Damien Kaur

Staff Software Engineer, Defensive Agent

(206) 555-7314 | damien.kaur@example.com | linkedin.com/example/damienkaur | Seattle, WA 98109

STRENGTHS

Security architecture
Built tenant boundaries, safe write controls, and credential checks before privileged security actions. Teams trusted those guardrails.

Durable execution
Used Temporal checkpoints, retries, and recovery paths for long running workflows. Failure reviews became practical design input.

Collaborative leadership
Architecture reviews and mentorship helped senior engineers make clearer tradeoffs. Peers regularly brought difficult designs for discussion.

Agent safety
Treated alerts and asset data as untrusted input, then separated model output from authorization. That boundary protected operations.

Production ownership
On call experience turned recurring failures into runbooks, metrics, and circuit breakers. Reliability improved through shared learning.

SKILLS

Python | Go | Rust | SQL | Distributed systems | Agentic systems | LLM systems | AWS | Kubernetes | Docker | Temporal | PostgreSQL | Neo4j | GraphQL | Multi tenant isolation

LANGUAGES

English — Native

SUMMARY

Staff Software Engineer with **11 years** building distributed security and cloud platforms, including **production** agentic and LLM backed systems. Leads architecture from design through production operation, retirement, and continuous improvement while contributing backend code in Python and Go. Creates durable execution with queues, retries, idempotency, checkpointing, cancellation, and **partial failure recovery**. Builds tenant scoped authorization with workload identity, short lived credentials, **safe write actions**, and hard isolation. Connects AI research with platform engineering by translating unclear product goals into practical roadmaps and MVP sequencing. Integrates EDR, SIEM, firewall, cloud IAM, PostgreSQL, Neo4j, GraphQL, AWS, Docker, Kubernetes, and Temporal. Raises quality through design reviews, mentorship, operational ownership, and clear observability. Ready to contribute this blend of security engineering, distributed systems judgment, and hands on delivery.

EXPERIENCE

Staff Software Engineer, Autonomous Defense Platform

Aegis Cloud Security | January 2023 - Present | Seattle, WA

Owns technical direction for autonomous remediation across endpoint, identity, firewall, and cloud controls. Leads architecture, production coding, operational decisions, **design reviews**, mentorship, and integration strategy for durable security workflows.

- Directed autonomous remediation **architecture** across endpoint, identity, firewall, and cloud control integrations.
- Built Temporal workflows with checkpoints, retries, idempotent activities, cancellation, and explicit recovery paths.
- Created Go and Python authorization tooling for **tenant scope**, resource validation, and **short lived credentials**.
- Normalized CrowdStrike, **Microsoft Defender**, SentinelOne, **cloud IAM**, and firewall APIs behind audited interfaces.
- Linked model decisions, tool requests, authorization outcomes, responses, and remediation state through explainable observability.
- Mentored senior engineers through architecture reviews, code reviews, and documented research tradeoffs.

Senior Software Engineer, AI Security Systems

Northstar Detection Labs | March 2020 - December 2022 | Bellevue, WA

Built production agentic security services connecting LLM workflows, cloud infrastructure, data stores, and customer facing controls. Partnered with product and research teams on secure delivery, reliability, and operational readiness.

- Built **Python** LLM workflows with deterministic policy checks before sensitive security operations.
- Developed AWS and Kubernetes services using **queues**, **retries**, deduplication, and idempotent consumers.
- Blocked **prompt injection** through controls for untrusted alert data and typed model outputs.
- Designed **PostgreSQL** workflow state and Neo4j asset relationships behind tenant aware **GraphQL**.
- Converted on call failure patterns into runbooks, metrics, circuit breakers, and safer retry behavior.
- Partnered with product and research teams on milestones, quality, latency, and cost decisions.

Software Engineer, Distributed Systems

Cascade Platform Engineering | July 2017 - February 2020 | Seattle, WA

Developed distributed services and cloud operations supporting tenant aware execution, configuration, authentication, telemetry, and reliable background processing. Grew into cross service reliability decisions, **production** support, and technical **mentorship**.

- Developed **Go** services carrying explicit tenant context across requests, data, jobs, and audits.

German Intermediate

MY CAREER

- Staff Software Engineer, Autonomous Defense Platform at Aegis Cloud Security (3.7 Years)
- Senior Software Engineer, AI Security Systems at Northstar Detection Labs (2.8 Years)
- Software Engineer, Distributed Systems at Cascade Platform Engineering (2.6 Years)
- Software Engineer, Backend Services at Harborline Software (2 Years)

- Created queue orchestration with retries, **idempotency** tokens, compensating actions, and status APIs.
- Operated **Docker** services on **Kubernetes** in AWS with health probes and deployment checks.
- Built PostgreSQL configuration and execution state services with tuned operational SQL.
- Integrated cloud APIs behind abstractions for authentication, pagination, rate limits, errors, and telemetry.
- Joined on call rotations and guided cross service reliability decisions through incident reviews.

Software Engineer, Backend Services

Harborline Software June 2015 - June 2017 Portland, OR

Built backend services, authenticated APIs, background jobs, database schemas, and development environments. Supported production reliability through testing, incident investigation, rollback planning, and clear technical documentation.

- Built TypeScript and **Python** backend services with authenticated APIs and background jobs.
- Developed PostgreSQL schemas and **SQL** queries with validation and rollback procedures.
- Added asynchronous API synchronization with bounded retries and persistent status records.
- Created Docker development environments that aligned service dependencies across engineering workflows.
- Tested API contracts, authorization rules, and failure cases before **production** releases.
- Investigated incidents through logs and metrics, then documented recurring operational issues.

PROJECTS

Durable Remediation Execution 2023

Connected Temporal workflows with tenant scoped tools, checkpointed progress, retry policies, and recovery paths. Close collaboration across engineering and research turned uncertain remediation ideas into explainable operational flows.

Agent Security Control Plane 2022

Combined Python LLM workflows, PostgreSQL state, Neo4j relationships, and tenant aware GraphQL. Partner discussions shaped policy checks that kept model output outside privileged authorization paths.

Cloud Integration Gateway 2019

Unified cloud API authentication, pagination, rate limits, errors, and telemetry behind stable service abstractions. Shared incident reviews helped engineers make safer integration decisions.

LEADERSHIP & AWARDS

- Technical leadership recognition for autonomous defense architecture and production security delivery.
- Engineering recognition for dependable distributed execution and practical incident ownership.
- Peer recognition for mentorship through architecture reviews, code reviews, and clear technical guidance.

EDUCATION

Bachelor's Degree in Computer Science

Oregon State University GPA: 0 2015 Corvallis, OR

Coursework: *Distributed systems, database systems, operating systems, software engineering*

CERTIFICATIONS

- AWS Certified Solutions Architect, Professional 2025
- Certified Kubernetes Application Developer 2024

TECHNICAL SKILLS

- **Programming Languages:** Python, Go, Rust
- **Agent Systems:** Agentic systems, LLMs, model output controls
- **Workflow Platforms:** Temporal, queues, retries

- **Cloud Platforms:** AWS, Azure, GCP
- **Container Platforms:** Docker, Kubernetes, health probes
- **Databases:** PostgreSQL, SQL, Neo4j
- **API Technologies:** GraphQL, REST, security APIs
- **Security Integrations:** CrowdStrike, SentinelOne, Microsoft Defender
- **Security Operations:** SIEM, firewalls, cloud IAM
- **Authorization Controls:** Tenant isolation, workload identity, short lived credentials
- **Reliability Engineering:** Idempotency, checkpointing, partial failure recovery
- **Observability:** Metrics, logs, tracing

PROFESSIONAL AFFILIATIONS

- Security engineering community participant focused on defensive automation, cloud controls, and safe agent systems.
- Distributed systems practitioner engaged with durable execution, reliability, observability, and operational learning.

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST