Chazz Pascual

San Francisco, CA 94112
(415) 612-7794
Chazzpasc@gmail.com
www.chazztin.com

Dedicated and highly skilled Security Operations professional with 10 years of experience monitoring, detecting, analyzing, and responding to cybersecurity threats across enterprise environments. Proven expertise in SIEM management, incident response, threat hunting, and SOC team leadership. Adept at integrating threat intelligence, automating response workflows, and improving overall security posture. Passionate about continuous improvement and mentoring junior analysts.

EXPERIENCE

Harris and Rosales, LLP — *Information Security Analyst /Data Specialist*

March 2023 - June 2024

- Managed and assigned employee access permissions for the Filvvine documentation system, improving security controls.
- Implemented workflow automation techniques, increasing data processing efficiency by 30%.
- Performed data cleaning and organization for client databases, ensuring compliance with legal requirements.
- Generated daily security audit reports on file and case access, enhancing transparency and monitoring.
- Used SQL to analyze trends and forecast data growth, aiding in client presentations and decision-making.
- Assisted in database security enhancements, reducing unauthorized access attempts by 25%.

Horizon Media — *Information Security Officer*

June 2020- March 2023

- Conducted daily audits of security access logs, reducing unauthorized entry incidents by 15%.
- Managed keycard issuance and access control systems, ensuring compliance with company security policies.
- Monitored and analyzed physical security data, producing reports on office entry and exit patterns.
- Performed security assessments and recommended enhancements to strengthen physical and digital security.

Almost Diamonds inc — *Threat Data Analyst*

November 2017 - June 2020

- Provided data analytics and security support, contributing to a 40% increase in secure client transactions.
- Designed and implemented advanced cybersecurity solutions to mitigate threats.
- Conducted vulnerability assessments and penetration testing to identify and remediate security gaps.
- Managed SIEM systems (Splunk, QRadar, LogRhythm) for real-time threat monitoring and response.
- Led incident response efforts, including investigation, containment, and recovery of critical systems.
- Trained employees on cybersecurity best practices, reducing phishing attack success rates by 35%.
- Ensured compliance with PCI DSS, HIPAA, and CCPA regulatory requirements.

SKILLS

- **SIEM Solutions:** Splunk, IBM QRadar, LogRhythm
- **Intrusion Detection & Prevention:** IDS/IPS, Suricata, Snort
- **Threat Intelligence & Vulnerability Management:** Nessus, Qualys, OpenVAS
- **Penetration Testing:** Kali Linux, Metasploit, Burp Suite
- **Digital Forensics:** EnCase, FTK, Autopsy
- **Networking & Security:** Firewalls (Palo Alto, Cisco ASA), VPNs, Zero Trust Architecture
- **Database & Scripting:** SQL, Python, Bash

Key Achievements:

- Reduced **unauthorized access incidents by 25%** through enhanced database security measures.
- Improved **phishing attack awareness** among employees, decreasing successful attacks by **35%**.
- Developed security playbooks that streamlined **incident response** and decreased resolution time.

Current Certifications

- **SEC** +– Certified in Cybersecurity
- CISSP - Certified Information Systems Security Professional
- **CSSLP** – Certified Secure Software Lifecycle Professional
- CCSK- Certificate of Cloud Security Knowledge

PROJECTS

Risk Assessment Framework Implementation – *Harris and Rosales, LLP*

- Developed and implemented a risk assessment framework for securing client and court information.
- Conducted comprehensive risk analysis, identifying and mitigating high risk vulnerabilities.
- Created incident response playbooks to standardize security procedures.
- Created multi-factor for critical zones in organization including new employees and government login.
- Implemented Defense-in-depth zoning public → reception → controlled → secure → critical

Proven methods for cost-effective facility security design -*Horizon Media*

- Implemented a Risk Based prioritization conduct a Security Risk Assessment to rank threats and asset criticality.
- Informed multiple departments of the cost security negligence and how that would effect each department's quarterly budget.
- Document Residual Risk after each mitigation so management can see ROI before approving new spend.

EDUCATION

University Of California, Berkeley — *Bachelor of Science (B.S.) in Computer Science*

September 2004 - May 2008