# MAGED BLASHRAM

AWS Cloud Security | Cybersecurity | SOC
m.blashram@gmail.com | +966 53 738 4474 | Riyadh, Saudi Arabia
github.com/Majed-Saeed | linkedin.com/in/maged-blashram | majed-devops.site

## PROFESSIONAL SUMMARY

Final-year Computer Science (Computer Security) student with an interest in Cloud Security, Cloud Computing, and AWS. I have used AWS services to build and secure cloud environments through my university and personal projects. I have also worked on projects such as a cloud security automation platform for my final-year project, which detects AWS misconfigurations and automatically remediates selected security issues. Familiar with Linux, Python, and security monitoring tools such as Splunk and Wireshark. Holder of the Google Cybersecurity Professional Certificate and currently preparing for the AWS Certified Solutions Architect – Associate certification. Seeking an internship in Cloud Security, AWS Cloud Engineering, or SOC, where I can apply my technical skills, gain hands-on industry experience, and continue learning.

## TECHNICAL SKILLS

- **Amazon Web Services (AWS):** AWS CLI, IAM, EC2, S3, VPC, CloudWatch, CloudTrail, AWS Config, Lambda, EventBridge, SNS, DynamoDB, Route 53
- **Automation & Tools:** Git, GitHub, Security Automation, Auto-Remediation, Python Scripting
- **Security Monitoring & SOC:** Splunk, SIEM, Snort (IDS), Log Analysis, Threat Detection, Incident Detection
- **Network & Tools:** Nmap, Wireshark, TCP/IP, VLANs, Inter-VLAN Routing, NAT, VLSM, Firewalls (WAF), RADIUS, SSO
- **Security Practices:** Identity & Access Management (IAM), Least Privilege, Compliance, Hardening, Endpoint Security
- **Programming & OS:** Python, Bash, Linux (Ubuntu, Kali), Windows

## PROJECTS

**Cloud Misconfiguration Detection & Auto-Remediation** · *Capstone / Final Year Project*

- Built a serverless, event-driven AWS pipeline (CloudTrail → EventBridge → Lambda) that detects high-risk security-group exposures in real time and auto-remediates them in ~5.3s on average — versus AWS Config's detect-only default, which flags but never closes the port.
- Designed an original risk-scoring engine (0–100, weighted by port sensitivity, exposure breadth, range, and protocol) and evasion-resistant CIDR-breadth detection that caught 100% of split-CIDR bypass techniques (vs 0% for exact-string matching); validated with an automated test harness at 12/12 scoring accuracy, with audit trails in DynamoDB, S3, and SNS email alerts.

*github.com/Majed-Saeed/aws-cloud-misconfiguration-auto-remediation* · *Tech: AWS Lambda, CloudTrail, EventBridge, AWS Config, EC2, S3, DynamoDB, SNS, CloudWatch, IAM, Python*

**Network Security Team Project — Workshop II** · *University Subject · Blue Team (Defensive Security) · UTeM*

- Participated in a university network security subject (16 students across four teams) simulating a Red-vs-Blue scenario on a 12-VLAN network; as part of the Blue Team, assisted in configuring defensive services including IDS monitoring, OS hardening, RADIUS, SSO, and a Web Application Firewall (WAF).
- Contributed to the team Hardening Report documenting vulnerabilities, countermeasures, and post-hardening validation; assisted with shared network design tasks including inter-VLAN routing, NAT, and VLSM addressing.

*Tech: IDS, OS Hardening (Windows/Linux), RADIUS, SSO, WAF, VLANs, Inter-VLAN Routing, NAT, VLSM*

**Splunk SIEM — Linux SSH Authentication Monitoring**

- Engineered a Splunk SIEM lab ingesting Linux auth logs and wrote search queries and alerts to detect SSH brute-force attempts and anomalous login patterns — SOC-style threat detection and log analysis.

*github.com/Majed-Saeed/splunk-linux-auth-monitoring* · *Tech: Splunk, SIEM, Linux, Syslog, Log Analysis*

**Cloud Engineering on AWS**

- Built a broad set of hands-on AWS labs spanning IAM (roles, STS AssumeRole, least-privilege and explicit-deny policies), EC2, S3, and VPC, plus CloudWatch and SNS alerting, CloudTrail audit logging, and Route 53 DNS — reinforcing secure, well-monitored cloud operations.

*github.com/Majed-Saeed/cloud-engineering-aws* · *Tech: AWS IAM, STS, EC2, S3, VPC, CloudWatch, SNS, CloudTrail, Route 53, AWS CLI*

**EC2 SSH Disaster Recovery**

- Recovered a locked-out EC2 instance through a disaster-recovery procedure — detached and remounted the root EBS volume on a rescue instance, repaired SSH configuration, and restored access with zero data loss.

*github.com/Majed-Saeed/ec2-ssh-disaster-recovery* · *Tech: AWS EC2, EBS, Linux, SSH, Disaster Recovery*

## EDUCATION

**Bachelor of Computer Science (Computer Security)** Expected Graduation: 2027
Universiti Teknikal Malaysia Melaka (UTeM) — Final Semester

## CERTIFICATIONS

- Google Cybersecurity Professional Certificate — Coursera / Google
- AWS Certified Solutions Architect – Associate — In Progress