

BRIGHT OPOKU BOATENG

CYBERSECURITY ANALYST | SOC & SECURITY OPERATIONS

Chicago, IL | +1 (872) 288-3134 | bryte50@gmail.com | [LinkedIn](#) | Portfolio: [bright-security.net](#)

PROFESSIONAL SUMMARY

Cybersecurity professional with hands-on experience in alert triage, security event investigation, threat detection, vulnerability management, phishing analysis, malware analysis, and incident response. Skilled in Microsoft Sentinel, Splunk, KQL, Tenable, Nessus, Active Directory, CVE/CVSS analysis, and MITRE ATT&CK. CompTIA Security+ certified with a Master of Cyber Forensics and Security.

TECHNICAL SKILLS

SOC Operations: Alert Triage, Alert Investigation, Security Monitoring, Incident Response, Threat Hunting, Phishing Analysis, Malware Analysis

SIEM & Detection: Microsoft Sentinel, Splunk, KQL, MITRE ATT&CK, Log Analysis, Threat Analysis

Vulnerability & Identity: Tenable, Nessus, CVE Analysis, CVSS Scoring, Active Directory, IAM, MFA, Zero Trust

Endpoint & Network: Microsoft Defender, EDR, TCP/IP, DNS, DHCP, IDS/IPS, Firewalls, Kali Linux

Frameworks & Scripting: NIST 800-61, NIST 800-171, NIST 800-53, RMF, ISO 27001, Python, PowerShell, Bash, SQL

PROFESSIONAL EXPERIENCE

Cybersecurity Intern | MyHeat | Remote | Oct 2025 - Dec 2025

- Improved incident prioritization by triaging security alerts, analyzing Microsoft Sentinel telemetry with KQL, and escalating suspicious activity for further investigation.
- Strengthened phishing and malware detection by analyzing suspicious emails, URLs, attachments, and related indicators to distinguish malicious activity from benign events.
- Prioritized remediation of security weaknesses by reviewing Tenable and Nessus findings, validating associated CVEs, and applying CVSS severity scores to assess risk.
- Strengthened identity-security investigations by reviewing Active Directory activity and access-related events for suspicious authentication behavior.

Security Support | College Board | Chicago, IL | Mar 2025 - Jun 2025

- Strengthened detection of anomalous activity by analyzing security events and system logs using Splunk and Microsoft Sentinel.
- Improved security-event investigation by using KQL to review SIEM data and identify suspicious activity requiring further analysis.
- Strengthened authentication and access security by applying IAM and Zero Trust principles to secure testing environments.

Operations Support Analyst | Vodafone | Jun 2021 - Jul 2024

- Improved detection of suspicious transactions by monitoring transaction systems and analyzing anomalous activity and security events.
- Reduced financial risk exposure by investigating transaction logs to identify suspicious patterns and support timely escalation.
- Reduced recurring service disruptions by investigating complex system incidents, identifying root causes, and supporting corrective actions.

CYBERSECURITY PROJECTS

SOC Detection and Monitoring Lab

- Improved SOC investigation skills by analyzing Windows security events, identifying failed authentication attempts and suspicious activity, reviewing security logs, and documenting findings through a structured investigation workflow.

Microsoft Azure Security & Identity Lab

- Strengthened Microsoft cloud security skills by working with Entra ID, Defender, Sentinel, Intune, Purview, Priva, and Copilot for Security to explore identity protection, threat monitoring, endpoint management, data security, privacy, and AI-assisted security operations.

Enterprise Vulnerability Assessment - Windows Server | Illinois Institute of Technology

- Exposed actionable security weaknesses through a black-box Kali Linux assessment that identified exposed services, misconfigurations, and privilege-escalation risks and informed risk-based remediation.

AWS Cloud Security Lab

- Strengthened cloud security knowledge by working with IAM, EC2, S3, CloudTrail, EBS, EFS, and Glacier to practice access management, storage security, and cloud activity monitoring.

EDUCATION & CERTIFICATIONS

Master of Cyber Forensics and Security - Illinois Institute of Technology, Chicago, IL | May 2026

B.Sc. Telecommunication Engineering - Kwame Nkrumah University of Science and Technology, Ghana | June 2019

CompTIA Security+ ce | Microsoft Security Essentials Professional Certificate | CompTIA CySA+ - In Progress