

# BRENDAN HIGGINS

✉ higgins.bren@gmail.com • in linkedin.com/in/higgins • 📍 Georgia, USA

## SUMMARY

I am a Cybersecurity Engineer and a strategic defender with a decade of experience, specializing in detection engineering, incident response, and cloud security. My passion lies in architecting and leading complex defensive initiatives, delivering innovative and resilient technical solutions, and constantly staying one step ahead of emerging threats through creative new defensive implementations.

## EXPERIENCE

FEDERAL RESERVE SYSTEM: NATIONAL INCIDENT RESPONSE TEAM		
Federal Reserve Bank of Richmond	richmondfed.org	
Advanced Cyber Security Advisor		Mar 2024 – Present
Senior Cyber Security Advisor		Oct 2021 – Mar 2024
Senior Cyber Security Analyst		Feb 2021 – Oct 2021
Federal Reserve Bank of San Francisco	frbsf.org	
Lead Cyber Security Analyst		Oct 2018 – Feb 2021
Cyber Security Analyst		Aug 2016 – Oct 2018

## SKILLS

**TECHNOLOGIES:** Splunk, Terraform, Gitlab/GitHub, Jupyter, Docker, KQL  
**LANGUAGES:** Python, PowerShell, Bash, Markdown, JavaScript, HTML/CSS  
**METHODOLOGIES:** CICD, Git, Agile/Scrum/Kanban

## EDUCATION

WESTERN GOVERNORS UNIVERSITY		Nov 2018
Master of Science: Cybersecurity and Information Assurance		
CALIFORNIA STATE UNIVERSITY – SAN BERNARDINO		Jun 2016
Bachelor of Science: Business Administration, Cybersecurity		

## CERTIFICATIONS

ISC2	Certified Information Systems Security Professional (CISSP)	2020
GIAC	Python Coder (GPYC)	2025
	Cloud Threat Detection (GCTD)	2023
	Cloud Security Automation (GCSA)	2021
	Exploit Researcher and Advanced Penetration Tester (GXPN)	2020
	Certified Windows Security Administrator (GCWN)	2019
	Certified Forensic Analyst (GCFA)	2019
	Continuous Monitoring Certification (GMON)	2017
	Certified Intrusion Analyst (GCIA)	2017
COMPTIA	Pentest+	2022
	Cloud+	2021
	Network+	2015
	Advanced Security Practitioner (CASP)	2015
	Security+	2014
OTHER	GitLab – DevOps Professional	2022
	Amazon Web Services (AWS) – Cloud Certified Practitioner	2020
	EC-Council – Computer Hacking Forensic Investigator (CHFI)	2018
	EC-Council – Certified Ethical Hacker (CEH)	2016
	FCC General Class HAM Radio License	2015

## PROFESSIONAL DEVELOPMENT

<b>PRESENTATION</b>	Splunk .conf21 – Security Triage in the Real World (SEC1222A)	2021
<b>TRAINING</b>	SANS 573: Automating Information Security with Python	2025
	BlackHat: Active Directory Attacks for Red and Blue Teams – Advanced Edition	2024
	SANS 541: Cloud Security Attacker Techniques, Monitoring, and Threat Detection	2023
	SANS 540: Cloud Security & DevOps Automation	2021
	SANS 660: Advanced Penetration Testing, Exploit Writing, & Ethical Hacking	2020
	SANS 505: Securing Windows & PowerShell Automation	2019
	SANS 508: Advanced Incident Response, Threat Hunting, & Digital Forensics	2018
	SANS 511: Continuous Monitoring & Security Operations	2017
	SANS 503: Intrusion Detection In-Depth	2016
<b>CONFERENCE</b>	Blackhat USA	2023
	Splunk .conf19	2019
	SANS Threat Hunting & Incident Response Summit	2018
	RFun 2017 (Recorded Future)	2017
	DEFCON 24	2016