 mejoran la detección y son necesarias para la intervención proactiva. Para bots evasivos y fraude se usa Bot Control dirigido, ATP y ACFP.
- Para que solo CloudFront llegue al ALB se usa una cabecera personalizada secreta exigida por el agente de escucha y la lista de prefijos administrada de CloudFront. Las políticas de cabeceras de respuesta añaden HSTS y otras cabeceras, con conjunto de reglas básico de CRS y el grupo de cuerpo de SQLi. CORS de S3 exige origen, método y cabeceras coincidentes, y las políticas de AWS IoT usan variables del objeto.
- Las restricciones geográficas de CloudFront actúan sobre toda la distribución con países. AWS WAF combina geo, IP y etiquetas de sesión, y limita la frecuencia agregan por IP de origen, clave personalizada como HTTPUser-Agent, con instrucciones de reducción de alcance. Las reglas JA3 y JA4 identifican la configuración TLS del cliente.

### Design, implement, and troubleshoot security controls for compute workloads

- EC2 Image Builder crea AMI con componentes STIG administrados por Amazon y componentes CIS de AWS Marketplace (solo en recetas de imagen, no de contenedor); el perfil de instancia necesita EC2InstanceProfile-ForImageBuilder y AmazonSSMManagedInstanceCore , y un script de limpieza elimina claves SSH y registros salvo que se reemplacen los datos de usuario sin crear perform_cleanup. Allowed AMIs por política declarativa, limita qué AMI se usan.
- Cada carga de trabajo recibe credenciales temporales de su propio rol: perfil de instancia en EC2, rol de ejecución en Lambda (confianza en lambda.amazonaws.com), rol de tarea para el código de ECS y rol de ejecución de tareas para descargar imágenes, registros y secretos, y EKS Pod Identity o IRSA para los pods. Para pasar un rol hace falta iam:PassRole, limitado por Resource e iam:PassedToService.
- Amazon Inspector analiza EC2 con SSM Agent y sin agente mediante instantáneas de EBS (modo híbrido) imágenes de ECR con el análisis mejorado (paquetes del sistema y de lenguajes) y Lambda con análisis estándar y de código. GuardDuty Runtime Monitoring detecta amenazas en ejecución en EKS, EC2 y ECS en Fargate con un agente gestionado; en Fargate es crítica que se descarga con el rol de ejecución de tareas.
- Patch Manager define el cumplimiento con líneas base de parches (reglas de aprobación, listas de parches rechazados, donde se revelan) y AWS-RunPatchBaseline analiza o instala. Una política de parches de Quick Setup cubre todas las cuentas y regiones de la organización. La validación confirma que se aplican las reglas de configuración de parches y el Amazon Inspector, que ofrece los hallazgos corregidos.

### Design and troubleshoot network security controls

- Los grupos de seguridad tienen estado, solo admiten reglas de permiso y pueden hacer referencia a otros grupos; las ACL de red no tienen estado, se aplican a la subred y evalúan las reglas desde el número más bajo, y decide la primera coincidencia. AWS Network Firewall filtra el tráfico que las tablas de rutas envían a sus puntos de enlace, con reglas sin estado (Pass, Drop, Forward to sfe) y con estado, como las listas de dominios permitidos.
- Direct Connect no cifra. AWS Site-to-Site VPN cifra en capa 3 sobre internet y MACsec en capa 2 entre router y dispositivo de Direct Connect en conexiones dedicadas. Para las objetos) con modo estricto, como la tabla de claves de un proveedor de identidad (IAM Identity Center o un IdP OIDC) y de proveedores de dispositivos como Jamf o CrowdStrike con política de firma se delega todo. Los puntos de enlace privados pueden ser balanceadores y demás, interfaces de red, CDN o KMS, y cada uno, la inspección este oeste y OCSF.
- Una subred aislada no tiene rutas fuera de su VPC. Las tablas de rutas separadas de Transit Gateway aíslan necesita el modo de dispersión para que el tráfico sea simétrico. Las ACL de red de enlaces por subred, los grupos de seguridad solo permiten y DNS Firewall filtra las consultas a Resolver.
- Network Access Analyzer hace un análisis estático de la configuración y devuelve como hallazgos las rutas que incluyen MatchPaths y no ExcludePaths, por ejemplo, tráfico de internet que evita un cortafuegos. Amazon Inspector genera periódicamente hallazgos de accesibilidad de red, solo para instancias EC2. Verified Access sustituye el acceso de red amplio de una VPN por acceso por aplicación evaluado en cada solicitud.

## 4. Identity and Access Management

20–20%

### Design, implement, and troubleshoot authentication strategies

- IAM Identity Center centraliza el acceso de los empleados a todas las cuentas con un IdP externo (SAML y SCIM) o con Active Directory; con IdP externo la MFA la administra el IdP. Cognito separa los grupos de usuarios (directorio y tokens) de los grupos de identidades (credenciales temporales por rol, también para invitados). IAM Roles Anywhere da credenciales temporales a servidores externos con certificados X.509.
- AWS STS emite credenciales temporales con AssumeRole, AssumeRoleWithSAML, AssumeRoleWithWebIdentity o GetSessionToken; el ID externo evita el suplente confuso, las políticas de sesión solo restringen y la identidad de origen persiste en el encadenamiento de roles. Una URL prefirmada de S3 caduca cuando caducan las credenciales que la firmaron, y s3:signatureAge limita su antigüedad.
- UnAccessDenied en AssumeRole suele deberse a que la política de confianza no incluye a quien llama o a que falta sts:TagSession o sts:SetSourceIdentity. En IAM Identity Center el usuario debe existir antes de iniciar sesión y el nameID debe coincidir con su nombre de usuario. AD Connector necesita los puertos 88 y 389 y una cuenta de servicio válida, y CloudTrail enmascara los nombres de usuario incorrectos.

### Design, implement, and troubleshoot authorization strategies

- Amazon Verified Permissions autoriza dentro de aplicaciones propias con políticas Cedar, e IAM Roles Anywhere da credenciales temporales a cargas fuera de AWS a cambio de certificados X.509 de una CA registrada. El acceso entre cuentas exige un permiso en la política de recursos o de confianza y otro en la política de identidad del llamante; sts:ExternalId y aws:SourceAccount evitan el suplente confuso.
- ABAC concede permisos cuando las etiquetas del principal coinciden con las del recurso, de modo que los recursos y proyectos nuevos no exigen editar políticas, a diferencia del RBAC por función. Se usan aws:ResourceTag, aws:RequestTag, aws:TagKeys y aws:PrincipalTag; IAM Identity Center y los IdP SAML envían atributos como etiquetas de sesión, y hay que proteger con Deny las claves de etiqueta que deciden el acceso.
- Un límite de permisos fija el máximo que las políticas de identidad pueden conceder a un usuario o rol, y una política de sesión limita una sola sesión temporal; los permisos efectivos son la intersección y ninguno concede nada. Para delegar la creación de roles se exige iam:PermissionsBoundary y se deniega cambiar o quitar el límite; la generación de políticas de IAM Access Analyzer parte de CloudTrail, pero no incluye iam:PassRole.
- El mensaje de acceso denegado distingue la denegación explícita (with an explicit deny) de la implícita (because no identity-based allows) e indica el tipo de política que hay que corregir. El simulador de políticas de IAM prueba políticas de identidad, límites, SCP y políticas de recursos aportadas sin solicitudes reales, pero no admite RCP; la validación de IAM Access Analyzer detecta errores antes de desplegar.
- IAM Access Analyzer detecta acceso no deseado con analizadores de acceso externo (recursos compartidos fuera de la zona de confianza, uno por región), interno (principales de la organización que llegan a recursos críticos) y no utilizado (roles, claves y permisos sin uso). Se corrige editando la política que concede el acceso; las reglas de archivo solo ocultan lo intencionado, y tras cambiar una RCP conviene volver a analizar el recurso.

## 5. Data Protection

18–18%

### Design and implement controls for data in transit

- Para exigir cifrado en tránsito se elige la política de seguridad del agente de escucha de ELB (los ALB no admiten políticas personalizadas) y se impone en la organización con la clave elasticloadbalancing:SecurityPolicy en SCP. En S3 se deniega con aws:SecureTransport en false; en CloudFront se usan las políticas de protocolo del espectador y del origen, y en API Gateway se desactiva el punto execute-api.
- Los puntos de enlace de puerta de enlace solo sirven a S3 y DynamoDB, no se cobran y no admiten acceso desde el entorno local; los de interfaz (PrivateLink) usan IP privadas y sí lo admiten. aws:SourceVpce en la política del bucket limita el acceso a un punto de enlace. Client VPN da acceso de red con cliente OpenVPN; Verified Access, acceso a aplicaciones sin VPN evaluando identidad y dispositivo.
- Algunos tipos de instancia Nitro cifran automáticamente el tráfico entre instancias de la misma VPC o de VPC emparejadas si no hay balanceador ni puerta de enlace de tránsito en medio. En EMR, el cifrado en tránsito se activa en una configuración de seguridad reutilizable con certificados (clave privada sin frase de contraseña). SageMaker cifra el tráfico entre contenedores con EnableInterContainerTrafficEncryption y reglas UDP 500 y ESP 50.

### Design and implement controls for data at rest

- S3 ofrece cuatro tipos de cifrado del servidor: SSE-S3 (predeterminado), SSE-KMS (control de la clave y auditoría en CloudTrail), DSSE-KMS (dos capas) y SSE-C (clave en cada solicitud). Las S3 Bucket Keys reducen las llamadas a KMS, no sirven con DSSE-KMS ni con objetos existentes sin copiarlos. El cifrado del lado del cliente evita que AWS vea el texto plano; un almacén de claves de CloudHSM da HSM de un solo inquilino con integración de KMS.
- S3 Object Lock en modo de cumplimiento impide a cualquier usuario, incluido el raíz, borrar o acortar la retención; el modo de gobierno se omite con s3:BypassGovernanceRetention. MFA delete solo lo activa el propietario raíz por CLI o API. La firma de código de Lambda con Enforce bloquea despliegues sin firmar. La validación de archivos de CloudTrail usa archivos de resumen firmados y validate-logs.
- S3 Lifecycle funciona con Object Lock, pero no borra versiones bloqueadas, y el bloqueo se mantiene en las transiciones. NoncurrentVersionExpiration con NewerNoncurrentVersions conserva las versiones recientes y borra los antiguos. Las políticas de ciclo de vida de EFS pasan archivos a IA y Archive y pueden devolverlos a Standard al primer acceso. En FSx for Lustre la retención automática es 0 días por defecto y las copias manuales no caducan.
- AWS Backup Vault Lock en modo de cumplimiento se vuelve inmutable al terminar el período de gracia; el modo de gobierno se puede quitar con permisos de IAM. Un almacén aislado lógicamente lleva ese bloqueo y se comparte con RAM, incluso fuera de la organización. Las copias entre cuentas exigen la misma organización y claves administradas por el cliente compartidas. DataSync evita internet con un punto de enlace de VPC.

### Design and implement controls to protect confidential data, credentials, secrets, and cryptographic key materials

- Secrets Manager rota secretos con rotación administrada (por ejemplo, la contraseña maestra de RDS con ManageMasterUserPassword) o con una función Lambda que sigue createSecret, setSecret, testSecret y finishSecret. La estrategia de usuarios alternos da credenciales válidas durante la rotación. Sin internet, la función necesita un punto de enlace de VPC. El acceso entre cuentas exige política de recursos y una clave administrada por el cliente.
- El material importado puede caducar, se renueva reimportando el mismo material con nueva clave de encapsulamiento y token, si caduca o se borra, la clave pasa a PendingImport. Las claves simétricas EXTERNAL rotan bajo demanda importando con NEW_KEY_MATERIAL y llamando a RotateKeyOnDemand; en multirregión, primero en la principal. Un almacén externo (XKS) usa un proxy propio, por internet o con un servicio de punto de enlace de VPC.
- Con material generado por AWS KMS, el servicio asume la durabilidad y admite rotación automática; el material nunca sale sin cifrar de sus HSM. Con material importado (origen EXTERNAL), el cliente responde de la durabilidad y guarda la copia original, puede fijar caducidad o borrarlo y reimportarlo, y solo hay rotación bajo demanda. El material importado no se puede exportar y sirve también para claves asimétricas y HMAC interoperables.
- Las políticas de protección de datos de CloudWatch Logs auditan y enmascaran datos confidenciales con identificadores administrados o personalizados (regex), por grupo o para toda la cuenta, incluidos los grupos futuros. El enmascaramiento ocurre en la ingesta, no es retroactivo, y solo quien tiene logs:Unmask ve los valores originales. Para prompts y respuestas de Bedrock se usan los filtros de información confidencial de Guardrails.
- Las claves multirregión de KMS comparten ID y material de claves entre Regiones y permiten cifrar en una y descifrar en otra sin llamadas entre Regiones; no se puede convertir una clave existente, la rotación se gestiona en la primaria y el material importado debe importarse en cada réplica. AWS Private CA es regional, se comparte entre cuentas con AWS RAM y conviene una jerarquía con raíz protegida y CA subordinadas emisoras.

## 6. Security Foundations and Governance

14–14%

### Develop a strategy to centrally deploy and manage AWS accounts

- AWS Organizations debe usar el conjunto de todas las funciones para tener SCP, RCP e integraciones de servicios; al migrar desde facturación unificada, las cuentas invitadas deben aceptar. Las cargas no deben estar en la cuenta de administración, a la que no afectan las SCP, y conviene una SCP que impida abandonar la organización. Las OU recomendadas incluyen Security, Infrastructure, Workloads, Sandbox, Suspended y Policy Staging.
- AWS Control Tower gobierna OU y cuentas con controles preventivos (SCP, RCP y políticas declarativas), de detección (reglas de AWS Config) y proactivos (hooks de CloudFormation antes del aprovisionamiento). Las cuentas existentes se incorporan registrando su OU o inscribiéndolas, sin recursos previos de AWS Config. Customizations for AWS Control Tower (CfCT) despliega plantillas, SCP y RCP propias en las cuentas que crea Account Factory.
- Las SCP fijan el máximo de permisos de las entidades de las cuentas miembro y las RCP el de sus recursos, también frente a identidades externas; ninguna concede permisos ni afecta a la cuenta de administración. Las políticas declarativas imponen una configuración de referencia de servicios como EC2 en el plano de control. Las políticas de exclusión de IA impiden que AWS use el contenido para mejorar sus servicios de IA.
- Los servicios de seguridad como GuardDuty, Security Hub CSPM, Macie, Inspector y AWS Config se administran desde una cuenta miembro designada como administrador delegado, no desde la cuenta de administración. GuardDuty e Inspector son regionales y exigen el mismo administrador en todas las Regiones; Security Hub CSPM ofrece la configuración central con políticas. Las SCP también se aplican a las cuentas de administrador delegado.
- Con el acceso raíz centralizado, la cuenta de administración o el administrador delegado de IAM eliminan las credenciales raíz de las cuentas miembro y realizan tareas privilegiadas con sesiones cortas de sts:AssumeRoot limitadas por una política de tarea. El usuario raíz de la cuenta de administración debe tener MFA, mejor con varios dispositivos, sin claves de acceso y con custodia repartida entre dos grupos para el acceso de emergencia.

### Implement a secure and consistent deployment strategy for cloud resources

- CloudFormation StackSets con permisos administrados por el servicio despliega plantillas en OU y cuentas de AWS Organizations, crea los roles necesarios y añade automáticamente las cuentas nuevas, pero no despliega en la cuenta de administración. CloudFormation Guard valida plantillas y JSON de Terraform con reglas de política como código y, como Guard Hook, bloquea recursos antes de crearlos; cfn-lint revisa sintaxis y propiedades.
- Las etiquetas (clave y valor, con distinción de mayúsculas) organizan los recursos por departamento, centro de costes o entorno. Las políticas de etiquetas estandarizan claves y valores y pueden bloquear valores no conformes, pero no evalúan recursos sin etiquetar; para exigir etiquetas se usan SCP o claves obligatorias para IaC. Los grupos basados en etiquetas son regionales, y Systems Manager actúa sobre destinos por etiqueta.
- AWS Firewall Manager aplica de forma centralizada políticas de AWS WAF, Shield Advanced, grupos de seguridad, ACL de red, Network Firewall y DNS Firewall a la organización o a cuentas, OU y recursos etiquetados, y cubre automáticamente los recursos nuevos. Requiere AWS Organizations con todas las características, una cuenta de administrador, AWS Config con registro continuo y, para Network Firewall y DNS Firewall, uso compartido con AWS RAM.
- AWS RAM comparte un recurso creado una vez con cuentas, OU o toda la organización; tras activar el uso compartido desde la cuenta de administración no hay invitaciones, y el permiso administrado del recurso compartido es el máximo que las cuentas consumidoras conceden con políticas de IAM. AWS Service Catalog comparte carteras como referencia sincronizada y usa restricciones de lanzamiento con un rol para aprovisionar sin dar permisos directos.

### Evaluate the compliance of AWS resources

- Las reglas de AWS Config evalúan recursos en modo de detección o proactivo, y la corrección automática usa documentos de Systems Manager Automation. Los conjuntos de conformidad de organización despliegan reglas y correcciones que las cuentas miembro no pueden modificar, el agregador ofrece una vista de solo lectura y EventBridge con SNS envía avisos. Security Hub CSPM centraliza hallazgos y usa reglas de automatización y acciones personalizadas.
- AWS Artifact ofrece informes de cumplimiento de AWS (SOC, PCI, ISO) que solo se comparten con auditores y reguladores por vías seguras, y permite aceptar acuerdos como el BAA para toda la organización desde la cuenta de administración. Para evidencias propias, AWS Config ofrece conjuntos de conformidad con historial y comprobaciones de proceso, y CloudTrail valida la integridad de sus registros; Audit Manager ya no admite clientes nuevos.
- AWS Well-Architected Tool revisa una carga de trabajo con la lente AWS Well-Architected Framework y su pilar de seguridad, identifica problemas de riesgo alto y medio y genera un plan de mejora; los hitos registran el estado para medir el progreso. Se pueden compartir cargas de trabajo (Read-Only o Contributor), lentes personalizadas publicadas y plantillas de revisión con la organización, y Trusted Advisor aporta comprobaciones automáticas.