Joshua Rubio

Glendale, AZ | 480.737.8929 | griffindefense@protonmail.com | LinkedIn

Cybersecurity & Threat Intelligence Expert

Over 10 years of hands-on experience securing critical systems, leading threat intelligence programs, and optimizing incident response across FinTech, financial services, and SaaS environments. Known for turning threat data into actionable defenses, building detection logic from the ground up, and thriving in high-stakes, zero-fluff security teams. Passionate about solving complex problems, sharing knowledge, and building secure systems without the vendor noise. Strong background in infrastructure hardening, vulnerability assessments, patch management, and risk mitigation strategies that align security with business goals.

Core Skills & Tools

- Threat Intelligence & Detection Engineering
- Incident Response | Threat Hunting | SOC Optimization
- Cloud Security (AWS, GCP) | Infrastructure Hardening
- MITRE ATT&CK | SIEM: Splunk ES, ELK, Sumo Logic, Chronicle
- EDR/XDR: CrowdStrike, Cortex XDR
- Terraform | Python | YARA | Sigma | Suricata | Bash
- Firewalls, IDPS, Antivirus, Proxies, Network Hardening
- Vulnerability Management & Security Audits
- Risk Assessment & Mitigation | Security Policy Development
- Security Frameworks: NIST, ISO 27001, ISO 22301
- GCTI, eCTHP, CCTIA | Pursuing CISSP

Professional Experience

SCATTIC – Phoenix, AZ

Senior SOC Analyst & Cybersecurity Consultant | Oct 2023 – April 2024

- Conducted company-wide infrastructure risk assessments and deployed controls to reduce exposure by 25%.
- Led vulnerability scanning, patch validation, and remediation efforts to improve system resilience and compliance.
- Performed internal security audits and penetration test coordination, resolving systemic weaknesses and prioritizing mitigations.
- Developed and documented incident reports and breach response actions; supported leadership in risk evaluation and planning.
- Collaborated with engineering and operations teams to align system hardening with business continuity

Mission Lane – Remote

Senior Cyber Threat Intelligence Analyst | Apr 2021 – Jun 2023

- Built a company-wide threat intelligence program from scratch, identifying risks and improving response accuracy by 50%.
- Developed detection engineering strategies, including custom YARA and Sigma rules for proactive defense.

- Provided real-time risk advisories during high-severity incidents; documented outcomes and coordinated lessons-learned reviews.
- Researched and recommended improvements to endpoint and network monitoring based on evolving threat trends.
- Led purple team simulations and vulnerability scanning initiatives across network and cloud environments.

Early Warning Services – Scottsdale, AZ

Cyber Threat Intelligence Analyst II | Jul 2018 – Jan 2021

- Led vulnerability and threat modeling engagements; assessed risk to enterprise assets and advised patch strategy.
- Developed automated playbooks and alert tuning for SIEM workflows, reducing MTTD (Mean-Time-to-Detection) and alert fatigue.
- Integrated external threat feeds and analyzed APT activity using MITRE ATT&CK alignment.

SOC Analyst / SOC Analyst II | Feb 2015 – Jul 2018

- Administered Splunk-based dashboards and real-time SIEM analysis; created escalation processes and playbooks.
- Handled incident response end-to-end, including triage, mitigation, documentation, and recovery.
- Built and deployed early SOAR functions, enriching alerts and auto-responding to common threat patterns.

Certifications

- GCTI – GIAC Cyber Threat Intelligence
- eCTHP – Certified Cyber Threat Hunting Professional
- CCTIA – Certified Cyber Threat Intelligence Analyst
- Python for Cybersecurity – InfoSec Institute / Custom Project-Based
- CISSP (In Progress) – Certified Information Systems Security Professional
- IBM Data Science Professional (In Progress)