Identify Resources for AWS Security Support

For security and operational health of your infrastructure, AWS Support provides:

* Real-time insight through AWS Trusted Advisor. Trusted Advisor helps provision your resources by following best practices. Trusted Advisor inspects your AWS environment and finds opportunities to save money, improve system performance and reliability, or help close security gaps.
* Proactive support and advocacy through Technical Account Manager (TAM). TAM is single point of contact and advocate who provides technical expertise across AWS services.

AWS Trusted Advisor

* An online tool that provides you real time guidance
* Help you provision your resources following AWS best practices
* Helpful for
  + establishing new workflows
  + developing applications
  + as part of ongoing improvement
* Recommendations should be taken regularly to help keep your solutions provisioned optimally.

identify resources for security support


AWS Professional Services

AWS Professional Services and the AWS Partner Network helps in creating and implementing solutions and engagements include:

* Enterprise Security Architecture. Evaluate the nature of the workloads you are deploying in AWS, along with your security needs and define an architecture and set of security controls that will protect your data and workloads according to best practices.
* Policies and Controls-Mapping. Examine your requirements based upon your security policy and any third party or regulatory mandates and provide detailed recommendations on how to satisfy those requirements and demonstrate compliance.
* Security Operations Playbook. Define the right organizational structures and processes to ensure that security controls are working correctly, as well as detect and respond to security issues that arise within your AWS environment.
* Business Unit Workshops. Work with IT and Business Leaders across your organization to understand their plans and strategies around Cloud adoption, educate them on the best way to satisfy their requirements while minimizing risks to the organization, and devise an organization wide security framework for deploying workloads on AWS.