DHANESH BABU

Security Engineer | SOC Analyst | Cloud Security Engineer | Incident Responder

Chennai, India | dhanesh0909@gmail.com | +91 78455 00169 | dhanesh.info | linkedin.com/in/dhaneshb

PROFESSIONAL SUMMARY

Security Engineer with 6+ years of experience in SOC operations, cloud security monitoring, incident detection and response (IDR), and vulnerability management across AWS, Azure, and GCP. Expertise in SIEM platforms (Splunk, Microsoft Sentinel), EDR tools (CrowdStrike Falcon), and SOAR-driven alert triage aligned to MITRE ATT&CK framework. Hands-on with Zero Trust architecture, IAM, RBAC, and compliance frameworks including ISO 27001, NIST CSF, SOC 2, and GDPR. AWS Certified Security Specialty (SCS-C02) and Microsoft SC-200 certified SOC analyst with proven track record reducing MTTD and MTTR across multi-cloud environments.

CORE COMPETENCIES

SOC Operations & Alert Triage	**Incident Detection & Response (IDR)**	**SIEM / SOAR / EDR Operations**
MITRE ATT&CK Framework	**Vulnerability Management (VM)**	**Cloud Threat Hunting (AWS/Azure/GCP)**
Zero Trust & IAM Architecture	**Compliance: ISO 27001 / NIST / SOC 2**	**Penetration Testing & Risk Assessment**

TECHNICAL SKILLS

SIEM / SOAR	Splunk, Microsoft Sentinel, AWS Security Hub, Azure Defender for Cloud, Prisma Cloud, Zabbix
EDR / Threat Detection	CrowdStrike Falcon (EDR), Microsoft Defender for Cloud, GuardDuty, AWS Inspector, Greenbone
Threat Frameworks	MITRE ATT&CK, CVSS Scoring, Kill Chain Analysis, Threat Intelligence, IOC/IOA Analysis
Cloud Platforms	AWS (Security Specialty Certified), Microsoft Azure, Google Cloud Platform (GCP)
Security Scanning	Prisma Cloud, Scout, Prowler, Burp Suite, SonarQube, Greenbone, Amazon Macie
Compliance	ISO 27001, NIST CSF, CIS Benchmark, SOC 2, FISMA, GDPR, SOX
IAM / Zero Trust	RBAC, IAM, AWS Organizations, ACM, Zero Trust Architecture, MFA, PAM
Scripting / DevSecOps	Python, Bash, Shell Scripting, CI/CD Security Integration, CloudFormation, IaC Security
Monitoring & Response	AWS CloudWatch, Azure Monitor, GCP Operations Suite, Datadog, Prometheus, Incident Playbooks
OS / Platforms	Ubuntu, RedHat, CentOS, Kali Linux, Kubernetes (EKS), Docker

CERTIFICATIONS

Jan 2026	Security Operations Analyst Associate - SC-200 (Microsoft) | SOC / SIEM / Sentinel
Jan 2026	Google Cloud Engineer Associate (GCP)
Jun 2025	Microsoft Azure Security, Compliance & Identity Fundamentals - SC-900
Jun 2024	**[TOP CERT] AWS Certified Security - Specialty (SCS-C02) | Highest AWS Security Certification**
Jan 2023	AWS Certified SysOps Administrator - Associate (SOA-C02)
May 2022	AWS Certified Cloud Practitioner (CLF-C02)
Mar 2022	Microsoft Azure Fundamentals (AZ-900)

PROFESSIONAL EXPERIENCE

Security Delivery Senior Analyst*Jan 2025 - Present*

Accenture | Bengaluru, India

- Monitored and triaged 500+ security alerts per week across AWS, Azure, and GCP using Splunk and Microsoft Sentinel SIEM, achieving average alert resolution time of under 4 hours and reducing false positives by 35%.
- Led incident detection and response (IDR) for 20+ cloud security incidents using SOAR-driven playbooks aligned to MITRE ATT&CK framework, reducing MTTR by 40% quarter-over-quarter.
- Managed CrowdStrike Falcon EDR across 300+ endpoints and Kubernetes (EKS) workloads; performed container vulnerability detection, triaged CVSS-scored findings, and enforced remediation SLAs within 48 hours for critical severity.
- Configured Prisma Cloud CSPM to enforce ISO 27001, SOC 2, GDPR, and NIST CSF compliance policies across 3 cloud environments; reduced compliance violations by 60% within 6 months.
- Conducted cloud threat hunting using MITRE ATT&CK TTPs across AWS CloudTrail, Azure Activity Logs, and GCP Audit Logs; identified and contained 3 advanced persistent threat (APT) indicators within first quarter.
- Implemented Zero Trust architecture by designing RBAC and fine-grained IAM policies across AWS, Azure, and GCP; eliminated 100% of over-privileged access findings in quarterly access reviews.
- Deployed AWS WAF, GuardDuty, Azure Security Center, and Google Cloud Armor; authored and maintained 15+ incident response playbooks, cutting mean time to detect (MTTD) by 30%.

Senior Security Engineer*Jul 2022 - Dec 2024*

CTG | Chennai, India

- Implemented AWS GuardDuty across 5 AWS accounts to continuously monitor for threats and unauthorized behavior; detected and remediated 200+ malicious activity events in first 90 days with zero production impact.
- Configured AWS Config with 50+ custom compliance rules to track resource changes and enforce audit trails; achieved 98% compliance score against CIS Benchmark and NIST 800-53 controls.
- Deployed centralized AWS WAF and Shield Advanced across AWS Organizations covering 10+ accounts; blocked 10,000+ malicious requests per month and prevented 2 DDoS events with zero downtime.
- Conducted automated vulnerability assessments using AWS Inspector and Amazon Macie across 150+ EC2 instances and S3 buckets; reduced critical and high CVSS vulnerabilities by 70% within 3 months.
- Performed penetration testing on 12+ cloud-hosted applications using Burp Suite and Prowler; delivered risk-ranked remediation reports resulting in 85% of critical findings closed within SLA.
- Led incident response for 15+ cloud security events using AWS Security Hub and Splunk SIEM; performed root cause analysis (RCA) and post-incident reviews, maintaining 99.9% uptime SLA.
- Audited cloud environments for SOC 2 Type II and SOX compliance; prepared evidence packages for 3 external audits with zero findings escalated to management.

System Engineer*Nov 2018 - Nov 2021*

Full Creative | Chennai, India

- Hardened 20+ Linux servers (Ubuntu, RedHat, CentOS) by implementing CIS Benchmark controls, enforcing MFA, and configuring host-based firewalls; reduced attack surface by 50% per quarterly security scans.
- Ensured GDPR compliance across customer data workflows by implementing data encryption, access controls, and conducting quarterly vulnerability assessments; zero compliance breaches reported.
- Managed AWS and GCP hosted environments for 5+ clients; administered Google Workspace for 100+ users including domain management, MFA enforcement, and data migration with zero data loss.
- Identified and remediated 30+ security risks across cloud environments; facilitated migration of 3 legacy systems to secure AWS cloud platforms, reducing infrastructure vulnerabilities by 45%.

EDUCATION

Bachelor of Engineering - Electronics & Communication Engineering*2014 - 2018*

Sri Krishna College of Engineering and Technology | Coimbatore, India