James Droste

845-709-1302 • james@droste.im
https://james.droste.im • https://linkedin.com/in/jtdroste

WORK EXPERIENCE

Amazon Web Services, Seattle, Washington

Security Engineer (7/2017 – Present)

- Apart of the AWS Security Operations team, which is responsible for the security and availability of all cloud, mobile products, and services offered by AWS.
- Investigated and responded to security incidents that have scaled across thousands of instances, and terabytes of data.
- Led conference calls with service teams to ensure and drive remediation of security issues.
- Provided guidance on security best practices, and incident response plans to service teams.
- Developed scripts and tooling to speed up Incident Response activities, and reduce manual investigation.
- Communicated and escalated across the AWS organization up to the Director/VP level of products and services to explain and establish business risk, and drive appropriate remediation.
- Prepared weekly executive reports of security incidents to ensure members of C level leadership are aware of current security issues and mitigations.

Amazon Web Services, Herndon, Virginia

Security Engineer Intern (6/2016 – 8/2016)

- Shadowed and participated in multiple on-call shifts for Incident Response at AWS. Performed as the primary on-call engineer for an on-call rotation.
- Shadowed and participated in other business units of the team, involving our tooling development, upgrade campaigns, and threat intelligence
- Designed an internship program for future Security Operations interns

VOLUNTEER EXPERIENCE

University at Buffalo Network Defense

(Virtual) Lecturer (8/2017 – Present)

- Served as a mentor for students interested in Cyber Security, as well as leadership for the Network Defense class.
- Setup and managed enterprise-level monitoring of the infrastructure including NetFlow capture, centralized logging, and centralized authentication. Developed runbooks / documentation for future setup and maintenance.
- Acted as “senior manager” for class infrastructure, providing guidance and direction for the classes cluster of 20+ VMware servers and internal networks.
- Developed tools to automate development and deployment of Cyber Defense competition pods, as well as programs to be used for defense-only competitions (scoring, reporting system).

EDUCATION

University at Buffalo, The State University of New York

Bachelor of Science in Computer Science
Independent Study: Network Security/Defense
Designed and taught curriculum to teach students an Introduction to Cyber Security

CERTIFICATIONS

Offensive Security Certified Professional (OSCP)

CONCEPTS

Computer Networking
Incident Response
OSI Model
OWASP Top Ten
Packet Analysis
TCP/IP

PROGRAMMING

C
C++
Golang
Java
JavaScript
MySQL
PHP
Python
Shell (bash, zsh)

SKILLS / ABILITIES

Cloud Technologies
  AWS
Log Management/ Visualization
  ELK, Graylog, Splunk
Networking
  Cisco IOS, pfSense, Palo Alto
OS Management/Hardening
  Debian, Ubuntu, CentOS, Fedora, FreeBSD, Mac OS X, Windows Server
Penetration Testing
  Cobalt Strike, Kali Linux, Metasploit
Virtualization
  OpenVZ, KVM, VMware ESXi, VirtualBox
VMware
  vSphere Administration, vMotion with DRS, Virtual Distributed Switches