SOLUTION BRIEF

AiStrike for AWS Investigation and Response

Cloud infrastructure today is the primary target for malicious actors. The risk of exposure of cloud assets continues to grow as organizations expand their cloud footprint and new cyberattacks targeting cloud infrastructure emerge.

AWS native security tools do a great job in providing visibility into security issues in the cloud. However, organizations are struggling with the piling backlog of alerts and continuous increase in meantime to respond (MTTR). Some key challenges security teams face include:

- Large volume of alerts
- Lack of context
- Duplicate or repeat alerts across different AWS entities and accounts
- Identifying the root cause of the alert
- Tracking down the origin of the artifact in the cloud software development lifecycle
- Manual remediation actions

AiStrike for AWS

AiStrike complements AWS native cloud security tools with automated investigation and response capabilities aligned to AWS detections enabling organizations to rapidly triage, investigate, and respond to the most critical cloud threats. Some of the key capabilities of AiStrike for AWS solution include:

Frictionless Integration with AWS Ecosystem Tools

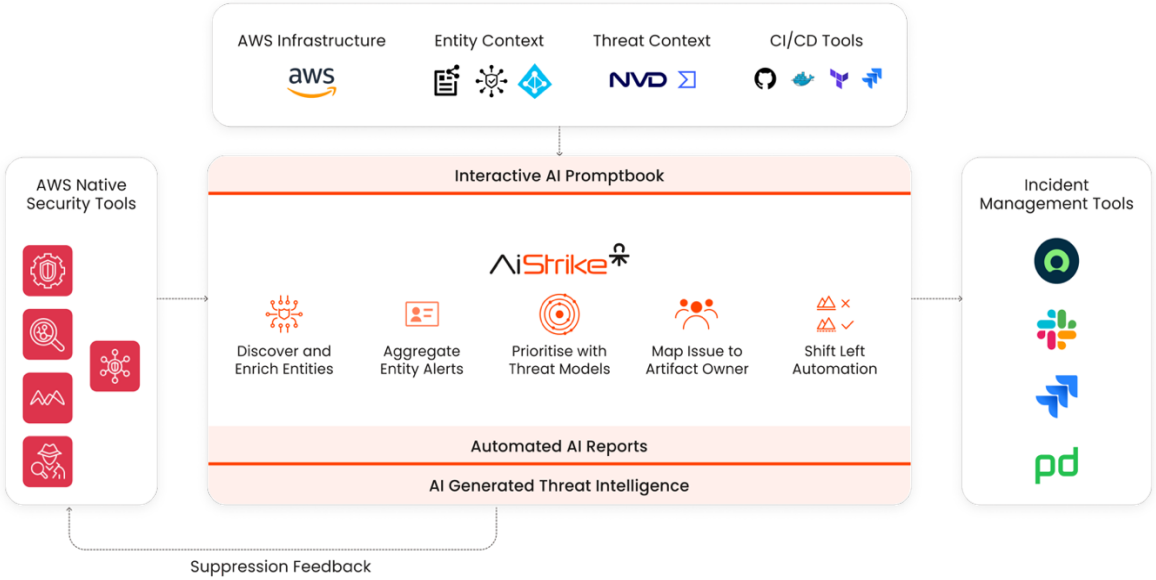
AiStrike seamlessly integrates with AWS infrastructure, AWS CloudTrail, and AWS native security tools for application security and threat detection including:

- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie
- AWS Access Advisor
- AWS Security Hub

Alert Context Enrichment

AiStrike automatically discovers AWS infrastructure and correlates it to findings from AWS security tools and the business context information, to create an enriched cloud infrastructure map.

Organizations get complete visibility into their cloud inventory, risk posture and business context with the ability to search and graphically visualize data and assess exposure using query and graph builder, and AI-guided promptbooks.



Analytics-based Entity Profiling

At the center of any activity on AWS is an AWS resource or entity such as a EC2 instance. AiStrike uses machine learning-based analytics to build a behavior profile of AWS entities. Any alert is compared against the baseline profile to suppress noise and identify rare and suspicious outlier activity.

Alert Correlation and MITRE Threat Modeling

AiStrike correlates alerts across AWS security tools and ties them to unique AWS entities. For example, correlating vulnerabilities identified by Amazon Inspector to GuardDuty alerts for the same host. With correlated alerts for the entity, AiStrike detects patterns such as:

a) Toxic combination of alerts aligned to MITRE ATT&CK stages. AiStrike prioritizes such alerts as a composite threat that requires immediate action
b) Repeated alerts that are tied to a common root cause and can be resolved by a single remediation action

In addition to the alert and vulnerability severity, AiStrike factors in behavior profile, MITRE stages, exposure, and business context to assign a true priority for an alert.

AiStrike creates an automated investigation report for every alert that outlines the complete context for the alert, prioritization, and recommended remediation actions.

Mapping Artifact to Origin and Owner

AiStrike automatically discovers and maps the artifact in the alert to its origin in the CI/CD pipeline. For example, in the case of a vulnerable EC2 image, AiStrike maps the EC2 image to its origin in the software code and the code owner. AiStrike updates its remediation workflow with the stakeholder information so that the right owner is notified of the expected remediation actions and timelines.

Single-Click Response Automation

AiStrike provides automation with one-click from the user interface to remediate issues from code to cloud. The automations are embedded in the workflows that are based on industry best practices. Users can customize the workflow to align with their own business needs. AiStrike provides detailed tracking and reporting on remediation status against pre-defined SLAs.

AiStrike integrates with industry standard incident management tools including, ServiceNow, JIRA, and Slack to provide a seamless remediation experience.

Alert Suppression in GuardDuty

AiStrike uses native GuardDuty APIs to create automated suppression rules for noisy and repeat alerts. Customers can review and apply the suppression rules with one-click from the AiStrike console.

Feedback to AWS

Where supported by AWS as in case of Amazon GuardDuty, AiStrike generates feedback for AWS product teams based on learnings from analyst response actions and feedback.

AI-Guided Co-Pilot

AiStrike simplifies the overall user experience from investigation to response with an AI-guided experience. End users can ask any question related to an alert, external threat, investigation, or response action and get AI-generated responses and automation. AiStrike AI co-pilot learns from trained datasets within AiStrike which avoids any direct exposure to internet and possibility of hallucination.

Get Started in Minutes

AiStrike is available on AWS marketplace. Click here to request a demo or visit AWS marketplace for more information.