NICOLAS PORTILLA GOMEZ

San Antonio, TX | 210-591-3070 | nicolasportillagomezwork@gmail.com | LinkedIn | GitHub | My Portfolio

SUMMARY

Senior cybersecurity student at UTSA (December 2026) and current Cybersecurity Incident Detection & Response Intern at Marathon Petroleum, with hands-on experience in EDR alert triage, SOAR automation, threat intelligence, OT security, and cloud IAM. Seeking a Fall 2026 internship or entry-level cybersecurity role.

EDUCATION

The University of Texas at San Antonio **Expected Graduation: December 2026**
Bachelor of Business Administration, Cybersecurity GPA: 3.72
Relevant Coursework: Operating Systems and Security, Telecommunications and Networking, Industrial Control Systems Security
Certifications: CompTIA Security+, AWS Certified Cloud Practitioner, Microsoft AZ-900, AZ-104 (in progress), Google Cybersecurity Professional Certificate

TECHNICAL SKILLS

Security Operations & IR: CrowdStrike Falcon (EDR, Real Time Response), Microsoft Defender, Google SecOps (SOAR playbooks), Proofpoint, Recorded Future, VirusTotal (GTI), Dragos (OT), incident response lifecycle
Cloud & Identity: Azure, Microsoft Entra ID (IAM), AWS, Google Cloud Platform (IAM administration), Wiz (CNAPP/cloud security), Docker
Networking: OSI model, VLANs, subnetting, STP, routing, Cisco IOS, Wireshark, OWASP
Scripting & Automation: Python, PowerShell, Bash, SQL, Git, CI/CD concepts
Frameworks & Compliance: NIST CSF, ISO 27001, GDPR, CIA Triad, risk management
Systems & Tools: Linux, Windows, macOS, ServiceNow, BeyondTrust Remote Support, Agile process planning

WORK EXPERIENCE

Cybersecurity Incident Detection & Response Intern **May 2026 – August 2026**
Marathon Petroleum, San Antonio, TX (Hybrid)

- Own security alerts end-to-end in a flat SOC structure, triaging and investigating detections in CrowdStrike Falcon and Microsoft Defender and driving each incident from initial alert through remediation and closure.
- Use Falcon Real Time Response to investigate, contain, and remediate threats on enterprise endpoints; create automated CrowdStrike workflows, supported by PowerShell and Python scripting, to streamline response processes.
- Triage and resolve alerts in Google SecOps, executing SOAR playbooks to drive consistent, repeatable investigations.
- Enrich investigations with threat intelligence from Recorded Future and VirusTotal (GTI); analyze reported phishing in Proofpoint.
- Monitor and investigate OT security alerts in Dragos, extending coverage across IT and OT environments.
- Support IAM administration in Microsoft Entra ID and GCP, applying least-privilege principles; document incidents in ServiceNow.

Cloud Security Intern **August 2025 – December 2025**
Trevenx, Remote

- Selected to the TrevenX Intern Team for sustained contributions to open-source cybersecurity across EDR, threat modeling, cloud security, and compliance automation.
- Implemented an AWS-based SIEM pipeline by forwarding GuardDuty findings to OpenSearch for real-time log analysis and visualization, strengthening threat detection and monitoring capabilities.

Level 1 Help Desk Technician **July 2025 – August 2025**
TEKsystems, Remote

- Resolved 30+ weekly service requests involving VoIP, IPTV, and DSL issues for 40+ rural ISPs, achieving a 92%+ first-call resolution rate.
- Operated 13+ diagnostic and CLI tools (Calix, SmartRG, Plume) to isolate root causes of network outages, reducing average customer downtime by 15–30 minutes; coordinated escalations with Tier 2, NOC, and vendor teams via ServiceNow and Zendesk.

EMT-B **December 2022 – September 2025**
Allegiance Mobile Health, San Antonio, TX

- Provided life-saving care across 100+ emergency responses with rapid triage, cross-team coordination, and HIPAA-compliant records.
- Trained 3+ new EMTs on unit protocols, stretcher operations, and radio procedures, improving onboarding and crew response times.

PROJECTS

AWS SIEM Log Analysis Project | Tools: AWS GuardDuty, OpenSearch, S3, VPC, Firehose

- Built a cloud-based SIEM pipeline by integrating GuardDuty with OpenSearch through S3 to centralize and analyze security logs.
- Designed real-time dashboards and configured high-severity alerts with trigger conditions to detect and escalate threats.

Azure Administration Lab Series (AZ-104) | Tools: Entra ID, RBAC, Azure Policy, ARM/Bicep, Azure Monitor — Portfolio

- Completed 13+ hands-on labs covering Entra ID identity, governance (RBAC, Azure Policy), virtual networking, storage, and VM administration.
- Deployed infrastructure as code with ARM templates and Bicep; configured backups, Site Recovery, and Azure Monitor alerting.

AWARDS AND EXTRACURRICULARS

UTSA President's List | Active member, CompTIA Student Chapter