Carl Gaspar

Email carlgaspar@pm.me
Website www.carlgaspar.com

Cybersecurity Officer

Persistent, detail-oriented Cybersecurity and Information Security professional with over 5 years of progressive experience operating within the private domain, dedicated to managing and enhancing security systems including safeguarding data. Highly skilled in facilitating data loss prevention as part of strengthening the overall institutional e-infrastructure. Proficient in contributing to the management of organizational digital frameworks and enhancing overall Cybersecurity measures. Able to thrive in fast-paced and challenging environments where accuracy and efficiency matter.

Core Competencies

• Security Assessment and Planning • Vulnerability Assessment and Management • Risk Assessment and Mitigation • Security Incident Response • Data Privacy • Security Implementation • Endpoint Secuirty • DLP Solution Maintenance & Monitoring • OWASP Top 10 • Cloud Access Security Broker • Amazon Web Services • Basic Linux • Basic Networking • CICD • Object Oriented Programming • Git • Python • Web Development: HTML, CSS, Javascript, ReactJS • Kotlin • SQL • Flutter • Dart • DynamoDB • Docker

Industry Certifications/Training

CompTIA Security+ (June 2021)
Symantec CloudSOC Administration R2 Course Training (March 2021)
Nessus Fundamentals (April 2023)
Microsoft Fundamentals (In-progress)

Professional Experience

FPG Insurance — April 2022 – Present

Jr. Cybersecurity Officer

- Implemented and managed a comprehensive Cybersecurity Policy, developing policies aligned with industry-standard procedures, conducting regular policy reviews, collaborating with the legal team to ensure security regulatory compliance and IT teams to align security measures with the policy, and providing employee seminars on best practices for data and system protection.
- Utilized the **STRIDE** framework with **Microsoft Threat Modeling Tool** to conduct threat modeling on applications and systems, regularly reviewing and updating the threat model to remain effective against new and emerging threats.
- Implemented and administered Snyk **Static Code Analysis** as part of the company's DevSecOps strategy to identify and remediate security vulnerabilities in code.
- Implemented and managed two powerful **Vulnerability Assessment** tools: **Acunetix** for web application vulnerabilities and **Nessus** for network and infrastructure vulnerabilities. And conducted regular scans with both tools to identify and remediate vulnerabilities promptly.
- Led the **incident response** efforts for the company's systems and applications, coordinating with IT and business teams to identify, contain, and remediate incidents in a timely manner.
- 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.

- Administered risk management software, including **Security Scorecard** and **Panorays**, to identify and assess risks to the company's systems and applications, analyzed results as well as provide recommendations for mitigation strategies and risk prioritization.
- Conducted monthly **Security Awareness Training** modules that were concise, easy to understand, and relevant to the current events and company's security needs while simultaneously ensuring employee participation.
- Implemented a robust **Inventory Management System**, streamlining tracking processes and optimizing inventory levels, resulting in reduced stockouts, improved order accuracy, and enhanced overall operational efficiency.
- Implemented and managed corporate wiki for the IT department using **Confluence** and **SharePoint**, improving documentation, collaboration, and document accessibility.
- Researched the appropriate security applications for the needs of the organization and developed a comprehensive plan for rolling out, including the documentations, timeline and communication plan to keep employees informed and trained throughout the process.
- Researched and evaluated tools and software solutions for use by the business and other non-security related tasks.
- Led the **MFA** (**Multi-Factor Authentication**), **PAM** (**Privileged Access Management**) and **XDR** (**eXtended Detection and Response**) solutions from inception to completion in order to meet the requirements for Cyber insurance, overseeing all aspects of **project management**, vendor comparison, purchase order requirements, on-boarding, administration and maintenance.

MFA (Multi-Factor Authentication)

- Successfully on-boarded 400+ users to the **MFA** including procurement of user guide and manuals, proper advisory communications, and managed Service Desk responsibilities ensuring the completion of the on-boarding process ahead of the assigned schedule.
- Coordinated with internal IT ensuring smooth integration of the **MFA** with our suite of tools.
- Conducted regular security assessments and audits of the MFA and integrated systems to identify issues and recommend improvements.
- Managed user provisioning and deprovisioning for MFA accounts, ensuring timely access for authorized users and revoking access for departing employees.

PAM (Privileged Access Management)

- Facilitated the on-boarding of IT administrators and servers onto the **Privileged Access Management (PAM)** platform.
- Implemented **PAM** policies tailored to seamlessly align with our existing infrastructure setup, with a key focus on safeguarding critical production servers to mitigate any potential downtime impact.
- Collaborated with cross-functional teams to define PAM strategies, policies, and procedures, aligning with industry best practices.
- Develop and deliver training sessions to educate employees on PAM policies, password management, and secure access practices.
- Provide regular reports and updates to senior management regarding the status of the PAM program, including risk assessments and improvements.

XDR (eXtended Detection and Response)

- Oversaw the on-boarding process of endpoints including network devices and servers onto the **XDR** (**eXtended Detection and Response**) platform.

- Worked with the vendor with the baselining and behavioral analysis to spot potentially suspicious activity on endpoints.

Ivoclar January 2022 – April 2022

IT Security Analyst

- Performed tasks as per global standards such as **ISO 27001** including continuous measurement of certain metrics for the Measurement Programs for **ISMS**.
- Conducted comprehensive **Vulnerability Assessment** on networks and specific machines to identify potential security threats based on various security information media.
- Executed and managed **Email Phishing Campaigns** to assess the security awareness and readiness of employees, providing valuable insights into potential security vulnerabilities and training needs.
- Monitored and analyzed security events and logs generated by the **Secure Access Service Edge (SASE)** solution, specifically **Zscaler**, to identify potential threats and vulnerabilities.
- Documented and maintained IT Security processes, policies, and procedures to ensure compliance with industry standards and regulatory requirements and made recommendations for improvements.
- Managed and processed workflows for ticket requests coming from different IT teams to prioritize and triage tickets based on severity, ensuring timely resolution of issues.
- Conducted in-depth security risk assessments and compliance checks to identify the corporate wide risk status of the organization.
- Worked with a **Threat Intelligence** platform to gain a black box view of the organization's security landscape and identify potential vulnerabilities and risks.
- Coordinated with vendors on how we can improve our use of their existing solution.
- Oversaw the project management, planning and research of a threat intelligence project.
- Demonstrated hands-on experience and exposure to **Microsoft Azure Cloud**, **Microsoft 365 Security** and **SCCM**.

Citco Group of Companies July 2018 – January 2022

IT Security Administrator

- Responsible for the administration, maintenance, and monitoring of the enterprise **Data Loss Prevention (DLP)** solution, serving a user base of over 6,000 employees.
- Monitored **DLP** policy compliance, investigated incidents, and ensured timely response and resolution of potential data breaches while working with vendors to render assistance.
- Collaborated with cross-functional teams to implement and maintain data protection measures, policies, and procedures in alignment with organizational objectives and industry standards.
- Collaborated with change management teams to ensure seamless deployment of patches, upgrades, and changes to the enterprise **Data Loss Prevention (DLP)** solution.
- Gained in-depth knowledge of incident response processes and procedures, including event escalation protocols
- Hands-on experience with scripting and automation using **Python**, **C#**, **PowerShell**, and **Bash**.
- Completed a comprehensive 6-month training program in industry-standard tools and programming languages including **Unix**, **Object Oriented Programming**, **Java**, and **C#**.
- Demonstrated hands-on experience and exposure to Symantec Messaging Gateway for email security, Cloud Access Security Broker (**CASB**) for cloud application security, **PAM** (Privileged Access Management), **LDAP** (Lightweight Directory Access Protocol), and **Active Directory**.

Education

Bulacan State University – Malolos, Bulacan, PH June 2014 – June 2018

Bachelor of Science in Information Technology

- GWA – 1.68*/5.0*

Projects

Personal Website – My personal website dedicated to documenting my personal experiences in fields of Cybersecurity, Software Development and beyond. **Minimal** version.
Technologies used: Hugo Framework (HTML and CSS), Google Analytics, Forestry/TinaCMS

CSE Reviewer – Android application created to help aspiring Civil Service Exam takers to pass the examination.
Technologies used: Flutter, Dart, Python, AWS (IAM, DynamoDB, Lambda, CloudWatch, API Gateway)

Pesofolio – Android application created to simplify tracking of stocks in the Philippine Stock Market.
Technologies used: Kotlin, Python, AWS (IAM, DynamoDB, Lambda, CloudWatch, API Gateway)

It’s More Find in the Philippines – Android game developed by my team and I as our final thesis at the University. I led the team of 5 people as the Project Manager and the Programmer.
Technologies used: C#, Unity3D, Photoshop