SUCCESS STORY

AHEAD deploys Elastic Security machine learning to decrease triage time, reduce false positives, and automate investigation and response

AHEAD enhances value to its clients, reducing triage time and false positives with Elastic Security

AHEAD uses machine learning in Elastic Security to decrease triage time, reduce false positives, and introduce automated investigation and response while improving its CSAT score and expanding revenues from new and existing clients.

Region	Industry	Solution
United States	Software & Technology	Elastic Security

Delivers market leading MTTR of 6.9 minutes

AHEAD maintained an MTTR of less than seven minutes for its clients even as security events increased by 50%.

73% reduction in triage time

With machine learning tools in Elastic Security, AHEAD dramatically cut triage rates, saving thousands of hours of analyst time.

92% automated resolution rate

AHEAD massively reduced manual interventions using machine learning tools in Elastic Security.

Leading digital platform and transformation provider boosts client security satisfaction and business growth with Elastic Security machine learning

AHEAD is a leading provider of digital platforms to some of the largest enterprises in the world. Alongside strategic consulting and managed services, it offers expertise in cloud, data, digital engineering, and automation. In addition to these services, AHEAD also offers managed security service provider (MSSP), offering clients cutting-edge protection against cyber-attacks.

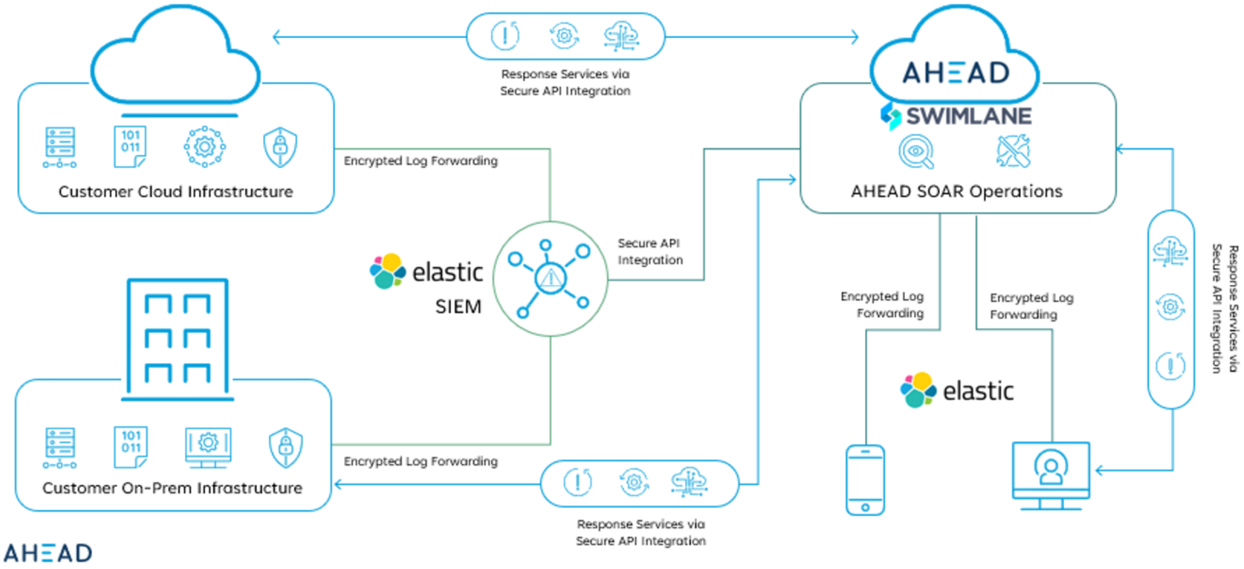
Recent years have seen a huge rise in security data sets from clients who have migrated to the cloud and have a fast-growing stable of software applications. The immense rise in data volume put additional pressure on AHEAD security analysts and threatened to increase the time needed to investigate alerts.

Ethan Butts, Lead SIEM Engineer, AHEAD, says, “Each month we talk to 265,000 users generating about 200 billion events, which correlate to 65,000 alerts. We needed a more flexible security platform to cut time to resolution and reduce analyst fatigue.”

Butts and his team chose Elastic Security to act as the security information and event management (SIEM) solution at the heart of AHEAD’s Managed SOC and XDR service. “Elastic stood out because it is cost-effective, simple to manage, and enables us to deliver an array of security services to clients,” says Butts.

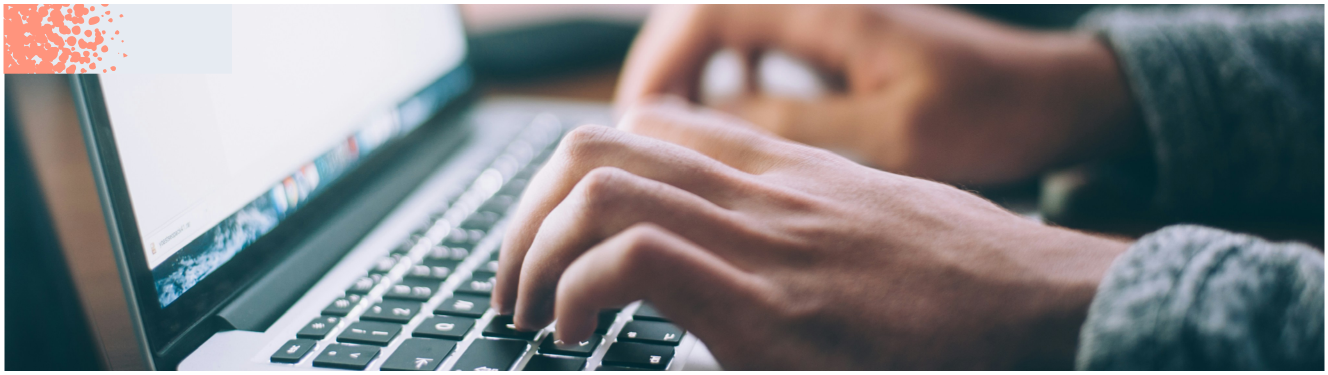
AHEAD now ingests client security data into Elastic running on Elastic Cloud where the data is enriched, aggregated, and connected to threat intelligence feeds. Elastic is also the data source for the organization's security orchestration, automation, and response (SOAR) system.

Managed SOC and XDR: Architecture


Response Services via Secure API Integration
Customer Cloud Infrastructure
Encrypted Log Forwarding
AHEAD
SWIMLANE
AHEAD SOAR Operations
elastic
SIEM
Secure API Integration
Encrypted Log Forwarding
Encrypted Log Forwarding
elastic
Response Services via Secure API Integration
Customer On-Prem Infrastructure
Encrypted Log Forwarding
Response Services via Secure API Integration
AHEAD

> The most incredible thing about Elastic is its adaptability. It can jump into any situation, system, or data set and be useful in record time.

Ethan Butts
Lead SIEM Engineer



Making good on machine learning

Elastic Security's advanced machine learning capabilities also influenced AHEAD's decision. AHEAD security analysts can leverage AI-driven alarms that highlight relevant information (influencer fields) within security events including user, country, IP address, or any captured data point. This eliminates much of the time needed to manually sift through vast amounts of data so that analysts can prioritize critical issues much faster.

Furthermore, machine learning helps reduce the burden of false positives. By analyzing historical data, algorithms build a database of "normal" activity patterns. This allows them to identify anomalies and suspicious events before they reach human analysts, significantly reducing the number of alerts requiring manual investigation.

Zach Kinkelaar, Detection Engineer for AHEAD, says, "You don't need to be a machine learning expert to create new rules. The user interface guides you through the process, making it easy to set up anomaly detection and gain valuable insights from data."

Kinkelaar gives the example of a user logging into a platform like Microsoft Office 365. Traditionally, a single login attempt from an unusual location might trigger an alert; however, Elastic enables the system to adjust to user travel patterns and recognize legitimate logins from new locations. If a user travels to France, for instance, and starts using Office 365 regularly, subsequent logins from France won't trigger new alerts.

Kinkelaar also highlights the role of Kibana dashboards that aggregate data at a central location for visualization and analysis. "Take the example of the end user traveling to France," he says. "Kibana shows you all the context concerning the user at the time of the alert, where they are, and what files they were accessing." As a result, the analyst doesn't have to search through thousands of logs to get a high-level view of the situation.

Another feature that accelerates investigations is the Elastic Security Timeline. The feature enables AHEAD analysts to see the sequence of events leading up to and following a security incident.
This chronological view helps paint a clear picture of an attacker's movements and facilitates faster threat identification.

Improved customer satisfaction and increased revenue

Since deploying Elastic, AHEAD has seen a rise in Customer Satisfaction (CSAT) scores, along with greater demand for security services and a corresponding increase in revenues. Thomas Lee, Managed Security - National Lead for AHEAD, says, “Elastic has enabled us to strengthen our position as a leading player in the security-as-a-service market.”

Elastic has also boosted overall security efficiency and scalability. Lee says, “Last year we saw a 50% rise in security activity leading to a total of 2.2 trillion SIEM events. In spite of this, AHEAD maintained a rapid mean time to response of 6.9 minutes.”

Above all, Elastic Security’s machine learning capabilities have significantly reduced analyst workloads. Butts says, “Brute-force attempts on Microsoft 365 accounts previously generated 1,000 alerts every two months, which we were forced to limit to a maximum of 250 in order to avoid overwhelming our analysts.”

With Elastic Security, AHEAD saw a 79% decrease in alerts and a 73% reduction in triage time for brute-force events alone. Additionally, AHEAD was able to significantly lower its brute-force alert threshold by 90% without missing critical threats.

AHEAD has also seen 5X increase in unique bull hits, leading to a remarkable 92% automated resolution rate. This translates to thousands of analyst hours saved, enabling the team to explore new service offerings like email security management, dark web monitoring, and SOAR workflows.

Expanding into observability and generative AI

With the success of its security initiative, AHEAD is now considering Elastic as an observability solution to provide context and event tracking across the wider IT environment. Kinkelaar has identified two potential use cases: high resource utilization that monitors RAM usage and discovers hosts with unusually high disk usage, and process monitoring to detect unusual processes and potential resource bottlenecks.

AHEAD is also looking forward to deploying Elastic AI Assistant, which uses generative AI to help clients more quickly understand and address security alerts. Kinkelaar says, “Imagine a scenario where a client receives a user login alert. Instead of contacting AHEAD for clarification, they can simply ask the AI assistant what the alert means.”

The AI assistant will not only explain the alert details, but also provide context. This includes determining if user data was accessed and suggesting relevant investigation guides based on the event. “Furthermore, AI can take action by automatically generating visualizations of user login trends. This empowers clients to delve deeper into potential security risks without needing AHEAD’s intervention for every step,” says Kinkelaar.

Collaborating for a secure future

Kinkelaar emphasizes the Elastic team’s role in AHEAD’s security initiatives. “We get exceptional support from Elastic. Every issue we raise is addressed promptly and thoroughly. This dedicated approach fosters a true partnership, so that Elastic feels like an extension of our own security team.”

AHEAD has also resonated with Elastic’s openness and resilience. “There’s a “can-do” attitude at Elastic, and they always work with us to find solutions. This collaborative spirit has consistently led to improved efficiency and effectiveness in our security services for clients,” says Kinkelaar.

> Elastic has transformed AHEAD’s security offering. We’ve been able to triple our data consumption and generate alerts while maintaining one of the best mean times to resolution in the industry.

Zach Kinkelaar
Detection Engineer, AHEAD

Address complex threats with Elastic Security, built on the Elastic Search AI Platform, to streamline SecOps.

Learn more