MAGNATAUR

Integration of AWS Cloud Adoption Framework and AWS Security Hub

Teddy Strelecky, MBA
Senior Project Manager

Magnataur Consulting
2320 Taylor St #23430
Dallas, Texas US
http://www.Magnataur.Net

What we will cover

- Introduction
- Background
- AWS Cloud Adoption Framework
- AWS Security Hub
- Where is the Client Now?
- Conclusion
- Resources

Introduction

Understanding how to manage each layer of technology and how to correlate the data your people, processes, tools, and customers generate feels like sorting through a sea misunderstandings and mixed signals. Without preparing your company through preparation of tomorrow's security requirements your security division may be not be preparing your company against future issues or oversight.

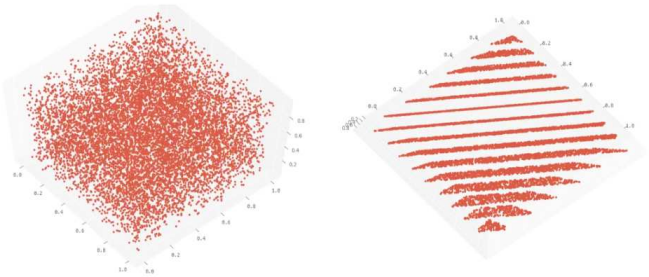

Figure 1: Why RANDU is a bad random number generator

As shown in Figure 1, what may appear as random data points from one angle is actually clear patterns when viewed from a different perspective. By adapting both Amazon Web Services (AWS) Cloud Adoption Framework (CAF) and AWS Security Hub our client was able to turn noise into information with new and improved perspective.

Magnataur's Digital Supply Chain delivered business outcomes speed while enabling fast & effective decision making in line with our client's business strategy. This white paper will provide the history behind the business case for security change, the specific AWS tools chosen, and the future growth opportunities for our client from this transition.

"We had an ally to have those conversations (about security)"

Background

The Client was a high minded, mission-focused company with an asymmetric risk profile. They were a smaller company with a big risk profile with huge data asset. "Without a dashboard, we didn't have clarity of how compliant we were", said the Client.

The Client's Cloud Security organization was preparing for the upcoming California Consumer Privacy Act (CCPA) regulations as well as market network scalability challenges as their SaaS Growth Journey marketplace & PaaS offering had become positioned for explosive adoption as the company continued to grow in client users. "We realized that Magnataur could provide the credible witness for their team to address the issue of security. (Through our partnership), we had an ally and bridge to have those conversations (about security)."

Magnataur was hired to provide advisement of Information Security through integration for applying AWS Cloud Adoption Framework and integrating AWS Security Hub, across 100% of the Client's infrastructure footprint. AWS Security Hub was dashboard needed to prompt business conversations. "Once we had (that) tool, those conversations could be held."

The consulting project was segmented with our business objectives for compliance of the Client's Information Security to risk management strategy, legal requirements and trust branding with the business's delivery of their products and services as shown in Client Information Security Alignment below.

Risk Management Strategy	Legal Requirements	Trust Branding
Risk Management procedures were designed and implemented as processes to enforce the Risk Management Policy The business defined acceptable risk profiles for different assets (Wunderman data, Intellectual Property, First Party Data) Implementation of automated controls and best practice architectures provided active risk mitigation and minimized the blast radius for compromised assets	Ensure that our Client's executives and employees are kept out of legal trouble Avoid fiscal damages via fines and penalties for regulatory non-compliance Ensure contractual data obligations (Protection, Processing, and Purging) are being followed	Our Client's mission of empowering champions to develop people is founded on the ability to build and maintain trust in the idea that data being shared, is being used for good With trust as a core marketing message, damage to the Client's brand, in the event of security incidents and privacy events, must be managed as a more significant risk than it would be for typical SaaS provider

AWS Cloud Adoption Framework (CAF) Solution

The Client sought advisory and engineering services from an outside consulting company which provided integration of cloud security with baseline security capabilities. Magnataur developed a two-phase approach using AWS Cloud Adoption Framework (CAF).

The partners chose AWS CAF based on its organizational controls and capabilities and its Well Architected Framework. This approach is organized into six "perspectives" of Business, People, Governance, Platform, Security and Operations (Figure 2).

Figure 2: Cloud Adoption Framework

Focusing on the Security perspective, Magnataur reviewed the Client's five core capabilities and their supplemental capabilities. The latter capabilities were then ranked according to Client priority and value so that a data-driven roadmap could be built.

Core Capabilities	Supplement Capabilities
Identity and Access Management	Business
Detective Control	People
Infrastructure Security	Governance
Data Protection	Platform
Incident Response	Security
	Operations

Magnataur implemented a two phase approach consisting of Phase zero [Plan and Define] and Phase one [Design and Deploy]. As is common in Cybersecurity, management knew that they needed to first turn unknown unknowns into known unknowns. Phase zero is key as the foundation of the AWS project should be established first to clarify what is known before executing on the delivery.

Phase zero is delivered in the first part and focused of then engagement with an assessment period to gather data within a business context so that informed decision making is possible.

The second [Phase one] involved managing the design and deployment of new security capabilities that deliver the most value with the least time to value against the data-driven roadmap (Figure 3). The AWS Cloud Adoption Framework explains each Deliverable in detail.

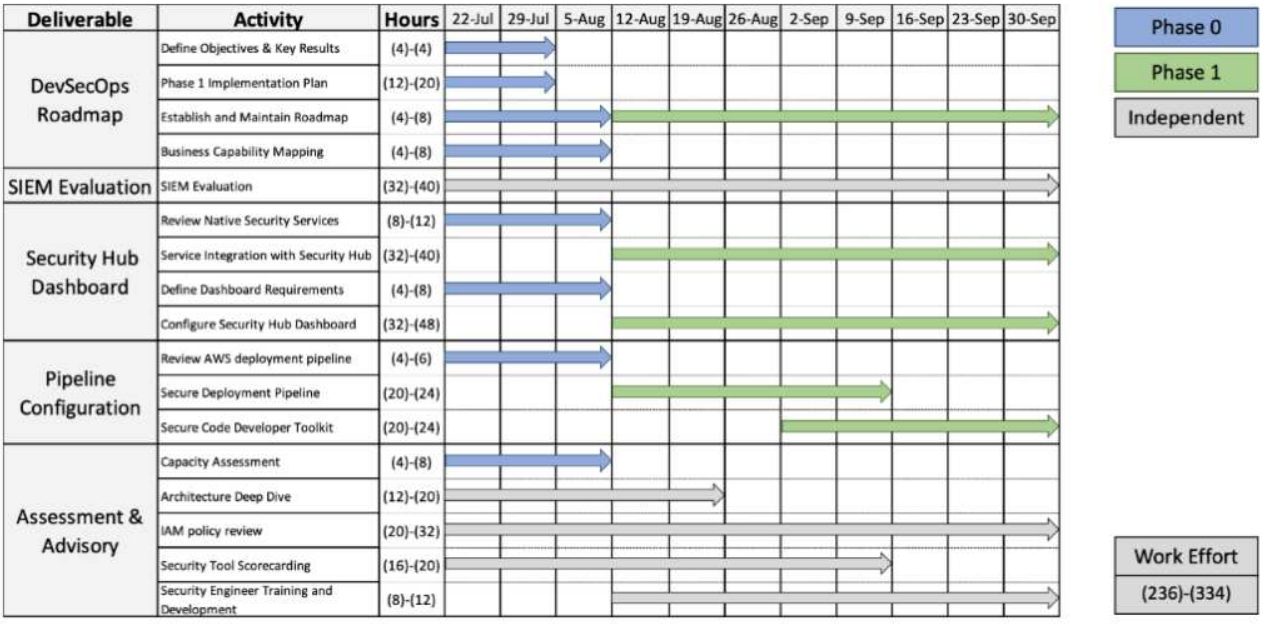

Figure 3: Engagement Timeline

AWS Cloud Adoption Framework

DevSecOps Roadmap: Develop a roadmap to guide your organization's cloud security maturation via data-driven decision making

SEIM Evaluation: Assist the Security Organization in the evaluation of and selection of SEIM tools and partners

Security Hub Dashboard: Design a Security Hub Dashboard with AWS service integrations for a single pane of glass compliance dashboard

Pipeline Configuration: Review and implement AWS security best practices for the currently implemented deployment pipeline

Assessments and Advisory Services: Conduct Assessments needed to support Roadmap generation and deliverable completion

AWS Security Hub Solution

At the end of the Phase zero [Plan and Define], a roadmap which could deliver a single pane of glass compliance dashboard was approved and chartered by the executive steering committee. Long term capabilities were evaluated and added to the DevSecOps roadmap as the organization was scaling into the market.

Market conditions (Covid-19 impacted industry) led to rapidly shifting business objectives. By integrating AWS Security Hub, the Client could quickly assess their high-priority security alerts and compliance status across AWS accounts in one comprehensive view or single pane of glass compliance dashboard, no matter how quickly the environment was shifting beneath their feet.

AWS Security Hub Services

GuardDuty: Continuously identify and alert on network related threats and supports end to end security response automation

Inspector: Vulnerability scanning and reporting for EC2 instances and machine images

Macie: Uses machine learning to automatically discover, classify, and protect sensitive data (PII) in AWS

Trusted Advisor: Recommends best practices around four categories: cost optimization, security, fault tolerance and performance

Config Rules: Conduct Assessments needed to support Roadmap generation and deliverable completion

Figure 4: AWS Security Hub

According to AWS, an organization's security organization implementation should not be a protracted effort. Rather, this process is an opportunity for best practice development with iterating your designs to meet your requirements. The AWS CAF Security Epics contain user stories (use and abuse cases) that can be completed during your sprints (Figure 4).

The five core security epics are fundamental in the control and capability categories that you should considered early on in your implementation. The augmenting the core epics drive availability, automation and audit excellence and should be integrated into each sprint.

AWS Security Hub Services

Identity and Access Management: Forms the backbone of your AWS deployment by establishing an account and be granted privileges before you can provision or orchestrate resources

Logging and Monitoring: AWS service provide a wealth of logging data to help you monitor your interactions with the platform

Infrastructure Security When you treat infrastructure as code, security infrastructure becomes a first tier workload that must also be deployed as code

Data Protection: Safeguarding important data is a critical piece of building and operating information systems, and AWS provides services and features giving you robust options to protect your data throughout its lifecycle

Incident Response: Automating aspects of your incident management process improves reliability and increases the speed of your response and often creates an environment easier to assess in after-action reviews

Security Epic	0	1	2	3
Identity and Access Management	Example: No relationship between on-premises and AWS identities.	Example: An approach is defined for workforce lifecycle identity management. IAM architecture is documented. Job functions are mapped to IAM policy needs.	Example: Implemented IAM as defined in architecture. IAM policies implemented that map to some job functions. IAM implementation validated.	Example: Automation of IAM lifecycle workflows.
Logging and Monitoring	Example: No utilization of AWS provided logging and monitoring solutions.	Example: An approach is defined for log aggregation, monitoring, and integration into security event management processes.	Example: Platform-level and service-level logging is enabled and centralized.	Example: Events with security implications are deeply integrated into security workflow and incident management processes and systems.

Figure 5: Capability Scorecard Example

Augmenting the Core 5 Epics

Resilience: High availability, continuity of operations, robustness and resilience, and disaster recovery are often reasons for cloud deployments with AWS

Compliance Validation: Incorporating compliance end-to-end into your security program prevents compliance from being reduced to a checkbox exercise or an overlay that occurs post deployment

Secure CI/CD (DevSecOps): Having confidence in your software supply chain through the use of trusted and validated continuous integration and continuous deployment tool chains is a targeted way to mature security operations practices as you migrate to the cloud

Configuration and Vulnerability Analysis: Configuration and vulnerability analysis gain big benefit from the scale, agility, and automation afforded by AWS

Security Big Data and Predictive Analytics: Security operations benefit from big data services and solutions just like any other aspects of the business

Where is the Client now?

"AWS Security Hub was the visual representation of what (the Client) needed." The Client added, "Security frameworks are the ground to stand on. If you can anchor solid ground then you have a target to aim (for). Until you have that rule book, you are (primarily) responding to ping pong balls."

The destination for most companies is what mandates are dictated from within security, privacy and trust. For example, Privacy and HIPPA laws will continue to be priorities for security. The Client plans on continuing their progress to prepare for future business partners and integration requests.

The Client plans on continuing to provide solutions for their backlog of privacy request from their unique customer base. Of these requests, Service Organization Control (SOC 2) compliance ranks among the highest given its goal to make sure that systems are set up so they assure security, availability, processing integrity, confidentiality, and privacy of customer data. SOC 2 is specifically designed for service providers storing customer data in the cloud. This means that SOC 2 applies to nearly every SaaS company, as well as any company that uses the cloud to store its customers' information.

Conclusion

Through the application of the AWS Cloud Adoption Framework and Security Hub a foundation of security prioritization and a window into the Client's scorecard was created. The Magnataur Momentum Framework© guided this Digital Supply Chain transformation which can be applied to companies experiencing similar security transition needs.

At Magnataur we believe that sometimes "The Only Way Is Through" when it comes to preparing your organization for tomorrow's security requirements. For more information on how we can help your company prepare for similar AWS integrations visit our website at https://www.magnataur.net/.

Resources

Why RANDU is a bad random number generator:
https://www.reddit.com/r/dataisbeautiful/comments/gv4fhr/oc_why_randu_is_a_bad_random_number_generator/

California Consumer Privacy Act (CCPA):
https://oag.ca.gov/privacy/ccpa

Cloud Adoption Framework (Intro):
https://d0.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

Cloud Adoption Framework (Security Perspective):
https://d1.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf

AWS Action Plan Template:
https://d1.awsstatic.com/professional-services/caf/AWS_CAF_Creating_an_Action_Plan_Nov2017.pdf