



Creando organizaciones Data-Driven con Elastic y Gen AI



¿Quién soy?

Sr. Solutions Architect en Elastic - LATAM

Hogar: Ciudad de México

Datos interesantes: Me encanta aprender nuevos idiomas y culturas (4 idiomas, viví en 7 países), apasionado por los retos y nuevas tecnologías

Historia de fondo (historial de trabajo):

Ingeniero en Sistemas Computacionales

Desarrollador de soluciones de biometría y core bancario.

1 año como investigador en Japón (principalmente Tokio, Osaka y Kanazawa)

Más de 10 años en arquitectura enterprise y transformación digital

Últimas empresas con las que colabore CA Technologies, Fujitsu Global y Outsystems



Alan Cuevas



¿Quién soy?

Dir. Comercial Ventus Technology

Hogar: Monterrey NL

Datos interesantes: Apasionado por la tecnología, una buena parrillada y la pesca.

Historia de fondo (historial de trabajo):

Ingeniero en Sistemas Computacionales.

Liderazgo comercial y tecnológico, oficina de proyectos y planeación estratégica

Últimas empresas con las que colabore Banorte y Ventus Technology



Edgar Garza

¿Qué es **Elastic**?

Follow the Sun with Elastic



00h00

NETFLIX

6:00 PM Watch a movie

NETSHOES

5:00 PM Shopping

SAP Concur 

4:00 PM Complete expenses



3:00 PM Pay bills



2:00 PM Update timesheet

 Adobe

1:00 PM Convert documents to PDF

B B C

Wake & read the news 7:00 AM



Travel to the office 8:00 AM

Lenovo

Start work 9:00 AM

Booking.com

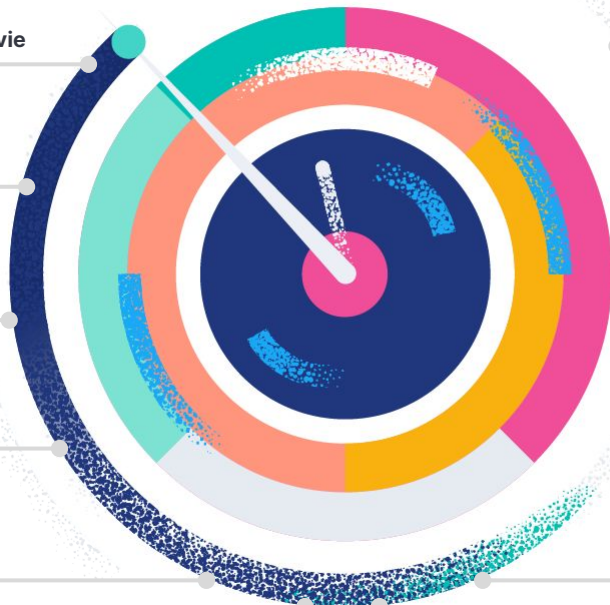
Book a business trip 10:00 AM

 **BARCLAYS**

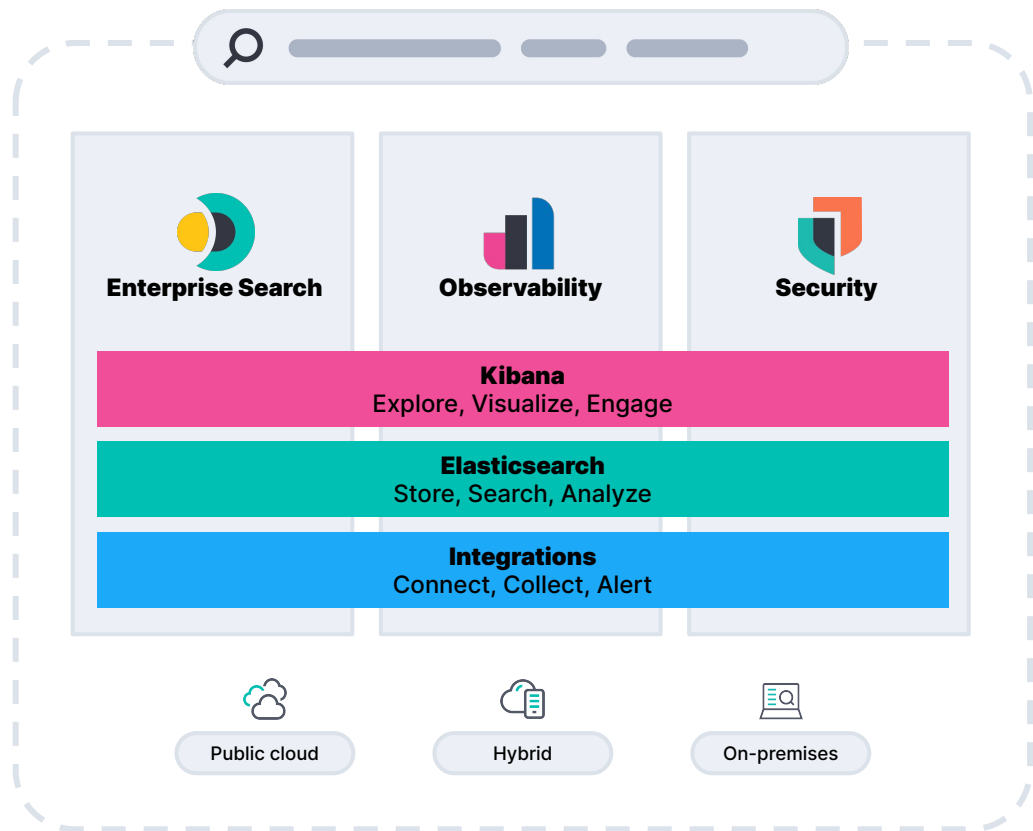
Check finances 11:00 AM

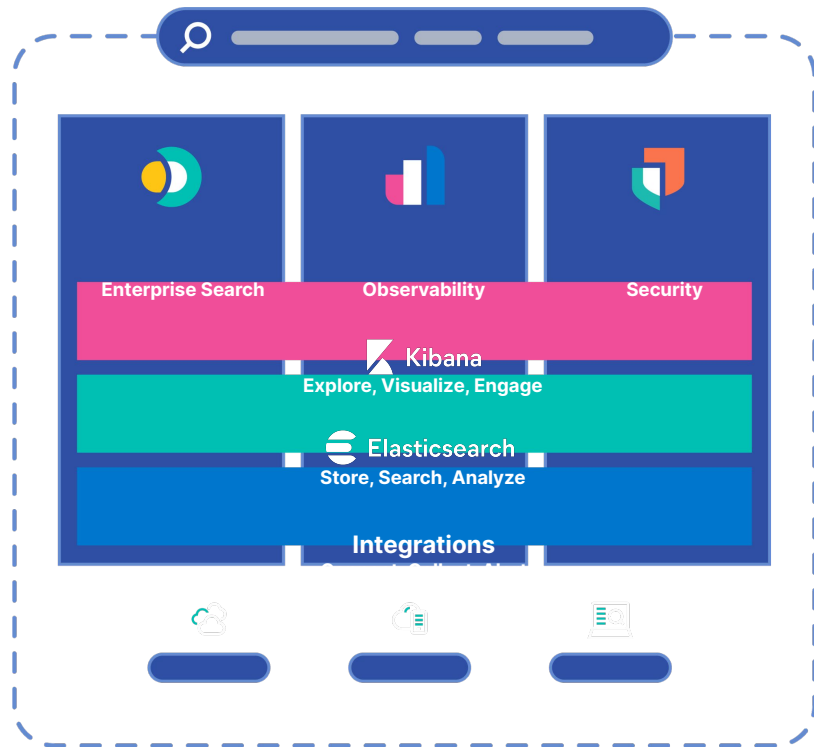
Uber

Order ride for work lunch 12:00 PM



The Elastic search platform





Una plataforma con 3 soluciones que ofrecen resultados relevantes en tiempo real



Clientes en diversas **industrias, segmentos y geografías.**

TECNOLOGIA	FINANZAS	TELCO	CONSUMER	HEALTHCARE	SECTOR PUBLICO	AUTOMOTRIZ / TRANSPORTE	RETAIL
							
							
							
							
							

Estamos cambiando cómo el mundo usa datos



¿Por qué esto es **relevante para mí?**

En el mundo siempre activo de hoy, el crecimiento y la transformación están fundamentalmente conectados a los datos.



Elastic ayuda a **los líderes** de las organizaciones a usar el **poder de la búsqueda** para **convertir los datos** en **resultados importantes**



CIOs & CISOs



Execs & Lines of Business

Mejore las experiencias de los clientes para impulsar el crecimiento de los ingresos



IT and Peers

Mejore la resiliencia operativa para reducir la interrupción de los ingresos y proteger la reputación de la marca



Risk and Compliance

Aumentar la privacidad, la ética y la seguridad para reducir el riesgo/fraude



Economic times

Consolidación de herramientas
Reduzca costos y aumente el ROI

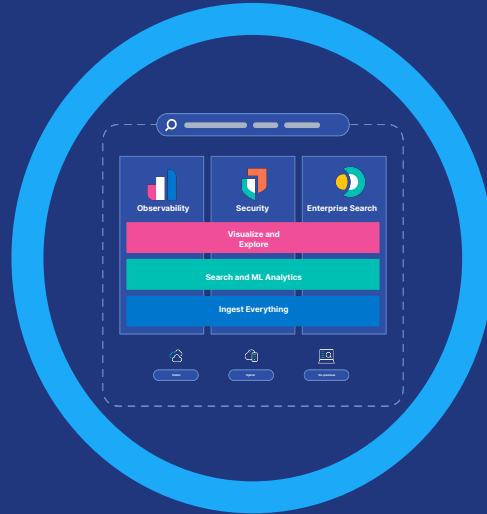
¿Qué hace que nuestro enfoque sea **diferente**?

Una plataforma única que comprar, mantener y administrar

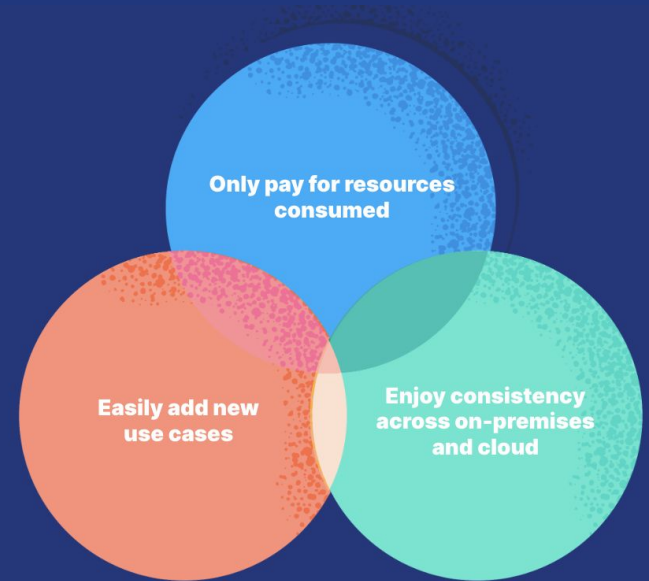


Consolidación de herramientas

Modelo de licenciamiento diferenciado basado en recursos consumidos



Eficiencias operativas



Modelo de negocios escalable

Generative AI en tu negocio

Descubriendo perspectivas a través de los datos

Un nuevo punto de inflexión ocurrió



El poder de la **Inteligencia Artificial Generativa** se basa en la forma como interactuamos con los **datos**

1
8

480EB

1 EB = 1000 PB = 1,000,000 TB

⋮ Data produced
⋮ daily by 2025



*Source: IDC Global DataSphere and StorageSphere Forecasts

Preocupaciones en torno a la IA generativa

50%

Desarrolladores

Observan una escasez de las habilidades necesarias para la IA generativa en su organización.

60%

Ejecutivos

Sienten un alto grado de urgencia por adoptar la IA generativa.

64%

Ejecutivos

Creen que faltan entre 1 y 2 años para implementar la IA generativa.

ESRE ofrece IA generativa que es más rápida, más precisa, a

[KPMG Generative AI Survey](#)
[The Prompt: Generative AI survey | Google Cloud Blog](#)



La IA Generativa **revolucionará** todos los negocios

100M

**Crecimiento de
Chat GPT**

Adopción de usuarios
en menos de 2 meses

300M

**Trabajos
automatizados**

Impacto previsto de la
IA generativa*

10ⁿ

**Cambios
tecnológicos**

Personalización,
automatización y
productividad

Queremos que la IA empresarial se desarrolle a la velocidad de la IA del consumidor

76%

Los compradores en línea abandonan un sitio web minorista después de una búsqueda fallida

1.8

Horas perdidas por los empleados buscando información cada día

Busqueda hoy.

The screenshot shows a search results page for 'pvc plumbing irrigation systems'. At the top, there is a search bar with the text 'Search' and a magnifying glass icon. Below the search bar, the results are displayed in a grid format. On the left side of the grid, there are three filter sections: 'Brand', 'Rating', and 'Price', each with a list of checkboxes and horizontal bars representing the number of items. The main grid contains four product listings, each with an image, a title, a star rating, a price, and an 'Add to Cart' button. The products are: 1. Orbit 3/4 in. PVC-Lock Slide Repair Fitting, priced at \$6¹⁶. 2. Alpine Corporation 1 in. x 25 ft. Schedule 40 Black PVC Ultra Flexible Hose, priced at \$40⁰⁶. 3. Orbit 1-1/2 In. PVC Sediment Filter, priced at \$62⁴⁶. 4. Rain Bird 1 in. In-Line Irrigation Valve, priced at \$17⁹⁷. The page also shows '68 Results' and 'Sort by: Best Match'.

Search results for: **pvc plumbing irrigation systems**

68 Results Sort by: Best Match

Brand	Rating	Price
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Product	Price
Orbit 3/4 in. PVC-Lock Slide Repair Fitting	\$6 ¹⁶
Alpine Corporation 1 in. x 25 ft. Schedule 40 Black PVC Ultra Flexible Hose for Koi Ponds, Irrigation, Water Gardens and More	\$40 ⁰⁶
Orbit 1-1/2 In. PVC Sediment Filter	\$62 ⁴⁶
Rain Bird 1 in. In-Line Irrigation Valve	\$17 ⁹⁷

HOY



tubería de pvc para sistema de riego

Busqueda en breve.

The screenshot shows a search results page for 'pvc plumbing irrigation systems'. The page features a search bar at the top with the text 'Search' and a magnifying glass icon. Below the search bar, the results are displayed in a grid format. On the left side, there are filters for 'Brand', 'Rating', and 'Price'. The main content area shows four product listings, each with an image, a title, a star rating, a price, and an 'Add to Cart' button.

Brand	Rating	Price
Orbit	★★★★★	\$6 ¹⁶
Alpine Corporation	★★★★★	\$40 ⁰⁶
Orbit	★★★★★	\$62 ⁴⁶
Rain Bird	★★★★★	\$17 ⁹⁷

HOY



tubería de pvc para sistema de riego

MAÑANA



¿Cuál es la lista de materiales y herramientas que necesito para construir un sistema de riego para mi patio trasero de 20 m² en CDMX?

Elastic proporciona el puente entre datos privados y GenAI

Base de datos sensibles
Multi-sistemas / información de nube
Base de Conocimientos Privada
Historias de casos



Elastic AI Assistant

Empodere a los equipos de Seguridad con GenAI

Valor Generado

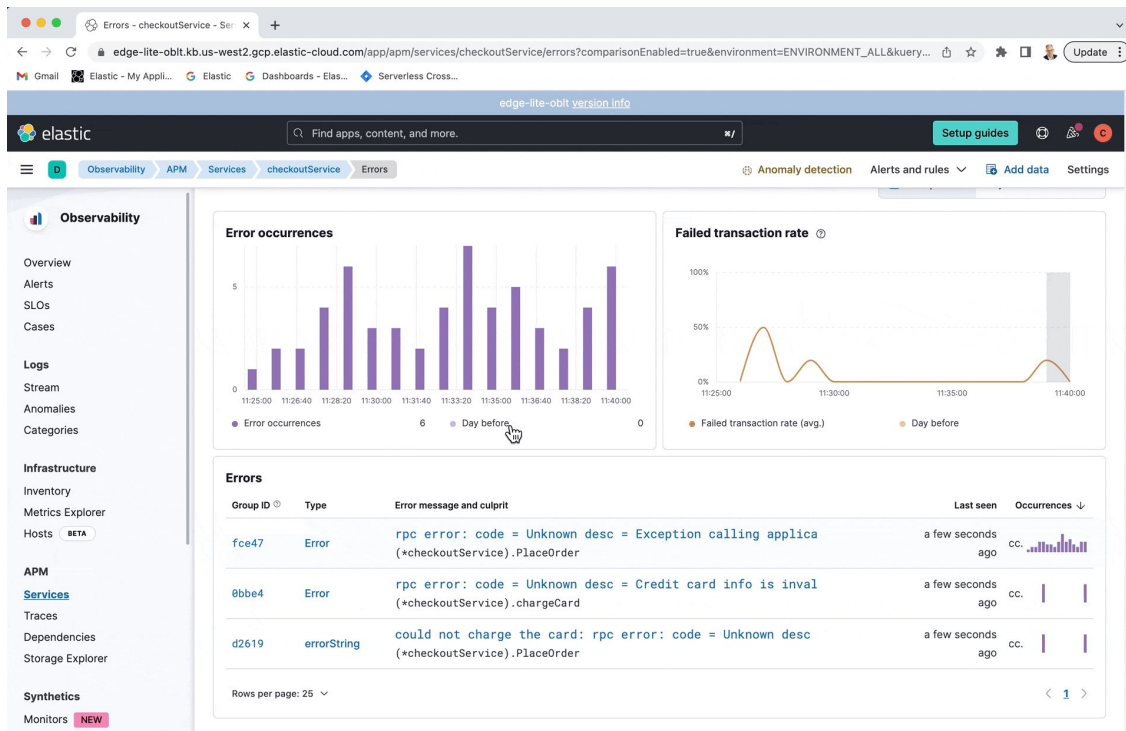
- Resolución de incidentes y seguimiento a alertas en contextos de datos privados
- Preguntas en lenguaje natural mediante la GenAI.
- Mejore el conocimiento de la operación de sus equipos de Security.
- Proporciona una manera sencilla de realizar un seguimiento del uso por usuario a través de un panel prediseñado.

The screenshot displays the Elastic Security interface. On the left, a navigation sidebar includes 'Security', 'Dashboards', 'Alerts', 'Findings', 'Timelines', 'Cases', 'Explore', and 'Intelligence'. The main area shows a list of alerts, with the top one selected: 'Memory Threat Prevention Alert: Windows.Trojan.Metasploit'. This alert is described as 'Generates a detection alert each time an Elastic Endpoint Security alert is received. Enabling this rule'. Below the alert list, several other alerts are visible, such as 'Unusual Windows Process Calling the Metadata Service', 'Anomalous Windows Process Creation', 'GCP Virtual Private Cloud Route Creation', 'GCP Virtual Private Cloud Route Deletion', 'Spike in Network Traffic to a Country', and 'Unusual Linux Username'. The right-hand pane provides a detailed view of the selected alert, including its status (Open), severity (High), risk score (73), and rule name. It also shows the alert reason, which details the process execution of 'notepad.exe' by 'james.spiteri' on 'bhusa-windows-2'. A 'Highlighted fields' table is also present, listing fields like 'host.name', 'agent.status', 'user.name', 'rule.name', 'process.executable', 'rule.type', 'process.name', 'process.parent.name', and 'process.args' with their corresponding values. At the bottom right, there is a 'Take action' button.

Field	Value	Alert prevalence
host.name	bhusa-windows-2	48
Agent status	Healthy	...
user.name	james.spiteri	15
rule.name	Windows.Trojan.Metasploit	3
process.executable	C:\Windows\System32\notepad.exe	6
Rule type	query	107020
process.name	notepad.exe	6
process.parent.name	cs5db455d821d79ef44975d61712506b5a89aeb63c0e940049b06b89947183.exe	3
process.args	C:\Windows\System32\notepad.exe	3

APM Error AI Assistant

“Explicue el error y
sugiera soluciones.”



Profiling AI Assistant

“Explicame el proceso/funciones más costosas dentro de fleet, y sugiereme como optimizarlos”

The screenshot shows the Elastic Universal Profiling interface. The browser address bar indicates the URL: `edge-lite-obit.kb.us-west2.gcp.elastic-cloud.com/app/profiling/flamegraphs/flamegraph?query=&rangeFrom=now-15m&rangeTo=now`. The Elastic logo and search bar are visible at the top. The navigation sidebar on the left includes sections like Inventory, APM, Services, Traces, Dependencies, Storage Explorer, Synthetics, Monitors, TLS Certificates, Uptime, Uptime Monitors, TLS Certificates, User Experience, Dashboard, Universal Profiling (BETA), Stacktraces, Flamegraphs, and Functions. The main content area is titled "Universal Profiling" and "Flamegraph". A search bar with the text "Filter your data using KQL syntax" and a "Last 15 minutes" filter is present. The Flamegraph itself is a heatmap showing CPU usage over time for various processes. A legend at the bottom identifies the processes: <symbolized frame>, Python, PHP, Native, Kernel, JVM/Hotspot, Ruby, and JavaScript. The URL at the bottom of the browser is `https://edge-lite-obit.kb.us-west2.gcp.elastic-cloud.com/app/profiling/functions?ku...`

Host Process AI Assistant

“Que es este proceso?
Como puedo
optimizar el uso de
CPU?”

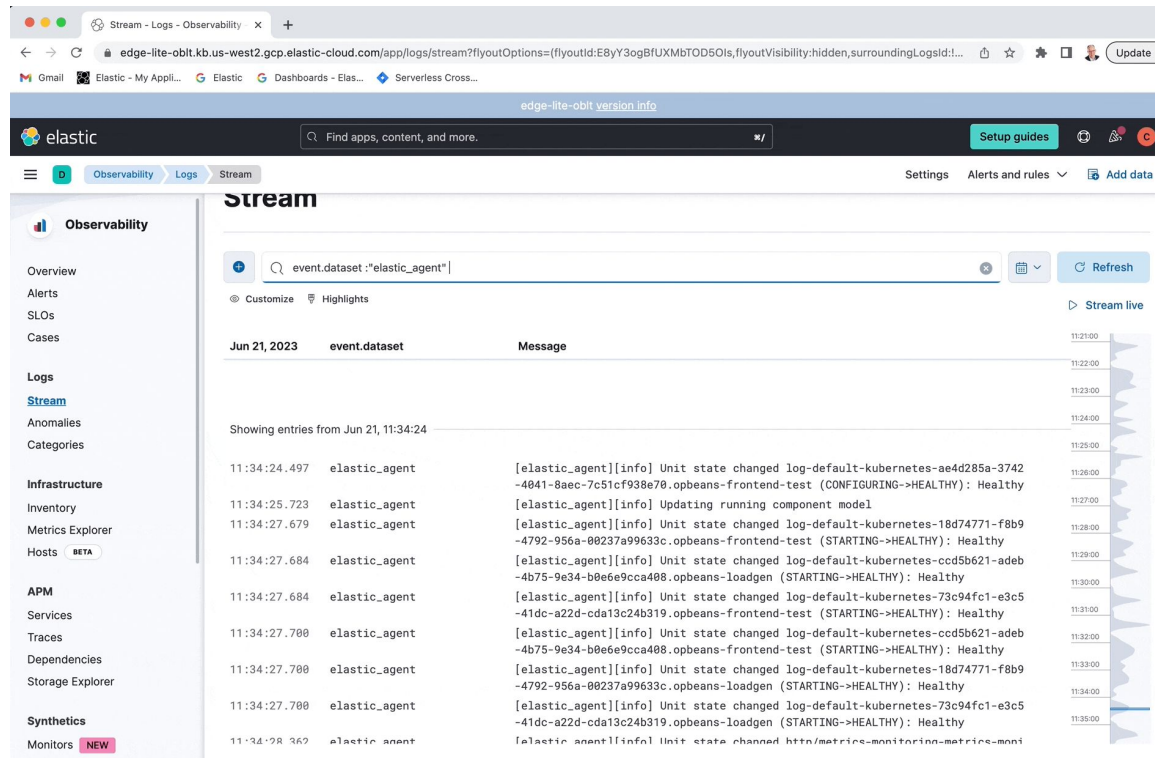
The screenshot shows the Elastic Observability interface for a host named `gke-edge-lite-obit-pool-1-00aa46be-t263`. The interface is divided into several sections:

- Hosts Summary:** Shows 6 hosts with an average CPU usage of 78.1%.
- Hosts Table:** Lists individual hosts with their CPU usage percentages.
- Process Summary:** Shows process counts for various states: Total processes (N/A), Running (N/A), Sleeping (N/A), Dead (N/A), Stopped (N/A), Idle (N/A), Zombie (N/A), and Unknown (N/A).
- Top processes:** A table listing the most active processes on the host.

State	Command	Time	CPU ↓	Mem.
> Sleeping	/opt/bitnami/java/bin/java -D...	00:59	79.8%	1.8%
> Sleeping	/bin/bash /opt/bitnami/script...	02:12	61.2%	0.7%
> Sleeping	/usr/share/elastic-agent/data...	1:56:09	34.7%	1.9%
> Sleeping	node /usr/share/heartbeat/.no...	00:17	25.5%	0.6%
> Sleeping	/usr/share/heartbeat/.cache/m...	01:01	20.9%	1.7%
> Sleeping	elastic-agent container -c /e...	1:56:11	20.9%	0.5%
> Sleeping	auditbeat -c /etc/auditbeat.y...	1:48:52	12.3%	0.5%
> Sleeping	/usr/share/heartbeat/.cache/m...	01:01	12.3%	0.7%
> Sleeping	/home/kubernetes/bin/kubelet ...	1:56:52	10.2%	0.7%

Log message AI Assistant

"Explicame este
mensaje del log,
generame un patrón de
búsqueda para
encontrar incidentes
similares"



The screenshot displays the Elastic Observability Stream interface. The search query is `event.dataset:"elastic_agent"`. The results table shows log entries from June 21, 2023, at 11:34:24. The messages are informational logs from the `elastic_agent` component, indicating state changes for various Kubernetes pods.

Time	Event Type	Message
11:34:24.497	elastic_agent	[elastic_agent][info] Unit state changed log-default-kubernetes-ae4d285a-3742-4841-8aec-7c51cf938e70.opbeans-frontend-test (CONFIGURING->HEALTHY): Healthy
11:34:25.723	elastic_agent	[elastic_agent][info] Updating running component model
11:34:27.679	elastic_agent	[elastic_agent][info] Unit state changed log-default-kubernetes-18d74771-f8b9-4792-956a-08237a99633c.opbeans-frontend-test (STARTING->HEALTHY): Healthy
11:34:27.684	elastic_agent	[elastic_agent][info] Unit state changed log-default-kubernetes-ccd5b621-adeb-4b75-9e34-b0e6e9cca488.opbeans-loadgen (STARTING->HEALTHY): Healthy
11:34:27.684	elastic_agent	[elastic_agent][info] Unit state changed log-default-kubernetes-73c94fc1-e3c5-41dc-a22d-cda13c24b319.opbeans-frontend-test (STARTING->HEALTHY): Healthy
11:34:27.700	elastic_agent	[elastic_agent][info] Unit state changed log-default-kubernetes-ccd5b621-adeb-4b75-9e34-b0e6e9cca488.opbeans-frontend-test (STARTING->HEALTHY): Healthy
11:34:27.700	elastic_agent	[elastic_agent][info] Unit state changed log-default-kubernetes-18d74771-f8b9-4792-956a-08237a99633c.opbeans-loadgen (STARTING->HEALTHY): Healthy
11:34:27.700	elastic_agent	[elastic_agent][info] Unit state changed log-default-kubernetes-73c94fc1-e3c5-41dc-a22d-cda13c24b319.opbeans-loadgen (STARTING->HEALTHY): Healthy
11:34:28.362	elastic_agent	[elastic_agent][info] Unit state changed http/metrics-monitoring-metrics-moni

Log Alert triage AI Assistant

"Que pudo causar este
pico en el log, y como
puedo arreglarlo?"

The screenshot displays the Elastic Observability Alerts interface. The browser address bar shows the URL: `edge-lite-oblt.kb.us-west2.gcp.elastic-cloud.com/app/observability/alerts?_a=(query:%27%27,rangeFrom:now-15m,rangeTo:now,status:all)`. The page title is "Alerts" and the breadcrumb is "Observability > Alerts".

Summary statistics at the top right: Rule count 1, Disabled 0, Snoozed 0, Errors 0. A "Manage Rules" link is also present.

A search bar contains the text "Search alerts (e.g. kibana.alert.evaluation.threshold > 75)". Filter buttons for "Show all", "Active", and "Recovered" are visible. A "Last 15 minutes" time range selector and a "Refresh" button are also present.

The alert status is shown as "1 Alerts" with a warning icon and "Active now". Below this is a line chart showing the alert count over time, with a peak at 11:45. The x-axis ranges from 11:31 to 11:45 on June 21, 2023.

Table headers: Columns, 1 field sorted, 1 alert, Fields. Updated 20 seconds ago.

Actions	Alert Status	Last updated	Duration	Reason
<input type="checkbox"/>	Active	Jun 21, 2023, 11:45:35.885 (UTC-4)	364 min	1093 log entries in the last 5 mins. Alert when > 1.

Liderazgo en Análisis de Seguridad, Log Analytics, y Búsqueda



Observability

Strong Performer in The Forrester Wave™: **AIOps**, Dec. 2022

Visionary in the Gartner® Magic Quadrant™ for **APM and Observability**, Dec. 2022



Security

Leader in The Forrester Wave™: **Security Analytics Platforms**, Dec. 2022

Visionary in Gartner® Magic Quadrant™ for **SIEM**, Oct. 2022

Major Player in the IDC MarketScape: Worldwide **SIEM** 2022 Vendor Assessment



Search

Leader in the Gartner® Magic Quadrant™ for **Insight Engines**, Dec. 2022

Leader in The Forrester Wave™: **Cognitive Search**, Jul. 2021

Gartner®

FORRESTER®



Gracias

Alan Cuevas - alan.cuevas@elastic.co
Edgar Garza - egarza@ventus-tech.com