aws

PartnerEquip: Live – Bangkok

Exclusive event for Specialized Partners

28 – 30 April 2026
Bangkok, Thailand

Security

The Security track at PartnerEquip: Live equips partner teams with the technical expertise and best practices needed to help customers build secure, compliant, and resilient cloud solutions on AWS. Across three days, participants will explore key security domains including AI security, data protection, identity and access management, network and application security, and threat detection and incident response.

This year's track prioritizes security considerations for generative AI workloads and emerging technologies helping partners address their customers' most pressing security requirements. Through builder sessions, hands-on labs, and expert-led discussions, attendees will learn to architect secure generative AI applications, implement defence-in-depth strategies, deploy advanced threat detection capabilities, and establish comprehensive data protection controls.

Built for technical practitioners at security-focused partner organizations, including Security Architects, Cloud Security Engineers, CISOs, Security Operations Leads, Compliance Managers, and AI/ML Security Specialists. This track delivers actionable knowledge and practical experience. Participants will gain the technical skills and AWS security expertise required to help customers reduce risk, meet compliance requirements, and accelerate secure cloud adoption while growing their AWS security practice.

PartnerEquip: Live – Bangkok

Day 1 Agenda

Tuesday, 28 April

Time (GMT+4)	Level	Title	Abstract
8:30am	**Registration and Breakfast**		
9:30am		**Welcome**	
9:45am	**100**	Keynote	Keynote
10:15am	**200**	AWS Partner Programs & benefits	AWS Partner Programs & benefits
10:45am		**Break**	
11:00am	300	AWS Security Incident Response: Quickly and safely respond to security incidents	AWS Security Incident Response is a new service that helps organizations rapidly prepare for, respond to, and recover from security incidents. It enables teams to triage findings, automate responses, and access 24/7 expert support for managing events like account takeovers and ransomware attacks.
11:30am	300	AWS detection and response innovations that drive security outcomes	We'll show you how to use AWS security services to protect workloads and data, centralize security monitoring, manage security posture continuously, and unify security data, while leveraging generative AI for security operations. Walk away with actionable insights for integrating AWS detection and response services to strengthen and simplify security across your AWS environment.
12:00pm		**Lunch**	
1:00pm	300	Security, Identity, and Governance Roadmap Transparency	AWS Service team presents key innovations and upcoming features for security services. Session highlights new tools and enhancements designed to strengthen cloud security, improve threat detection, and streamline incident response across AWS environments.
1:45pm	300	Vulnerability Management at scale with Amazon Inspector	Transform your security posture with Amazon Inspector's new and enhanced vulnerability management capabilities. This session shows how to gain complete visibility of security risks from code to cloud. Learn to track vulnerable container images in production, implement automated code scanning, and validate infrastructure as code. Discover how Inspector's new third-party repository integrations and security guardrails help ensure consistent secure coding practices.
2:30pm		**Break**	
2:45pm	300	GuardDuty Extended Threat Detection - Expansion coverage to EKS	Amazon GuardDuty Extended Threat Detection helps you identify sophisticated, multi-stage attacks targeting your AWS accounts, workloads, and data. Learn how this new capability uses AI/ML to automatically correlate security signals across AWS services, presenting attack sequences from compromised EKS clusters as single, critical-severity findings. See how attack sequence findings include incident summaries, detailed event timelines, and MITRE ATT&CK® mapping.
3:30pm	300	Threat Detection and Response Workshop	This workshop is designed to get you familiar with the AWS threat detection and response services, best practices, use cases, and then use what you learn to dive deeper into scenarios. All of this is designed to prepare you and help you operate more securely on AWS. This workshop goes though overviews, operationalization, and deployment of each of the services: Amazon GuardDuty, Amazon Inspector, AWS Security Hub, Amazon Macie, and Amazon Detective.
4:45 pm		**Wrap Up**	
5:00 – 6:00pm		**Evening Networking Event (off-site, badge required)**	

PartnerEquip: Live – Bangkok

Day 2 Agenda
Wednesday, 29 April

Time (GMT+4)	Level	Title	Abstract
8:30am	Registration and Breakfast		
9:30am		Welcome	
9:45am	400	Advanced AI Security: Architecting Defense-in-Depth for AI Workloads	Dive deep into advanced security architectures for AI workloads, exploring how to protect your workload against sophisticated attack vectors. Through technical examples, we'll implement secure architectures for AI workloads, covering identity, fine-grained access policies, and secure foundation model deployment patterns.
10:15am	300	Compliance Risk and Privacy on AWS: What You Need to Know	Learn about managing AI risks and regulatory compliance, with examples in ASEAN's financial sector. This session explores navigating several ASEAN regulations—including requirements across Thailand , Indonesia, Singapore, Philippines and Vietnam. Leverage on AWS's Shared Responsibility Model and compliance tools to build innovative and responsible AI solutions that satisfy regional regulators and drive partner success.
10:45am		Break	
11:00am	300	Agentic AI security on AWS	Organizations can accelerate agentic AI adoption on AWS while maintaining enterprise-grade security that scales automatically as they grow. This talk will cover AWS's approach to securing generative AI using ubiquitous authorization, Zero Trust, and a defense-in-depth strategy to address common vulnerabilities such as the OWASP top 10 for LLM.
11:30am	200	Ask Experts Anything Panel	Ask the Expert Panel is an opportunity to connect with leaders from across AWS in a Q&A format.
12:00pm		Lunch	
1:00pm	400	Bedrock Security Deep Dive	In this session, you will learn about how to securely use Amazon Bedrock. You will learn about Bedrock security features, such as model tenancy, access control, client connectivity, and data privacy.
1:45pm	300	Secure AI Agent Operations with Amazon Bedrock AgentCore and Identity Controls	This session explores Amazon Bedrock AgentCore, AWS's fully-managed agentic platform for building, deploying, and operating AI agents securely at scale. We'll cover AgentCore's framework-agnostic support , model independence, and enterprise security features including VPC connectivity and session isolation. We'll then dive deep into Amazon Bedrock AgentCore Identity, examining how specialized workload identities enable secure authentication, authorization, and credential management for agents.
2:30pm		Break	
2:45pm	300	AWS Security Agent (Preview), Secure by design, protected by analysis	A service that analyzes application design documents, architecture diagrams, and infrastructure-as-code files to provide automated security recommendations and identify potential security gaps throughout the development lifecycle, and complete your existing penetration testing efforts.
3:30pm	300	Next-Gen SOC: Building Autonomous Incident Response	Security operations teams are drowning in alerts and are seeking ways to transform alert fatigue into strategic advantage through agentic AI. In this workshop, build intelligent agents using Amazon Quick Suite and Amazon Bedrock AgentCore that deliver skills on-demand to guide analysts, automate alert triage, and do more with less. Your agents will enrich findings with business context for smarter prioritization, access AWS account information in real-time, and investigate logs while collecting evidence automatically.
4:45 pm		Wrap Up	
5:00 – 9:00pm		Evening Networking Event (off-site, badge required)	

PartnerEquip: Live – Bangkok

Day 3 Agenda

Thursday, 30 April

Time (GMT+4)	Level	Title	Abstract
8:30am	Registration and Breakfast		
9:30am	Welcome		
9:45am	300	AWS KMS Best Practices and the Post-Quantum Roadmap	In this session, we will take a deep dive into AWS Key Management Service (KMS), exploring best practices, real-world use cases, and common misconceptions. Additionally, we will discuss post-quantum cryptography at AWS, including its current state, challenges, and roadmap for the future. Join us to gain insights into securing your cryptographic assets today while preparing for the post-quantum era
10:15am	300	Architecting a Secrets Management Strategy that Scales	Explore centralized and decentralized approaches to secrets management in cloud-native applications. Learn how to leverage AWS Secrets Manager, KMS, and Config to implement a balanced strategy that serves both developer and security needs. We'll cover architectural trade-offs and best practices for compliance and auditing across different implementation patterns.
10:45am	Break		
11:00am	300	IAM Architecture patterns, Getting builders into AWS	So, you're designing an AWS multi-account structure, and looking for recommendations on how to control access for builders? In this talk we will discuss multiple ways of managing identities in AWS and provisioning access to AWS services and resources while highlighting some of the trade-offs that may be encountered. You will walk away with practical examples, best practices, and considerations on how to successfully manage access across AWS accounts.
12:00pm	Lunch		
1:00pm	300	From Validated to Trusted: Building Your AWS MSSP Practice	This session is your guide to joining the AWS MSSP Competency, a rigorous, industry-first standard that validates partners across seven critical security domains. Discover how to build a trusted, high-quality managed security practice, leverage native AWS services, and unlock new growth opportunities with customers who need real protection, not just promises.
1:45pm	300	AWS Shield - Network Security Director	Get a deep dive into the AWS Shield- Network Security Director, a new service, now in preview, that allows you to discover network resources, analyze connectivity, understand misconfigurations, and get AI-assisted remediation recommendations with Amazon Q.
2:30pm	Break		
2:45pm	300	Top 10 Best Practices for Network Security with Network Firewall & DNS Firewall	This session covers real-world customer use cases and common issues to avoid when developing policies and rules. Practical tips, common scenarios, new feature releases, and troubleshooting strategies are also addressed to equip you with the skills needed to fortify your organization's network defence on AWS. Learn the top ten recommendations for getting started with Network Firewall and Amazon Route 53 Resolver DNS Firewall policy creation.
3:30pm	300	Securing AWS Network Traffic: Network Firewall & DNS Firewall Workshop	This workshop combines practical security implementation with real-world threat scenarios, including analyzing Sliver malware C2 communications and implementing least privilege access controls. You'll gain hands-on experience with Suricata rules, AWS managed threat intelligence, traffic analysis, and advanced network security monitoring.