

# CYRISTAL N. JOSEPH

**Cybersecurity Analyst | Security Operations | Threat Detection | Incident Response**

New York, NY | cyrisjoseph@outlook.com | linkedin | github | portfolio

---

Cybersecurity and Risk Management professional with experience supporting security operations, incident response, and threat detection across enterprise environments. Skilled in monitoring security events, identifying vulnerabilities, and translating intelligence into actionable mitigation strategies aligned with governance and compliance practices. Demonstrates strong investigative mindset, technical curiosity, and commitment to strengthening organizational resilience through proactive defense capabilities.

**Target Roles:** Cybersecurity Analyst | Security Operations Center Analyst | Threat Intelligence Analyst | GRC Analyst

---

## STRATEGIC FOCUS

Security Operations | Threat Detection | Incident Response | Governance Risk & Compliance (GRC) | Cloud Security Fundamentals | Identity & Access Management | Vulnerability Identification | Security Monitoring | Log Analysis | Risk Mitigation | Business Continuity | Technical Documentation

---

## CERTIFICATIONS

CompTIA Security+ | AWS Certified Cloud Practitioner | CompTIA A+ | Google AI Essentials Certificate | Google Business Intelligence Certificate | Google Cybersecurity Certificate | Google IT Support Certificate | Google Project Management Certificate | Lean Six Sigma Green Belt

---

## TECHNICAL TRAINING

*Cloud Computing*

**NPower**

**New York, NY**

- Built foundational AWS knowledge using EC2 and S3 cloud resources
- Applied business continuity principles including backup and recovery concepts
- Supported provisioning and configuration of cloud infrastructure environments

*Cybersecurity*

**NPower**

**New York, NY**

- Configured firewall, VPN, and intrusion detection lab environments
  - Built security testing labs using Kali Linux, Metasploitable, and Oracle VM VirtualBox
  - Practiced vulnerability identification and defensive security techniques
- 

## PROJECTS

*(All projects available to view on GitHub; featured work highlighted in portfolio)*

**Cybersecurity Vulnerability Lab**

Tools: Kali Linux | Nmap + Nikto | Oracle VM VirtualBox | Bash terminal | IDS concepts

- Built virtualized cybersecurity lab environments to practice vulnerability identification and defensive security techniques
- Configured and tested intrusion detection concepts within controlled environments
- Performed vulnerability exploration exercises using intentionally vulnerable systems

- Strengthened understanding of attacker methodologies and defensive monitoring concepts

### **AWS Honeypot-Canary Environment Simulation**

Tools: AWS S3 | IAM (Identity & Access Management) | Amazon GuardDuty | Amazon Cloudwatch | Amazon EventBridge + SNS

- Designed and configured a cloud-based honeypot environment in AWS using EC2 and S3 to simulate attacker interaction and monitor malicious activity
- Implemented detection concepts aligned with the shared responsibility model to understand cloud security boundaries and risk exposure
- Analyzed simulated threat activity within the environment to strengthen understanding of cloud-based attack vectors
- Applied business continuity and recovery strategies to ensure resilience within cloud infrastructure

## **PROFESSIONAL EXPERIENCE**

*Security Operations Center Analyst*

**NBCUniversal**

*03/2026 to present*

**New York, NY**

- Analyzed real-time security events across 220+ integrated surveillance and alarm systems to detect, assess, and escalate potential threats in alignment with incident response protocols
- Generated and maintained audit-ready incident reports and activity logs, documenting 16+ daily security events to support compliance, risk management, and investigative efforts
- Orchestrated cross-functional incident response communications, ensuring rapid escalation and coordination of high-priority security events to minimize operational impact
- Identified patterns across recurring security incidents, contributing to improved threat detection capabilities and strengthening proactive risk mitigation strategies

*Global Security Command Center Analyst*

**BlackRock**

*02/2023 to 03/2026*

**New York, NY**

- Improved threat detection accuracy by 30% through use of open intelligence sources, geolocation tools, and global monitoring platforms to identify credible threats impacting enterprise operations
- Achieved 83% resolution efficiency within a 5-minute response window for high-priority incidents, supporting rapid containment and minimizing operational disruption
- Reduced travel-related risk exposure by 11% through analysis of global threat patterns and proactive mitigation adjustments aligned to organizational risk tolerance
- Monitored real-time security alerts, assessed incident severity, and escalated emerging threats according to established incident response procedures
- Translated threat intelligence findings into actionable insights supporting organizational resilience and continuous risk mitigation efforts

*Automation Systems Administrator*

**Capsule**

*11/2022 to 02/2023*

**New York, NY**

- Identified and remediated system vulnerabilities contributing to a 21% improvement in pharmaceutical fulfillment delivery performance

- Increased operational resilience by 13% through preventative maintenance planning across automated robotics and sensor-based fulfillment systems
- Documented technical issues, root causes, and remediation steps to improve system reliability and support continuous operational efficiency
- Applied risk-aware troubleshooting techniques to maintain stability of automated infrastructure and reduce disruption risk

*Fixed Building Security*

*01/2022 to 10/2022*

**Madison Square Garden Entertainment Corp**

**New York, NY**

- Reduced security risk exposure by 10% through proactive monitoring, screening, and triage of high-volume event activity involving 4,000+ attendees
- Identified and escalated vulnerabilities impacting facility security operations, contributing to improved protective security posture
- Supported safe execution of high-profile events by maintaining situational awareness and enforcing security protocols

*Security Officer*

*12/2018 to 01/2022*

**CBS**

**New York, NY**

- Strengthened incident response coverage through continuous CCTV monitoring and real-time escalation of suspicious activity
- Reduced unauthorized access incidents by 8% through enhanced identity verification and controlled entry procedures
- Supported enforcement of access control protocols protecting personnel, facilities, and organizational assets

---

## **EDUCATION**

*Bachelor of Arts (B.A.), International Political Economy & Diplomacy and Religion & Politics*  
**University of Bridgeport** **Bridgeport, CT**