

# Joe Pate

<https://linkedin.com/in/whoisjoepate/>  
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 process.

## 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

### Logs 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 1<sup>st</sup>/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), serving two public security incidents [**1 - Malicious Links**] [**2 - Dropbox Sign**]
- 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
- Integrated our detections service into the Threat Intelligence Platform to communicate Mitre ATT&CK coverage
- Standardized alarm documentation through the **Alerting and Detection Strategy (ADS) Framework**
- Detections workstream lead 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

- 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
- Co-lead the on-site network security response during the 2017 **Whole Foods** PoS security incident
- 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 calendar automation to help analysts trade distant shifts