

Application Security Architect

United States: Pittsburgh, Pennsylvania

eve@cybersn.com

University of Phoenix

5/2020 - PRESENT

Acme Sign Corp

Cloud Forensics Analyst • Engineering

35% Architecture and Design

Provide design and oversight into identity and access management (IAM)

- Maintain architecture diagrams
- Maintain data models
- Maintain privileged identity management
- Perform password vaulting
- IAM Products

Perform product security design

- Determine security requirements
- Define roadmaps

Perform infrastructure security design

- Firewalls
- IDS/IPS

Define standards, procedures and policies

Perform cloud security design

- Determine security requirements
- Define roadmaps
- Create security procedures
- Create security policies
- Type of Cloud

35% DevSecOps

Perform development operations (DevOps) tasks

- Support continuous integration and continuous delivery (CI/CD)
- Migrate from monolithic architectures to micro-service architecture
- Maintain the CI/CD product suite

Participate in the code review and QA process

- Develop testing criteria
- Perform quality assurance (QA) testing

Perform automated and/or orchestrated deployment of code

Program and write scripts

- For the automation of recurring tasks
- For proof of concepts
- Languages

30% Red Team

Prepare Redteam exercises

- Develop threat scenarios, cyber exercises, attack simulations
- Individual red team exercise objectives, attack design and scopes
- Attack/C2 Infrastructure design
- Rules of engagement

Implement, maintain and secure red team attack/C2 Infrastructure

Develop tailored and proof of concept (POC) exploits

Conduct Red Team exercises

- Reconnaissance
- Weaponization
- Social Engineering
- Exploitation
- Basic Command and Control (C2)

Technologies

Ansible • AWS Container Service • Amazon Web Services (AWS) • Python • C •
Checkpoint • Palo Alto • Centrify • CyberArk • IBM Identity • Snort • Tipping Point

5/2018 - 6/2019

Flynn's Arcade

Red Team Tester • Entertainment

35% DevSecOps

Perform development operations (DevOps) tasks

- Support continuous integration and continuous delivery (CI/CD)
- Migrate between on-prem and cloud environments
- Migrate from monolithic architectures to micro-service architecture
- Maintain the CI/CD product suite

Perform security operations (SecOps) tasks

- Risk Assessments
- Vulnerability Assessments
- Security code reviews

Participate in the code review and QA process

- Perform quality assurance (QA) testing
- Perform Software Development

Provide infrastructure support

- Provision servers and services
- Manage backups

Maintain software applications

- Webservers
- Databases

Perform automated and/or orchestrated deployment of code

Program and write scripts

- For the automation of recurring tasks
- For proof of concepts
- Languages

35% IT Support

Install, setup and troubleshoot

- Laptops and workstations
- Physical servers
- Cloud providers
- Security services

Administer accounts and access controls

- Cloud resident business applications
- File access
- Cloud Identity Management

30% Sales Engineering

Defining the criteria and performing technical evaluations of client networks and computing environments and providing feedback to

Assisting the sales team with business development

Gathering, coalescing and conveying customer requirements to product management and engineering teams

Creating and delivering statements of work (SOWs) and technical project plans incorporating service and program management activities

Researching competitive landscape to derive technical differentiation and value propositions

Deliver of product demonstrations

- Proof of Concepts (POCs)

- Proof of Values (POVs)

Technologies

Ansible • AWS Container Service • Bamboo • Jenkins • Kubernetes • Puppet • Amazon Web Services (AWS) • Azure • Python • C • C# • C++ • Oracle • Microsoft SQL Server • Rapid7 Nexpose • Nessus • NGINX • Apache • Endpoint Detection and Response (EDR) • Host-based firewalls • Network/Application firewalls
