**Summary: Searching Events in Chronicle (Google Cloud SIEM)**

**Chronicle's Search Capabilities**

* **Primary search field** allows filtering by:
  + hostname, domain, IP, URL, email, username, file hash
* Two main search types:
  + **UDM (Unified Data Model) Search** – normalized data
  + **Raw Log Search** – unprocessed logs, useful for unnormalized fields or troubleshooting ingestion

**YARA-L Language**

* Used to define **custom detection rules**
* Useful for identifying specific behaviors (e.g., data exfiltration)
* Powerful for **proactive threat detection** within ingested log data

**Example UDM Search Query**

metadata.event\_type = "USER\_LOGIN" AND security\_result.action = "BLOCK"

* metadata.event\_type = "USER\_LOGIN": Targets login events
* security\_result.action = "BLOCK": Filters for failed/blocked logins
* **Logical operator AND** ensures both conditions must be met

**Interpreting the Results**

* **Search results page includes:**
  + Search query (shown for reference)
  + **Bar graph** timeline (visual trend of activity)
  + **Event list** with timestamps and assets (e.g., devices/users involved)
  + **Raw log access** for deeper analysis

**Quick Filters**

* Located on the left panel
* Allow dynamic filtering by fields like:
  + target.ip, principal.user.email, asset.hostname, etc.
* Save time by refining search results instantly

**Key Takeaway**

Chronicle's combination of **UDM search**, **raw log access**, and **quick filters** empowers security analysts to locate and analyze specific security events efficiently, whether during routine monitoring or deeper investigations.