carahsoft

elastic

Elastic Engineer Accreditation Workshop

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Elastic, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/elasticresources

Join Events & Webinars:
carah.io/elasticevents

Discover Technology Solutions:
carah.io/elastic

Learn About Procurement:
carah.io/elasticcontracts

Connect With Our Team:
elastic@carahsoft.com
571-590-6810

ELASTIC SECURITY

Engineer Accreditation Workshop

Hosted at Carahsoft · Federal & Public Sector Partner SEs

PRESENTERS

- **Peter Gignac** Senior Solutions Architect — Partner
- **Thonda Taylor II** Senior Solutions Architect — Partner

August 11, 2026 | elastic · The Search AI Company

WORKSHOP OUTCOMES

Today's Goal

- ✓ Pass the accreditation test
- ✓ Demo Elastic Security confidently
- ✓ Position Elastic for federal use cases

Elastic Security SE Accreditation

Badge confirmed on-site today

- ✓ Hands-on SIEM lab experience
- ✓ Agentic SOC demonstration
- ✓ FedRAMP & SOAR differentiation

AUGUST 11, 2026 · CARAHSOFT

Workshop Agenda

TIME	DURATION	TOPIC
9:00-9:30	30 min	👋 Welcome, Setup & Accreditation Overview
9:30-10:00	30 min	🔍 Elastic Security Deep Dive
10:00-12:00	120 min	🧪 Security Analyst Essentials Lab (9.x)
11:30-12:30	60 min	🍽️ Lunch
12:30-1:30	60 min	🤖 Agentic SOC Demonstration
1:30-1:45	15 min	☕ Break
1:45-2:15	30 min	💬 Partner Q&A & Federal Discussion
2:15-2:45	30 min	🎖️ Accreditation Test & Badge Confirmation

SETUP

Before We Begin: Prerequisites

Partner Portal Access

1. Go to elastic.co/partners
2. Click ‘Partner Portal Login’
3. Select ‘Request Access’ if new
4. Required for accreditation registration
5. Takes ~5 minutes to complete

Environment Setup

- Laptop with browser (Chrome preferred)
- WiFi connected — confirm network
- Instruqt lab link ready:

  🔗 `https://ela.st/carahsoft-partners`

- Elastic partner portal login credentials

PARTNER ENABLEMENT

Partner Learning Paths — get engaged

From foundation to certified delivery — three levels, all self-paced. Free training starts today.

FREE TRAINING
elastic.co/training

PARTNER ENABLEMENT CENTER
elastic.co/partners

01 · START — 02 · CERTIFY — 03 · DELIVER

START HERE

Foundation & Accreditations

Self-paced · On-demand

- Elastic Fundamentals
- Search AI, Obs & Security Fundamentals
- Partner Portal overview & Workshops
- Partner Sales Professional track
- Partner Sales Engineer track
- Partner Solutions Architect track

Get Accredited → Partner Portal

GET CERTIFIED

Certifications

Self-paced · On-demand

- Elasticsearch Engineer
- Elastic Observability Engineer
- Elastic Security for SIEM
- Data Analysis with Kibana
- Free self-paced or paid ILT
- Cohorts up to 25

Earn Certifications → learn.elastic.co

GO DEEPER

Service Delivery Enablement

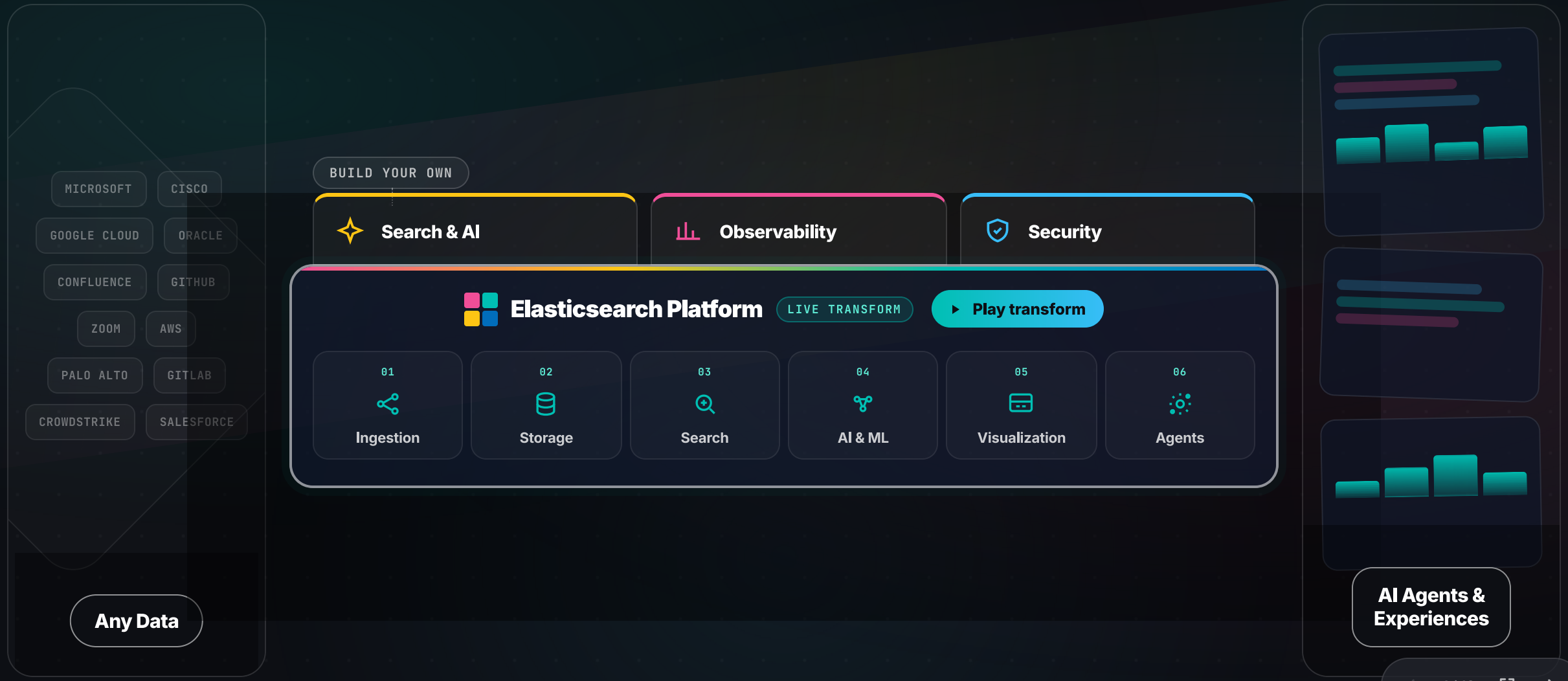
Requires certification

- Phase 1: Foundational labs & delivery
- Phase 2: Deep-dive in chosen area
- Phase 3: Assessment to validate readiness
- Unlocks billable delivery on engagements

Start Service Delivery → Partner Portal

ASK **Pick a path this week — accreditation first, then certs, then billable delivery. I'll help you get into the Partner Portal.**

Elastic provides precise context for AI and Search



SECURITY DEEP DIVE

Elastic Security: Core Tenets & Platform

SIEM
Unified security analytics for logs, metrics & alerts

Detection Engine
Rules-based + ML detection with MITRE ATT&CK mapping

AI Capabilities
Attack discovery, auto-triage & natural language queries

FedRAMP Ready
Authorized for US federal workloads & data sovereignty

CORE TENETS

Unified Security Operations
SIEM + EDR + Cloud Security on one platform. Single workflow for detection, investigation, and response.

Open and Transparent
300+ integrations, open-source rules, community-shared detections. No vendor lock-in.

Distributed Data Mesh
Federated search across distributed data sources. No centralization required.

AI-Powered Operations
AI Assistant uses NLP to streamline alert investigation, incident response, and query generation.

TEST NOTE

"Approach Agent-less Data Collection" is **NOT** a core tenet — Elastic uses Elastic Agent for data collection.

Storage tiers: data ages down. Cost falls.

Hot → Warm → Cold → Frozen — automated lifecycle. Frozen lands as a searchable snapshot in S3.

Consumption / cost — Storage spend drops as data ages through each tier — $$$ → ¢

Query stays live — Search slows a bit — no re-hydration, still online — ms → min

Hot

NOW · DAYS

COST / GB — $$$

Fast SSDs · full replicas

QUERY — ms

Instant search

Real-time detections, ML jobs & live dashboards.

Warm

WEEKS

COST / GB — $$

Fewer replicas · still local

QUERY — ~s

Still quick

Recent history — queried less often, still snappy.

Cold

MONTHS

COST / GB — $

Dense nodes · max compress

QUERY — secs

Slower · still online

Compliance window without the SSD bill.

Frozen

YEARS

COST / GB — ¢

Object store pricing

QUERY — min

No rehydrate · still searchable

SEARCHABLE SNAPSHOT

Lives in S3

Query object storage without restoring a full copy first. Enterprise.

S3 · object store

PUNCHLINE **100% searchable across every tier — no re-hydration. Frozen = searchable snapshot in S3.**

AUTOMATED ILM · COST ↓ · YEARS RETAINED

Deployment, Licensing & Architecture

Licensing Tiers

- **Free / Basic**: Core features only
- **Platinum**: Advanced ML features
- **Enterprise**: Searchable Snapshots + Endpoint Response Actions + ECK automation

Pricing: resource-based. **Single SKU** — Security + Observability + Search.

MSSP Multi-Tenancy

- Dedicated cluster per tenant **(recommended)**
- Optional overview via Cross-Cluster Search (CCS)
- Single shared cluster for all tenants **NOT recommended**
- Independent scaling + data isolation per tenant

Monitoring Best Practice

Use a **DEDICATED** Elastic deployment for monitoring — never the production cluster. If production has issues, a co-located monitoring setup is also unavailable.

Endgame Migration: Soak Period

Run Elastic Agent alongside Endgame Sensor. Confirm Elastic Defend detects the same events before full cutover. **NOT** for backups, analyst training, or system reboots.

SECURITY DEEP DIVE

Cloud Security, MTTR & Certifications

Cloud Security & CSPM

- **CSPM** identifies misconfigurations AND detects real-time threats in cloud environments.
- **Coverage:** AWS, Azure, GCP — runtime threats, compliance posture, misconfiguration alerts.

SIEM EDR Cloud Security

Elastic Certifications for Security Professionals

DEEP TECHNICAL

Elastic Certified Engineer

Cluster management, performance, and configuration.

SECURITY-SPECIFIC

Elastic Security for SIEM

Threat detection, investigation, and response workflows.

Reducing MTTR

Elastic treats security as a **data problem** — enabling comprehensive analysis and rapid threat hunting across all sources. This underpins attack progression insights + IR workflow integration.

Beyond This Badge

This workshop earns the **Security SE accreditation**. Full certifications are deeper, exam-based paths available in the Elastic partner portal.

LAB

Hands-On Lab: Security Analyst Essentials

90–120 minutes | **Elastic 9.x** | Self-paced via Instruqt | https://ela.st/carahsoft-partners

01

Elastic SIEM

- → Navigate the Security dashboard
- → Ingest & normalize log sources with ECS
- → Build timeline investigations
- → Host isolation and response actions

02

Detection Engine

- → Enable prebuilt MITRE ATT&CK rules
- → Create a custom threshold detection rule
- → Manage alerts: triage, investigate, close
- → Understand rule severity & risk scoring

03

AI Capabilities

- → Run Attack Discovery on alert clusters
- → Use the AI assistant for triage queries
- → Write ES|QL queries in natural language
- → Review AI-generated case summaries

AGENTIC SOC · AIOPS PIPELINE + ELASTIC WORKFLOWS · 12:30–1:30 PM

From alert to closed case — machine speed, human judgment

01

Alert Ingestion

Unify the signal plane before AI ever touches a case.

Logs · EDR · Cloud telemetry

02

AI Triage

Prioritize real attacks and collapse noise into narrative.

Attack Discovery · Auto-summarize

03

Elastic Workflows

Automate response with platform-native logic — no bolt-on SOAR tax.

Automated response · SOAR-free logic

04

Resolution & Report

Close the loop with an AI-written narrative ready for leadership.

Case closed · AI narrative

KEY TAKEAWAY

Elastic Workflows replaces standalone SOAR — native automation at no additional license cost.

ARCHITECTURAL COMPARISON

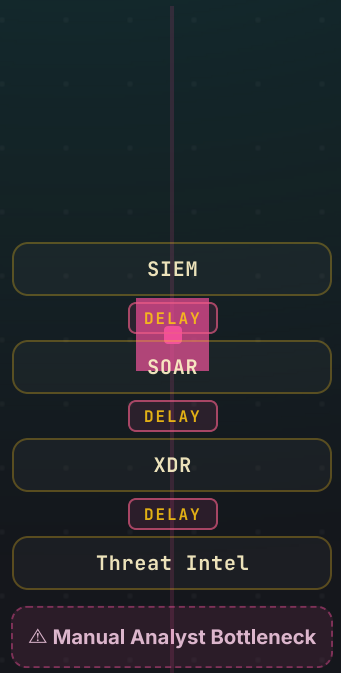
You can't bolt on an Agentic SOC

Meeting adversaries at machine speed requires a platform where data, AI, and automation are native.

HUMAN-IN-THE-LOOP

Legacy SOC

Slow, manual process. Analyst is the bottleneck. Disconnected tools create friction.



PRIMARY FOCUS

HUMAN-ON-THE-LOOP

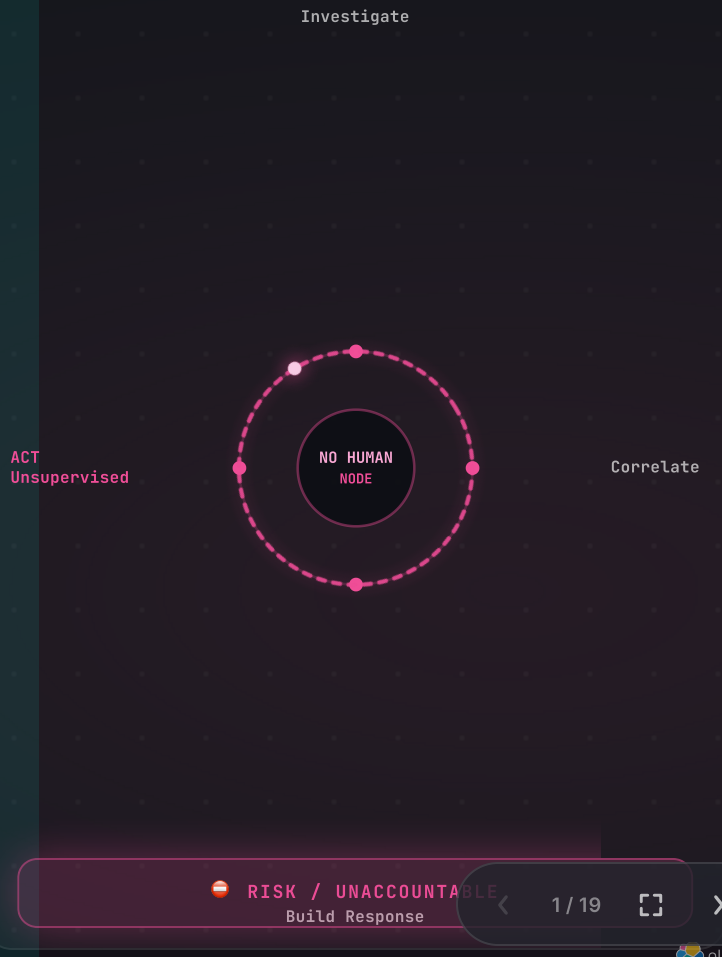
Agentic SOC

Machine speed with human judgment. Platform builds, analyst approves. Native, unified architecture.

NO OVERSIGHT

Theoretical Autonomous SOC

No human oversight. Risky and irresponsible. Not for security teams.



elastic

ACCREDITATION PREP

Test Review: Know Before You Go

25 questions · ~30 minutes · Pass = badge awarded on the spot

Core Tenets & Platform

4 TENETS — KNOW ALL

Unified Ops | Open / Transparent | Data Mesh | AI-Powered Ops

TRAP

"Agent-less Data Collection" is **NOT** a tenet.

UNIFYING STACK

SIEM + EDR + Cloud Security on one single-SKU tech stack.

Data Architecture

ELASTIC AGENT — TWO JOBS

Protects hosts **AND** queries OS for detection data.

PIPELINES VS ECS

- **Pipelines:** pre-indexing transform — not viz/access
- **ECS:** common fields; 300+ auto-normalized

ANY DATA, ANY SOURCE

Apps, Cloud, DBs, Hosts, Users, Network, IoT/OT.

Detection and AI

1,000+ PREBUILT RULES

Aligned to **MITRE ATT&CK** — not NIST, ISO, or OWASP.

ATTACK DISCOVERY & AI ASSISTANT

Prioritizes attacks into AI narratives; NLP streamlines investigations & queries.

AUTOMATION

Correlation rules + AI/ML — **not** static/manual only.

Storage Tiers & Retention

- **Hot:** real-time detections, ML jobs, live dashboards — fastest
- **Warm:** recent data, queried less often
- **Cold / Frozen:** Searchable Snapshots — low-cost long-term. Requires **Enterprise** (not Free/Basic or Platinum)

Licensing and Deployment

PRICING & MULTI-TENANCY

Resource-based (no per-user). **Dedicated cluster per tenant** — shared cluster not recommended.

ENTERPRISE UNLOCKS

Searchable Snapshots · Endpoint Response Actions · ECK automation.

MONITORING

Dedicated deployment — never monitor on production itself.

Cloud, MTTR & Migration

CSPM

Misconfigurations **AND** real-time cloud threats.

ENDGAME SOAK & MTTR

Run Agent + Endgame for parity. Security as a **data problem** → rapid hunting.

CERTIFICATIONS

Elastic Certified Engineer · Elastic Security for SIEM — deep exam paths.

⚠ HIGH-YIELD WATCH-OUTS

"Agent-less" is NOT a tenet · Hot tier = real-time detections · **Enterprise** for Searchable Snapshots · CSPM = misconfigs **AND** real-time threats · **MITRE ATT&CK** (not NIST or ISO)

CLOSE

Accreditation Test & Badge

2:15–2:45 PM · **Badge confirmed on-site today**

What to Expect

FORMAT	Partner portal online assessment
DURATION	Approximately 30 minutes
COVERAGE	SIEM, Detection Engine, AI features
SCOPE	Elastic 9.x content from today's lab
PASS	**Badge awarded immediately** upon passing
RETAKE	Available if needed after review

Steps to Get Your Badge

1. Log in to the Elastic Partner Portal
2. Navigate to Training & Accreditation
3. Select 'Elastic Security SE Accreditation'
4. Complete the assessment
5. Download and share your badge
6. Add to LinkedIn & partner portal profile

YOU'RE ACCREDITED

You're Now an Elastic Security SE

Share Your Badge

LinkedIn + partner profile

@Elastic

Run a Customer Demo

Use **today's lab flow** as your demo script

Enable Your Team

Share the **Instruqt link** with your colleagues

elastic