PROFESSIONAL SECURITY OPERATIONS ENGINEER · CHEAT SHEET · CERTIFYDECK

Google Cloud Certified Professional Security Operations Engineer

Dominios, pesos oficiales y habilidades clave del temario de Professional Security Operations Engineer, para repasar antes del examen.

Nivel: Advanced (Professional) Duración: 120 min Fuente: guía de estudio oficial de Microsoft Learn

1. Platform operations

13–13%

Enhancing detection and response

- Google SecOps recibe datos de Google Cloud por ingesta directa (Cloud Logging, Cloud Asset Metadata y hallazgos de Security Command Center Premium) o por Cloud Storage cuando hay que filtrar antes. Los registros Data Access conviene filtrarlos para evitar volumen sin valor, y los hallazgos de SCC no admiten filtro. Para amenazas del navegador se reenvían los registros de Chrome Management con el conector de Chrome Enterprise.
- El Content Hub de Google SecOps reúne Content Packs (ingesta, detecciones seleccionadas y paneles), integraciones de respuesta, playbooks, bloques y búsquedas guardadas. Tras instalar una integración hay que configurar sus conectores, acciones y una instancia por entorno antes de usarla en un playbook. Las actualizaciones se prueban antes en el modo staging del IDE, y Dynamic Mode elige la instancia del entorno del caso.
- Cada herramienta cubre un hueco distinto: Security Command Center detecta en registros (Event Threat Detection, con módulos personalizados), sin agentes (VM Threat Detection) y en tiempo de ejecución (Container y Cloud Run Threat Detection); Cloud Logging avisa con alertas basadas en registros sin pasar por el SIEM; y Google SecOps correlaciona hallazgos de SCC con otros registros mediante reglas y detecciones seleccionadas.
- La matriz MITRE ATT&CK de Google SecOps muestra la cobertura por técnica: una tarjeta con cero reglas y tipos de registro disponibles es una oportunidad de detección. Las reglas propias cuentan solo con la clave technique en sus metadatos, y el cálculo se afina por estado en vivo y de alertas. Los conjuntos Managed Detection Testing comprueban que los datos tienen el formato que esperan las detecciones seleccionadas.
- Gemini en Google SecOps genera consultas de búsqueda y reglas YARA-L a partir de lenguaje natural, resume casos y ayuda a crear playbooks. El Triage and Investigation Agent decide si una alerta del SIEM es verdadero o falso positivo con GTI, búsquedas y árbol de procesos; no procesa alertas de conectores de SOAR. Integrado en un playbook, su veredicto y confianza permiten ramificar la respuesta.

Configuring access for human and non-human identities

- Los usuarios entran en Google SecOps con Cloud Identity o Google Workspace, o con un IdP SAML u OIDC mediante Workforce Identity Federation (solo SSO iniciado por el proveedor de servicios). El servidor MCP remoto de SecOps usa OAuth 2.0 con IAM, el rol MCP Tool User y, para federados, un proveedor dedicado; los agentes de producción usan su propia identidad. La API de GTI usa claves en la cabecera x-apikey.
- El acceso a funcionalidades de Google SecOps (feature RBAC) se controla con IAM en el proyecto vinculado: roles predefinidos como Chronicle API Admin, Editor, Viewer y Limited Viewer, o roles personalizados con permisos chronicle.*. Con Workforce Identity Federation se asigna google.groups y se conceden roles a principalSet de grupos. En proyectos compartidos, una condición sobre modifiedGrantsByRole limita qué roles concede un administrador.
- Data RBAC limita qué datos ve cada usuario de Google SecOps mediante ámbitos formados por etiquetas (tipo de registro, namespace o etiquetas propias). El usuario con ámbito recibe Chronicle API Restricted Data Access con una condición de IAM sobre el nombre del ámbito; el acceso global prevalece. Reglas, tablas de datos y listas de referencia también se vinculan a ámbitos, y las detecciones seleccionadas solo las ven usuarios globales.
- Google SecOps escribe registros de auditoría con el servicio chronicle.googleapis.com: la actividad de administración (crear reglas, actualizar feeds) siempre se registra, y para guardar las búsquedas UDM hay que activar Data Read en los registros de acceso a datos de Chronicle API. Se consultan en Logs Explorer por principalSubject y methodName; leerlos exige Private Logs Viewer y los principales exentos reducen volumen.
- Las automatizaciones deben usar identidades no humanas con mínimo privilegio: una cuenta de servicio asociada al recurso o suplantada con Workload Identity (lo que recomienda la integración de Security Command Center) en vez de claves JSON; una clave de API estándar no identifica a ningún principal. En GTI se usan claves de cuentas de servicio del grupo, y el servidor MCP de SecOps exige MCP Tool User más un rol de Chronicle API.

2. Data management

20–20%

Ingesting logs for security tooling

- El recopilador de Bindplane (basado en OpenTelemetry) lee canales de Windows Event y los envía con un exportador por tipo de registro (WINEVTLOG, WINDOWS_SYSMON); a gran escala se usan pasarelas tras un balanceador. Para Google Cloud, la ingesta directa reenvía Cloud Logging, Cloud Asset Metadata y hallazgos de SCC Premium sin filtrar por hallazgo; los registros de aplicaciones de GKE van por Cloud Storage y un feed.
- Cada regla de Event Threat Detection indica qué registros necesita: Cloud DNS para dominios maliciosos, flujo de VPC, firewall o Cloud NAT para IP maliciosas, registros de acceso a datos (con pgAudit en Cloud SQL para PostgreSQL) para bases de datos, y Workspace solo con activación a nivel de organización. En Google SecOps, cada conjunto de detecciones seleccionadas documenta sus fuentes, como GCP_RUN o el contexto de Cloud Asset Metadata.
- Cada parser corresponde a un único tipo de registro y convierte el registro sin procesar en UDM; lo que no asigna se queda en el registro sin procesar. La página Parsers solo muestra parsers prediseñados de tipos ya ingeridos, y Compare parsers enseña la diferencia de código y la salida UDM de una muestra editable. Desactivar las actualizaciones automáticas fija la versión; Skip update crea un parser personalizado.
- Una extensión del parser añade asignaciones a un parser predeterminado o personalizado sin sustituirlo; un parser personalizado sí lo sustituye y deja fuera las actualizaciones. Hay una extensión por tipo de registro, con enfoque sin código (JSON sencillo) o de fragmento de código (XML, CSV, Grok), y sus asignaciones prevalecen. Los campos repetidos admiten Append o Replace, y solo se aplica a datos nuevos salvo que se pida un Log Replay.
- La normalización convierte cada registro en un evento UDM con metadata.event_type, marca de tiempo y al menos un nombre (principal, target, src, intermediary, observer, about), de modo que fuentes distintas comparten semántica y reglas. Los espacios de nombres separan activos con IP solapadas, y el enriquecimiento y el alias añaden contexto en la ingesta; para cobertura total se usan tablas de datos y uniones con el grafo de entidades.

Implementing a baseline of user, asset, and entity context

- La inteligencia relevante es la que toca tu entorno: la pestaña IOC Matches muestra los indicadores de los feeds vistos en tus eventos (con coincidencia retroactiva sobre datos históricos), ATI prioriza esas coincidencias (Active Breach, High, Medium), el Emerging Threats Center cruza campañas de GTI con tus IoC y reglas activadas, y los threat profiles de GTI recomiendan actores y campañas según sector y región.
- Los datos de eventos (Cloud Audit Logs, el System Log del IdP, Sysmon, DNS) registran acciones y se normalizan como eventos UDM; los datos de entidad (OKTA_USER_CONTEXT, AZURE_AD_CONTEXT, CMDB, Cloud Asset Metadata como GCP_IAM_CONTEXT) describen usuarios y activos y alimentan el Entity Context Graph. El contexto tiene un intervalo de validez y se consulta con campos graph.*, no con una búsqueda UDM de eventos.
- El alias vincula indicadores de un mismo activo o usuario (DHCP enlaza IP, MAC y hostname; CS_EDR enlaza ID de activo y hostname) y permite enriquecer los eventos. Cada tipo sigue su lógica: hashes por primera coincidencia, activos combinando hostname, MAC y asset_id con la IP solo como alternativa, y siempre dentro del mismo espacio de nombres. Para cobertura completa en reglas, se recomienda unir con el grafo de entidades.

Configuring and Ingesting Threat Intelligence

- Los IoC de terceros se ingieren con el tipo de registro de IoC adecuado (MISP_IOC, STIX, CSV_CUSTOM_IOC...) para que el parser los convierta en entidades del ECG con source_type ENTITY_CONTEXT, metadatos de amenaza e intervalo de validez; los datos de GTI llegan con la integración BYOL (GCP_THREATINTEL) o con ATI. Las reglas YARA-L unen eventos con esas entidades, y un retrohunt sin alertas revisa el histórico.
- Google Threat Intelligence ofrece Livehunt (reglas YARA sobre cada archivo que analiza, con avisos en IoC Stream) y Retrohunt (archivos pasados y corpus de goodware para falsos positivos), Digital Threat Monitoring (monitores sobre la web y la dark web: credenciales, marcas, dominios), Private Scanning de archivos y URL sin compartirlos, y Google Insights, donde pesa más el número de organizaciones que los avistamientos.

3. Threat hunting

18–18%

Performing threat hunting across environments

- Las búsquedas UDM de Google SecOps rinden más filtrando por campos optimizados (metadata.event_type, principal.hostname, target.ip) y acotando el intervalo; los campos enumerados no admiten expresiones regulares, las listas largas de valores van en tablas de datos con in, Gemini convierte frases en lenguaje natural en consultas editables, y el intervalo de búsqueda sigue la hora del evento, no la de ingesta.
- Las búsquedas estadísticas UDM combinan filtro, match (agrupación, también por día u hora con by u over every), outcome con funciones como count, count_distinct, sum o earliest, y order y limit; no admiten condition ni la ventana over de las reglas. Los campos vacíos cuentan como valores, así que hay que filtrarlos. Para análisis de comportamiento continuo, Risk Analytics for UEBA ofrece reglas gestionadas.
- Logs Explorer filtra entradas con el lenguaje de consulta de Logging (log_id, protoPayload, SEARCH) pero no agrega; para contar y agrupar se usa Observability Analytics con SQL. En Google SecOps, la búsqueda UDM cubre eventos normalizados y la búsqueda de registros sin procesar (raw=) encuentra cadenas no analizadas. La exportación a BigQuery (datalake: events, rule_detections, ioc_matches, entity_graph) permite análisis histórico y uniones SQL.
- La búsqueda de amenazas en colaboración con respuesta a incidentes se apoya en SIEM Search: los eventos UDM y las detecciones encontrados pueden adjuntarse a un caso nuevo o existente como evidencia, y las búsquedas guardadas con variables ${...} se comparten con la organización. El Threat Hunt Agent crea casos etiquetados Threat Hunt, y las listas de seguimiento elevan el riesgo solo de las entidades indicadas.
- Las hipótesis de búsqueda pueden nacer de la exposición (rutas de ataque, combinaciones tóxicas y puntuaciones de Risk Engine en SCC, que son simulaciones y no evidencias), de la inteligencia (Threat Profiles de GTI y el feed del Emerging Threats Center filtrado por sector y coincidencias de IoC) y del comportamiento, como dominios con first_seen_time reciente en el Entity Context Graph.

Leveraging threat intelligence for threat hunting

- Para buscar IOC en el histórico de Google SecOps se usan búsquedas UDM con tablas de datos (in %tabla.columna), la búsqueda de registros sin procesar para cadenas no mapeadas a UDM y BigQuery para IOC multidimensionales como IP y puerto. La coincidencia de IOC es también retroactiva, y las entidades IOC propias necesitan metadata.threat para coincidir más allá de unos cinco días.
- Para detectar patrones de ataque nuevos, el Emerging Threats Center cruza campañas de GTI con tu telemetría, muestra reglas asociadas y desactivadas, y Gemini redacta reglas para los huecos que un analista aprueba. ATI prioriza IoC por Active Breach, High y Medium. En SCC, Risk Engine detecta combinaciones tóxicas y puntos de estrangulamiento, visibles en Issues y Findings.
- La puntuación de riesgo de entidad de Google SecOps suma la detección de mayor riesgo más una ponderación del resto, se normaliza entre 1 y 1000 y se calcula en ventanas de 24 horas o 7 días. Las reglas pueden asignar riesgo con risk_entity_to_score, consultar graph.risk_score indicando la ventana o alertar con eventos ENTITY_RISK_CHANGE; la página de la entidad muestra sus hallazgos y anomalías.
- Un retrohunt aplica una regla YARA-L a datos históricos y conviene lanzarlo con las alertas desactivadas. Las reglas de varios eventos reevalúan bloques en pasadas de ajuste, ampliables con Ensure enrichment completeness. Los resultados de búsqueda UDM y de reglas difieren, por ejemplo con campos repetidos (usar any). Para comparar con SQL, BigQuery recibe la exportación de SecOps y Cloud Logging ofrece conjuntos vinculados.
- La búsqueda proactiva con inteligencia combina Google Threat Intelligence (Livehunt aplica reglas YARA a cada archivo analizado y avisa en el IoC Stream; Retrohunt revisa el histórico y un corpus de goodware para probar falsos positivos) con reglas de Google SecOps: reglas YARA-L sobre el ATI Fusion Feed y conjuntos Mandiant Hunting con las alertas desactivadas.

4. Detection engineering

20–20%

Developing and implementing mechanisms to detect risks and identify threats

- Google SecOps compara de forma automática los eventos UDM con los IOC de Google y de feeds propios, en tiempo real y de forma retroactiva, y muestra en IoC Matches los activos y usuarios implicados. Applied Threat Intelligence añade coincidencias sobre CVE y TTP de reglas estándar y YARA-L sobre eventos, incidentes, Entity Context y datos de referencia sin procesar (raw = true).
- Las reglas YARA-L definen la lógica de detección con secciones events, match, condition y outcome, y pueden usar ventanas de salto (over), fijas (by) y deslizantes ancladas a un instante (after), y Google SecOps evalúa las de búsqueda con varias condiciones y ejecuciones de ajuste para los datos más recientes.
- Risk Analytics for UEBA compara la actividad con el historial; en reglas propias, $risk_score fija el valor y $risk_entity lo asigna a la entidad, y las reglas aplican un factor a entidades concretas.
- Para buscar IoC tras una alerta, Google SecOps lanza una búsqueda de registro sin procesar que queda para datos sin normalizar. La función de métricas event.count() permite alertar por umbrales, y para detectar ausencias, el evento placeholder time_until_now() cuenta el tiempo transcurrido desde el último evento real.
- Para reducir falsos positivos, Google SecOps ofrece listas de valores, de referencia y dinámicas, y permite excluir entidades y patrones en la detección. Además, incluye reglas de supresión nativas y la función outcome: is_false_positive(), que marca las alertas descartadas para entrenar el modelo.
- Las reglas YARA-L de Google SecOps pueden unir eventos UDM con enriquecimientos de Google Threat Intelligence y datos de contexto. Las reglas de exclusión nativas y las personalizadas pasar al feed GTI_IOC, filtrando por Applied Threat Intelligence solo coincidencias verificadas; los IoC se descartan automáticamente a los 90 días sin coincidencias, salvo que se marquen como críticos.
- Sin ATI, la integración BYOL importa listas de IoC como GCP_THREATLIST para cruzarlas con UDM y generar alertas.
- Para la vista de una alerta en Google SecOps, Overview, Graph y Alert JSON muestran los datos relevantes del UDM, y el Graph expande las entidades relacionadas.
- La Security Command Center, Vulnerability Assessment y Cloud Asset Inventory aportan CVE y hallazgos de configuración mal configurada, y Compliance Manager los mapea a controles. La puntuación de exposición prioriza los riesgos relacionados de vulnerabilidades y configuración incorrecta.
- La detección se apoya en integraciones como Google Cloud Armor, Cloud IDS y Cloud Logging, y en fuentes de terceros como CrowdStrike Falcon, Palo Alto Networks y Wiz, que aportan telemetría de endpoint, red y nube.
- La tasa de falsos positivos se reduce con reglas YARA-L que usan allow lists, umbrales y condiciones de ausencia, y con el modelo de riesgo de UEBA, que prioriza solo desviaciones significativas frente a la línea base.
- Para validar y ajustar las detecciones antes de activarlas, Google SecOps ofrece Test Rule y Run Rule Against Past 30 Days, que muestran cuántas coincidencias habría generado una regla en el pasado.
- Para probar las detecciones de forma segura, Security Command Center simula ataques reales en entornos aislados (Attack Exposure Scores) y Google SecOps ofrece Test Rule y Run Rule Against Past 30 Days, que muestran cuántas coincidencias habría generado una regla en el pasado.

Leveraging threat intelligence for detection

- Applied Threat Intelligence asigna prioridades Active Breach, High y Medium a las coincidencias de IoC según el veredicto y la severidad de GTI, la presencia en investigaciones de Mandiant y otros factores; las prioridades media y baja son solo informativas.
- Para buscar IoC tras una alerta en Google SecOps, la búsqueda UDM con grupos agrupa los hallazgos por host, usuario o proceso, y la vista de resultados permite ver la línea temporal de cada grupo.
- Para priorizar alertas de IoC en Google SecOps y reducir falsos positivos: suppression rules y la función outcome: is_false_positive() marcan eventos descartados, y Threat Tuning ajusta el feed GTI_IOC excluyendo dominios o IP de CDN y servicios legítimos.
- Para la vista de una alerta en Google SecOps, Overview, Graph y Alert JSON muestran los datos relevantes del UDM, y el Graph expande las entidades relacionadas.
- Applied Threat Intelligence solo importa IoC verificados; los IoC se descartan automáticamente a los 90 días sin coincidencias, salvo que se marquen como críticos.
- Sin ATI, la integración BYOL importa listas de IoC como GCP_THREATLIST para cruzarlas con UDM y generar alertas.
- Para la vista de una alerta en Google SecOps, Overview, Graph y Alert JSON muestran los datos relevantes del UDM, y el Graph expande las entidades relacionadas.
- La Security Command Center, Vulnerability Assessment y Cloud Asset Inventory aportan CVE y hallazgos de configuración mal configurada, y Compliance Manager los mapea a controles. La puntuación de exposición prioriza los riesgos relacionados de vulnerabilidades y configuración incorrecta.
- La detección se apoya en integraciones como Google Cloud Armor, Cloud IDS y Cloud Logging, y en fuentes de terceros como CrowdStrike Falcon, Palo Alto Networks y Wiz, que aportan telemetría de endpoint, red y nube.
- La tasa de falsos positivos se reduce con reglas YARA-L que usan allow lists, umbrales y condiciones de ausencia, y con el modelo de riesgo de UEBA, que prioriza solo desviaciones significativas frente a la línea base.
- Para validar y ajustar las detecciones antes de activarlas, Google SecOps ofrece Test Rule y Run Rule Against Past 30 Days, que muestran cuántas coincidencias habría generado una regla en el pasado.
- Para probar las detecciones de forma segura, Security Command Center simula ataques reales en entornos aislados (Attack Exposure Scores) y Google SecOps ofrece Test Rule y Run Rule Against Past 30 Days, que muestran cuántas coincidencias habría generado una regla en el pasado.

5. Incident response

18–18%

Containing and investigating security incidents

- Para recoger pruebas de un incidente en Google Cloud se hace primero una instantánea de los discos de la VM, posible con el disco conectado, sabiendo que no captura la memoria; los datos volátiles se recogen con herramientas en Session y Command Center. El panel Threats se usa para evaluar y priorizar los hallazgos de amenaza y Google Security Operations Overview para ver métricas de ingesta y detección.
- En Google SecOps, la vista de una alerta ofrece Overview, Graph y Alert JSON, y el Graph expande las entidades relacionadas.
- La Security Command Center, Vulnerability Assessment y Cloud Asset Inventory aportan CVE y hallazgos de configuración mal configurada, y Compliance Manager los mapea a controles. La puntuación de exposición prioriza los riesgos relacionados de vulnerabilidades y configuración incorrecta.
- La detección se apoya en integraciones como Google Cloud Armor, Cloud IDS y Cloud Logging, y en fuentes de terceros como CrowdStrike Falcon, Palo Alto Networks y Wiz, que aportan telemetría de endpoint, red y nube.
- La tasa de falsos positivos se reduce con reglas YARA-L que usan allow lists, umbrales y condiciones de ausencia, y con el modelo de riesgo de UEBA, que prioriza solo desviaciones significativas frente a la línea base.
- Para validar y ajustar las detecciones antes de activarlas, Google SecOps ofrece Test Rule y Run Rule Against Past 30 Days, que muestran cuántas coincidencias habría generado una regla en el pasado.
- Para probar las detecciones de forma segura, Security Command Center simula ataques reales en entornos aislados (Attack Exposure Scores) y Google SecOps ofrece Test Rule y Run Rule Against Past 30 Days, que muestran cuántas coincidencias habría generado una regla en el pasado.

Building, implementing and using response playbooks

- Google SecOps SOAR ejecuta playbooks que automatizan la respuesta a incidentes, con integraciones nativas y personalizadas, y permite crear bloques reutilizables y probarlos en modo sandbox.
- Un playbook de respaldo (prioridad 3, trigger All) no es destructivo, las acciones sensibles pasan a Manual con Approval y Time to respond, y el Skip Manual descarta las previas si falla.
- Los playbooks se activan por alertas, casos o entidades, y pueden ejecutarse en modo interactivo o automático.
- Para enriquecer un caso, Get Related Associated Context trae entidades, alertas y eventos relacionados, y el bloque Entity Graph muestra sus relaciones.
- Los parámetros se definen en variables, filtros y condiciones, y los resultados de pasos anteriores se usan en los siguientes.
- Playbook Integrations instalan integraciones y bloques, y Recommendations sugiere nuevos playbooks según el contexto.
- Antes de usar un playbook en producción, se recomienda probarlo con datos reales y revisar el modo sandbox.

Implementing the case management lifecycle

- Los SLA de SOAR pueden ser de alerta o de caso, un SLA de caso por etapa solo corre en esa etapa y no se reinicia al volver, uno por prioridad se reinicia al cambiarla, y una acción de playbook prevalece sobre etapa y prioridad. Al vencer, se escala y registra.
- Para cerrar un caso se completa una evaluación por plantilla, se clasifica como True Positive o False Positive, se elige una causa raíz y se añade un resumen final.
- Los casos se agrupan por entidades comunes, reglas o tiempo, y se pueden fusionar manualmente o con reglas automáticas.
- Para escalar un caso se asigna a un analista o grupo, se cambia su prioridad o etapa y se notifica por correo o chat.
- Para gestionar el ciclo de vida de un caso, Case Overview muestra el resumen y la línea temporal, y Case Wall permite colaborar con notas, archivos y menciones.
- Para cerrar un caso se completa una evaluación por plantilla, se clasifica como True Positive o False Positive, se elige una causa raíz y se añade un resumen final.
- Los casos se agrupan por entidades comunes, reglas o tiempo, y se pueden fusionar manualmente o con reglas automáticas.
- Para escalar un caso se asigna a un analista o grupo, se cambia su prioridad o etapa y se notifica por correo o chat.
- Para gestionar el ciclo de vida de un caso, Case Overview muestra el resumen y la línea temporal, y Case Wall permite colaborar con notas, archivos y menciones.

6. Observability

11–11%

Developing and maintaining dashboards to provide insights

- Los KPI de respuesta se leen en paneles predefinidos: el Response Health Hub compara el MTTR de cierres automáticos y manuales, separa el tiempo total del playbook del tiempo activo de las acciones y muestra colas, adjuntos, fallos y ejecuciones terminadas. El panel Triage and Investigation Agent Metrics sigue volumen, veredictos y la valoración de los usuarios sobre esos veredictos.
- Los paneles de Google SecOps usan consultas YARA-L 2.0 con un prefijo por origen de datos (eventos, detection, ioc, ingestion, case, playbook...), con match u outcome y sin condition. Los predefinidos no se editan: se duplican. Todos respetan data RBAC; los datos de SOAR solo los ven usuarios globales, y las métricas de ingesta exigen ámbitos con etiquetas estándar como el namespace.
- Cada plataforma genera sus informes: en SOAR, el informe del caso (DOC, XLSX o CSV) con muro y acciones; en SecOps, descargas de paneles (CSV completo, PDF y PNG solo lo visible) e informes programados por correo o enlace a Cloud Storage; en SCC, el informe de riesgos en PDF con rutas de ataque y combinaciones tóxicas; en GTI, PDF de informes y resúmenes Report Digest.

Configuring health monitoring and alerting

- La salud de la ingesta se vigila con métricas de Google SecOps en Cloud Monitoring: Total ingested log count con Metric absence y agrupado por collector_id o ingestion_source detecta orígenes silenciosos, y Total ingested log size controla el volumen diario contratado, no quota_limit. El Health Hub muestra orígenes y parsers fallidos o irregulares, Last Ingested frente a Last Normalized y fallos silenciosos de credenciales de feeds.
- Los paneles de Google SecOps combinan gráficos de varios orígenes de datos (métricas de ingesta, detecciones, casos, playbooks) con consultas YARA-L que llevan sección match u outcome. Los paneles seleccionados, como Health Hub o Response Health Hub, son de solo lectura: se duplican para personalizarlos. Para unir métricas, políticas de alertas y registros de Google Cloud en una vista se usa un panel personalizado de Cloud Monitoring.
- Google SecOps publica métricas de ingesta en Cloud Monitoring (Chronicle Collector Ingestion y Normalizer, Outofband para feeds) que se filtran por log_type, feed_name, collector_id o state. Para el volumen diario se usa Total ingested log size con ventana de un día y umbral, no quota_limit, y conviene agregar con sum y agrupar por project_id para evitar falsas alertas.
- Los canales de notificación de Cloud Monitoring incluyen correo, SMS, Slack, PagerDuty, webhooks, Mobile App y Pub/Sub. Se recomienda redundancia con correo o Pub/Sub, ya que Slack, PagerDuty, webhooks y Mobile App comparten un punto de fallo; para automatización o endpoints privados se usa Pub/Sub, autorizando a la cuenta de servicio de notificaciones como Pub/Sub Publisher.
- En instancias con proyecto BYOP, Google SecOps envía los registros de actividad de los feeds a Cloud Logging (log_id chronicle.googleapis.com/ingestion_activity; los feeds de STS usan storage_transfer_job). Debug with logs abre Logs Explorer filtrado por el feed, Ask Gemini Cloud Assist responde sobre volúmenes y errores, y el Health Hub muestra el último problema de cada origen.