# YVES NICOLAS TAGNE TOUMNE

Montgomery Village, MD | (227) 241-0235 | ttynicos@gmail.com | Active **Secret Clearance**

## PROFESSIONAL SUMMARY

Cloud Security Engineer with **8+ years** of experience architecting enterprise security solutions across AWS, hybrid cloud, and containerized environments. Expertise in vulnerability management, DevSecOps pipeline integration, and infrastructure hardening supporting **FedRAMP, NIST 800-53, FISMA, PCI-DSS, and DISA STIG** compliance. Achieved **80% reduction in critical vulnerabilities** across 500+ systems while leading cross-functional remediation with global teams in regulated federal and commercial environments.

## CORE COMPETENCIES

**AWS Security:** Security Hub, GuardDuty, Inspector, Config, CloudTrail, IAM, VPC, Lambda, EKS/ECS

**Compliance:** FedRAMP, FISMA, NIST 800-53, RMF, PCI-DSS, DISA STIGs, CIS Benchmarks

**Vulnerability Tools:** Qualys VMDR/WAS, Prisma Cloud, Tenable Nessus, Rapid7, AWS Inspector

**Systems:** Linux (RHEL, Ubuntu, CentOS), Windows Server, System Hardening, Patch Management

**Container/DevOps:** Kubernetes, Docker, Jenkins, GitHub Actions, GitLab CI/CD, Terraform, Ansible

**Programming:** Python, Go, Bash, PowerShell, YAML, JSON, Infrastructure as Code

## PROFESSIONAL EXPERIENCE

**Senior Cloud Security Engineer**

*Medtronic — Remote (Contract) | May 2023 – Present*

- Architected enterprise AWS security program for 200+ cloud resources, implementing Security Hub, GuardDuty, and automated incident response that reduced mean time to detection by 65%
- Led vulnerability management using Qualys VMDR, achieving 80% reduction in critical findings through remediation tracking, executive dashboards, and cross-functional escalation protocols
- Designed container security for EKS/ECS workloads with Prisma Cloud runtime protection and image scanning, achieving 95% automated vulnerability detection before production deployment
- Embedded security gates into CI/CD pipelines (Jenkins, GitLab, GitHub Actions) enforcing SAST, DAST, and SCA standards that blocked 340+ vulnerable deployments quarterly
- Developed Python/Bash automation for vulnerability analysis and compliance metrics, reducing manual security operations by 60%, configured AWS Config for CIS Benchmark compliance monitoring
- Established SLA-driven remediation framework reducing MTTR from 45 to 12 days across hybrid Linux/Windows environments while maintaining 99.5% patching compliance

**Senior Security Engineer / Cloud Security Specialist**

*Deloitte — Washington, DC | June 2022 – May 2023*

- Led vulnerability management for 300+ federal systems using Qualys VMDR and Prisma Cloud, achieving 75% reduction in POA&M findings within 6 months for civilian agency clients
- Architected AWS security controls aligned with FedRAMP Moderate baseline, configuring Security Hub, GuardDuty, CloudTrail, and Config for continuous monitoring in GovCloud
- Implemented Kubernetes security scanning with admission controllers, network policies, and runtime protection enabling ATO approval for 3 mission-critical federal systems
- Managed quarterly PCI-DSS vulnerability scanning for financial services clients, coordinating penetration testing with zero critical findings during annual QSA audits

- Integrated vulnerability scanners into Jenkins and AWS CodePipeline, establishing security gates for Docker, Kubernetes, and Terraform deployments preventing 200+ non-compliant releases
- Executed Linux/Unix hardening aligned with DISA STIGs using Ansible playbooks, achieving 98% compliance across RHEL and Ubuntu fleets, coordinated remediation across 4 time zones

**DevSecOps Engineer / Vulnerability Management Specialist**

*Cognizant — Various Locations | May 2016 – May 2022*

- Designed enterprise vulnerability management program using Qualys VMDR and Tenable Nessus for 500+ cloud and on-premises systems across retail, financial, and healthcare sectors
- Pioneered container security for Docker/Kubernetes environments with image scanning, registry controls, and runtime detection reducing container incidents by 70%
- Built CI/CD security integrations (Jenkins, Tekton, GitHub Actions) with automated gates blocking critical vulnerabilities, achieving 90% automated detection rate
- Administered Linux (RHEL, CentOS, Ubuntu) and Windows Server environments including hardening, patch management, user access, and security configuration per CIS Benchmarks
- Led quarterly PCI-DSS assessments for retail/financial clients, coordinating cross-functional remediation to maintain continuous compliance status
- Developed PowerShell and Bash automation for Windows/Linux remediation enabling automated patching and configuration enforcement, reducing admin effort by 50%
- Performed hands-on system administration including service configuration, log analysis, and troubleshooting across hybrid infrastructure supporting 24/7 operations
- Implemented IaC security scanning for Terraform/CloudFormation, identifying misconfigurations pre-deployment and reducing cloud security incidents by 45%

## CERTIFICATIONS & EDUCATION

**Certifications:**

- AWS Certified Security – Specialty
- CompTIA Security+
- AWS Certified Solutions Architect – Professional
- AWS Certified Cloud Practitioner
- Azure Administrator Microsoft Certified – Associate
- Azure Solutions Architect Expert
- Certified Kubernetes Security Specialist (CKS)
- AI Security & Governance Certified
- Agile Foundations Certified
- SAFe 6 Scrum Master Certified
- Professional Scrum Master I (PSM I) Certified
- Project Management Essentials Certified (PMEC)
- Six Sigma Yellow Belt Certified

**Education:**

Master of Cybersecurity Technology
*University of Maryland Global Campus — 2026*

Petroleum & Water Supply Specialist
*US Army Quartermaster School — 2024*

Bachelor of Science in Quality Health Safety Environment
*Catholic University of Central Africa — 2016*

## LINKEDIN PROFILE URL

https://www.linkedin.com/in/yves-tagne-21b22382