George J. Ontiveros III

Platform & Low-Level Security Engineer

San Antonio, TX · gontiveros292@gmail.com · linkedin.com/in/george-ontiveros · github.com/devbrewster · georgeonti.com

SUMMARY

Security engineer with 7+ years across incident response, vulnerability management, and application/product security, now leading AI trust & safety reviews at Accenture Federal Services and building AI-driven security automation as founder of CVERiskPilot. Independent research concentrates on low-level and hardware security — Linux kernel exploitation and crash-dump forensics, firmware reverse-engineering, and bootloader/embedded analysis — documented across 180+ published investigations. Comfortable owning ambiguous, cross-functional security problems from research through production.

CORE FOCUS

- **Low-Level & Hardware Security (research):** Linux kernel exploitation & crash-dump analysis, firmware RE (SquashFS, binwalk), bootloader/embedded (U-Boot, I²C/EEPROM), rootkit & memory forensics (Volatility 3, crash)
- **OS & Container Security:** Linux, Docker/containers and isolation, CVE triage and remediation, hardening
- **DFIR & Incident Response:** host triage, memory forensics, SIEM threat hunting (Splunk), MITRE ATT&CK mapping
- **Security Automation:** AI agents for security research, multi-scanner pipelines, CI/CD security tooling (SAST/DAST/SBOM, secrets, IaC)
- **Languages & Tools:** Python, Bash, C (reading/RE), Git/GitHub, Docker, Splunk, ACAS, JFrog, Prisma, Grype, Wiz

EXPERIENCE

Senior AI Trust & Safety Specialist — Accenture Federal Services *2026 – Present*

- Lead a **12-person cybersecurity & AI trust-and-safety team (scaling to 20)** reviewing third-party AI applications, cyber operations, and enterprise support for one of the world's leading AI companies.
- Stood up the operation from scratch — 10 SOPs, onboarding/training, and automated metrics dashboards for analysts and leadership — and carried the team through three mission pivots while maintaining delivery continuity.
- Review AI applications against platform trust & safety and security requirements, surfacing abuse patterns, policy violations, and AI-specific risks (prompt injection, model abuse, data leakage, agentic-application risks).

Founder & Security Engineer — CVERiskPilot LLC *2025 – Present*

- Built an AI-driven vulnerability-triage platform whose multi-model agent **automates security research** — ingesting 11 scanner formats, enriching with CVE/EPSS/KEV, and producing prioritized, explained remediation.
- Shipped a published CLI scanner (dependencies, secrets, IaC, API routes) with automated policy verdicts, **reducing manual security overhead in build, test, and release workflows.**
- Implemented a tamper-evident, signed audit trail (Ed25519 + Merkle tree) and control mapping across 13 compliance frameworks.
- Hardened the platform via self-dogfooded scanning: access-control fixes, dependency upgrades, and container-image security.

Application Security Architect — Accenture Federal Services (MD&I R&D / Assets Enablement) *2024 – 2026*

- Helped build and test an **agentic application that automates review of security reports** for federal use cases.
- Performed application and container security reviews across DAST, SAST, OSS/SBOM, JFrog, Prisma, Grype, and Wiz.
- Redesigned the risk-assessment workflow for POA&M generation and onboarded new reviewers on the process.

Jr. Incident Handler — Insight Global / U.S. Dept. of State *2021*

- Detected, analyzed, and responded to malware, insider-threat, and data-breach incidents; performed malware analysis, forensics, and post-incident reporting.

SOC Analyst — Insight Global / Army Unified Capabilities *2020 – 2021*

- Triaged Splunk alerts and drove incident response; performed ACAS vulnerability review and produced remediation reporting.

Patch & Endpoint Administration — Millennium Software & Staffing (DoD) *2022 – 2024*

- Administered patch management for 2,000+ DoD medical devices (CONUS/OCONUS); maintained FDA/DoD compliance.

Corporal, Embarkation Specialist — United States Marine Corps *2010 – 2014*

- Led small-team logistics, training, and operational readiness in high-accountability environments.

SECURITY RESEARCH & WRITING

- 180+ documented security investigations (Hack The Box) across hardware/firmware, Linux kernel exploitation, DFIR/memory forensics, and full-chain penetration testing.

- Selected retired write-ups published at **georgeonti.com** — firmware RE, kernel crash/rootkit analysis, CVE-2024-1086 (nf_tables), U-Boot/EEPROM secret recovery, and multi-stage Linux compromise.

EDUCATION & CERTIFICATIONS

- B.S., Cybersecurity — Hallmark University, 2019
- CompTIA Security+