AWS AI COMPETENCY

AI-Powered Autonomous Cloud Security Operations

Powered by Agentic AI and Generative AI on AWS

Delivered by Batif Services Private Limited

● PUBLIC CASE STUDY

CLIENT	INDUSTRY	MARKET SEGMENT	CASE STUDY TYPE
Dedups.ai	Cloud Security / Software and SaaS	Technology (B2B)	Public

The Opportunity

Dedups.ai set out to build an AI-powered cloud security operations platform on AWS that continuously monitors cloud environments, identifies security risks and misconfigurations, investigates findings, explains business impact, recommends remediation, and supports controlled automated remediation - shrinking the gap between detection and response.

The goal was to reproduce the judgement of an experienced security analyst at machine speed and scale: not just surfacing findings, but correlating them, reasoning about their impact, and preparing safe, standardized remediation - all while keeping a human firmly in control of any consequential change. In effect, the platform acts as a tireless first responder that triages and prepares, so security engineers can focus on decisions rather than data-gathering.

Why It Mattered

Cloud environments generate security findings from many services at once, and volume grows with every new workload. Security teams spend significant time turning those raw findings into safe, prioritized action - time that does not scale linearly with headcount. The pain points were clear:

- High volumes of findings arriving continuously from multiple security and monitoring services.
- Heavy manual effort to correlate related findings and identify the affected resources.
- Difficulty prioritizing which risks demanded immediate attention versus routine handling.
- Slow, manual preparation of remediation steps for each class of issue.
- Delayed response to high-risk issues, leaving misconfigurations exposed longer than acceptable.
- Investigation knowledge lived in individual analysts' heads, making the process hard to standardize.
- Every action needed an audit trail, yet manual investigation rarely produced consistent records.

Without automation, high-risk misconfigurations could stay exposed longer than acceptable while teams struggled to keep pace with cloud growth. Dedups.ai needed a system that could investigate at machine speed, standardize how findings are handled, and preserve human oversight and a complete audit trail at every step.

How Batif Solved It on AWS

Batif Services Private Limited designed and delivered an event-driven, serverless-first security operations platform on AWS. Findings from AWS Security Hub, Amazon GuardDuty, Amazon Inspector and AWS Config are routed through Amazon EventBridge into investigation workflows orchestrated by AWS Step Functions and AWS Lambda. Amazon Bedrock analyzes each finding to explain root cause, assess impact and generate remediation recommendations.

Sensitive remediation passes through human approval gates before execution. Security evidence and reports are stored in Amazon S3 and a managed database, with dashboards and APIs for continuous monitoring - keeping humans in control of consequential actions. The workflow encodes an analyst's playbook: gather context, correlate, assess, recommend, and only then act with approval.

The architecture is intentionally modular. New finding sources can be added to EventBridge without changing the investigation logic, and remediation actions are defined as discrete, permissioned steps - so the platform can grow in capability while its safety guarantees stay intact.

Solution Blueprint

Architecture Flow

AWS Security Services -> Amazon EventBridge -> Step Functions / Lambda -> Amazon Bedrock -> Investigation & Risk Analysis -> Human Approval (where required) -> Automated Remediation -> Verification -> Security Dashboard / Reports

Detect - aggregate findings from across the estate

- AWS Security Hub, Amazon GuardDuty, Amazon Inspector and AWS Config generate security and compliance findings.
- Amazon EventBridge captures findings and triggers the right investigation workflow based on type and severity.
- AWS CloudTrail supplies the activity context - who did what, when - used during investigation.
- New sources can be onboarded to EventBridge without altering downstream logic.

Investigate - reason about impact and priority

- AWS Step Functions and AWS Lambda orchestrate a structured investigation across permitted AWS resources.
- Amazon Bedrock correlates related events, explains root cause and assesses business impact in plain language.
- The platform prioritizes risk and generates standardized, repeatable remediation recommendations.
- Agentic steps operate strictly within least-privilege boundaries, so investigation never exceeds its mandate.

Remediate & Verify - act safely, then confirm

- Sensitive or high-impact actions pass through human approval gates before any change is made.
- Approved remediation runs through Lambda under least-privilege IAM roles scoped to the specific task.
- Post-remediation verification confirms the issue is genuinely resolved rather than merely acknowledged.
- Evidence, decisions and outcomes are recorded in Amazon S3 to form a complete, auditable trail.

Intelligence at Work

The platform pairs generative AI with agentic, tool-using workflows to investigate and act safely across the cloud environment. Generative AI supplies the reasoning and explanation; the agentic workflow supplies the controlled, permissioned action. Core capabilities include:

- Natural-language security explanations of findings, root cause and business impact.
- Automated correlation of related events and affected resources into a single coherent picture.

- Risk prioritization across incoming findings, so the most urgent issues rise to the top.
- Recommended, standardized remediation steps that codify best practice.
- Agentic investigation across permitted AWS resources, gathering context the way an analyst would.
- Controlled remediation with human approval gates for sensitive or high-impact actions.
- Post-remediation verification, closing the loop and confirming resolution.

Model choice: Anthropic Claude 5.0 Sonnet on Amazon Bedrock was selected for its strength at correlating findings and producing clear, standardized remediation guidance; Amazon Titan Text and Meta Llama 3 were also evaluated on reasoning quality, consistency and cost. Amazon Bedrock keeps model choice flexible, allowing the platform to adopt stronger models over time without re-architecting the workflow.

The AWS Toolkit

AWS Service	Purpose
Amazon Bedrock	Foundation model layer for security explanation, impact assessment and remediation recommendations.
AWS Security Hub	Central aggregation of security findings and posture across the environment.
Amazon GuardDuty	Threat detection feeding findings into the investigation pipeline.
Amazon Inspector	Vulnerability and workload findings for prioritization and remediation.
AWS Config	Configuration and compliance findings used to detect misconfigurations and drift.
AWS CloudTrail	Activity history used as context during investigation and for audit.
Amazon EventBridge	Event-driven triggering of investigation workflows from incoming findings.
AWS Step Functions	Orchestration of multi-step investigation and remediation workflows with approval gates.
AWS Lambda	Serverless execution of investigation logic and approved remediation under least privilege.
Amazon S3	Secure storage of security evidence, decisions and generated reports.
Amazon CloudWatch	Observability across workflows, model invocation and platform health.
AWS IAM & AWS KMS	Least-privilege authorization for every action and customer-managed encryption keys.
Amazon API Gateway	Exposes monitoring and reporting APIs for the platform.

Engineered for Trust

Security and Governance

- Backend Lambda and workflow components run inside a dedicated VPC with private subnets; API access is controlled through Amazon API Gateway.
- Evidence and reports are encrypted at rest with AWS KMS keys in Amazon S3; all data in transit uses TLS 1.2 or higher.
- AWS IAM enforces least privilege, with remediation roles scoped narrowly to the specific action they perform.
- Every investigation and remediation step is retained as an auditable trail via AWS CloudTrail and stored evidence.

Responsible AI

- Investigations and recommendations are grounded in actual findings, resource context and activity history - never invented.
- The platform explains root cause, business impact and the evidence behind each remediation recommendation.
- Sensitive and automated remediation is governed by approval gates, keeping humans in control of consequential change.
- Agentic actions stay within permitted resources under least privilege, so autonomy never outruns authorization.

Batif's Delivery Role

Batif Services Private Limited acted as the end-to-end design and delivery partner, owning the engagement from architecture through to operations and handover:

- AWS solution architecture across detection, investigation and controlled remediation.
- Security-service integration including Security Hub, GuardDuty, Inspector, Config and CloudTrail.
- AI and generative AI implementation on Amazon Bedrock for grounded investigation and remediation.
- Agentic workflow design encoding the analyst playbook into Step Functions and Lambda.
- Approval-gate and guardrail design to keep humans in control of sensitive actions.
- Dashboard and API integration for centralized monitoring and reporting.
- Security governance including least-privilege IAM, KMS encryption and complete audit logging.
- Deployment, operational monitoring, runbook creation and knowledge transfer to the Dedups.ai team.

Value Delivered

- Reduced manual investigation effort across incoming findings, freeing analysts for higher-value work.
- Faster response to high-risk cloud security issues through automated, event-driven investigation.
- Standardized, consistent remediation recommendations that no longer depend on individual expertise.
- Centralized visibility into the security posture of the environment.
- An auditable investigation and remediation trail for compliance, review and continuous improvement.
- Human oversight preserved for every consequential action, balancing speed with safety.
- Scalable security operations that keep pace with cloud growth without proportional headcount.

Built to Scale

- Highly available: EventBridge, Step Functions, Lambda, S3, API Gateway and Bedrock span multiple Availability Zones.
- Auto-scaling: serverless orchestration absorbs finding-volume spikes without manual capacity management.
- Serverless-first: no self-managed infrastructure, reducing operational overhead and simplifying operations.
- Extensible: new finding sources and remediation actions plug in without reworking the core workflow.

- Cost-efficient at scale: pay-per-use services keep spend aligned to actual finding volume and activity.