Calvin L. House, Jr.

Email: clhouse310@gmail.com | LinkedIn

SUMMARY

Highly accomplished and results-oriented Cloud Security Analyst with 7+ years of progressive experience in cybersecurity, specializing in security operations and incident response. Proven ability to design, implement, and optimize cloud security postures for complex environments, including AWS. Adept at developing detection logic, mentoring junior analysts, and providing actionable recommendations to enhance organizational security.

SKILLS & EXPERTISE

- **Cloud Security:** AWS Security, Cloud Detection & Response, Cloud Incident Response, Cloud Forensics, Cloud Security Posture Management (CSPM), Serverless Security, Container Security (Docker)
- **Security Operations:** SIEM (Elastic Stack, Splunk, ArcSight, QRadar), Threat Detection Engineering, Alert Triage, Threat Hunting, Vulnerability Management (ACAS, IAVM, STIGs), Security Baselines
- **Incident Response:** Digital Forensics, Incident Handling, Containment, Eradication, Recovery, Post-Incident Analysis, Reporting
- **Frameworks & Methodologies:** MITRE ATT&CK, NIST Risk Management Framework (RMF), NIST SP 800-53
- **Technologies:** AWS, Linux, Networking, Virtualization, Docker, Bash, PowerShell, ServiceNow, RSA Archer

CERTIFICATIONS & COURSEWORK

- ISC2 Certified Information Systems Security Professional (CISSP)
- AWS Certified Cloud Practitioner
- SANS FOR509 - Enterprise Cloud Forensics and Incident Response

EDUCATION

Hagerstown Community College

- A.A.S., Cybersecurity, December 2017
- A.A.S., Network Administration, May 2017

PROFESSIONAL EXPERIENCE

Senior Cloud Detection & Response Analyst | March 2024 – Present | Rapid7, LLC, Arlington, VA

- Provide expert cloud security insights to platform, UX, engineering, and product teams, directly enhancing the Rapid7 Insight platform's cloud detection and response capabilities.
- Collaborate with customers to identify and remediate critical cloud security and visibility gaps, delivering tailored, actionable recommendations to fortify their cloud security posture.
- Develop comprehensive training modules and documentation to improve cloud alert triage and cloud incident response procedures.
- Partner with the Threat Intelligence and Detection Engineering (TIDE) team to design, develop, and meticulously test novel alert logic, specifically targeting emergent threats in cloud environments (e.g., AWS, Azure, GCP) often missed by native security services like AWS GuardDuty or Microsoft Defender for Cloud.
- Mentor and cross-train junior analysts and leadership, significantly elevating the team's overall cloud security knowledge and expertise.
- Perform alert triage for cloud-based security alerts such as AWS GuardDuty and Microsoft Defender for Cloud using complex log sets to identify attacker activity and incident scope.
- Lead cloud based incident response engagements helping customers contain the incident, assess scope, and provide detailed after actions reports with concise mitigation and remediation steps.

Managed Detection and Response (MDR) Analyst | March 2021 – March 2024 | Rapid7, LLC, Arlington, VA

- Triage and analyze a high volume of diverse security alerts, including endpoint, network, and malware incidents, utilizing the InsightIDR platform.
- Led critical incident response engagements, guiding customers through detection, containment, eradication, and recovery phases of complex security incidents.
- Authored detailed incident reports outlining scope, impact, and comprehensive mitigation and remediation strategies for customers post-incident.
- Contributed to alert tuning and the creation of new detection rules in collaboration with the Threat Intelligence and Detection Engineering (TIDE) team.
- Conducted proactive threat hunts for onboarding and existing customers, identifying advanced persistent threats and malicious activities not detected by existing logic.

Cyber Threat Analyst | January 2020 – March 2021 | Raytheon Technologies, Dulles, VA

- Served as overnight shift lead, managing scheduling, customer assignments, mentorship, and acting as a primary escalation point for shift analysts.
- Developed video training content and documentation to onboard and enhance the skills of junior analysts.
- Efficiently triaged and prioritized security alerts across multiple SIEM platforms, including Splunk, ArcSight, and QRadar.
- Managed and tracked incidents and investigations using platforms such as RSA Archer and ServiceNow.
- Supported security engineers in alert tuning and the development of new detection capabilities.

Security Engineer | July 2019 – November 2019 | Synergy BIS, Kerneysville, WV

- Contributed to the establishment of robust security baselines for systems within the United States Coast Guard.
- Mapped legacy Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) requirements to NIST SP 800-53 security controls.
- Assisted in defining organization-specific security requirements based on NIST SP 800-53 controls.

Information System Security Officer | September 2018 – July 2019 | General Dynamics IT, Frederick, MD

- Provided essential Information Assurance services for the US Army Medical Research Institute of Infectious Diseases (USAMRIID).
- Updated and ensured compliance of Institute security policies with NIST SP 800-53 Audit and Accountability controls.
- Supported the successful installation and configuration of a SIEM solution to meet SP 800-53 audit controls.
- Actively participated in vulnerability management activities, adhering to DISA and Information Assurance Vulnerability Management (IAVM) guidance.
- Utilized Assured Compliance Assessment Solution (ACAS) for comprehensive vulnerability scanning, tracking, and compliance checks against Security Technical Implementation Guides (STIGs) and Security Content Automation Protocol (SCAP).
- Assessed new software and systems to determine and mitigate risk levels for the Institute.
- Assisted in system categorization and security control selection for DoD systems in accordance with the Risk Management Framework (RMF).

Help Desk Specialist | October 2017 – September 2018 | Cherokee Nation Businesses, Frederick, MD

- Provided Tier 1 and Tier 2 technical support for US Army Medical Research Institute of Infectious Diseases (USAMRIID), managing tickets in Remedy.
- Assisted in the large-scale migration of all Windows 7 systems to Windows 10 as directed by Army directives.
- Documented storage devices for secure storage and destruction in compliance with the Institute's data retention and lifecycle policy.
- Automated software installation and user data backups using basic PowerShell scripts.
- Assisted with STIG remediation and system patching processes.

System Technician | January 2013 – October 2017 | Washington County Public Schools, Hagerstown, MD

- Provided Tier 1 and 2 technical support for Washington County Public Schools (Pre-K-12).
- Created custom operating system images for workstations using Windows Deployment Services (WDS).
- Installed and troubleshot various types of audio/visual equipment and software.
- Racked and configured various types of networking equipment and servers.