JAYSON **FONG**

contact@jaysonfong.org | jaysonfong.org | github.com/Jayson-Fong | linkedin.com/in/jaysonfong

Seeking positions in enterprise infrastructure and full-stack development with interests in security and automation.

Work Experience

Georgia Institute of Technology, Information Security Operations Analyst – Atlanta, GA Aug 2022 – Present

- Developed SIEM rules and watches for an Elastic stack to detect anomalies in network and user activity.
- Crafted behavioral and correlation-based alerting rules for Cortex XDR backed by heuristics from threat intelligence and historical incidents combined with automations to proactively defend IT assets.
- Analyzed endpoint and network activity through EDR and packet capture tools to identify and contain security incidents while advising system administrators.
- Designed dashboards for Kibana, Splunk, ServiceNow, and Cortex XSOAR/XDR to enhance workflow efficiency through visualizations, dynamic content, and pre-configured filters.
- Authored comprehensive documentation to facilitate staff training, focusing on threat hunting methodologies, SIEM utilization, and proficient analysis of endpoint data.
- Responded to and researched incoming reports from customers pertaining to endpoint security software, phishing, abuse reports, and vulnerability disclosures.
- Built CLI and web-based tools in Python, TypeScript, and POSIX Shell to automate incident response.

Anomaly Detection with Elasticsearch Watchers Project

Created an alert suppression system using Elasticsearch Watchers, Painless, and chained inputs to allow custom aggregations with Query DSL to prevent alert fatigue and improve true positive rates while detecting anomalous network and user logon activity.

Automated Endpoint Detection Alert Analysis and Formatting Project

Developed a RESTful API, command-line tool, and web interface using Python, Flask, and Next.js, enabling analysts to quickly extract Cortex XDR incident details from Cortex XSOAR while automatically determining a verdict for common alerts and formatting details uniformly in preparation for submission to ServiceNow.

Mick Capital Pty. Ltd. - BuiltByBit, Systems Administrator & Software Engineer – Remote Oct 2018 – Present

- Oversaw the development and implementation of hybrid infrastructure, orchestrating technology stacks integrating AWS and on-premises systems for a marketplace and software placeholder injection system.
- Administered DNS records in Cloudflare and configured web security settings integrated with a web server for page-specific rate limiting matches and WAF rules with automated mitigations based on server loads.
- Managed an on-premises BELK stack for website search and system log analysis.
- Developed add-ons and migration scripts in PHP and SQL for the XenForo platform to automate workflows.

Advertisement Manager Project

Crafted an add-on for the XenForo platform in PHP to automate website advertisement slot auctions with proxy bidding and performance tracking, providing customers with demand-based pricing.

XenForo 2 Upgrade Project

Constructed Bash and PHP scripts to migrate data from an existing XenForo deployment to a pre-configured, upgraded target, transforming data in a MariaDB database and syncing data between servers with rsync.

Georgia Tech Research Institute – Quantum Systems, Research Intern – Atlanta, GA Jun 2022 – Jul 2022

- Investigated quantum error correction codes and created visualizations using Python.

Interbix Holdings LLC, Chief Operating Officer – Remote Apr 2017 – May 2021

- Directed the procurement and colocation of hardware for hypervisors and web servers.
- Implemented the SolusVM virtualization platform for managing OpenVZ and KVM virtual machine clusters.
- Investigated and responded to incoming network abuse reports.
- Worked with customers to identify and deploy technical solutions with a focus on game and web servers.
- Managed Google Workspace as an IdP and integrated applications using SAML.
- Maintained a cPanel shared hosting web server with CloudLinux.

Certifications

Systems Security Certified Practitioner (SSCP) – ISC2 Jan 2024 – Jan 2027
CompTIA Cybersecurity Analyst+ (CySA+) ce – CompTIA Dec 2023 – Dec 2029
CompTIA Security+ ce – CompTIA Dec 2023 – Dec 2029
Apollo Graph Developer Associate – Apollo Graph Nov 2023 – Present
Microsoft Certified: Security Operations Analyst Associate – Microsoft Nov 2023 – Nov 2024
Oracle Certified Professional: Java SE 11 Developer – Oracle Jul 2021 – Present
CompTIA Data+ ce – CompTIA Jul 2021 – Jul 2024

Other Credentials

Associate of ISC2 – ISC2 Dec 2023 – Dec 2024
Configuring SIEM security operations using Microsoft Sentinel – Microsoft Nov 2023 – Present

Education

Georgia Institute of Technology – Atlanta, GA Jun 2022 – May 2024
Candidate for Bachelor of Science in Computer Science, GPA: 3.48/4.00

- Concentration in Information Internetworks and Intelligence

Technical Lead, Capstone Design Project for Unyson System Aug 2023 – Present

- Implemented GitHub Actions to automate application deployment workflows.
- Created an API using Apollo GraphQL with Type-GraphQL, Prisma ORM, and CockroachDB deployed using the Serverless Framework onto AWS Lambda.
- Directed the development of a single-page-application using Next.js, React.js, TailwindCSS, and Apollo Client for client interactions hosted on Cloudflare Pages.

Team Technical Lead, 2023 DOE CyberForce Competition Sept 2023 – Nov 2023

- Deployed Elastic Agent with Fleet on Windows and Linux-based virtual machines for EDR supplemented with Beats for application-specific logging.
- Oversaw vulnerability management using Nessus and performed analysis of software configurations to identify alongside patch undetected vulnerabilities.
- Led endpoint analysis efforts using Elastic Security, Defend and OSQuery to identify and isolate attacks.
- Remediated web-based vulnerabilities in an existing JavaScript codebase through static code analysis and automated web application scanning.

University of California San Diego Extended Studies – Remote Sept 2021 – Jun 2022
Certificate in Futures: iOS Programming, GPA: 4.00/4.00

Gwinnett Technical College – Lawrenceville, GA May 2019 – Dec 2021
Associate of Applied Science in Computer Programming, GPA: 4.00/4.00

- National Technical Honor Society
- Phi Theta Kappa

Skills

Programming:	Java, SQL, Python, C++, PHP, TypeScript, CSS, HTML, POSIX/Bash Shell, Painless
Querying:	Elastic (KQL, EQL, Query DSL, Lucene, SQL); Splunk (SPL); Cortex (XQL, DT)
Technologies:	Docker, Git, MariaDB, NGINX, Redis, Oracle Database, Elastic, Cortex, GraphQL
Infrastructure:	Cloudflare, Amazon Web Services, Elastic Cloud, CockroachDB Cloud
Coursework:	Enterprise Cybersecurity Management, Computer Networking, Database Systems, Project Management, Information Security Strategies and Policy, Internet and Public Policy

Volunteer Experience

Discovery High School – Lawrenceville, GA Aug 2021 – May 2022

- Leveraged Google Apps Script integrating Google Sheets and Forms to automate volunteer management.
- Acted as a class aid for an AP Computer Science A course with a remote instructor, assisting students with course concepts and creating resources to improve learning outcomes.