

Jared Keyes, CISSP

CLOUD ENGINEER

Jared.Keyes3@gmail.com

443-947-0585

[LinkedIn](#)

PROFESSIONAL SUMMARY

I've spent the past year focused on my Bachelor's of Science in Cybersecurity from Purdue Global. My coursework has covered areas such as Linux Administration, Python Programming, and Cybersecurity Best Practices. I have 4+ years of experience in IT with roles as a Network Engineer, Cyber Analyst, and Cloud Engineer using tools such as SolarWinds, Carbon Black, Malwarebytes, EC2, S3, VPCs, IAM, CloudWatch, CloudTrail, CloudFormation, GuardDuty, PowerShell, BASH, Ansible, and Grafana.

EXPERIENCE

March 2023 – Present

BS in Cybersecurity, Purdue Global, Full-Time Student

Coursework, including linux administration, coding (Python), and Cybersecurity (vulnerability management, risk assessment, legal and regulatory frameworks, network defense, and threat modeling).

May 2022 – March 2023

Amazon Dedicated Cloud Engineer, Amazon Web Services

As an Amazon Dedicated Cloud Engineer, I deployed and maintained multiple AWS services, such as DataSync and Storage Gateway, while using services such as CloudWatch, CloudTrail, and CloudFormation to continuously monitor the health and status of services to ensure high availability and resiliency, and responded to events in a timely manner to minimize customer impact.

Key Aspects include:

- Used AWS Linux EC2, S3, Python, and Bash Scripting to build and automate a testing environment, reducing testing time for new releases from two days to a few hours.
- Built services in new regions and maintained enterprise architecture using CloudFormation, bringing services to millions of new customers.
- Maintained and improved our CI/CD pipeline, working closely with the development team to troubleshoot failed deployments and improve productivity.
- Managed fleets of hundreds of Linux servers, including provisioning, updating, and decommissioning.
- Used logs from multiple sources, including application, OS, and AWS services logs, to diagnose and remediate problems.

- Led and facilitated twice-weekly team meetings, promoting open dialogue and collaboration to solve complex challenges.
- Created or updated documentation, wikis, and runbooks.

September 2021 – May 2022

Cyber Analyst, *Cyberpoint LLC*

As a Cyber Analyst, my role included assisting in constructing and standing up a brand-new cybersecurity program. Using my knowledge of the systems in place and industry best practices, I also monitored the network for any potentially malicious or undesired activity.

Key Aspects include:

- Monitored, detected, contained, and remediated IT threats on a dynamic security operations team using Elastic tools and AWS services, including CloudWatch, CloudTrail, and GuardDuty.
- Helped establish cyber security program, including writing policy and creating and running tabletop exercises.
- Worked closely and gave recommendations to the NOC team for securing cloud infrastructure, minimizing attack vectors, and remediating poor configuration/practices.
- Developed and maintained productive relationships with internal and external stakeholders to achieve company objectives.
- Provided threat and vulnerability analysis and continuously developed detection analytics.
- Investigated, documented, and reported on information security issues and emerging trends.
- Analyzed and responded to previously undisclosed software and hardware vulnerabilities (zero-day).

February 2019 – September 2021

Network Engineer/Information System Security Officer, *ThalesTCT*

As the network engineer and Information System Security Officer for ThalesTCT, I set up, configured, maintained, and monitored the network to provide 99.99% uptime while keeping the network secure and meeting all compliance standards set forth by the company.

Key Aspects include:

- Identified events and responded to threats with appliance upgrades, rule creation, and report generation.
- Established ACLs (Access Control Lists) and blocked unnecessary ports that improved network and server security.
- Configured and managed switches, routers, and firewalls.

- Monitored logs and network activity using SolarWinds Security Event Manager (SEM) to identify events and respond to threats.
- Implemented industry best practices, such as CMMC, FISMA, and NIST guidelines, to improve security posture and comply with government standards.
- Leveraged exceptional listening and empathy skills to establish a supportive team environment, which contributed to creating a positive and inclusive team culture, boosting team satisfaction and morale.

CERTIFICATIONS

AWS Certified Solutions Architect Associate

AWS Certified Cloud Practitioner

ISC² Certified Information System Security Professional (CISSP)

CompTIA Cybersecurity Analyst+

CompTIA Security+

EDUCATION

March 2023 – Anticipated completion December 2024

BS in Cybersecurity, Purdue Global, Full-Time Student

Maintaining a 3.92 GPA while completing courses in cybersecurity.