



# CHRISTINA PARRY

STAFF SECURITY ENGINEER

732-397-6620 

christinaparry3@gmail.com 

## SKILLS

- Automation / Python, Docker, Airflow
- CI/CD / Prefect, CircleCI, Github, Github Actions
- IaC / Terraform, Spacelift
- Cloud / AWS, Azure, GCP
- Data / ELK Stack, AWS (S3/DynamoDB), Splunk, NiFi, Kafka, Grafana
- Detections / OSINT, Sigma Rules, Zeek
- Front-End / HTML, CSS, JavaScript, jQuery
- Reporting / Datadog, Sigma, Snowflake

## EDUCATION

### B.S. IN APPLIED SCIENCES AND ENGINEERING

Rutgers University,  
School of Engineering /  
Piscataway-New  
Brunswick, NJ

- Electrical and Computer Engineering Concentration
- Minors in Computer Science and Economics

## CERTS

- HBS Leadership Coaching Strategies
- AWS Cloud Practitioner
- SANS GSEC Security Essentials

## SERVICE

- BSides NYC Speaker
- BSides LV PvJ CTF Blue Team Captain
- mWISE Speaker
- AWS Community Builder
- WiCyS Mentoring Program Mentor
- New York Road Runners Volunteer

## EXPERIENCE

### HUNTRESS

Staff ThreatOps Developer, R&D Team / Remote (Greater NYC)

August 2022 – Present

#### LEADERSHIP

- Serve as a technical lead for several ThreatOps core systems, tooling, and apps used by global SOC team.
- Drive and implement quarterly Security roadmap initiatives, mentor junior developers and analysts.
- Engage with Product and Security teams to integrate internal tools into product for ease of use to the SOC.
- Speak at conferences for Huntress and related work, help with interviewing candidates for Security roles.

#### SOFTWARE DEVELOPMENT

- Fluent in Python, energized by data analysis at scale, automation, and open-source tech.
- Equip SOC and Threat Hunt teams with advanced analysis and investigation tools (Flask, Python, Docker), utilizing Windows, macOS, and ITDR telemetry, malware analysis, and intelligence feeds.
- Develop and maintain infrastructure as code (AWS, Terraform) and CI/CD pipelines (Github Actions).

#### DETECTION ENGINEERING & THREAT INTEL

- Architect and implement open-source Threat Intelligence platform, partnering with SOC, DE, and Threat Intel stakeholders to onboard, ingest multiple feeds, and scale as efficiently as possible.
- Deliver numerous Proof-of-Concepts to Security teams in the form of 2-week sprints, shipping end-to-end solutions to Security Researchers related to EDR, ITDR/M365, SIEM, and SAT.
- Spearhead coverage analysis efforts and tech solution for 500+ detections via MITRE's ATT&CK Framework by heatmapping fired signals to associated TTPs, used by leadership for threat reporting.

### TWITTER

Security Engineer, Detection & Response Team / New York, NY

November 2021 – July 2022

- Led automation efforts for IP/host enrichment workflows with Python and SOAR platform.
- Developed and productionized detections in Splunk, while providing training on building detections.
- Facilitated creation of data source catalog to identify coverage and gaps on Twitter's network.
- Improved Carbon Black Cloud policies to tighten network controls for 10,000+ endpoints.
- Assisted in daily investigation and alert triage, also engaging in on-call rotation for escalations as needed.

### MORGAN STANLEY

Security and Data Engineer / New York, NY

October 2019 – October 2021

- Expanded data and enrichment capabilities for our Cyber Detection Platform, an in-house analytic system leveraged by engineers and analysts for threat hunting, insider threat, anomaly detection and host-based coverage analysis (Python, ELK, Apache NiFi, open-source software).
- Owned and maintained 40+ data pipelines (>10TB/day) used by global Fraud and Cyber Analytics team.
- Comfortable automating data extraction with Python and ingesting data feeds & security logs.
- Developed Splunk dashboards, alerts, reports, and analytics to monitor data quality and usage.
- Created a POC for ML classification algorithm for anomaly detection for hardware assets.

Technical Project Manager / New York, NY

November 2017 – October 2019

- Consistently drove business deliverables and technical requirements for investment products portfolio.
- Led Grassroots Agile transition by introducing projects with Scrum and Kanban boards.
- Partnered with platform owner and key stakeholders to envision annual product roadmap for Insurance

Technology Analyst / New York, NY

August 2017 – November 2017

- Participated in 15-week technical training program, solidifying coding fundamentals and SDLC practices.
- Created Sorting Hat, an interactive data visualization dashboard leveraging multiple NLP clustering algorithms, compiled requirements in JIRA, helped develop front-end interface.

Technology Summer Analyst / New York, NY

June 2016 – August 2016

- Tracked approvals for five ongoing projects, analyzed budgets, and supported development team with regression testing efforts, while on the Investment Products & Services IT team.
- Developed and categorized 500+ business requirements for Mutual Fund Order Entry system.

### AT&T

Technology Developer Intern / Middletown, NJ

June 2015 – August 2015

- Developed a web-based mobile application, implemented back-end framework and frontend edits.
- Worked in Chief Security Office's Mobility Lab, set-up servers and booting software in OpenStack Lab, simulated DNS reflection attacks using Python.