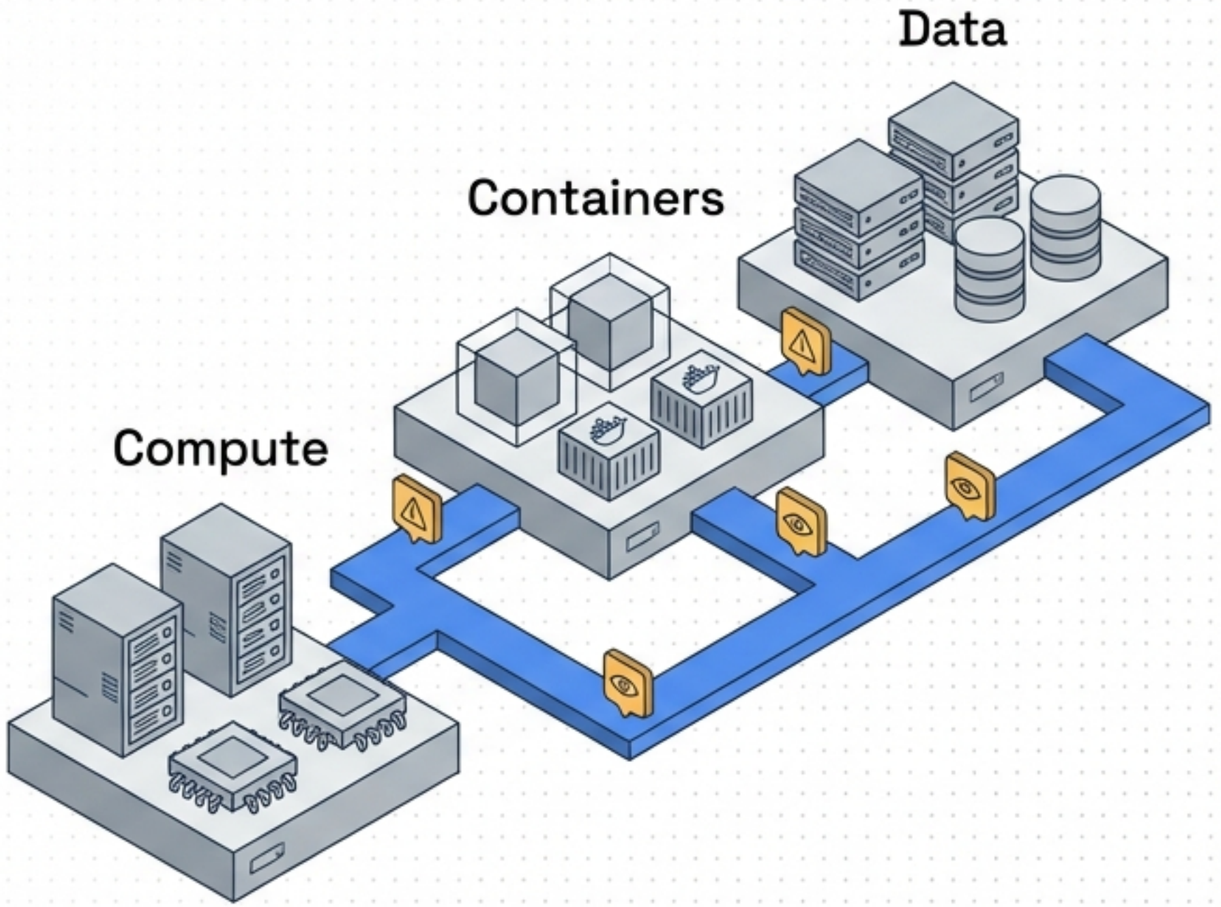
The Google Cloud Security Blueprint

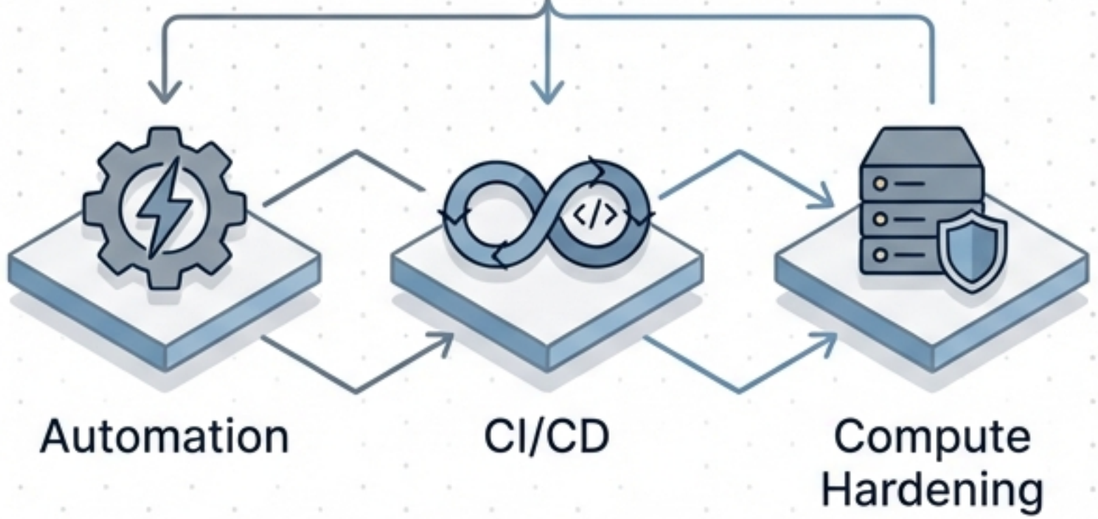
- **Primary Focus:** Managing Operations (Automating Security & Configuring Visibility)
- **Exam Weight:** ~19% of the PSE Certification
- **Core Concepts:** Infrastructure Automation, Supply Chain Security, Pervasive Logging, and Threat Detection



NotebookLM

The Dual-Pillar Security Framework

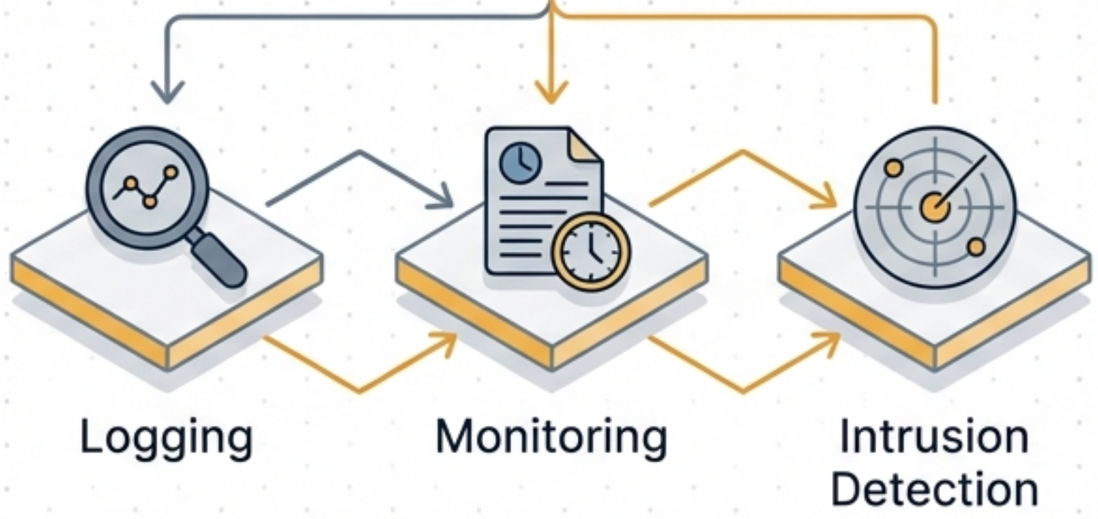
4.1: Proactive Prevention



Pillar 1: Automating Defense

Hardens infrastructure and application security prior to deployment. Focuses on shifting security left, enforcing cryptographic supply chain integrity, and preventing configuration drift.

4.2: Pervasive Visibility

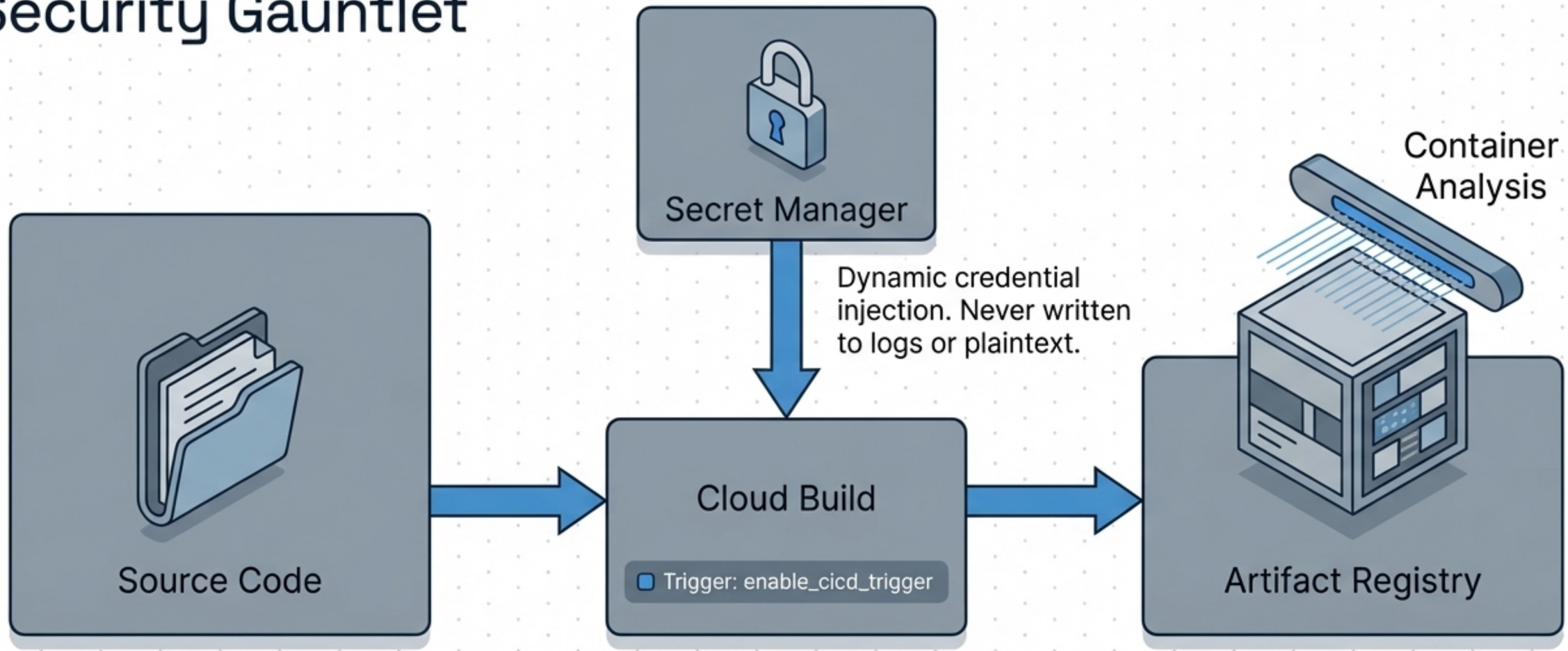


Pillar 2: Configuring Detection

Captures security-relevant events and generates actionable alerts. Focuses on network forensics, immutable audit trails, and automated response to anomalous activity.

NotebookLM

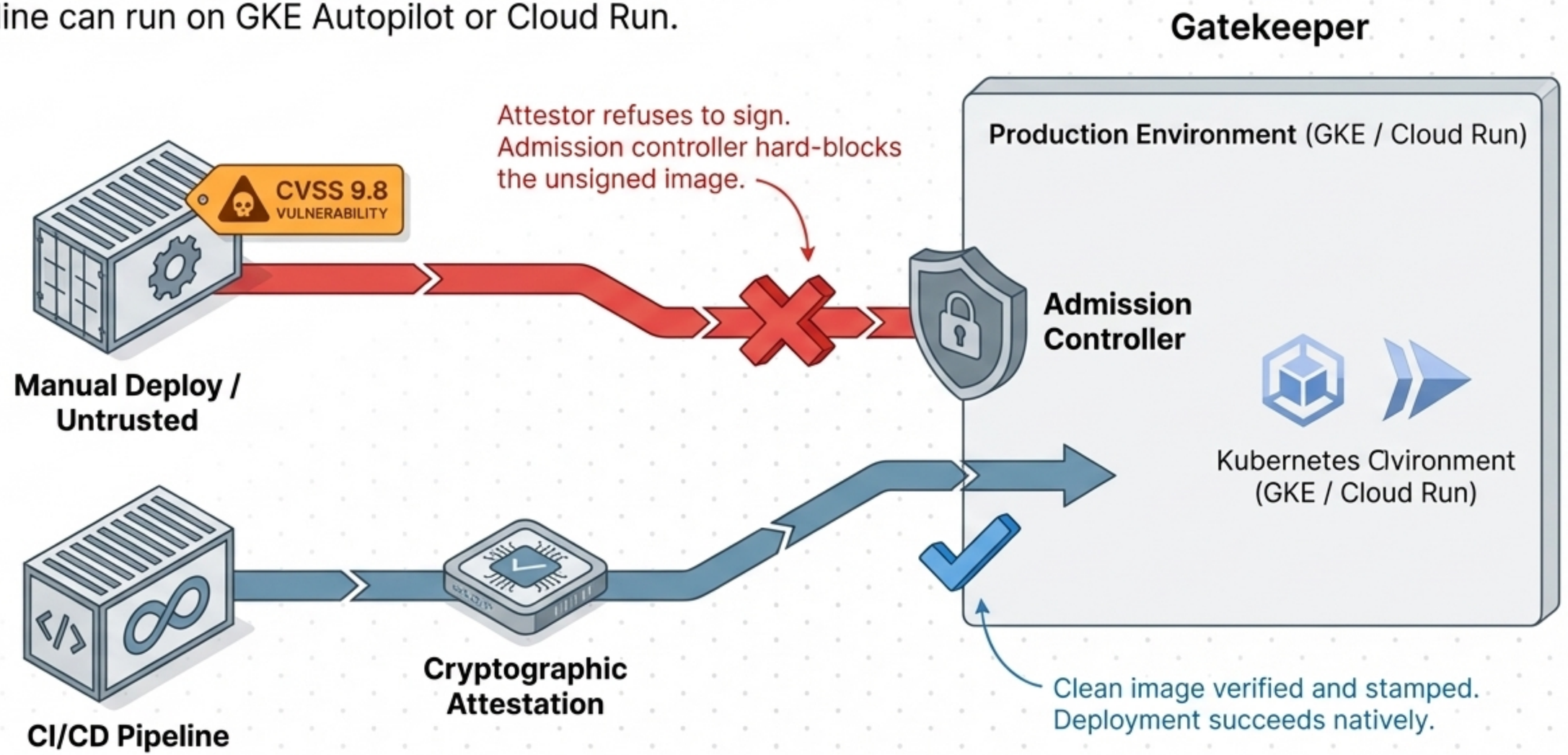
The Automated Security Security Gauntlet



NotebookLM

Cryptographic Supply Chain Integrity

Only images built, scanned, and signed by the trusted pipeline can run on GKE Autopilot or Cloud Run.



NotebookLM

Hardening the Compute Layer

Virtual Machines (Shielded VMs)

Secure Boot: Prevents loading unsigned bootloaders and kernel modules.

vTPM: Virtual Trusted Platform Module storing cryptographic integrity measurements.

Integrity Monitoring: Compares live boot measurements against known-good baselines to alert on deviation.

Containerized Workloads (GKE / Cloud Run)

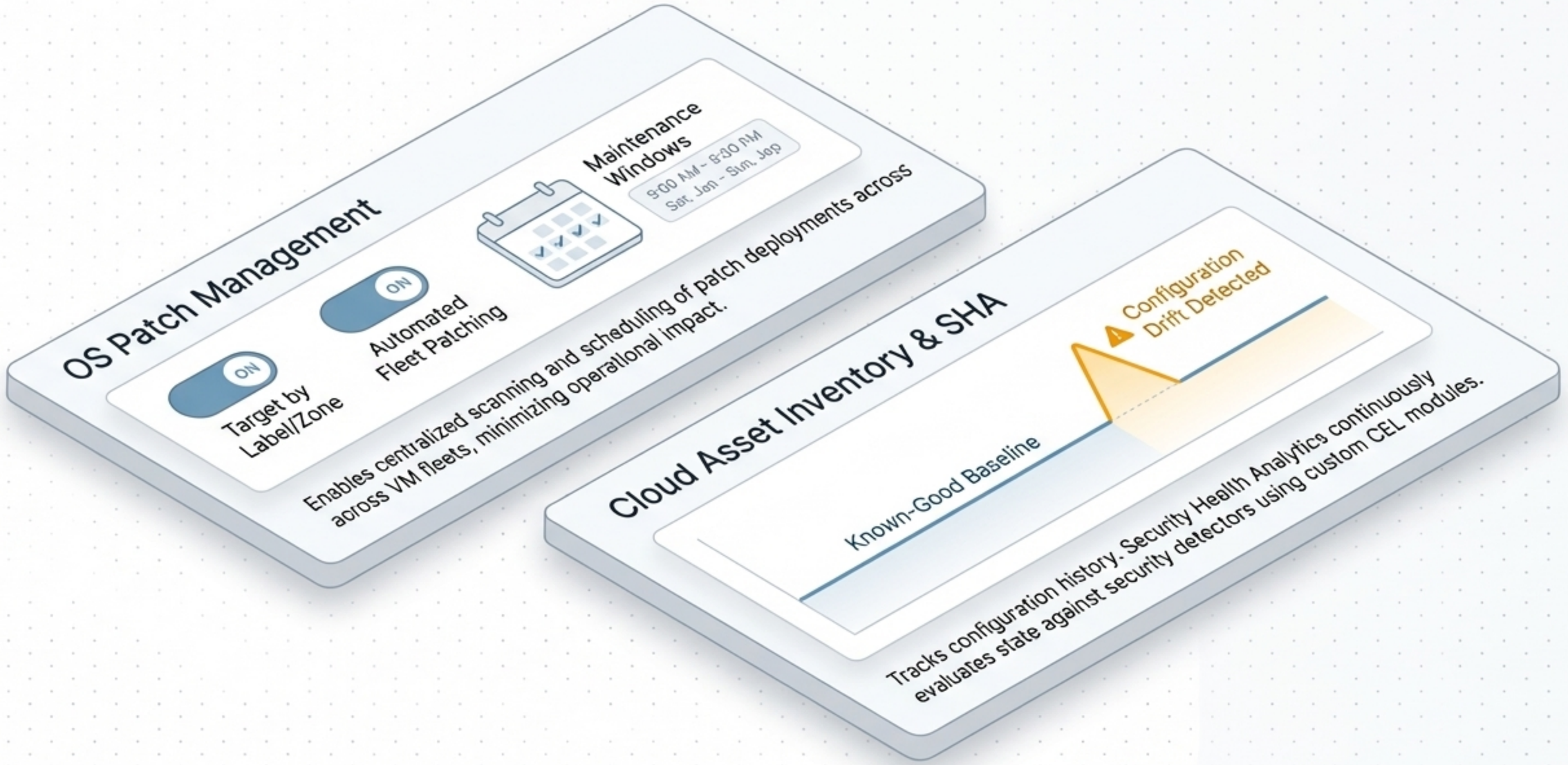
Minimal Surface: Utilize distroless base images with no shell and no package manager.

Privilege Reduction: Enforce non-root user execution.

Immutability: Mount read-only root filesystems to block runtime tampering.

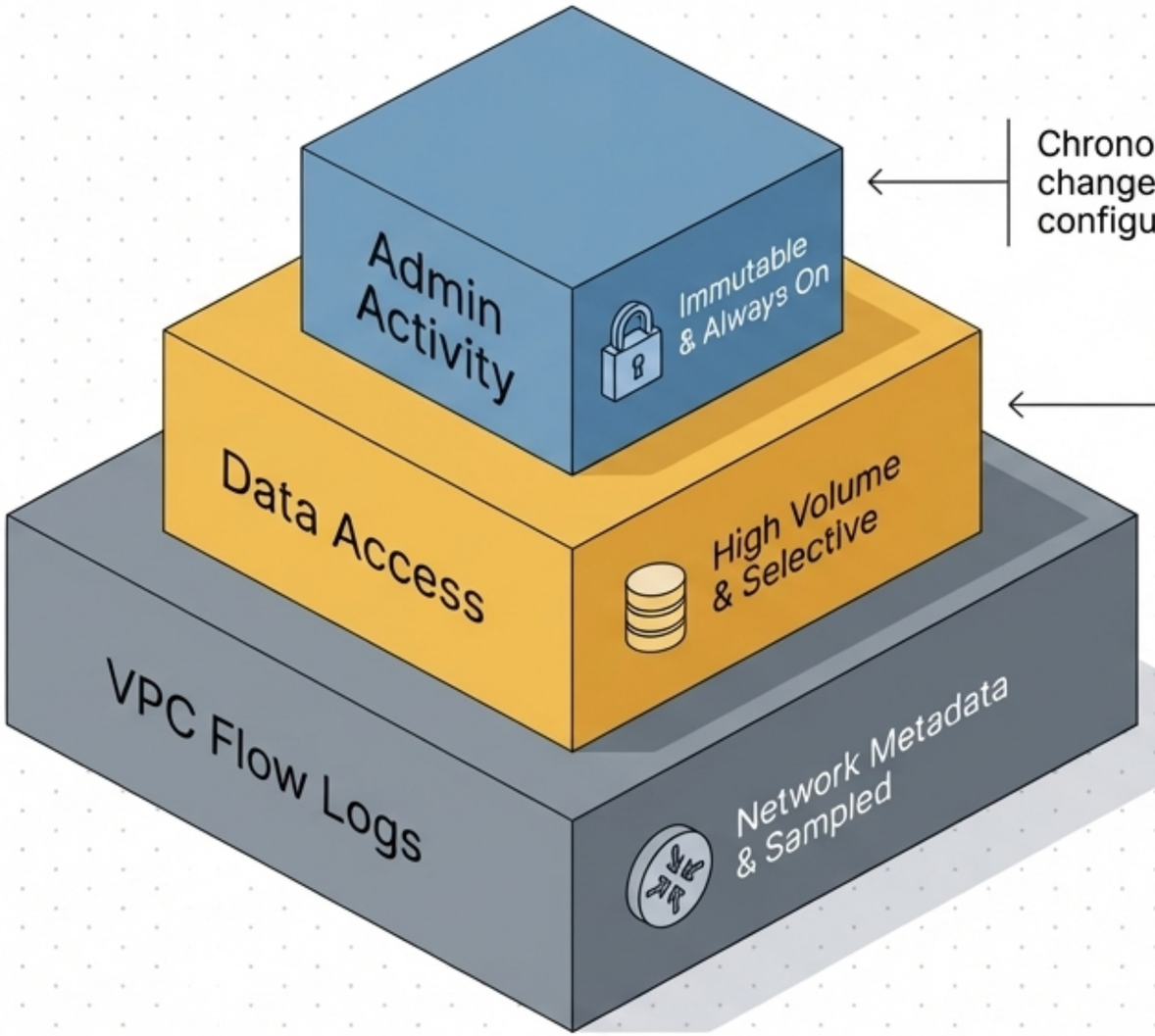
NotebookLM

Maintaining State at Scale



NotebookLM

The Cloud Logging Taxonomy



Chronological record of all infrastructure changes, IAM modifications, and configuration API calls.

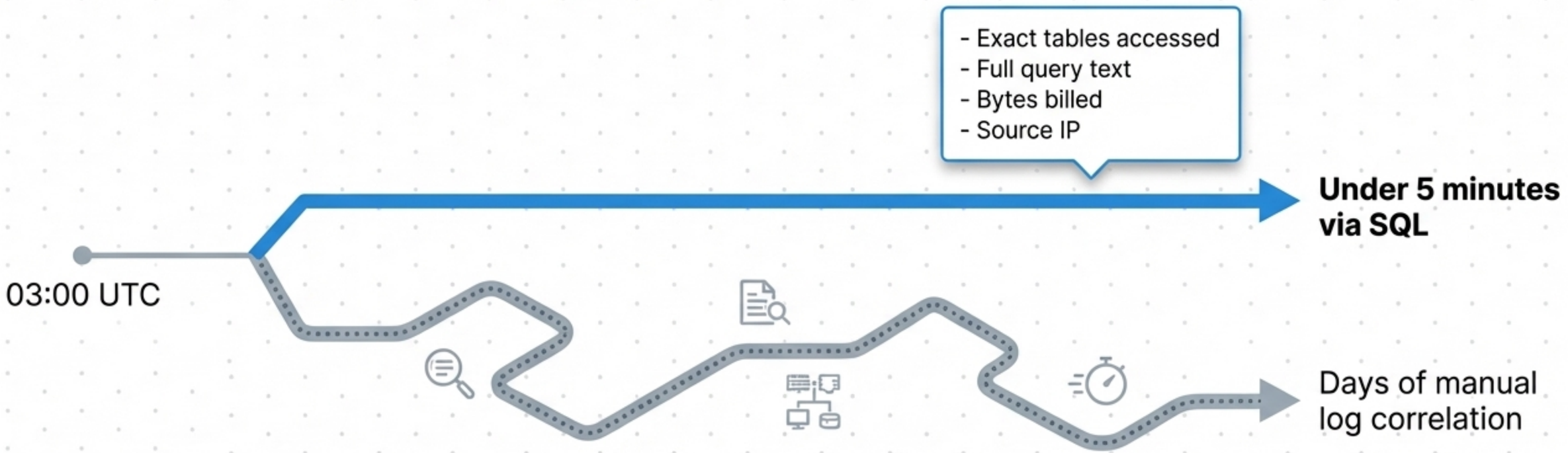
Records API calls reading or writing user data. Disabled by default due to cost; enabled selectively for sensitive services.

Captures subnet-level network metadata (IP, port, bytes). Sampling rates balance forensic completeness with cost reduction.

NotebookLM

Accelerating Incident Response

SIEM Alert: Anomalous 50GB BigQuery Export



The Resolution: Because the organization routed Data Access audit logs to a dedicated BigQuery dataset, analysts reconstruct the complete scope of the exfiltration instantly using direct SQL.

NotebookLM

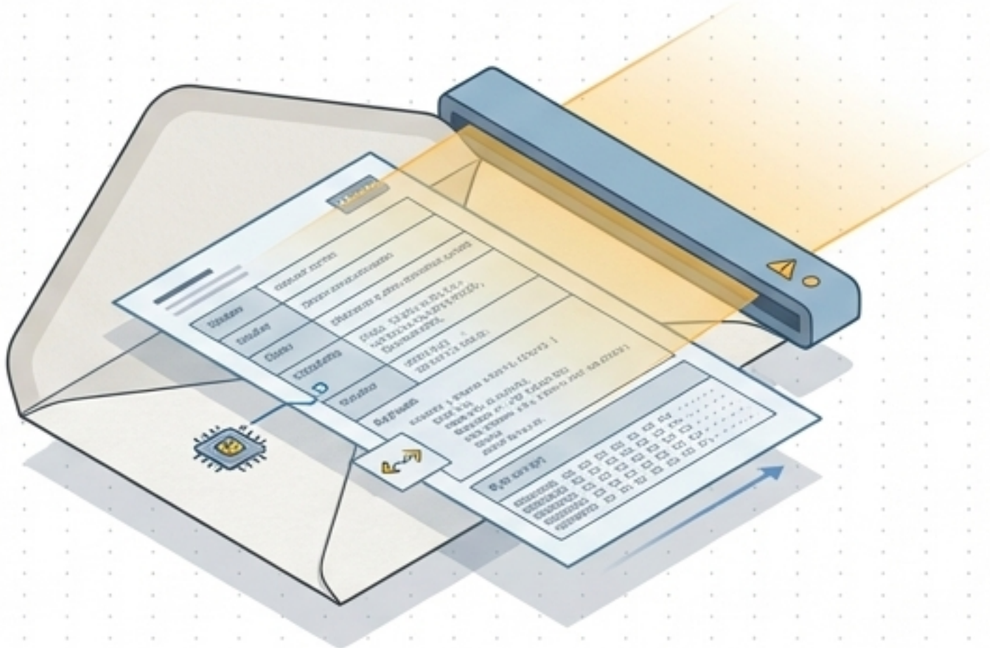
Depths of Network Forensics

VPC Flow Logs & Firewall Logs

Metadata Inspection

Captures connection metadata and rule-match evidence. Shows who talked to whom, proving blocked intrusions and validating allow rules without seeing the data inside.

Packet Mirroring

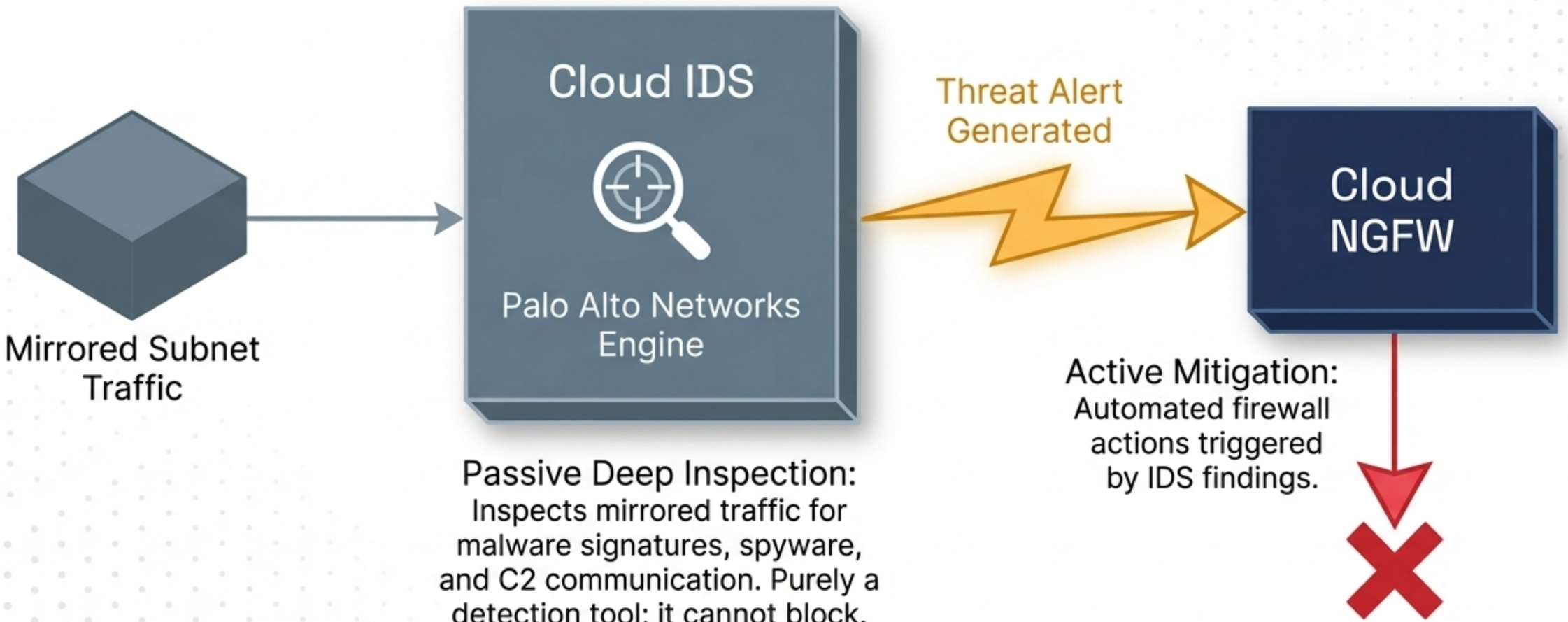


Payload Inspection

Copies the full packet payload from VM instances to an Internal Load Balancer. Feeds deep network analysis and east-west traffic forensics by inspecting the actual contents.

NotebookLM

Intrusion Detection and Automated Response



NotebookLM

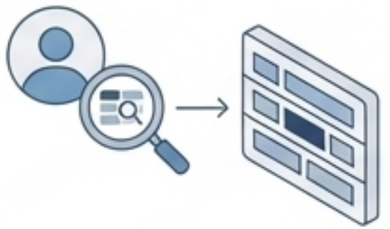
Architecting a Scalable Logging Strategy

1. What to collect?

Admin Activity (always), Data Access (sensitive only), Flow Logs (network).

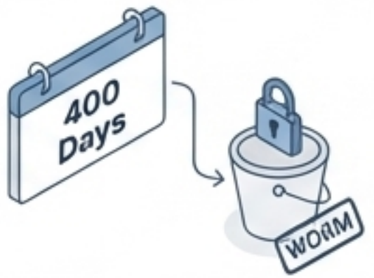
2. Where to store?

Default buckets for ops vs. Locked compliance buckets for archival.



3. Who has access?

Scoping Access: Log Views grant teams "logging.viewAccessor" access to specific log subsets (filtering PII) without exposing the entire bucket.



4. How long to retain?

Ensuring Compliance: Mandate 400-Day Minimum retention for Admin Activity logs via sinks to Cloud Storage, secured with Bucket Lock for WORM immutability.

NotebookLM

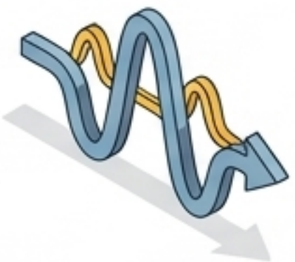
Log Routing and Analytics Destinations

Cloud Storage

The primary destination for low-cost, long-term WORM compliance and archival.

BigQuery

The destination for highly complex, SQL-based forensic analysis, anomaly detection, and vast historical querying.



Pub/Sub

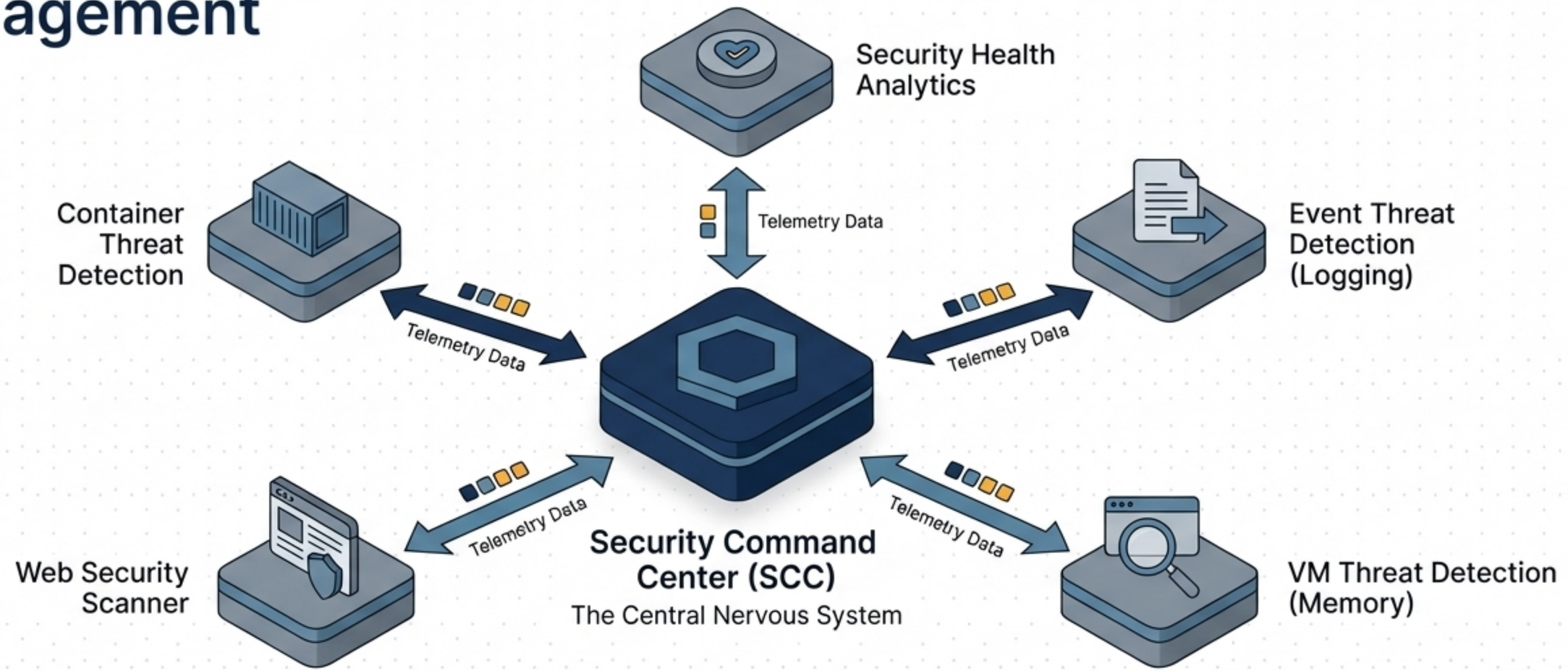
The real-time streaming router for forwarding logs to external SIEMs or downstream processing pipelines.

Log Analytics

An upgraded Cloud Logging bucket feature enabling rapid, in-console SQL querying without incurring BigQuery export or query costs.

NotebookLM

Unified Posture Management



Continuous Feedback Loop: SCC consolidates the entire environment's posture into a single actionable dashboard. It utilizes Custom CEL modules and Pub/Sub notifications to integrate directly with organizational ticketing and SIEM workflows.

NotebookLM