AiStrike

CASE STUDY

# Global Software Design Company Leverages AiStrike to Investigate Cloud Alerts

**87%**
Alert Noise Suppression

**$287K**
Annual Savings in Man Hours

**2 Weeks**
Time to Deploy and Value

# CASE STUDY : GLOBAL SOFTWARE DESIGN COMPANY LEVERAGES AISTRIKE TO INVESTIGATE CLOUD ALERTS

## The Challenge:

The organization uses native security tools from the cloud service provider (CSP) to monitor their cloud environment. The native detection tools generate excessive noise with overwhelming volume of low-fidelity alerts, making it challenging to focus on real security threats. Additionally, the company has separate teams for cloud security and security operations, introducing inconsistencies and blind spots in responding to threats.

Key challenges faced by the organization includes:

- **Alert Fatigue :** Too many alerts from Cloud Security Posture Management (CSPM) and Cloud Detection and Response (CDR) tools
- **Limited resources :** >10% alerts vetted and investigated, leading to potential security gaps
- **Blind Spots :** Cloud security team operates in isolation from the Security Operations Center (SOC), leading to inconsistencies and likelihood of missing critical threats

## The Solution:

To address the challenges above, the organization sought a solution that aligned to their unique requirements. They selected AiStrike, an AI-powered security automation solution, due to its next-gen AI capabilities and its ability to maximize the return on investment (ROI) on their existing tools and resources.

With AiStrike, the organization was able to automate investigation for every alert in the cloud environment.

The solution leveraged purpose-built AI and ML models to:

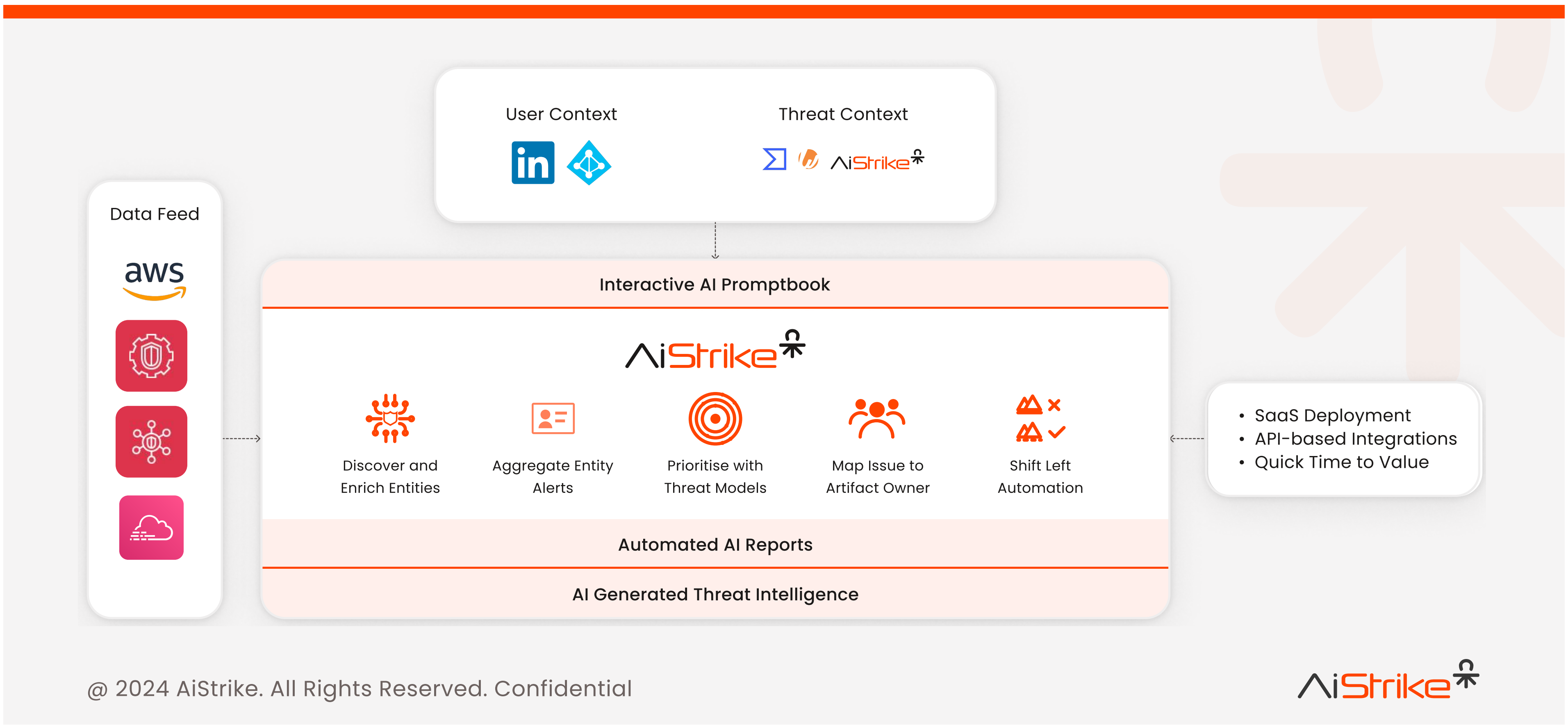
- **Consolidate Alerts by Root Cause :** AiStrike grouped related alerts to identify the underlying issues, reducing noise and simplifying the investigative process.
- **Prioritize High-Risk Threats :** Critical alerts were elevated based on risk, allowing the security team to focus on the most important threats while deprioritizing lower-risk alerts that did not require immediate attention.
- **Continuously Evaluate Threat Posture :** AiStrike continuously assessed the organization's cloud security posture against emerging threats, providing proactive risk management and minimizing exposure to new attack vectors.
- **Consistently Investigate and Prioritize Alerts :** AiStrike eliminated subjectivity with an consistent AI-powered alert investigation aligned with the SOC methodology. This approach bridged gaps and resolved blind spots caused by varied methods used by different teams.

## The Deployment:

AiStrike was deployed as a Software-as-a-Service (SaaS) solution, seamlessly integrating with the organization's existing data feeds through API-based connections. The deployment process was quick and efficient, with AiStrike becoming fully operational in the customer environment within just two weeks.

Key aspects of the deployment included:

- **SaaS Delivery :** AiStrike was implemented as a cloud-based service, minimizing the need for extensive on-premises resources and enabling rapid setup.
- **API-Based Integration :** AiStrike's API integration with the organization's data sources ensured seamless ingestion of events alerts and security events from existing tools.
- **Quick Time to Value :** Within two weeks, AiStrike began delivering prioritized alerts, comprehensive investigation reports, and actionable remediation recommendations, allowing the security teams to take quick actions.


User Context
Threat Context
AiStrike
Data Feed
aws
Interactive AI Promptbook
AiStrike
Discover and Enrich Entities
Aggregate Entity Alerts
Prioritise with Threat Models
Map Issue to Artifact Owner
Shift Left Automation
Automated AI Reports
AI Generated Threat Intelligence
• SaaS Deployment
• API-based Integrations
• Quick Time to Value
@ 2024 AiStrike. All Rights Reserved. Confidential
AiStrike

## Business Impact:

By implementing AiStrike, the organization gained complete visibility into their cloud risk posture, distinguishing between routine hygiene issues from high-risk threats requiring immediate actions. AiStrike not only provided detailed, actionable remediation steps but also offered automation options to expedite responses. This enhanced visibility and automation enabled organization to make informed, risk-based decisions to mitigate threats and identify opportunities to address routine hygiene issues and strengthen overall cloud security.

Key Business Benefits of AiStrike:

- **Save Analyst Time :** AiStrike automated mundane tasks in alert triage and investigation, saving over 60% of Analyst time
- **Cost Savings :** With AiStrike, Company achieved an annual saving of $287,000 due to improved operational efficiency with potential for further savings as the solution is scaled across more environments.
- **Risk Reduction :** Initial risk reduction of over 50% with prioritization of critical threats and automated one-click remediation.

> “ AiStrike gave us visibility into issues that would have otherwise gone unnoticed. By grouping hygiene issues, it helped us cut through the noise and focus on the critical behaviors requiring attention. The best part of AiStrike is the user experience—it simplifies the Analyst's work while providing Executives like me with the precise information needed for informed decision-making. ”
>
> - Chief Information Security Officer

## About AiStrike:

AiStrike is committed to solving security investigation and response challenges for modern organizations with AI-powered automation. By reducing alert volume by up to 85%, AiStrike helps security teams overcome alert fatigue, while enriching and prioritizing critical alerts for smarter decision-making and faster mean time to resolution (MTTR). With AiStrike, organizations gain the advantage of real-time alert triage, guided investigation, and automated response – all within one intuitive platform. AiStrike’s custom AI models are run locally, ensuring data privacy and security.

Discover more at www.aistrike.com or follow us on LinkedIn.