

# Staff Software Engineer - Identity Domain

Dublin, Ireland | Vectra AI

Vectra® is the leader in AI-driven threat detection and response for hybrid and multi-cloud enterprises. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single platform. Powered by patented Attack Signal Intelligence, it empowers security teams to rapidly prioritize, investigate and respond to the most advanced cyber-attacks. With 35 patents in AI-driven threat detection and the most vendor references in MITRE D3FEND, organizations worldwide rely on Vectra AI to move at the speed and scale of hybrid attackers. For more information, visit [www.vectra.ai](http://www.vectra.ai).

## About Vectra AI

Vectra AI is transforming cybersecurity through AI-driven threat detection and response. Our platform brings together network, identity, cloud, SaaS, and security telemetry to uncover attacker behaviour, identify risk, and help security teams investigate and respond before threats become breaches.

Identity is changing rapidly. Alongside human users, organisations increasingly rely on AI agents, service accounts, workloads, applications, API tokens, and other non-human identities to access systems and act autonomously. These technologies create enormous opportunity, but also a rapidly expanding attack surface.

Vectra's Identity Domain is responsible for detecting and reducing identity-based risk across identity providers and SaaS environments, including human, machine, and non-human identities.

## The Opportunity

We are looking for a Staff Software Engineer to provide technical leadership within Vectra AI's Identity Domain, with particular expertise in the emerging security challenges created by AI agents, machine identities, and non-human identities (NHIs).

This is a senior individual contributor role for an engineer who combines strong software engineering with deep curiosity about how customers build and operate modern identity systems.

You will need to understand how AI agents are created, deployed, authenticated, permissioned, and connected to enterprise systems and translate that understanding into security capabilities that protect customers as this new attack surface evolves.

The Identity team owns end-to-end delivery: from ingesting and normalising identity telemetry, through analytics and detection, to publishing detections and findings and making identity observability data available across the Vectra platform.

You will lead complex engineering initiatives across that lifecycle, remain hands-on with architecture and code, and help teams make strong technical decisions while delivering reliable customer outcomes.

## What You'll Do

- Design and deliver capabilities across the full Identity lifecycle: telemetry ingestion, normalisation, enrichment, analytics, detection, findings, and observability
- Build systems that help customers discover, understand, monitor, and protect human and non-human identities
- Help define how Vectra models AI agents, service accounts, workloads, OAuth integrations, tokens, and other machine identities
- Apply expertise in how customers build, deploy, authenticate, authorise, and permission AI agents and automated workloads
- Partner with Security Research and Product Management to turn evolving attack techniques and customer problems into durable product capabilities
- Correlate identity signals with network, cloud, and SaaS telemetry to reveal activity isolated controls may miss
- Help define and execute technical strategy for Identity products, services, data models, and engineering practices
- Lead design and code reviews, identify technical risks early, and maintain a high bar for reliability, security, observability, and maintainability
- Work across team and service boundaries, partnering with Data Platform, Cloud Platform, Data Science, SRE and others
- Engage with Product, field teams, and customers to understand deployment patterns, security concerns, and emerging use cases
- Mentor engineers, share knowledge broadly, and help develop technical leadership across the team

## What You'll Bring

### Required

- Significant professional software engineering experience building and operating production systems
- Strong expertise in distributed systems, architecture, coding, and technical problem solving
- Demonstrated ability to lead complex initiatives and influence technical decisions beyond your immediate team
- Strong understanding of modern identity systems, including authentication, authorisation, credentials, tokens, and privileged access
- Expertise in AI agents, machine identities, workload identities, service accounts, non-human identities, or closely related identity-security problems
- Practical understanding of how organisations build, deploy, authenticate, and permission AI agents and automated systems
- A customer-oriented mindset and enthusiasm for understanding how technology is used in real-world environments
- Experience building reliable, observable cloud-based services
- Strong judgment when balancing engineering quality, security, technical debt, customer needs, and business priorities
- Demonstrated ability to mentor engineers and raise the effectiveness of teams around you

### Preferred

- Deep knowledge of Entra ID, OAuth/OIDC, SaaS identity ecosystems, workload identity, secrets, or machine-to-machine authentication
- Experience building security capabilities for AI agents or autonomous systems
- Experience with behavioural analytics, detection engineering, anomaly detection, or high-volume security telemetry
- Cybersecurity product experience

## What Success Looks Like

- Vectra delivers differentiated security capabilities for AI agents and non-human identities
- The Identity team moves efficiently from new telemetry ingestion to customer-visible detections, findings, and observability
- Customers gain meaningful visibility into machine identities, their privileges, behaviour, and risk
- Complex initiatives land predictably with a consistently high engineering bar
- Engineers across the team grow through effective technical leadership and mentoring

## Why This Role Matters

The definition of identity is changing. Increasingly, the actor accessing sensitive enterprise systems may be an application, workload, automation, or AI agent acting autonomously and with significant permissions.

Securing this world requires understanding not only whether an identity authenticated, but what it is, what it can access, how it normally behaves, and whether its actions make sense in context.

As a Staff Software Engineer in the Identity Domain, you'll help Vectra solve that problem end to end, from the data we ingest, through the detections we create, to the findings and observability our customers depend on.

Vectra provides a comprehensive total rewards package that supports the financial, physical, mental and overall health of our employees and their families. Compensation includes competitive base pay, incentive plan eligibility, and participation in the employee equity plan (stock options).

Specific benefits offered vary by location, but commonly include health care insurance, income protection / life insurance, access to retirement savings plans, behavioral & emotional wellness services, generous time away from work, and a comprehensive employee recognition program.

Vectra is committed to creating a diverse environment and is proud to be an equal opportunity employer.

We are committed to equal employment opportunity for all applicants.