CHARLES OKEKE

5009 Roese Avenue South bloomfield, Ohio 43103 614206-2304 okekeemeka20@gmail.com
website: https://charlesokeke.github.io/

Skilled SOC analyst with expertise in incident response investigation, risk management, threat mitigation and vulnerability management. Well-versed in direct and remote security event investigation with strong critical thinking, communication and people skills. Able to thrive in fast-paced and challenging environments where accuracy and efficiency matter.

WORK EXPERIENCE

SOC Analyst

01/2020 to Present

Nationwide Mutual Insurance

One Nationwide Plaza Columbus, Ohio 43215-2220

Currently responsible for investigating and analyzing security incidents/events generated by security tools (Crowdstrike,Palo Alto, Akamai, Splunk, Iboss, AWS Guarduty, Azure NSG, F5) and third-party intelligence(F-ISAC). Initiated, responded, and conducted investigations on suspicious and anomalous events related to services, applications, endpoints, servers, containers, databases and cloud assets. Investigated, collected, and analyzed IOC associated with phishing campaigns,web application attacks, malicious executables associated with APT groups,triaged tickets and implemented mitigative actions namely containment/isolation of servers and endpoints, token revocation, password resets, and hash/domain/IP blocking as a consequence of established true positive incidents. Furthermore, wrote scripts for automating repetitive investigative task and created work-flow documents for security investigations. Engaged in analysis and investigation of incidents/events involving data exfiltration, C2 beaconing and layer 7, 4 and 3 based attacks. Implemented and lead detection of undetected post-exploitation activities through structured and unstructured threat hunting activities leveraging MITREs established TTPs framework (tactics, threats and procedures). Furthermore, conducted investigations involving observed suspicious container runtime, images, pods and name-spaces running on AWS and Azure cloud environments and worked with SOAR team to implement, tuning and review of detection logics to improve overall fidelity and reduce the level of false positives.

Security Analyst

03/2019 to 01/2021

STATE OF OHIO DAS

30 E. Broad St., Columbus, Ohio 43215

Responsible for the management and configuration of SIEM(Qradar) and web Proxy (BlueCoat) tools. Participated in the development of technical and IT risk profile assessment plans for several state applications using the ServiceNow application platform. Documentation of backup architecture of IDS/IPS applications. Identified, Investigated and mitigated malware attacks through log analysis, malware and traffic and sandbox analysis. Developed and wrote reports on compromised accounts and conducted weekly application and systems scans for remediation, documentation and identification purposes. Leveraged advanced Office 365 platform protection for email, endpoint, and identity protection

Governance Risk and Compliance

CIS Security

- Performed security reviews, to identify gaps in the security posture of State of Ohio agencies and develop controls assist in the remediation identified security gaps
- Assisted in development of technical and IT risk profile assessment plans for agencies using CIS RAM Methodology and 20 CIS Security Controls.
- Conducted risk analysis (e.g., threat, vulnerability, and probability of occurrence) on new systems and applications for initial installations and major updates.

Enterprise Vulnerability Management

- Assisted in conducting assessments of threats and vulnerabilities, determining deviations from acceptable configurations, enterprise or local policy; assessing the level of risk and determining appropriate mitigation countermeasures in operational and nonoperational situations
- Assisted in measuring the effectiveness of defense-in-depth architecture against known vulnerabilities.

Security Engineering

- Tuned and configured log sources for SIEM(Qradar) and assisted in integration of log sources and managed user roles and permissions in SIEM application. Participated

Security Incident Response Team

- Assisted in investigation of security events related to IT systems, networks and servers
- Identified, analyzed, and mitigatigated threats to internal IT systems, and/or Networks using Windows Advanced Endpoint protection (WDATP), packet sniffing tools and EDRs
- Tested, maintained, and reviewed infrastructure hardware and software required to effectively manage computer network defense and resources. Leveraged O365 Advanced Threat Protection platform to provide endpoint, identity and email protection. Assisted in the response to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats.
- Identified and assessed potential web-based attacks to facilitate incidence triage response process.

SKILLS

- Cloud(Azure & AWS)
- Unix & Bash scripting
- Python Scripting
- JavaScript

EDUCATION

Franklin University

Bachelor’s
Cyber Security/ Information Security
201 S Grant Ave, Columbus, OH 43215
05/2015 to 05/2019

CERTIFICATIONS

- CEH
- Security+
- CYSA+