JAWS PANKRATION 2024

Maximizing Compliance with AWS Security Hub

Strategic Approaches for Organizational Control Objectives

Keitaro HAYASHIMOTO

JAWS-UG Nagasaki Leader

Agenda

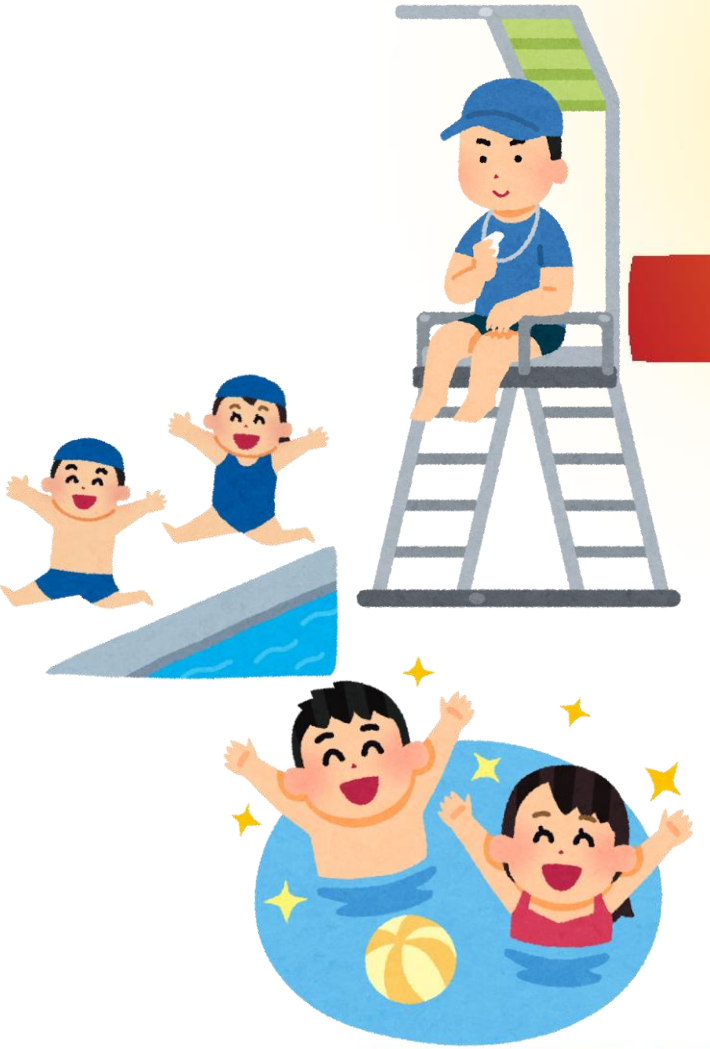
- Importance of Control Objectives
- What is the AWS Security Hub?
- Case Study
- Effective Strategies for Operating AWS Security Hub
- Conclusion

Importance of Control Objectives

- First, what are the control objectives?
  For example, if you were to go on a diet, you would first determine your goal weight, or/and abdominal circumference.
  In the same way, it needs to have an objective (goal) to operate information security compliance.
- Why are control objectives important?
  By defining the control objectives (i.e., goal), it will be able to consider what means to use to reach the goal.
  For example, in soccer, to move the ball forward (i.e., get closer to goal), it should consider whether to dribble through or pass the ball.

What is AWS Security Hub?

- “Info-Sec Watchtower” in AWS
  AWS Security Hub is a cloud security service that provides a comprehensive view of security posture across the AWS account. It aggregates, organizes, and priotizes security alerts from various AWS services and third-party products, providing a single pane of glass for managing security and compliance.
- Hmmm, can you explain it more clearly?
  In a pool analogy, AWS Security Hub is like lifeguard. When it detects any risks in or around the pool (i.e., the AWS account), it lets you, the pool manager.



Case Study

- **It All Started with an AWS Security Hub Alert**
  In the project I was involved in, we adopted the AWS Foundational Security Best Practices as the baseline rules for AWS Security Hub. One day, the project manager discovered a control failure caused by inbound traffic being allowed in the default security group of the VPC. He deleted the problematic security group rule and reported to me, saying, “I removed the rule from the security group since it had an issue.”
- **Suddenly, the Database Server Became Unreachable**
  The EC2 instance that had the default security group applied was responsible for database migration. As we were preparing for the release, a notification came from the CI/CD pipeline indicating that the database migration had failed. Upon investigating the cause, we found that the EC2 instance couldn’t reach the database server. From identifying the issue to resolving it, the deployment process ended up taking a significant amount of time.

Case Study

- What Went Wrong?
  It seems that the project manager and the engineer were in a state of mutual dependency.

If there's an alert in AWS Security Hub, the project manager will consult with us first.

Engineer

Since there is an alert in AWS Security Hub, it should be fine to delete the security group rule.

Project Manager

Effective Strategies for Operating AWS Security Hub

- Common Sense in information security compliance
  As mentioned earlier, I refer to the situation where project stakeholders have different perceptions while managing information security compliance as a lack of Common Sense.
  So, how can we establish common sense and effectively utilize AWS Security Hub?
- The Key to establish Common Sense is Process Standardization
  I believe that the mutual dependency illustrated in the case study stems from a lack of process standardization. Without established processes, project stakeholders may not know how to properly respond to alerts from AWS Security Hub. As a result, they are forced to take actions they believe are correct, even if those actions may not be appropriate from another perspective.

Approaches to Process Standardization

- Determine if It Falls Within the Scope of Control Objectives

  When AWS Security Hub raises an alert, the first step is to consider whether the alert falls within the scope of the control objectives. If the alert reveals a gap in the control objectives, you should revise the control objectives themselves before addressing the alert. On the other hand, if there is no gap in the control objectives and the alert is outside the scope of those objectives, it is acceptable to disable the control for that alert.

Out of the Scope In of the Scope

Approaches to Process Standardization

- Balance with Business Requirements and Architecture

  When addressing an alert, it is necessary for project stakeholders to discuss how to proceed with the remediation based on business requirements. Additionally, just because AWS Security Hub raises an alert does not mean it always needs to be addressed (as illustrated in the case study). Through appropriate discussions among project stakeholders, it is possible to establish well-founded common sense backed by control objectives, thereby enabling smooth operation of AWS Security Hub.

Conclusion

- Leveraging AWS Security Hub allows organizations to effectively manage their information security compliance and enhance their overall security posture. However, the key to success lies not just in implementing the tool, but in ensuring that the entire project team shares a common understanding and responds based on standardized processes. Specifically, when addressing alerts provided by AWS Security Hub, it is crucial to assess the alerts against predefined control objectives and consider the balance with business requirements when deciding on the appropriate course of action.
- In this way, AWS Security Hub becomes more than just a monitoring tool; it serves as the foundation for shaping the organization's security culture and achieving sustainable compliance.

Thank you for listening.