





## MICHAEL RODRIGUEZ

### Cybersecurity Engineer

 [m.rodriguez@email.com](mailto:m.rodriguez@email.com) |  (555) 987-6543 |  [github.com/mrodriguez](https://github.com/mrodriguez) |  Austin, TX

---

### OBJECTIVE

Dedicated Cybersecurity Engineer with expertise in network security, threat hunting, and security automation. Seeking to leverage 4+ years of experience in protecting critical infrastructure and implementing robust security solutions in a challenging environment.

---

### CORE COMPETENCIES

**Security Operations | Threat Analysis | Incident Response | Risk Assessment**  
**Security Architecture | Compliance Management | Vulnerability Management | Security Automation**

---

### TECHNICAL EXPERTISE

**Security Platforms:** Splunk Enterprise, IBM QRadar, CrowdStrike Falcon, SentinelOne  
**Network Security:** Fortinet, Checkpoint, Cisco Firepower, pfSense, Suricata  
**Cloud Security:** AWS Security Hub, Azure Sentinel, Google Cloud Security Command Center  
**Programming:** Python, Go, JavaScript, PowerShell, Bash  
**Operating Systems:** Windows 10/11/Server, Linux (CentOS, Debian), macOS

---

### PROFESSIONAL EXPERIENCE

#### Cybersecurity Engineer | SecureNet Industries | Jan 2022 - Present

- Architected security solutions for hybrid cloud environment serving 5,000+ employees
- Implemented automated threat hunting workflows, reducing mean time to detection by 50%
- Managed security operations center (SOC) tools and coordinated with external threat intelligence feeds
- Conducted red team exercises and security assessments, identifying 150+ vulnerabilities

- Developed Python scripts for security automation, improving efficiency by 45%

#### **Information Security Analyst | CloudFirst Technologies | Jun 2020 - Dec 2021**

- Monitored enterprise security infrastructure using multiple SIEM platforms
- Investigated and responded to 300+ security incidents, maintaining detailed forensic documentation
- Implemented endpoint detection and response (EDR) solutions across enterprise environment
- Created security policies and procedures aligned with NIST Cybersecurity Framework
- Collaborated with development teams to integrate security into CI/CD pipelines

#### **Junior Security Engineer | CyberDefense Corp | Aug 2019 - May 2020**

- Assisted in deployment and configuration of security tools and technologies
- Performed regular vulnerability scans and coordinated remediation efforts with system administrators
- Supported compliance audits for PCI DSS and HIPAA requirements
- Maintained security documentation and contributed to incident response playbooks

---

### **EDUCATION & TRAINING**

**Master of Science in Cybersecurity** | University of Texas at Austin | 2019

**Bachelor of Science in Information Technology** | Texas State University | 2017

#### **Continuous Learning:**

- SANS Training: SEC504 (Hacker Tools and Incident Handling)
- Cloud Security Alliance: Certificate of Cloud Security Knowledge

---

### **CERTIFICATIONS**

✓ **Certified Information Security Manager (CISM)** - 2023


✓ **GIAC Security Essentials (GSEC)** - 2022


✓ **CompTIA CySA+** - 2021


✓ **Microsoft Azure Security Engineer Associate** - 2023


---

### **KEY ACHIEVEMENTS**

 **Threat Reduction:** Decreased successful phishing attempts by 75% through enhanced email security and user training programs

 **Automation Success:** Developed custom SOAR playbooks reducing incident response time from 4 hours to 30 minutes

 **Compliance Leadership:** Successfully led organization through SOC 2 Type II audit with zero findings

 **Cost Optimization:** Identified and eliminated redundant security tools, saving \$120K annually