PartnerEquip: Live – Dubai

Exclusive event for Specialized Partners

24-26 March 2026
Dubai, UAE

Security, Identity and Governance track

The AWS PartnerEquip: Live Security, Identity and Governance track empowers partners with technical expertise to architect solutions that address evolving customer challenges across modern cloud and AI environments.

Spanning three days, explore critical domains from cloud security posture management to AI-powered threat detection and agentic-AI security. Discover how to leverage AWS foundational services including GuardDuty, Security Hub, and WAF, as building blocks for enhanced partner solutions, while mastering AI security patterns that combine AI and security services into co-ideated customer solutions.

Address real-world requirements including data sovereignty and hybrid environment security using AWS first-party and third-party capabilities, delivering the simplified, integrated security solutions customers demand.

Designed for technical practitioners including Security Architects, Security Engineers, Security Operations specialists, Compliance Leads, AI Security Specialists, and CISOs at security-focused partner organizations.

Dive Deep through face-to-face engagements with AWS Subject Matter Experts via presentations, hands-on workshops, and collaborative problem-solving sessions that deliver actionable expertise for immediate application.

PartnerEquip: Live – Dubai

Day 1 Agenda

Tuesday, 24 March

Time (GMT+4)	Level	Title	Abstract
8:00am	**Registration and Breakfast**		
10:00 am	**Welcome**		
10:15 am	200	Opening & Keynote	Keynote
10:30 am	200	AWS detection and response innovations that drive security outcomes	Discover 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 security across your AWS environment.
11:15 am	**Break**		
11:30 am	300	AWS Security Incident Response with AI investigative agent: Quickly and safely respond to security incidents	AWS Security Incident Response helps organizations rapidly prepare for, respond to, and recover from security incidents. It enables teams to triage findings, automate responses, and access expert support for managing events like account takeovers and ransomware attacks. Now with AI Investigative agent, it automatically gathers and analyzes security evidence across multiple AWS data sources, then presents findings in clear, actionable summaries
12:00 pm	300	GuardDuty Extended Threat Detection - Expansion coverage	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. Discover how this helps security teams spend less time on first-level analysis and more time responding to critical threats to minimize business impact.
12:30 pm	**Lunch**		
1:30 pm	300	AWS Security Hub: A unified AI-Powered cloud security solution	learn about the new and improved AWS Security Hub. With new AI-powered capabilities, unifies visibility to detect, prioritize, and respond to critical security issues to help protect customer's cloud environment. It correlates and enriches security signals, delivering actionable insights and enabling streamlined response. Learn how the service helps unify security operations, provide enhanced risk context and prioritizes analysis.
2:15 pm	300	Digital Sovereignty on AWS with insights into the UAE Sovereign Launchpad	Partners working in regulated industries such as healthcare, financial services and public sector often come across concerns around digital sovereignty. In this session, we provide practical steps to help you meet sovereignty requirements in the region, covering the AWS is sovereign-by-design and insights into the UAE sovereign Launchpad
3:00 pm	**Break**		
3:15 pm	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 use what you learn to dive deeper into scenarios. Designed to prepare you to operate more securely on AWS. It 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 – 7:00pm	**Welcome Reception (badge required)**		

PartnerEquip: Live – Dubai

Day 2 Agenda

Wednesday, 25 March

Time (GMT+4)	Level	Title	Abstract
9:00am	Registration and Breakfast		
10:00 am	Welcome		
10:15 am	300	AI Security Grounding - What makes security different?	This session provides a grounding on what makes AI applications and agents different from regular workloads. Security is top of mind for customers deploying AI workloads, as they operate differently compared to traditional workloads. This presentation covers a deep dive into four key expectations: structured outputs, data accuracy, deterministic, and authorization built-in.
10:45 am	300	Agentic AI Security Best Practices	This session provides a comprehensive security framework for deploying Agentic AI systems covering the AWS AgentCore services architecture, OWASP threat vectors, defense-in-depth strategies across identity management, network protection, and application security, with emphasis on the unique risks introduced by autonomous AI agents that can independently execute actions, access tools, and make decisions without constant human oversight
11:15 am	Break		
11:30 am	300	AWS Security Agent, 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.
12:00 pm	100	Ask Experts Anything Panel	Ask the Expert Panel is an opportunity to connect with leaders from across AWS in a Q&A format.
12:30 pm	Lunch		
1:30 pm	200	Innovations in Infrastructure Protection to strengthen your network	In this session, learn about new capabilities in infrastructure protection services like AWS Network Firewall, Amazon Route 53 DNS Firewall, AWS WAF, and AWS Shield, to simplify your application protection, streamline robust egress protections and gain insight into your network and edge security. Dive deep into how to gain insight into network and edge security, rising bot threats, network attacks, and proactive identification of network configuration issues.
2:15 pm	400	AI services and Agentic AI applications Security Deep Dive	In this session, you will learn about how to securely use Amazon Bedrock and AgentCore. You will learn about AI model security features, such as model tenancy, access control, client connectivity, and data privacy. Discover how to securely host agentic applications with AgentCore Identity and policy
3:00 pm	Break		
3:15 pm	300	Next-Gen SOC: Building Autonomous Incident Response	In this workshop, build intelligent agents using Amazon Quick Suite and Amazon Bedrock AgentCore that deliver skills on-demand to guide analysts and automate alert triage. Your agents will enrich findings with business context for prioritization, access AWS account information in real-time, and investigate logs while collecting evidence automatically. Through hands-on exercises with MCP tools, deploy a solution that improves mean time to resolve, and transforms security operations from reactive to proactive threat hunting
4:45 pm	**Wrap Up**		
5:00 – 8:00pm	**Evening Networking Reception (badge required)**		

PartnerEquip: Live – Dubai

Day 3 Agenda

Thursday, 26 March

Time (GMT+4)	Level	Title	Abstract
9:00am	**Registration and Breakfast**		
10:00 am	**Welcome**		
10:15 am	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 and secure strategy. We'll cover architectural trade-offs and best practices for compliance and auditing across different implementation patterns.
10:45 am	300	IAM Access Analyzer for Security Pros	In this session, we'll go deep on IAM Access Analyzer, focusing on both the how and why behind key features like unused, external and internal access analysis, as well as policy validation and custom policy checks. We'll demystify automated reasoning and how we can better support customers on their journey to least privilege together.
11:15 am	**Break**		
11:30 am	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 and real-world use cases. we will discuss post-quantum cryptography at AWS, 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.
12:00 pm	300	AWS Shield - Network Security Director	Get a deep dive into the AWS Shield- Network Security Director, a new service, that allows you to discover network resources, analyze connectivity, understand misconfigurations, and get AI-assisted remediation recommendations with Amazon Q.
12:30 pm	**Lunch**		
1:30 pm	300	IAM Architecture patterns, Getting builder into AWS	So, you're designing an AWS multi-account structure, and looking for ways 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. You will walk away with practical examples with best practices.
2:15 pm	300	Advanced Policy Evaluation	Dive into the world of policy evaluation, head first. We will examine several different types of policies (Service Control Policies, Resource Control Policies, Permissions Boundaries, Resource Policies, Identity Policies) and how they are evaluated.
3:00 pm	**Break**		
3:15 pm	400	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.
4:45 pm	**Wrap Up + End of Week Survey**		