ALEJANDRO GARCIA

Threat Hunting · Detection Engineering · DFIR · Cloud Security

Forsyth, GA | CyberJudoSec@gmail.com | LinkedIn | Portfolio | GitHub

PROFESSIONAL SUMMARY

Threat Hunting and DFIR professional with 8+ years of combined IT and cybersecurity experience specializing in hypothesis-driven investigations, detection engineering, and adversary behavior analysis across enterprise and cloud environments. Experienced identifying sophisticated threats across endpoint, identity, network, and cloud telemetry using Microsoft Sentinel, Splunk, and Defender XDR. Strong expertise uncovering attacker techniques such as lateral movement, credential abuse, persistence, and C2 through observation-driven and behavior-based hunting methodologies. Proficient in KQL, SPL, Python, and PowerShell for detection development and deep log analysis. Skilled in leveraging OSINT and threat intelligence platforms to enrich investigations and map adversary activity to MITRE ATT&CK.

CORE SECURITY SKILLS

- Threat Hunting & Detection Engineering
- Incident Response & Digital Forensics
- MITRE ATT&CK Mapping
- Threat Intelligence Analysis
- Log Analysis & Correlation
- Identity Threat Detection
- Cloud Security Monitoring
- Observation-Driven Hunting
- Hypothesis-Based Detection

SECURITY PLATFORMS & TOOLS

SIEM	Microsoft Sentinel · Splunk · Elastic SIEM
Endpoint	Defender XDR · Defender for Endpoint · Defender for Identity · Defender for Office 365
Identity	Microsoft Entra ID · Active Directory · Okta · Wiz · Forcepoint
Cloud	AWS · Microsoft Azure · Google Cloud Platform · IAM · CloudTrail · Azure Monitor
OSINT / Intel	Maltego · Shodan · VirusTotal · Censys · SpiderFoot · ZeroFox · SecurityTrails
Scripting	KQL · Splunk SPL · Python · PowerShell · Bash · Regex · JSON Parsing
Network	Wireshark · tcpdump · DNS Analysis · HTTP/S Analysis · nmap · pfSense
OS	Kali Linux · Ubuntu · Windows Server · REMnux · macOS
Frameworks	MITRE ATT&CK · NIST CSF · NIST SP 800-53

PROFESSIONAL EXPERIENCE

Threat Hunting & Forensics Analyst

2026 – Present

Business Operational Concepts · Remote

- Conduct proactive, hypothesis-driven threat hunts across endpoint, identity, and cloud telemetry using Sentinel, Splunk, and Defender XDR to identify adversary behavior and lateral movement
- Develop and optimize detection logic using KQL, SPL, Python, and PowerShell, improving visibility into credential abuse, persistence mechanisms, and C2 activity
- Investigate complex incidents including phishing, C2 beaconing, privilege escalation, and identity compromise through multi-source log correlation

- Enrich investigations using OSINT tools (Maltego, SpiderFoot, Shodan, VirusTotal) to identify malicious infrastructure and threat actor patterns
- Map adversary behavior to MITRE ATT&CK, strengthening detection coverage and enabling standardized investigation workflows
- Document threat hunting methodologies and detection improvements to support repeatable, scalable security operations

Cyber Defense Analyst II
2024 – 2026

SAIC · Remote

- Monitored and triaged enterprise security alerts across SIEM and endpoint platforms, analyzing malware, phishing, and authentication anomalies
- Conducted log correlation and IOC analysis to identify indicators of compromise and unauthorized access attempts
- Supported incident response workflows by documenting findings, escalating threats, and improving alert handling procedures
- Assisted in detection tuning efforts to reduce false positives and improve signal-to-noise ratio across alert pipelines

Cloud Migration Consultant
2024 – 2025

MassMutual · Remote

- Supported enterprise cloud migration across AWS and Azure environments, reviewing IAM configurations and validating logging and monitoring for cloud workloads
- Leveraged Nexthink to proactively identify endpoint performance issues, network disruptions, and security-impacting anomalies
- Collaborated with security teams to support investigations and resolve access and authentication-related issues

IT Operations Center Analyst I / Service Desk Analyst II
2021 – 2023

Chewy · Plantation, FL

- Supported Windows systems, VPN connectivity, and enterprise authentication environments in high-volume operational settings
- Utilized Nexthink analytics to diagnose and resolve endpoint and network issues while maintaining secure and stable operations
- Escalated security-related incidents and supported IAM troubleshooting across enterprise platforms

THREAT HUNTING & SECURITY LAB PROJECTS

Microsoft Sentinel · KQL · Defender for Identity
2025

Impossible Travel Detection

- Built KQL detection queries in Sentinel to identify impossible travel login patterns — sign-ins from distant locations within physically impossible timeframes
- Correlated with Defender for Identity signals and reconstructed full attacker timeline; detection fired 4 hours before automated alerting
- Documented reusable detection rule template with false positive mitigations (T1078, T1550.002)

Maltego · Shodan · VirusTotal · Censys
2025

Malicious Infrastructure Investigation

- Pivoted 3 seed indicators to 12 related infrastructure nodes via Maltego transforms, SSL certificate pivoting, and passive DNS analysis
- Delivered structured threat intelligence report with IOC list, infrastructure relationship map, and ATT&CK technique mappings

Wireshark · tcpdump · Kali Linux
2024

Network Traffic Analysis Lab

- Confirmed DNS tunneling (dnscat2-style) with 180+ queries/minute to bulletproof resolver and Base64-encoded subdomain payloads
- Produced SOC-reusable detection notes with Wireshark filter signatures and IOC documentation

pfSense · nmap · VirtualBox

2024

Firewall & Network Segmentation Lab

- Designed and implemented 3-VLAN segmented architecture with default-deny rules; all 5 nmap validation tests passed
- Eliminated unrestricted lateral movement — attacker pivot path reduced from full network to single VLAN

CERTIFICATIONS

- Certified Ethical Hacker (CEH) — EC-Council
- GIAC Security Essentials (GSEC)
- GIAC Foundational Cybersecurity (GFACT)
- CompTIA Security+
- CompTIA Network+
- CompTIA A+
- CompTIA Infrastructure Specialist
- AWS Solutions Architect Associate
- AWS Cloud Practitioner
- Microsoft Azure Administrator AZ-104
- Microsoft Azure Fundamentals AZ-900
- Cisco CCNA
- Okta Certified Professional

EDUCATION

Bachelor of Science — Computer Science (In Progress)
Trident University International
Expected 2026

Associate of Science — Cybersecurity
Trident University International
2023

ONLINE PRESENCE

Portfolio	hackth3br0nx.github.io
GitHub	github.com/Hackth3br0nx
TryHackMe	tryhackme.com/p/Hackth3br0nx
Codefinity	codefinity.com/cv/35ba2da4-c3c9-459d-8d83-78a67c4f45fd
Threat Hunting	threathuntinglabs.com/u/hackth3br0nx