Keonnii Ashman

Senior Security And Compliance Analyst @ Disney

Email: 12s-tn9-5da@mail.dice.com

Phone: 3478867246

### Summary

|  |  |
| --- | --- |
| Previous | Cyber Security Analyst @ The Digitrust Group |
| Preferred | Senior Security and Compliance Analyst |
| Location | CA, US |
| Desired Work Settings | No Preference |
| Willing to Relocate | No |
| Work Authorization(s): | Authorized to work in the United States on a full-time basis. |
| Security Clearance Info: | US Citizen (for security purposes) |
| Employment Type | Full-time Part-time Contract - Independent Contract - W2 Contract to Hire - Independent Contract to Hire - W2 |
| Total Experience | 10 years |
| Education | Unspecified |
| Profile Source | Dice |
| Profile Downloaded | Monday, December 9, 2024 |

**KEONNII ASHMAN**

WOODLAND HILLS, CA **|**  **| |** [https://www.linkedin.com/in/keonnii-ashman-5661a286/]

**EXECUTIVE SUMMARY**

**Dynamic Cyber Security Professional** with expertise in evaluating, recommending, and implementing cutting-edge technologies to fortify cybersecurity defenses. Recognized for spearheading global team development and maintaining 24/7 SOC support. Proficient in devising Cloud security strategies and leveraging tools like Splunk, AWS, and Kibana to enhance operational efficiency. Adept at performing technical analysis to identify and mitigate threats, ensuring robust security postures. Proven track record in leading cross-functional teams, driving process improvements, and delivering actionable insights to stakeholders.

**Tools:** Tanium, IBM BigFix, KACE, Qualys, Redlock, Prisma Cloud, nMAP, LogMeIn, Bomgar, Wireshark, Volatility, Kibana, Cyber Chef, Cylance, Kaspersky, Metasploit, AirWatch, RSA Console, Tenable, AppDynamics, AWS Console, GCP Console, Azure Sentinel, Ms Defender, Office 365, ServiceNow, Jira, Wiz.io, SysDig, GitHub, SAP, Box, Qradar, SharePoint, Splunk ES/SOAR, Active Directory

**Languages:** Regex, Splunk, Python, Assembler, Java, Kibana

**EXPERIENCE**

**Cisco,** Global Team Leader for SOC AUS/ USA Region **11/2020 – 04/2024**

* Spearheaded research and evaluation of cutting-edge cybersecurity technologies, driving enhancements in program capabilities
* Developed and maintained Cloud security playbooks for ongoing training and adherence to SLAs, ensuring robust defense mechanisms while orchestrating team development initiatives in Cloud environments
* Updated, managed, and developed dashboards utilizing tools like ServiceNow, Splunk, AWS, and Kibana, enabling comprehensive review of metrics for stakeholders
* Managed/Monitored cloud security posture using AWS Security Hub, SysDig, Wiz.io to identify potential misconfigurations and provide container security
* Investigated Failed API authentications and provided feedback to ensure remediation.
* Conducted technical reviews and analysis of system and network events to proactively identify and mitigate threat-related activities, ensuring a secure environment. Led the AUS/USA region in maintaining 24/7 support within the SOC, ensuring uninterrupted operations as an Incident Commander.

**Disney,** Senior Security Compliance Analyst for Corrective Action / Patch & Vulnerability Management **04/2021 – 09/2023**

* Identified and recommended solutions to mitigate discovered vulnerabilities, contributing to enhanced security posture and risk mitigation using Tenable, Qradar
* Provided samples for auditing to ensure Sarbanes Oxley Compliance.

**Disney,** Senior Security and Compliance Analyst for Vulnerability Management **07/2019 – 04/2020**

* Developed and presented business cases to management, enhancing security posture and mitigating advanced threats
* Supported the PCI DSS compliance program by reviewing evidence of compliance, driving necessary system and processing improvements, ensuring completion of annual compliance reports
* Helped build/improve an exception process to manage policy compliance deviation, ensuring adherence to security standards
* Collaborated with Resolver Groups to update Security Standards for all technologies against Disney Segments, facilitating alignment and compliance
* Managed/Monitored cloud security posture using Redlock/Prisma Cloud to conducted policy compliance scans and delivered reports to technology owners, ensuring adherence to security policies and standards

**The Digitrust Group**, Cyber Security Analyst **07/2017 – 07/2019**

* Utilized expertise in Intrusion Detection/Prevention Systems and rule/signature writing to bolster cyber defense capabilities
* Analyzed and reported cyber threats, contributing to the identification, investigation, and monitoring of threat actors while developing internal processes and standards for threat intelligence workflow
* Adhered to Service Management procedures and met SLAs, optimizing operational efficiency and client satisfaction
* Managed customer escalations, providing support for status reports and briefs to senior leadership, and guaranteeing effective communication and resolution
* Created relevant detection logic for security alerts.
* Populated and maintained an intrusion database, offering vital data analysis support for informed decision-making
* Created and maintained Kibana Dashboards, facilitating real-time monitoring and analysis of security logs.

**AIG**, Team Lead Help Desk / Mobile Administrator / Queue Coordinator  **08/2014 – 07/2017**

* Trained junior members of IT team regarding work instructions, polices and service level agreements.
* Administered Identity and security access globally for human/functionally accounts across multiple systems and applications. Including onboarding /offboarding, incident/problem management associated with access entitlements and terminations as well as Emergency & Privileged Access management.

**EDUCATION & CERTIFICATIONS:**

**Southern Connecticut State University,** New Haven — *Bachelor of Science Computer Science*

Splunk Fundamentals

Cylance Security Professional