Koniag Government Services

SIEM Optimization and Support for M-21-31 on AWS

November, 2024

Customer: US Federal Agency
The Agency required a robust and efficient Security Information and Event Management (SIEM) solution to protect its vast network and data.

Team: Koniag Government Services (KGS) and AWS

Customer Challenge:
Government Customer needed to optimize its SIEM capabilities to better respond to the increasing cybersecurity threats and comply with Executive Order 14028 and OMB Mandate M-21-31. The agency required a solution that could efficiently ingest, store, retrieve, and correlate log data to inform stakeholders about potential events and incidents quickly. Additionally, Agency sought to improve its overall cloud presence and security posture.

Solution:
KGS implemented a comprehensive cloud migration and optimization strategy leveraging AWS services:

1. Cloud Migration: EC2 architected and implemented a secure cloud environment on AWS to host Government Customer's SIEM solution, Splunk Enterprise Security which was further enhanced by Splunk Security Orchestration and Automation, and Splunk User Based Analytics, also hosted and operating in the secure EC2 instance.
2. Log Management: Utilized AWS CloudWatch Logs for centralized log collection and management, enabling efficient ingestion and storage of log data from various AWS services, on-premises sources and data ingest from 74 other cloud service providers to include Azure
3. Data Processing: Implemented AWS Lambda functions to process and normalize log data before ingestion into Splunk, ensuring consistent data format and quality.
4. Scalable Infrastructure: Deployed Splunk Enterprise Security on Amazon EC2 instances, utilizing Auto Scaling groups to handle varying workloads efficiently.
5. Data Storage: Leveraged Amazon S3 for cost-effective long-term storage of historical log data, with lifecycle policies to transition data to Amazon Glacier for archival purposes.

6. Security Enhancements: Implemented AWS Identity and Access Management (IAM) for fine-grained access control and AWS Key Management Service (KMS) for encryption of sensitive data.
7. Monitoring and Alerting: Configured Amazon CloudWatch alarms and AWS SNS to provide real-time notifications for critical security events.

Outcomes and Results:

- Improved Threat Detection: The optimized SIEM solution on AWS enabled Agency to detect and respond to security threats faster than the previous on-premises system ***reducing our mean time to detect by over 200% and reduced the mean time to contain by over 400%.***
- Cost Reduction: By leveraging AWS's pay-as-you-go model and optimizing resource usage, Agency reduced its SIEM infrastructure and licensing costs by 30% or $2 million dollars annually.
- Scalability: The new cloud-based SIEM can now handle a 420% increase in threat volume, addressing the surge in cybersecurity incidents since the start of the pandemic.
- Compliance: The solution helped Agency meet the requirements of Executive Order 14028 and OMB Mandate M-21-31, ensuring proper log management and correlation capabilities, one of only 3 executive agencies to meet the EL3 deadline.
- Enhanced Visibility: Stakeholders now have access to more comprehensive and timely security insights, improving overall incident response and decision-making processes.
- Future-Ready: The cloud migration has positioned Agency to more easily adopt and integrate future AWS security services, ensuring the agency stays at the forefront of cybersecurity best practices.