Chaos is a Ladder-

Navigating Sophisticated Cyber Attacks with Machine Learning & Threat Intel

Simranjeet Ahuja
Principal Solution Architect- Security Specialist
Feb-2026

Who am i?

- Simranjeet Singh Ahuja
- Principal Solution Architect- Security Specialist
- 3rd Qtr. in Elastic
- 18+ years in Cyber Security
- Worked as Sales Engineer, Project Manager, PS Consultant, Support Engineer throughout my career.
- Last stint- NetWitness (RSA) as Tech Lead / Sr. SE

Qualifications-

- MBA- Technology Management from IIT Delhi
- M-Tech- IT from IP Univ, Delhi
- B-Tech- IT from IP Univ, Delhi
- Diploma- Business Management- Kyoto University, Japan

elastic


COMPLEX
COMPLICATED

Problem Statement

The Uncomfortable Truth-

What would be Chaos in Security?

Chaos is not randomness, chaos is complexity behaving unpredictably at scale.

Google Cloud (or any hyperscaler), you have:

- Millions of API calls per day
- Ephemeral compute instances
- Autoscaling Kubernetes pods
- Service accounts acting autonomously
- Developers in multiple geographies

Each component behaves correctly.

But together? The system produces emergent behavior.

That’s’ Chaos

The Uncomfortable Truth-

Why Modern attacks are invisible?

Modern System today-

- Distributed
- Event Driven
- Identity Centric
- API First
- Cloud Native

Security ≠ Perimeter
Security = Telemetry + Correlation + behavior modeling

elastic

The Uncomfortable Truth-

Why Signature detection fails?

Signatures detect-

- Known Malware’s
- Known IP’s
- Known exploits

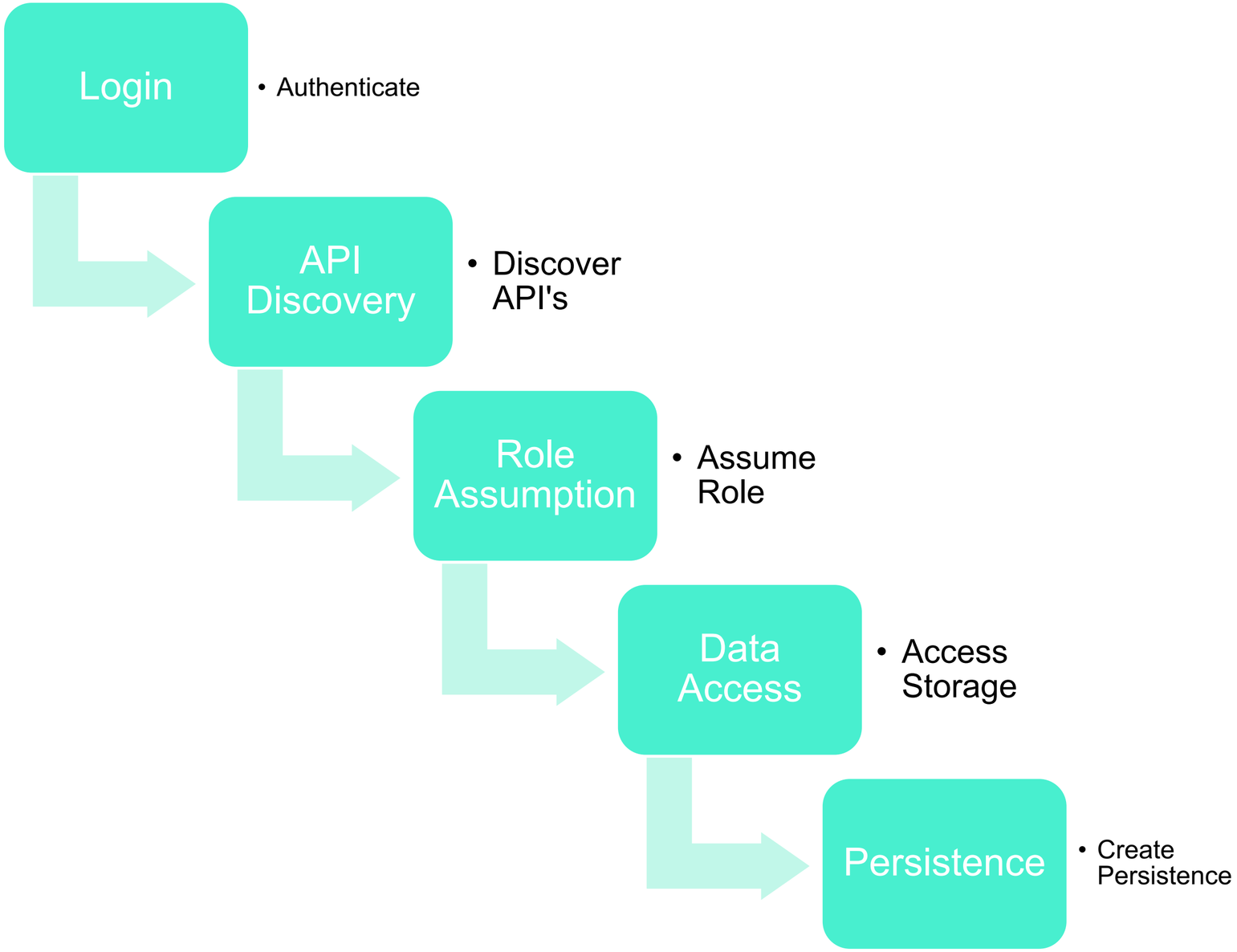
Modern attacks use-

- Valid Credentials
- Valid API’s
- Valid Infrastructure

elastic

Attack Walkthrough

Attack as a Workflow



Each Step Individually-

- Legitimate
- Logged
- Expected

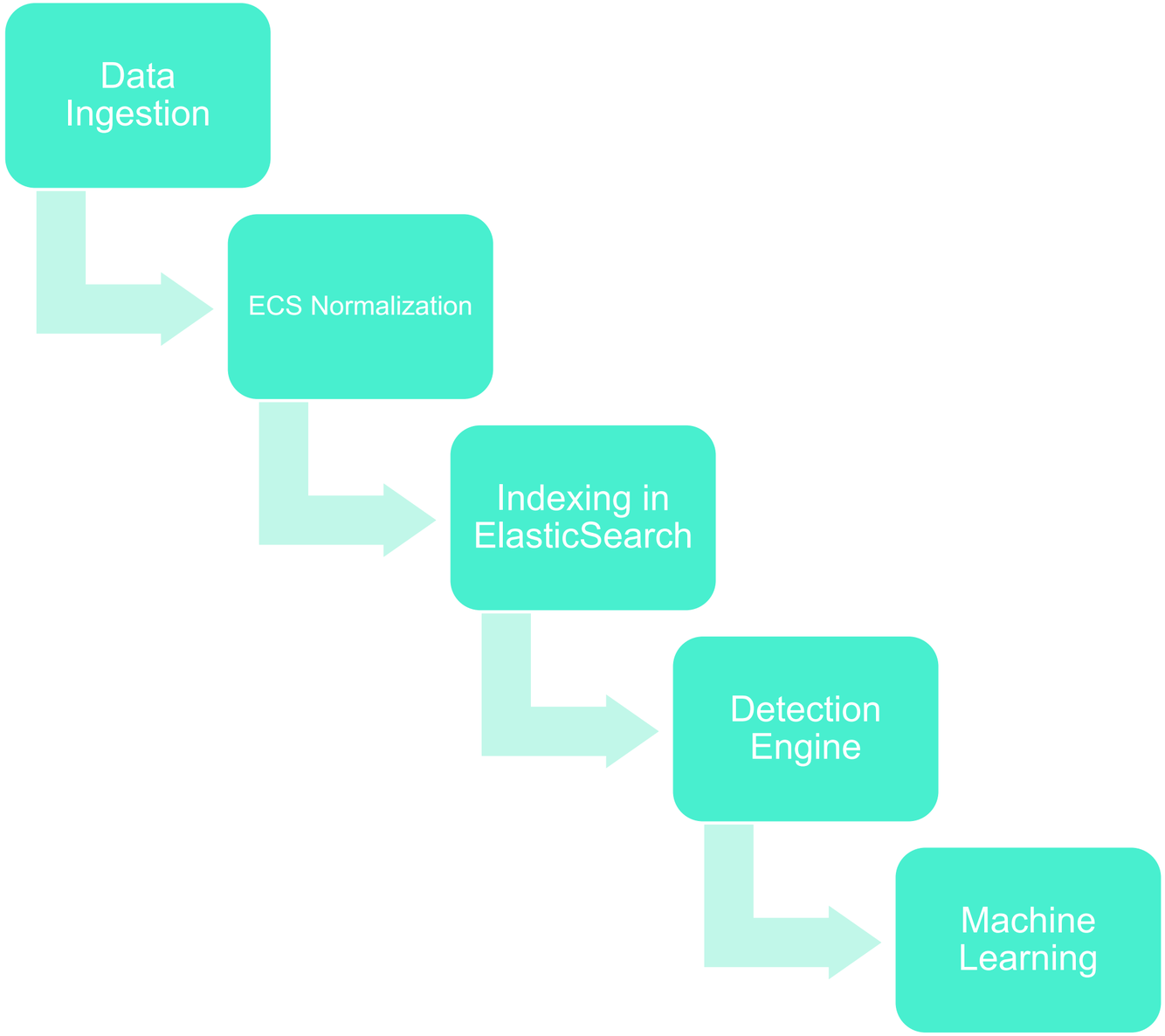
Hence, event is harmless

Detection Requires-

- Sequence Modeling

elastic

Elastic Architecture



elastic

Attack Workflow- Detection with Behavior Modeling

- Per-User Login Patterns
- Per-Host process patterns
- API Usage baselines
- Data Transfer Baselines

Statistical ML Models

- User X logs at 3am from another country

Unsupervised- Anomaly Score

Attackers optimize around thresholds, ML optimizes around deviation.

Threshold rule:
Alert if > 5GB download

Attacker:
Download 200MB/hour

ML detects:
Rare pattern over time

elastic

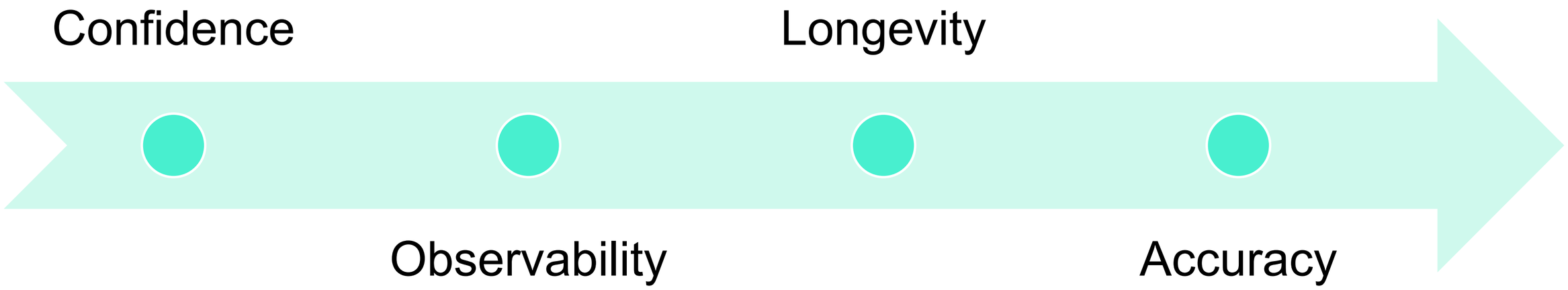
Threat Intel- Let’s Add Context

- Known bad IPs
- Known Domains
- Malware Hashes
- Campaign Attributes

elastic

Information to Intelligence

COLA Scoring Concept



elastic

Detection Ladder

elastic

Attack Detection Lifecycle

ML
- Login Anomaly

EQL
- IAM Escalation

ML
- Rare Data access

Threat Intel
- IOC Enrichment

ML
- Risk score threshold

elastic

What does this mean?

- Structured Logs
- Identity Visibility
- Correlation of Data telemetry
- Context enrichment
- Risk score threshbold

ML

To Summarize

Profound Reality

High-dimensional, high-velocity, legitimate behavior, where malicious intent is indistinguishable from automation.

That’s why we need:

- Machine Learning → to detect deviation
- Threat Intelligence → to detect intent
- Correlation → to detect narrative

Without modeling it, chaos overwhelms defenders.

With modeling, **chaos becomes a ladder.**

elastic

In the End…

“Happiness can be found, even in the darkest of times, if one only remembers to turn on the light.”

Prof. Albus Dumbledore

elastic

Thanks!

elastic