Joe Pate

https://linkedin.com/in/whoisjoepate/
stress@lotsofmoving.parts | 302.440.4540

EDUCATION

UCF
B.S. in Information Technology
December 2014 | Orlando, Fl
College of Eng. & Computer Sciences
Dean's List (Later Semesters)
Major GPA: 3.44 / 4.0

CERTIFICATIONS

GIAC (EXPIRED)
2017 GCTI (#1144)
2017 GCFA (#13368)
2019 GWAPT (#6137)

SKILLS

PROGRAMMING
AWS • Python • **Panther** • SQL
Working Proficiency:
C • GCP • Java • Javascript • PHP • **OCI**
Familiar:
Boto3 • JSON • LaTeX • Pandas
PySpark • Selenium • YAML
ANALYTICAL
AWS Security • Databricks • Snowflake
Suricata • Splunk
Forensic Proficiency:
.eml/.msg • Linux • MacOS• Windows
Log Sources of Familiarity:
AWS CloudTrail • GuardDuty •
CrowdStrike Falcon Data Replicator
Github Audit • Okta System • Zscaler

AWARDS

2023 Dropbox Team Taco "Capitan"
2021 Amazon Security "Bias for Action"
2021 US Patent **10904292B1** Granted
2020 US Patent **10740151B1** Granted
2014 1st/10 **NCCDC** National Champions (Team Member)

SOCIETIES

2018 **lockFALE** Seattle Ops Team
2014 **Hac@kUCF** Vice President

LINKS

Github:// **working-as-designed**
LinkedIn:// **whoisjoepate**

EXPERIENCE

DROPBOX Sr. SecEng (IC4), Detections & Response Team
Nov 2022 – Nov 2024 | Seattle, WA

- Lead Incident Responder for the Detections and Response Team (DART), seeing two high profile public security events [1] [2]
- Transitioned security case management operations and metrics from Jira to Tines
- Co-developed and monitored insider risk detections for multiple Reduction in Force (RIF) events
- Lead emergent issues with Audit, Compliance, Risk teams, documenting playbooks and interaction outcomes
- Mentored several great security engineers into their first enterprise incident response role

AMAZON.COM Sr. SecEng (L5-6), Detections & Monitoring Team
July 2018 – June 2022 | Seattle, WA

- Founded a team producing security alarms from GuardDuty, CloudTrail, and Linux endpoint telemetry sources
- Built, operated, and deprecated a multi-tenant cloud-native detection engine identifying security events from hundreds of thousands of AWS accounts
- Standardized alarm documentation through the **Alerting and Detection Strategy (ADS) Framework**
- Integrated our detections service into the Threat Intelligence Platform to communicate Mitre ATT&CK coverage
- 2021 **Log4Shell** and **Twitch** Large-Scale Security Event detections workstream lead
- Accomplished interviewer with 100 combined phone screen or interviews performed
- Promoted to SecEng 3 (L6) in July 2021

AMAZON.COM SecEng (L4-5), Security Incident Response Team
June 2016 - July 2018 | Seattle, WA

- Responder for security incidents within the retail portion of Amazon and subsidiaries
- Negotiating, triaging, and resolving responsible disclosure of vulnerabilities through the security@ mailbox
- Created requirements and performed UAT for development of custom case management solution
- Selected for travel to Austin TX during the 2017 **Whole Foods security event**
- Promoted to SecEng 2 (L5) in October 2017

FIREEYE Event Analyst, FireEye-as-a-Service
Jan 2015 – May 2016 | Reston, VA

- Four on, four off security analyst monitoring network and endpoint intrusion detection system (IDS) events
- Produced and updated **Snort** and **OpenIOC** detections for use in customer environments
- Developed shift scheduling automation (Python)