Carl Gaspar

email@carlgaspar.com | carlgaspar.com | linkedin.com/in/carlignn

OVERVIEW

Cybersecurity professional with 8+ years across GRC, TPRM, vulnerability management, incident response, and security infrastructure. Led enterprise rollouts of MFA, PAM, XDR, and DLP – and builds internal tools that replace manual workflows – from TPRM risk scoring to compliance verification. Complemented by hands-on experience in scripting, automation, and software development.

SKILLS

Security: TPRM | GRC | PCI DSS | HITRUST | Incident Response | Vulnerability Assessment | Threat Modeling | Malware Analysis | SIEM | EDR | DLP | PAM | IAM | Endpoint Security | Network Security | DevSecOps

Technical: Python | Bash | PowerShell | Power BI | PostgreSQL | AWS (IAM, DynamoDB, Lambda, API Gateway) | Docker | Git | CI/CD | Linux | Kotlin | Flutter | ReactJS

EXPERIENCE

IT Security Analyst III, Convey Health Solutions **February 2024 – Present**

- Led TPRM efforts: SIG questionnaire reviews, document/artifact validation, and risk assessments. Reorganized 5 years of vendor data in ZenGRC, cutting turnaround time by 75%.
- Run daily and weekly security operations across a 10-tool stack (CrowdStrike EDR, Varonis DLP, LogRhythm SIEM, Proofpoint, Nessus, Forcepoint, MaaS360, M365 Security, Duo MFA, AD auditing), and serve in the on-call rotation for after-hours monitoring and escalation of high-priority incidents.
- Built a TPRM web app that ingests SIG questionnaires and/or documents via drag-and-drop, auto-scoring and generating PDF risk assessments – replacing the manual Excel workflow.
- Led on-site TPRM audits, HITRUST, and PCI DSS walkthroughs at multiple locations (Manila, Davao, Iloilo) for both internal company sites and BPO partners.
- Developed Power BI dashboards pulling data from security tool APIs and daily reports, providing visibility into SIEM alerts, ticket volumes by priority level, email activity, analyst turnaround time, and operational metrics.
- Administered Delinea Secret Server (PAM) across four integrated AD environments – completed initial rollout and owned upgrades, onsite/offsite backups, DB maintenance, access control, and MFA integration.
- Analyzed threat intelligence from security tools, validating malicious IPs and domains via AbuseIPDB and VirusTotal, and implementing geoblocking and IP blocking rules in Palo Alto firewalls.
- Reviewed DLP egress alerts from Digital Guardian and CrowdStrike DLP, investigating potential data loss incidents, reaching out to users to validate egress activity, and ensuring timely response.
- Partnered with Varonis Engineering to migrate to the cloud platform and identify and remove open access folders.
- Conducted user access reviews across multiple applications in support of HITRUST and PCI DSS compliance, matching system user lists against HR records and Active Directory. Automated the process to replace manual VLOOKUP and AD checking workflows.
- Built a terminal application using the CrowdStrike API to automatically verify endpoint agent installation on new domain-joined machines, significantly reducing manual compliance checks.

Jr. Cybersecurity Officer, FPG Insurance **April 2022 – February 2024**

- Led three enterprise security initiatives from inception to completion – MFA, PAM, and XDR – to meet Cyber insurance requirements. Oversaw vendor evaluation, procurement, onboarding, policy implementation, and ongoing administration. Successfully onboarded 400+ users to MFA a month ahead of schedule.
- Developed and managed the company's Cybersecurity Policy framework, collaborating with legal and IT teams to ensure regulatory compliance and conducting employee seminars on security best practices.
- Led incident response efforts, coordinating with IT, business teams, and senior management to identify, contain, and remediate security incidents.
- Administered risk management platforms (Security Scorecard, Panorays) and conducted monthly Security Awareness Training for employees, developers, and administrators – covering data protection, PAM policies, password management, and secure access practices.
- Utilized the STRIDE framework with Microsoft Threat Modeling Tool to conduct threat modeling on applications and systems, keeping models current against emerging threats.

- Deployed Snyk Static Code Analysis as part of the DevSecOps strategy, and managed Acunetix (web) and Nessus (network) for ongoing vulnerability assessments and remediation, with adherence to OWASP Top 10 standards.
- Analyzed phishing emails and their attachments to identify potential threats and vulnerabilities, providing recommendations for mitigation strategies and educating employees on how to recognize and avoid phishing attacks.
- Established IT asset inventory for visibility and control, and led software evaluation including security and compliance vetting before procurement.
- Managed corporate knowledge base via Confluence and SharePoint, improving IT documentation and cross-team collaboration.

IT Security Analyst, Ivoclar **January 2022 – April 2022**

- Performed compliance tasks based on ISO 27001 standards, including ISMS measurement programs and in-depth security risk assessments to identify the corporate-wide risk status of the organization.
- Conducted vulnerability assessments on networks and endpoints, and executed email phishing campaigns to evaluate employee security awareness.
- Monitored and analyzed security events via Zscaler (SASE), identifying potential threats and recommending improvements.
- Researched and evaluated threat intelligence solutions, selecting and working with Security Scorecard to gain an external view of the organization's security landscape and identify potential vulnerabilities and risks.
- Documented and maintained IT Security processes, policies, and procedures to ensure compliance with industry standards and regulatory requirements and made recommendations for improvements.

IT Security Administrator, Citco Group of Companies **July 2018 – January 2022**

- Administered and monitored the enterprise Data Loss Prevention (DLP) solution serving 6,000+ employees, investigating incidents, managing event escalation protocols, and ensuring timely breach response.
- Collaborated with cross-functional and change management teams to implement data protection policies and deploy DLP patches and upgrades.
- Developed automation scripts using Python, C#, PowerShell, and Bash to streamline security operations.
- Graduated the company’s 6-month training program (Unix, OOP, Java, C#); applied to production work on CASB, PAM, LDAP, Active Directory, and Symantec Messaging Gateway.

EDUCATION

Bachelor of Science in Information Technology, Bulacan State University **June 2014 – June 2018**

CERTIFICATIONS

- **Nessus Fundamentals** (April 2023)
- **CompTIA Security+** (June 2021)
- **Symantec CloudSOC Administration R2** (March 2021)

PROJECTS

- **TPRM Risk Assessment Tool** – Web app that ingests SIG questionnaires via drag-and-drop, auto-scoring and generating PDF risk reports; Python stack.
- **CSE Reviewer –** Android quiz app (3,000+ Civil Service Exam questions) with Flask admin panel; Flutter, Dart, Python, Firebase, Docker, GitHub Actions.
- **Homelab –** Self-hosted infra: Proxmox VE, TrueNAS, OPNSense, Docker, Tailscale, Backblaze B2, and more.
- **Personal Website –** Life, tech, cybersecurity, and development blog; Hugo, TinaCMS, Netlify, Cloudflare, Giscus.
- **Pesofolio** – Android PSE stock tracker; Kotlin, Python, AWS (IAM, DynamoDB, Lambda, API Gateway).