

Samuel Giacinto

Cybersecurity Infrastructure Engineer

linkedin.com/in/sgiacinto
samuel@giacinto.info
571-309-2971
Arlington, VA, 22209-1427

Experience

Viasat (Signal Processing Infrastructure)

Sr. Cluster Networking Engineer, 2022-02 › 2023-04 (50hr/wk., Remote)

- › Owned complete lifecycle of Python/Django REST API exposing cluster metrics to Grafana dashboards for cluster maintenance and triage with internal OpenAPI documentation. (DOCKER, GRAFANA, KUBERNETES, MYSQL, OPENAPI, PYTHON, REST)
- › Developed Python cluster alerting plugin, adding host metrics (Memory, CPU, and GPU NUMA assignments) exposed by above API as triggers for team-appropriate Slack alert messages sent via internal load-balancing queue. (KUBERNETES, NUMACTL, NVIDIA SMI, PYTHON, REST, SLACK API)
- › Optimized existing cluster data collection DaemonSet, cutting non-compliant event ingestion to Slack message time 5:00 to 0:01 (avg) via push-based notifications, reducing team incident support time 26% overall (0:27 to 0:20). (DASHBOARD VERSIONING, GRAFANA, KUBERNETES, MYSQL, PYTHON, REST)

Deloitte (Federal Cyber-Risk Advisory)

Cyber-Risk Consultant, 2021-09 › 2022-02 (45hr/wk., Remote)

Cyber-Risk Analyst, 2019-08 › 2021-09 (40hr/wk., Rosslyn, VA)

- › Developer for 3 client change requests, modifying code and database structures to facilitate multi-party approval for financial permission requests for a mid-size civilian Federal client's >10,000 user Oracle Identity & Access Management (IAM) solution. (ECLIPSE IDE, JDK [7/8], REST APIS, ORACLE SERVLETS, ORACLE SQL DEVELOPER)
- › Developed suitability requirements examining AWS RDS and EC2 solutions against project requirements with supporting documentation for an Oracle financial application replatform for a mid-sized Federal Client. (AWS, RDS, EC2, ORACLE, JAVA APPLETS)
- › Implemented environment agnostic authentication automation, executing email-based two-factor quality assurance sub-tests 2x faster than manual entry (0:06 vs. 0:12). (AUTOHOTKEY, KEEPASS, OUTLOOK COM, PYTHON, RPA, SELENIUM)
- › Solicited 16 key personnel candidates, evaluating them against best-fit requirements for a 10 year, \$110M proposal, garnering an internal 'Applause Award' and ultimately staffing the winning proposal for Deloitte (2022).

Cisco (Advanced Services)

Security Solutions Engineer II, 2018-05 › 2018-08 (50hr/wk., Cary, NC)

Security Solutions Engineer I, 2017-05 › 2017-08 (50hr/wk., Cary, NC)

- › Evaluated solution suitability against client requirements integrating Cisco technologies, executing line-item Windows endpoint validation testing on-site in client labs for a \$45M VPN service contract, garnering 2 internal 'Connected Recognition' awards. (CISCO ANYCONNECT, IDENTITY SERVICES ENGINE (ISE), FIREPOWER)
- › Automated verification for text-based Cisco switch configurations, verifying best practices ~5x faster than best-case manual verification (0:28 vs. 2:20) without human error, saving ~2 labor minutes per configuration. (CISCO IOS, PYTHON, RPA, REGEX)

U.S. Securities & Exchange Commission (Enforcement)

Litigation IT Specialist, 2016-05 › 2016-08 (40hr/wk., Washington D.C.)

- › Automated litigation record integrity checks comparing host databases to S.E.C. Evidence Tracking Intranet, eliminating a >9,800 case verification backlog 15x faster than manual processing (0:06 vs. 1:28), saving 223 labor hours. (MICROSOFT ACCESS, AUTOHOTKEY, HTML DOM, RPA, WINDOWS COM)

Education

Virginia Tech (B.S. Computer Engineering)

Honors College Pamplin Scholar, Math Minor, Cum Laude, 2015-07 › 2019-05

- › **Lockheed Martin** (Non-Blocking Multicast Switching Network), 2018-08 › 2019-05 (10hr/wk.) – Architected FPGA implementation of patented non-blocking multicast switching concept, with parallel input vector generation software comparing theoretical and experimental I/O latency. (C++, FPGA, MATLAB, INTEL CYCLONE V, NAND LOGIC, VERILOG)
- › **Hume Cybersecurity Center** (Lateral Malware Research), 2017-02 › 2018-03 (10hr/wk.) – Correlated port, protocol, and time stamps of alerts, ingesting 465GB of Virginia Tech appliance logs using Python data analysis tools to compose multi-variable triggers for proactive Virginia Tech SOC alerting algorithms. (ORACLE ARGUS, FIREEYE, MYSQL, NETFLOW, PYTHON, SNORT)