aws competency

AWS Security Competency

Consulting Partner Validation Checklist

January, 2019
Version 3.0

aws partner network

Table of Contents

INTRODUCTION **3**

EXPECTATIONS OF PARTIES **3**

AWS SECURITY COMPETENCY PROGRAM PREREQUISITES **4**

AWS SECURITY CONSULTING PARTNER VALIDATION CHECKLIST **6**

1.0 Security Practice Overview 6
2.0 Security Consulting Categories 7
3.0 Standard Solution Delivery Patterns and ISV Tooling 10

Introduction

The goal of the AWS Competency Program is to recognize APN Partners who demonstrate technical proficiency and proven customer success in specialized solution areas. The Competency Partner Validation Checklist is intended for APN Partners who are interested in applying for AWS Competency. This checklist provides the criteria necessary to achieve the designation under the AWS Competency Program. APN Partners undergo an audit of their capabilities upon applying for the specific Competency. AWS leverages in-house expertise and a third-party firm to facilitate the audit. AWS reserves the right to make changes to this document at any time.

Expectations of Parties

It is expected that APN Partners will review this document in detail before submitting an application for the AWS Competency Program, even if all of the prerequisites are met. If items in this document are unclear and require further explanation, please contact your Partner Development Representative (PDR) or Partner Development Manager (PDM) as the first step. Your PDR/PDM will contact the Program Office if further assistance is required.

When ready to submit a program application, APN Partners should complete the Partner Self-Assessment column of the AWS Competency Program Validation Checklist set forth below in this document.

To submit your application:

1. Log in to the APN Partner Central (https://partnercentral.awspartner.com/), as Alliance Lead
2. Select “View My APN Account” from the left side of the page
3. Scroll to “Program Details” section
4. Select “Update” next to AWS Competency you wish to apply for
5. Fill out Program Application and Click “Submit”
6. Email completed Self-Assessment to competency-checklist@amazon.com

If you have any questions regarding the above instructions, please contact your APN Partner Development Representative/Manager.

AWS will review and aim to respond back with any questions within five (5) business days to initiate scheduling of your audit or to request additional information.

APN Partners should prepare for the audit by reading the Validation Checklist, completing a self-assessment using the checklist, and gathering and organizing objective evidence to share with the auditor on the day of the audit.

AWS recommends that APN Partners have individuals who are able to speak in-depth to the requirements during the audit. The best practice is for the APN Partner to make the following personnel available for the audit: one or more highly technical AWS certified engineers/architects, an operations manager who is responsible for the operations and support elements, and a business development executive to conduct the overview presentation.

AWS Security Competency Program Prerequisites

AWS Security Competency Partners provide solutions to, or have deep experience working with businesses to help them implement continuous integration and continuous delivery practices or helping them automate infrastructure provisioning and management with configuration management tools on AWS.

The following items will be validated by the AWS Competency Program Manager; missing or incomplete information must be addressed prior to scheduling of the validation review.

1.0 APN Program Membership		Met Y/N
1.1 Consulting Partner Tier	Partner must be Advanced or Premier APN Consulting Partner before applying to the Security Competency Program.	
1.2 Security Specialist Certified Personnel	In addition to the certification/training requirements for APN tier compliance, APN Partner must have: ▪ ≥ 5 AWS Certified Security – Specialists	
2.0 AWS Customer Case Studies		**Met Y/N**
2.1 Security-Specific Customer Case Studies	Partner must have four (4) AWS customer case studies specific to completed Security projects; two (2) of these case studies must be publicly referenceable case studies. These Case studies must not be repeated from another AWS Competency application. Partner must provide the following information for each case study: ▪ Name of the customer ▪ Problem statement/definition ▪ What you proposed ▪ How AWS services were used as part of the solution ▪ Third party applications or solutions used ▪ Start and end dates of project (Case studies must be for projects started within the past 18 months, and must be for projects that are in production*, rather than in pilot or proof of concept stage) ▪ Outcome(s)/results This information will be requested as part of the Program Application process in APN Partner Central. ***Note:*** *Case studies must be for projects that are in production, rather than in pilot or proof of concept stage. Projects that are still in development stage will not be accepted, except: if a project was in a pilot stage and the Partner can provide evidence that the customer ultimately rejected the project, ending its development, it will be considered.*	
2.2 publicly Available Case Studies	2.2.1 Two (2) of the four (4) AWS customer case studies must be public; evidence must be in the form of publicly available case studies, white papers, or blog posts. ***Note:*** *For best practice on how to write an accepted Public Case Study See Here*	
	2.2.2 Public case studies must be easily discoverable on the Partner's website, e.g., must be able to navigate to the case study from the Partner's home page. Partner must provide link to these case studies.	
	2.2.3 Public case studies must include the following: ▪ Reference to the customer name, Partner Name, and AWS ▪ Problem statement/definition ▪ What you proposed ▪ How AWS services were used as part of the solution ▪ Outcome(s)/results ***Note:*** *Public case studies are used by AWS upon approval into the Competency to showcase the Partner's demonstrated success in the practice area and provide customers with confidence that Partner has the experience and knowledge needed to develop and deliver solutions to meet their objectives.*	

2.3 Security Specific Case Study Criteria	The Security Competency is intended to identify and promote APN Partners who help customers secure their AWS Infrastructure and in-house applications. As a result, the following are guidelines for valid Security projects. All case studies must meet these criteria: ▪ We are looking for customer use cases that have a principal narrative around Security. The customer needed the project completed because of primarily a specific security need, not, because security was a supporting detail. ▪ The case study must have high industry impact, technical significance, or be delivered at a large, global scale ▪ We are looking for use cases that involve a process and people transformation in addition to technical enablement and delivery We are looking for use that involve large components of automation and remove manual work. Use cases that include zero automation will not be considered ▪ We are looking for case studies that include examples of using AWS native Controls (Such as AWS CloudTrail and Amazon GuardDuty) being extended with ISV tools ▪ We are looking for case studies that adhere to the Security Perspectives of the Cloud Adoption Framework (Security Perspective of the AWS Cloud Adoption Framework (CAF) ▪ We are looking for customer deployments that are for production and/or mission-critical use. There should be a minimum of 25 of instances in the customer's AWS account that are protected when workload is based on EC2 Case studies must describe customer impact as a result of the move from traditional on-premise models to a Security approach leveraging AWS and the perspectives presented in the Cloud Adoption Framework	
3.0 AWS Security Practice and Focus		**Met Y/N**
3.1 APN Partner Practice Landing Page	AWS customers are looking for expertise in the development and delivery of Security solutions; a Partner's internet presence specific to their AWS Security practice provides customers with confidence about the Partner's Security capabilities and experience. APN Partner must have a landing page that describes their AWS Security practice, AWS solutions and Competency use cases, technology solutions, links to AWS case studies, and any other relevant information supporting the Partner's expertise related to Security and highlighting the work on AWS. Security practice page must be accessible from APN Partner home page. Home page is not acceptable as a practice page unless APN Partner is a dedicated Security consulting company and home page reflects Partner's concentration on Security. ***Note:*** *For best practice on how to build an accepted APN Partner Practice Landing Page See Here*	
3.2 Security Thought Leadership	AWS Security Competency Partners are viewed as having deep domain expertise in Security, having developed innovative solutions that leverage AWS services. APN Partner must have public-facing materials (e.g., blog posts, press articles, videos, etc.) showcasing the APN Partner's focus on and expertise in Security. Links must be provided to examples of materials published within the last 12 months.	
4.0 APN Partner Self-Assessment		**Met Y/N**
4.1 AWS Competency Partner Program Validation Checklist Self-Assessment	APN Partner must conduct a self-assessment of their compliance to the requirements of the AWS Security Consulting Partner Validation Checklist. ▪ APN Partner must complete all sections of the checklist. ▪ Completed self-assessment must be emailed to **competency-checklist@amazon.com**, using the following convention for the email subject line: "[APN Partner Name], Security Competency Consulting Partner Completed Self-Assessment." ▪ It is recommended that Partner has their Solutions Architect or Partner Development Manager (PDM) review the completed self-assessment before submitting to AWS. The purpose of this is to ensure the Partner's AWS team is engaged and working to provide recommendations prior to the audit and to help ensure a positive audit experience.	

AWS Security Consulting Partner Validation Checklist

In preparation for the validation process, APN Partner should become familiar with the items outlined in this checklist and prepare objective evidence, including but not limited to: prepared demonstration to show capabilities, process documentation, and/or actual customer examples. Partners are not limited to the four (4) case studies submitted as part of the prerequisite process but should be prepared to describe how the new case studies meets the minimum acceptable criteria for an AWS Security case study if being used during the validation.

The AWS Competency Program is guided by AWS best practices and Well Architected Framework.

1.0 Security Practice Overview		Met Y/N
1.1 Customer Presentation	APN Partner has a company overview presentation that sets the stage for customer conversations about their AWS Security capabilities and showcases APN Partner's demonstration capabilities. Presentation contains information about the APN Partner's AWS Security capabilities, including AWS-specific differentiators, and standardized packaged security offerings that are available to customers. e.g., what is unique about the APN Partner's practice that can only be accomplished leveraging AWS and how their packaged offerings include those capabilities. Overview presentations contain: ▪ Company history ▪ Office locations ▪ Number of employees ▪ Customer profile, including number and size of customers, including industry ▪ Overview of Security Philosophy, Practices, and Tools Evidence must be in the form of a presentation delivered by a business development executive at the beginning of the validation session and should be limited to 15 minutes.	
1.2 AWS Security Services Leveraged	AWS customers seeking Security consultants view AWS Security Competency Partners as the go-to experts in the field. Potential customers often ask for examples of solutions built for other customers when choosing a APN Partner and want confidence that consultants are up to date on AWS services. For fifteen (15) of the following AWS Security services: ▪ AWS Identity and Access Management (IAM) ▪ Amazon GuardDuty ▪ Amazon Macie ▪ Amazon Inspector ▪ AWS Config ▪ AWS Config Rules ▪ AWS CloudTrail ▪ Amazon CloudWatch ▪ AWS CloudWatch Events ▪ AWS Lambda ▪ AWS Key Management Service (KMS) ▪ AWS CloudHSM ▪ AWS WAF ▪ AWS Direct Connect ▪ AWS Shield and Shield Advanced ▪ AWS Secrets Manager ▪ AWS Certificate Manager ▪ Amazon Cognito ▪ AWS Single Sign-On	

	▪ AWS Firewall Manager APN Partner can provide the following: ▪ Examples of customer solutions leveraging each service ▪ If AWS service is not being leveraged by an active customer, a hypothetical use case is available including where that service should be considered and how it will be supported ▪ Description of how services are supported by APN Partner, alone or as part of a solution comprising multiple services ***Note**: Evidence may also be found in the submitted customer case studies (Prerequisites, Section 2.0), AWS Security Practice and Focus (Prerequisites, Section 3.0), during the customer presentation (Section 1.1 above), or during review of other sections.*	
1.3 Maintaining AWS Expertise	APN Partner can describe how they stay current on Security-related AWS Services/tools. Evidence must be in the form of a verbal or written description on enablement materials leveraged by APN Partner to stay current on AWS services and features. Evidence is also required to demonstrate that APN Partner has the minimum number of AWS Certified Security Specialists (see Prerequisites, 1.2) as full-time employees.	
1.4 Security Solution Selling	APN Partner can describe how Security opportunities are identified, how their sellers are trained to identify and sell those opportunities, and specific demand generation/lead generation efforts associated to their AWS Security practice. Evidence must be in the form of a verbal description how APN Partners engage with customers, their internal sellers, and AWS sellers if applicable.	
1.5 AWS Sales Engagement	APN Partner can describe how and when they engage with AWS sellers and AWS Solutions Architects. Evidence must be in the form of a verbal description for how and when they engage AWS sellers or Solutions Architects on an opportunity or in the form of a demonstration of the AWS Opportunity Management tool with sales qualified opportunities submitted (sales qualified = budget, authority, need, timeline, and competition fields completed).	
1.6 Security Training for Internal Personnel	APN Partner has process to ensure that there are sufficient Security trained personnel to effectively support customers. Evidence must be in the form of: ▪ An established training plan including on-boarding processes that identify job roles (sellers, solutions architects, project managers) and required training paths ▪ A verbal description of methods used to allocate required resources to Security projects	

2.0 Security Consulting Categories

AWS Security Competency Partners provide deep technical and consulting expertise helping large enterprises adopt, develop, and deploy complex security projects. Customers have many different needs when it comes to security. A customer may need their infrastructure designed from the ground up, they may want automation to help with incident response, or they may want their environment to meet the requirements of an audit regime. In order to properly showcase the best APN Partner for specific customer needs, it is important to highlight referenceable areas of strength, depth, and experience.

As such, Security Competency Partners must apply to a single specialization below and meet the criteria for that category. AWS Security Competency Partners are able to guide customers through all phases of security project development including the integration of native AWS Security Services, controls, and APN Partner ISV solutions as required.

Below are the four (4) Security Consulting categories that an APN Partner may apply for. All four (4) customer case studies must be in the category applied for. Included are detailed examples of the solutions that would be delivered to the respective category and the expected details and themes that case studies must align to.

2.1 Security Engineering	Met Y/N	Notes
Security is job zero at AWS. To maintain a continuously strong security posture, it is important to plan and build your AWS environment correctly from day one. The Security Engineering sub-category is focused on the design, deployment, and maintenance of AWS Infrastructure, customer assets and software, and the tools used to secure it. Case studies in the Security Engineering category should follow the guidance of the AWS Well Architected Framework and include details of how each pillar was used in the design decisions.		

2.1.1 Security and Infrastructure Provisioning	Practitioners should have an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion using AWS CloudFormation. APN Partner has methodologies leveraging standard templated infrastructure provisioning and recommends as a key factor for repeatable deployments to customers wanting to leverage automated Security approaches. Some example infrastructure includes: • Deploying Security infrastructure, tools, and services across many AWS accounts and regions (firewalls, IDS, proxies, etc.) • VPC and Network design. Must including multi-VPC design patterns and multi-region redundancy • Designing security infrastructure for secrets management, DDoS Resiliency, Identity and Access Management Evidence must be in the form of custom AWS CloudFormation templates leveraged for the four (4) submitted customer case studies with description as to whether they encourage use of AWS standardized CF templates, create templates for the customer, or teach customers how to create templates.		
2.1.2 Centralization	APN Partner and associated case studies must have a processes and methods for providing centralized deployment and management of assets across many AWS accounts, AWS regions, networks, and third-party tools. This centralization must include centralized management of native and third-party tooling, centralization of logging, centralization of identities, and centralization of security alerts/findings. Evidence must be in the form of a customer implementation description and must include an architectural diagram and AWS CloudFormation template, where appropriate.		
2.1.3 Inventory, Classification, and Hardening	APN Partner has processes and methodologies to conduct AWS resource inventory, assess current state configuration, review and store historical changes, and send change notifications. By leveraging AWS Config, AWS Inspector, AWS CloudTrail, AWS EC2 Systems Manager, or third-party tools, APN Partner is able to create remediation plans and provide guidance to enhance a customer's environment by aligning to the principals of the Well-Architected Framework. APN Partner must show documented processes and provide technical demonstration of how policies are managed, and the methods used to automate these functions. Evidence must be in the form of technology demonstration and process documentation provided to customer as part of their Security conversion.		
2.1.4 ISV and Custom Tooling	Customers have the need to deploy security tools in a scalable manner that will provide operational excellence and not impact the environment. APN Partner must provide a package offering of standardized tools offered to customers and demonstrate how they are deployed and managed. When native AWS tools were not used or are lacking desired features, APN Partner must provide guidance and documentation regarding why a tool was selected and the security outcomes they are achieving with it. Evidence must be in the form of architectural diagrams and AWS CloudFormation templates.		

2.2 Security Operations and Automation	**Met Y/N**	**Notes**

Automation and CI/CD are core components of any modern Security strategy in AWS. Often referred to as "DevSecOps" or "SecDevOps", the primary goal is to approach security with a developer mindset. Security tasks should be automated with code, audited, and have as much human interaction removed as possible. This helps safeguard access to data, provides less errors, and scale scant resources. By using continuous delivery practices, security practitioners can now respond to more events, investigate incidents more thoroughly, and provide their organization a stronger security posture. In short, the Security Operations and Automation category focuses on the empowering the people and processes of a security team.			
2.2.1 Infrastructure and Security as Code	APN Partner provides the ability and mechanisms to migrate manual security infrastructure builds and processes into automated, codified, and repeatable processes. APN Partner provides guidance to centralize all standard AWS infrastructure deployment patterns as code stored in a centralized source control repository such as Git. As an example, APN Partner must provide guidance for building out core services such as golden AMI build pipelines, or standard processes of how to update and maintain Security Groups Evidence must be in the form of process documentation describing software release process and examples of how APN Partner teaches customer how to build and deploy such tasks as an AMI Pipeline or updating/creating AWS Security Groups.		
2.2.2 Security CI/CD	APN Partner has the ability to inject security processes indirectly into the software build to compile source code, run tests and security checks with AWS Inspector or third-party tool, and produce software packages/AWS configuration changes that are ready to deploy. All changes and releases to the AWS environment should solely go through this pipeline. APN Partner has processes that support provisioning, managing, and scaling CI/CD servers according to needs of the overall organization. Evidence must be in the form of process documentation describing development and testing processes and examples of how APN Partner teaches customer how to accomplish the same.		
2.2.3 SOC implementation and Incident Response	APN Partner can advise on the design, implementation, and enablement of a SOC. APN Partner provides customers the ability to detect, respond, forensically investigate, and remediate/recover from incidents. APN Partner must have the ability to analyze AWS telemetry including AWS CloudTrail, Amazon GuardDuty Findings, AWS WAF Logs, AWS S3 Access Logs, Amazon VPC Flow Logs, as well as OS and Application logs. APN Partner must have the ability to integrate these security workflows, alerts, and logs into a centralized SIEM and ticketing system. Evidence must be provided in the form of standard IR playbooks and demonstration of automated response plan.		
2.3 Governance, Risk, and Compliance		Met Y/N	Notes
APN Partners in this category have a proven track record of helping customers build environments in that cloud that adhere to industry standards, pass internal/external audits regimes, and have achieved third party certification.			
2.3.1 Third Party Certification, Attestation, and Auditing	APN Partner has helped a customer design and build an environment that has achieved a third-party certification, attestation, or passed a third-party audit such as PCI, or SOC 2anSO 2 etc. E Evidence must be in the form of an approved third-party attestation of compliance or certification for the project the APN Partner implemented.		
2.3.2 Security Playbooks and Standard Operating Procedures	APN Partner has helped a customer designing organizational-wide security playbooks and standard operating procedures. This includes a standard playbook for incident response, the ability to create self-policing guard rails and/or the ability to detect "configuration drift" away from a standard. Evidence must be in the form of the playbooks and documented operational guidelines.		
2.4 Application Security		Met Y/N	Notes

Application Security is focused on helping customers test and protect their code from threats. By performing code reviews, penetration testing, and providing these AWS Partners can help customers with such example tasks as finding bugs in their code, advise customers on choosing the appropriate encryption library, to assessing the permissions of their S3 Bucket policies.			
2.4.1 Penetration Testing	APN Partner has an understanding of AWS penetration testing policies and works with customers to conduct tests, implement processes around regular penetration testing/vulnerability scanning of their applications and infrastructure, while still complying with AWS policies. APN Partner works with customers to resolve any identified vulnerabilities to ensure that their applications meet a target security bar and their AWS environment meets the standards of AWS Well-Architected Framework. Evidence must be in the form of sample of a customer penetration test results report that was supplied to a customer.		
2.4.2 Code Reviews and Application Development	APN Partner provides deep expertise in a particular programming language or software engineering paradigm. APN Partner may write whole applications or modules for a customer. APN Partner code assessments can find and remediate bugs, recommend best practices and idioms, or act as subject matter experts in such example areas of encryption, tenant separation, or application resiliency. These reviews must include assessments of how AWS services are used and accessed as part of application design. This can include source code review, static analysis, etc. Evidence must be in the form of customer testimonial, Git/bug tracker history, or publications.		
2.4.3 Application and Operating System Hardening	APN Partner can provide industry best practices for hardening and configuring applications and operating systems to industry standards or vendor best practices. As an example, this may be to CIS standards or mandating that an application is only using FIPS-certified software libraries. Evidence must be in the form of automated scripts and/or documentation that includes the processes and steps taken to achieve the hardening		

3.0 Standard Solution Delivery Patterns and ISV Tooling		**Met Y/N**	**Notes**
3.1 Best Practices	APN Partner has introduced design patterns and security playbooks that help the customer achieve and consistently deliver best practices around the **AWS Cloud Adoption Framework** (CAF) Core Security Epics of IAM, Logging and Monitoring, Incident Response, Data Protection, and Infrastructure Security which can include such case study examples as: ▪ Automated deployments of standardized VPCs that meet specific security guidelines (PCI, NIST) ▪ Standardized setup of multiple AWS accounts for specific functions (Dev, Test, Prod, Identity, Logging, Security, Shared Services) ▪ Standard for playbook to Incident Response in the cloud ▪ Automated deployments of specific application stacks ▪ Automated deployments of specific third-party security tools ▪ Standardized on-boarding/off-boarding Evidence must be in the form of a customer implementation description and must include an architectural diagram and AWS CloudFormation template, where appropriate.		

3.2 Security Tooling	APN Partner must have a playbook and design pattern for standardized security tooling they recommend to customers to meet their security and compliance needs, including ALL of the following: ▪ AWS Account Security Assessment (Root Credential Storage, S3 Bucket Permissions, IAM Permissions, etc.) ▪ Identity, Access Control, and Federation (Secrets Management, SSO, Privileged User Management, Host/App AuthZ/AuthN) ▪ Web Application Firewall (WAF) ▪ DDoS protection ▪ Firewall and Networking Infrastructure (NGFW, Micro-Segmentation, Security Group Management, Network Analysis/Packet Capture) ▪ Remote Connectivity Infrastructure ▪ Endpoint, Host Security (EDR/EPP) and Container Security ▪ File Integrity Monitoring (FIM) ▪ Intrusion Detection and Prevention (IDS/IPS) ▪ Centralized Logging, Monitoring, and/or SIEM ▪ Proxies and Egress Access ▪ Encryption and Key/Secrets Management of S3, EBS, DynamoDB ▪ Data Loss Prevention (DLP) If the tool is NOT part of the AWS Security Competency, APN Partner must provide reasons why the solution was chosen and what mechanisms they have in place to make sure it meets the standards of the Security ISV Competency. Evidence must be in the form of a customer implementation description and must include an architectural diagram and AWS CloudFormation template, where appropriate.		

AWS Resources

Title	Description
How to Build a Practice Landing Page	Provides guidance how to build a Practice/solution page that will meet the prerequisites of the Program.
How to write a Public Case Study	Provides guidance how to build a Public Customer Case Study that will meet the prerequisites of the Program.
How to build an Architecture Diagram	Provides guidance how to build a architecture diagrams that will meet the prerequisites of the Program.
Partner Readiness Doc	Provides guidance and best practice examples of the Program perquisites.

AWS reserves the right to make changes to the AWS Competency Program at any time and has sole discretion over whether APN Partners qualify for the Program.