Uday Kiran Ravoori| Cloud Security Analyst

Dallas, TX | +1 (469) 431-2693 | udayravoorik.r@gmail.com | LinkedIn

Summary

Cloud Security Analyst with **3 years** securing **AWS infrastructure**, **conducting security assessments**, and **managing vendor risk**. **Reduced incident response time 40%**, **prevented 180+ misconfigurations through automated scanning**, and built **Python automation processing 30,000+ security events daily**. Managed **IAM governance for 450+ users across 35 accounts** while conducting **threat hunting** and **incident response**.

Skills

- **Cloud & Security Platforms**: AWS, Amazon Web Services, AWS Security Hub, GuardDuty, Config, IAM, IAM Identity Center, Organizations, CloudTrail, CloudWatch, S3, VPC, ECS, Lambda, CSPM, Cloud Security Posture Management, Splunk, SIEM
- **Security Tools & Scanning**: Checkov, Nessus, Prowler, ScoutSuite, Vulnerability Scanning, IaC Security, Container Security Scanning, Threat Detection, Security Automation
- **Programming & Development**: Python, boto3, SQL, Bash, Scripting, API Integration, Security Automation, Log Analysis
- **Security Operations**: Incident Response, Threat Hunting, Security Monitoring, Cloud Security Assessments, IAM Governance, Access Management, Alert Investigation, Root Cause Analysis, MITRE ATT&CK
- **Infrastructure Security**: Infrastructure as Code, IaC, Terraform, CloudFormation, CI/CD Security, Docker, Container Security, Kubernetes, DevSecOps
- **Compliance & Risk Management**: Third-Party Risk Management, TPRM, Vendor Risk Assessment, CIS Benchmarks, NIST CSF, ISO 27001, SOC 2, GDPR, Compliance Auditing

Professional Experiences

Cloud Security Analyst (Contract)| KnowBe4 | Remote (US) **Jul 2025 – Present**

Global cybersecurity SaaS company (~1,500 employees) specializing in security awareness training. Primary cloud security analyst responsible for monitoring AWS infrastructure, investigating security alerts, and responding to incidents across production and development environments

- Monitored and investigated 600-900 security alerts weekly across AWS environments using Splunk SIEM, AWS Security Hub, and GuardDuty, reducing mean time to response by 40%
- Administered AWS IAM operations across 35 production and development accounts supporting 450+ users, performing quarterly access reviews and reducing standing privileged access by 55%
- Conducted security assessments for 45-55 cloud workloads annually against CIS AWS Foundations Benchmark, coordinating remediation with engineering teams and achieving 65% reduction in high-severity findings
- Developed Python automation scripts using boto3 for CloudTrail log analysis, security group auditing, and compliance reporting that process 30,000+ events daily, saving 30 hours monthly
- Configured and maintained Checkov scanning in CI/CD pipelines for infrastructure-as-code and Docker container image security reviews, working with DevOps teams to prevent 180+ misconfigurations from production
- Monitored security configurations for Amazon ECS workloads including task definitions, IAM roles, and network policies, using SQL queries in Splunk to analyze container access patterns and runtime behaviors
- Investigated cloud security incidents as primary responder including credential compromise and unauthorized API calls, performing root cause analysis using CloudTrail and implementing preventive controls
- Performed proactive threat hunting across AWS CloudTrail and VPC Flow Logs using Splunk SPL and SQL queries to identify anomalous patterns, creating 8 custom detection rules over 12 months

Security Analyst| CRISIL | India **Jul 2021 – Jul 2023**

Global financial analytics firm (~5,000 employees). Security Analyst on Information Security team with responsibilities spanning third-party vendor risk assessments, AWS IAM governance, and security operations support for hybrid cloud and on-premises infrastructure

- Conducted comprehensive third-party vendor security assessments against NIST Cybersecurity Framework, evaluating information security practices, cloud security controls, and regulatory compliance, completing 25-30 vendor evaluations annually
- Monitored ongoing security risk for 40+ active third-party vendor relationships through quarterly reviews, security incident tracking, and compliance certification verification, maintaining centralized risk register
- Supported SOC 2 Type II and ISO 27001 audit activities by collecting security control evidence, documenting procedures, and demonstrating configurations, contributing to successful audits
- Performed AWS IAM access reviews for 350+ users across 10 accounts, conducting monthly access certifications and collaborating with infrastructure teams to reduce permissions by 40%
- Supported security operations team with event investigation for hybrid infrastructure, analyzing 120-180 alerts monthly using SIEM SQL queries, CloudTrail analysis, and endpoint tool correlation
- Performed security reviews of containerized application deployments in development environments, identifying misconfigurations in Docker and Kubernetes pod security policies, RBAC settings, and network policies during quarterly assessments
- Conducted quarterly cloud security configuration reviews using AWS Security Hub and Config against CIS AWS Benchmark, documenting 100-200 findings per review and coordinating remediation efforts

Security Analyst Intern| CRISIL | India **Jan 2021 – Jun 2021**

Six-month internship within Information Security team at CRISIL's Mumbai office, supporting security operations and learning cloud security fundamentals

- Assisted security operations team with daily security monitoring and alert investigation from SIEM and AWS CloudTrail, reviewing suspicious activities under guidance of senior security analysts
- Supported AWS IAM administration activities including user provisioning requests, quarterly access reviews for 200+ users, and multi-factor authentication compliance verification using AWS Console
- Performed weekly vulnerability scans using Nessus across development and production systems, tracking findings in ticketing system and coordinating remediation progress with system administrators
- Completed foundational AWS training including Security Fundamentals and Cloud Practitioner concepts through hands-on work supporting production environments, preparing for full-time Security Analyst role

Education

Master of Science | Cybersecurity Technology and Policy | University of Texas at Dallas
Bachelor's | Electrical and Computer Engineering | Reva University, India

Projects

Multi-Account AWS Security Framework

- Designed automated security monitoring architecture for multi-account AWS environment with Security Hub, GuardDuty, and CloudWatch
- Developed 15 Python detection rules using boto3 for IAM anomalies, unauthorized access patterns, and CIS Benchmark compliance violations
- Implemented centralized logging and security dashboards for simulated three-tier enterprise environment with dev, staging, and production accounts

Certification

CompTIA Security+ (DXX5W9KYQ2QQQHSW)
Google Cybersecurity Certification