Joe Pate

Seattle, Washington | stress@lotsofmoving.parts | 302.440.4540

I'm a decadal Information Security practitioner with focus on security incident detection and response. I enjoy making and integrating tools to improve operational processes.

EDUCATION

UNIVERSITY OF CENTRAL FLORIDA
B.S. in Information Technology
College of Eng. & Computer Science
December 2014 | Orlando, FL
Major GPA: 3.44 / 4.0

CERTIFICATIONS

GIAC
2017 **GCTI** • 2017 **GCFA** • 2019 **GWAPT**

SKILLS

CODING
Languages:
C • Java • JavaScript • LaTeX • PHP • Python • SPL • SQL
Libraries:
Boto3 • Pandas • **panther-analysis** PySpark • Selenium
Clouds:
AWS • **GCP** • **OCI**

ANALYTICAL
AWS Athena • Databricks • Snowflake
Forensic Proficiency:
EML/MSG • Linux • macOS• Windows
Logs of Familiarity:
AWS CloudTrail • Amazon GuardDuty CrowdStrike Falcon Data Replicator Github Audit • Okta System Suricata • 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 Operations Team
2014 **Hack@kUCF** Vice President

LINKS

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

EXPERIENCE

DROPBOX Senior SecEng (IC4), Detections & Response Team
November 2022 – November 2024 | Seattle, WA

- Fulfilled Lead Incident Response role for the Detections and Response Team (DART), serving the 2023 **URL Sharing** and the 2024 **Dropbox Sign** incidents
- Migrated security case management operations and metrics from Jira to Tines
- Co-developed and monitored insider risk detections for multiple reduction in force events
- Managed emergent issues in collaboration with Audit, Compliance, and Risk teams; documented playbooks and engagement outcomes
- Mentored five security engineers as they transitioned into their first enterprise incident response roles

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

- Founding threat detection team member focused on protecting the business' AWS environments by leveraging CloudTrail, GuardDuty, and Linux host process telemetry
- Designed, developed, and operated a cloud-native detection system to analyze and enrich security logs spanning hundreds of thousands of AWS accounts to produce actionable threat detections
- Integrated our detection system with the Threat Intelligence Platform to convey Mitre ATT&CK coverage
- Standardized alarm documentation used by four separate organizational roles via the Palantir **Alerting and Detection Strategy Framework**
- Led a threat hunting workstream during the 2021 Log4Shell and **Twitch** security incidents
- Accomplished interviewer with 100+ combined phone screen, in-person, or virtual 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

- Responded to security incidents from across Amazon's retail business and subsidiaries
- Triaged, negotiated, and resolved responsible disclosure of vulnerabilities through the security@ mailbox
- Collaborated to create requirements and performed user acceptance testing for development of custom case management solution
- Co-led the on-site network security response during the 2017 **Whole Foods** point of sale security incident
- Promoted to SecEng 2 (L5) in October 2017

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

- Participated in a four-on-four-off shift to monitor and analyze threat activity derived from network and endpoint security appliances
- Produced and maintained **Snort** and **OpenIOC** detections for use in customer environments
- Developed a shift schedule calculator, allowing team members to view shift assignments on arbitrary dates in the schedule