Marcus Chen

Senior Cybersecurity Analyst

(415) 555–0182
m.chen@email.com
linkedin.com/in/marcuschen
San Francisco, CA

Professional Summary

Results-driven Senior Cybersecurity Analyst with 7+ years of experience protecting enterprise environments across finance, healthcare, and technology sectors. Specialized in threat detection engineering, incident response leadership, and security automation. Proven track record of reducing breach detection time by over 40% and building high-performing security operations teams. Adept at translating complex threat landscapes into actionable defense strategies for executive stakeholders.

Technical Expertise

Threat Detection & Response
SIEM Management, EDR, SOAR Automation, Threat Hunting, Alert Triage, MITRE ATT&CK Mapping

Network Security
Firewalls, IDS/IPS, VPN, NAC, Packet Analysis, DNS Security, Network Segmentation

Cloud Security
AWS GuardDuty, Azure Sentinel, IAM, CSPM, Container Security, Serverless Hardening

Risk & Compliance
NIST CSF, ISO 27001, PCI DSS, SOC 2, GDPR, Vendor Risk Assessment

Security Automation
Python, Bash, PowerShell, SOAR Playbooks, API Integration, Log Parsing

Digital Forensics
Disk Imaging, Memory Analysis, Timeline Reconstruction, Chain of Custody, Evidence Handling

Professional Experience

Senior Cybersecurity Analyst Mar 2022 – Present
Nexa Technologies | San Francisco, CA

- Led a team of 4 SOC analysts monitoring 50,000+ endpoints across 12 global offices, reducing mean time to detect from 6.1 hours to 3.5 hours through automated correlation rule deployment
- Designed and deployed a custom SOAR platform integrating SIEM alerts with automated response playbooks, cutting average incident response time from 4.2 hours to 47 minutes
- Conducted 30+ tabletop exercises and purple team engagements annually, hardening defenses against ransomware and APT-style attack chains across cloud and on-premise environments
- Architected a zero-trust network segmentation strategy for a 2,000-user organization, reducing lateral movement risk by 68% within the first two quarters of implementation
- Mentored 6 junior analysts through structured training modules and pair-investigation rotations; authored the organization-wide incident response runbook adopted across all business units
- Managed vendor security assessments for 15+ third-party integrations, identifying and driving remediation of 23 critical vulnerabilities prior to production deployment

Security Operations Analyst Jun 2019 – Feb 2022
Synapse Defense Solutions | Austin, TX

- Monitored and triaged 8,000+ daily security events using SIEM and custom correlation rules, sustaining 99.7% alert coverage with an under 2% false positive rate across a Fortune 500 client portfolio

- Led forensic investigations on 15+ confirmed breaches, producing detailed root cause analyses and board-ready remediation plans; findings contributed to 3 successful cyber insurance claims
- Implemented a threat intelligence pipeline aggregating feeds from 6 commercial and open-source providers, enriching SIEM alerts with real-time indicator-of-compromise matching and TLP-based sharing
- Automated vulnerability scanning across 3,000+ assets using agentless and agent-based tools, establishing a risk-based patching SLA that reduced critical vulnerability exposure by 73%
- Partnered with DevOps teams to embed security controls into CI/CD pipelines, shifting static analysis and dependency scanning left and reducing production security defects by 60%

Junior SOC Analyst Jul 2017 – May 2019
Vertex Security Group | Denver, CO

- Performed Level 1 and Level 2 triage on 2,500+ weekly security alerts, consistently meeting the 15-minute SLA for critical incidents and maintaining 98% documentation completeness
- Designed and executed weekly phishing simulation campaigns for 500+ employees, improving organizational phishing reporting rates from 12% to 58% over 18 months
- Maintained and tuned 40+ SIEM correlation rules across Windows, Linux, and network device log sources, reducing daily alert volume by 35% without sacrificing detection coverage
- Contributed 200+ standard operating procedures to the SOC knowledge base, cutting new-hire onboarding time from 6 weeks to 3 weeks

Certifications

CCDS
Certified Cyber Defense Specialist
Apex Accreditation Board | 2024

ATAP
Advanced Threat Analysis Professional
Meridian Institute | 2023

SORE
Security Operations & Response Expert
Nimbus Certification Council | 2022

CSAC
Cloud Security Architecture Certified
Vertex Professional Board | 2021

NDFP
Network Defense & Forensics Practitioner
Synapse Credentialing Authority | 2020

IRMC
Incident Response Management Certified
Nexa Standards Body | 2019

Education

M.S. Cybersecurity 2015 – 2017
Apex Institute of Technology | San Jose, CA
Thesis: *Automated Threat Correlation Using Graph Neural Networks on Heterogeneous Log Sources*

B.S. Computer Science 2011 – 2015
Meridian University | Chicago, IL
Concentration in Network Security | Dean's List, 6 Semesters

Technical Projects

ShadowTrack Threat Intelligence Platform 2023 – Present
Open-source threat intelligence aggregation and analysis platform processing 500,000+ indicators daily. Implemented automated IOC extraction, STIX/TAXII integration, and a REST API serving 20+ internal tools. Built with Python, PostgreSQL, and containerized microservices deployed on Kubernetes.

Automated Phishing Response Framework 2021
Python-based framework automating phishing email analysis, URL sandboxing, attachment detonation in isolated

environments, and templated user notification. Reduced analyst time per phishing report from 18 minutes to under 3 minutes across a 12-analyst SOC team.