A small, time-bound collection of job descriptions for security partner roles or roles close to security partner work as a complement to Breanne Boland's 11 August 2022 Diana Initiative talk.

More on this subject

- Finding the Less-Risky Path Together: Security Partnership at Gusto
- Reinventing Cybersecurity
- My BSidesSF talk video and blog post
- Netflix on appsec partnerships, part one and part two

Find me

- breanneboland.com (with links to slides and everything above)
- twitter.com/breanneboland

6 June 2022, Datadog, Developer Advocate - Security
https://www.datadoghq.com/careers/detail/?gh_jid=4187885

Developer Advocate - Security

New York, USA, Remote; Massachusetts, USA, Remote; Colorado, USA, Remote; Washington, USA, Remote; California, USA, Remote; Texas, USA, Remote; Oregon, USA, Remote

About Datadog:

We're on a mission to build the best platform in the world for engineers to understand and scale their systems, applications, and teams. We operate at high scale—trillions of data points per day—allowing for seamless collaboration and problem-solving among Dev, Ops and Security teams globally for tens of thousands of companies. Our engineering culture values pragmatism, honesty, and simplicity to solve hard problems the right way.

The Team:

We are a growing global team of engineers, evangelists, and advocates across North America and Europe, who focus on enabling Datadog's user and developer community to build great things on Datadog's cloud monitoring platform. Our team works with freedom and autonomy, focusing on delivering high impact, quality content.

The Opportunity:

In this role you will be hands-on with the great products we're building to help our users stay safe in the cloud. In this role you'll work in a variety of content mediums: blog posts, presentations, security research, and open source software to name a few of the options available. You will foster relationships with our Datadog users, developer communities, and the security community. Finally there will be many opportunities to help other Datadog employees build their own advocacy skills.

You Will:

- Speak at conferences and meetups to build Datadog's reputation as a leader in security.
- Partner with product engineering teams to improve the product and tell great stories
- Improve our user facing documentation
- Design security simulations
- Collaborate with our community of open-source contributors

- Research and discover threats to Cloud Service Providers (AWS, GCP, Azure), Linux workloads, containers, and Kubernetes
- Share our research through blogging, public speaking, webinars, and research papers
- Discover and demonstrate new attack and defense techniques and develop detection methods for them
- Collaborate with our in house Security Research Director and team to generate threat intelligence
- Work across the Datadog organization to help mentor and develop other security stories

Who You Are:

- You have publicly available samples of your work in the community. This could include writing, presentations, open source projects, or whitepapers
- You have experience in one or more security roles as a practitioner and are interested in developing content based on that experience.
- You are fluent-reading and writing in at least 2 programming languages (e.g. Ruby, Python, Go, bash, powershell).
- You are comfortable and familiar with modern infrastructure such as IaaS cloud services and containers.
- You enjoy self-driven exploration and education on new technologies and languages.
- You are able to transform dry technical topics into engaging, informative and interesting educational materials.

Bonus Points:

- Real-world SIEM and/or cloud-native security tool experience
- You have experience producing videos which distill complex technical concepts into content easily understood by both technical and non-technical audiences.
- You already are an active member of the Security or language communities in your region
- Familiarity with SIEM, Compliance, Endpoint Monitoring
- Incident Response experience
- Experience building security solutions at scale

Why You Should Apply:

- Generous and competitive global and US benefits
- New hire stock equity (RSUs) and employee stock purchase plan
- Continuous career development and pathing opportunities
- Internal mentor and buddy program cross-departmentally

- Friendly and inclusive workplace culture

Is this you? Send your resume and links to your Github profile and public writing samples.

In accordance with the Colorado Equal Pay Transparency Rule (“EPT”)

At Datadog, we are committed to providing competitive pay and benefits that are in line with industry standards. We analyze and carefully consider several factors when determining compensation, including your work history and professional experience. These considerations potentially can cause your compensation to vary.

The Developer Advocate - Security position has an annual starting salary of $144,000, and a competitive equity package. The actual pay may be higher depending on your skills, qualifications, and experience. In addition, Datadog offers a wide range of employee benefits. To learn more about Benefits click here.

June 2020
https://jobs.netflix.com/jobs/210140918

Application Security Engineer, AppSec Reviews and Assessments

•

Remote, United States

- Security

At Netflix, we do one thing - entertainment - and we aim to do it really well at scale. We have a strong engineering organization that enables us to achieve these business objectives and a unique culture that guides us. This also means that our security team needs to operate differently than a traditional security team. We do not operate with traditional gating mechanisms but instead focus on enabling our customers. We provide them with clear, opinionated security guidance and usable, scalable, secure by default offerings to make pragmatic risk decisions for Netflix.

The Application Security teams at Netflix are responsible for securing the software footprint that we create to run the Netflix product, the Netflix studio, and the business. We have previously invested in the idea of strategic security partnerships and engineering investments to scale our Application Security program. As the Netflix business and engineering workforce has grown, our software footprint has also grown and become more heterogeneous. We are now complementing our security partnerships and engineering investments with increased investments to serve the Appsec Professional Services charter (services like bug bounty, pentesting, product security incident response, threat modeling, security reviews, and developer security education).

We are hiring an Application Security Engineer for the newly formed Appsec Reviews and Assessments team. In this role, you will work closely with engineering teams that build software to support the Netflix product, studio and enterprise to provide critical Appsec services. We are looking for folks who are excited about pragmatic risk, continuous operational improvement and customer-centric security experiences.

Desired background:

- You are an early career Application Security engineer (2-5 years of experience).
- You have a strong application security background with a focus on providing practical technical guidance to engineering teams.

- You have experience with threat modeling, security design reviews, security architecture, pentesting and bug bounty handling.
- You have experience working collaboratively with engineers.
- You have strong verbal and written communication skills.

Finally, here are a few more reasons why we love this work and think that you will too:

- You will work with an industry-leading security team with many learning and growth opportunities.
- You will have the opportunity to research new ideas and share your ideas across the community.
- You will work closely with domain experts in diverse areas such as microservices architecture, big data, compute platforms, and content delivery networks.

Lead Product Security Engineer (Dedicated Security Partner)

Marqeta United States Remote 5 days ago 2 applicants

- https://www.linkedin.com/jobs/view/3180750613

Full-time · Mid-Senior level

501-1,000 employees · Financial Services

3 company alumni · 3 school alumni

See recent hiring trends for Marqeta-JW. Try Premium for free

- Actively recruiting

Marqeta powers innovative payment solutions for many of the apps and services you enjoy daily. Our open API provides unprecedented flexibility and control for industry-leading companies such as Uber, Coinbase, J.P.Morgan, and Block, to manage payment operations in real-time.

Our team is a mix of industry experts and technology innovators who take a dynamic approach to solving challenging problems. Marqeta was named a 2022 Glassdoor Best Place to Work, highlighting our company culture and collaborative work environment. We are building a global team as diverse as the markets we serve and we'd love it if you joined us on our mission to change the way money moves.

We're a remote-first company. You have the choice to work from wherever you're happiest and most productive, whether that's from home, a co-working space, or one of our four global offices, depending on your location. It's uncommon for candidates to match all job requirements, but if you're not far off, we want to hear from you.

Marqeta is growing a Security Engineering team with the goal of setting a new industry standard for security in the payments space. In this role, you will support secure product development for the world's first modern card issuing platform.

Marqeta's Product Security team seeks engineers with expertise in Application Security OR whom have a strong interest in Application Security with domain expertise in core Software Engineering, to support our Product team's capacity to deliver secure products and services.

You will use your domain expertise in software development and vulnerability remediation strategies to help Marqeta's Engineering org develop industry compliant services, implement security tooling within modern CICD pipelines, develop and deploy secure containerized (ECS,

K8s) microservices, and define minimum viable secure products (MVSPs) within a highly regulated space. This role may also support training and security awareness initiatives, with an emphasis on developing healthy partnerships with engineering leadership. The right candidate for this role either is excited to develop a skillset applying modern App Sec and Prod Sec standards into tangible deliverables, or has the background and hands-on experience to do so out of the gate.

As a Lead Prod Sec Engineer, you are responsible for secure by design initiatives in product, threat model validation, coordinating security reviews, and shepherding teams to adopt and implement application security tooling. Marqeta's Prod Sec Engineers have strong influence within the Product Engineering org, and knowledgeable individuals who can communicate with empathy and act with practicality will do especially well in this role.

Why are we so excited about this new role? Because security is central to our mission "to be the global standard for modern card issuing, empowering builders to bring the most innovative products to the world." Also, we're passionate about creating a culture of belonging and inclusion - this includes welcoming a variety of backgrounds, levels and career stages. The requirements listed in our Prod Security Engineer job descriptions are guidelines, not hard and fast rules. If this job intrigues you, but you think you might not meet all of the qualifications, please apply anyway!

Come work alongside a strong and strategically expanding security team and enjoy opportunities to apply your knowledge in new ways.

Product Security Engineering at Marqeta is a remote-first team and headquartered in Oakland, California.

What You'll Do

- Build scalable platform services and libraries
- Champion security across engineering
- Develop custom SAST tooling/rules and improve defect detection
- Track and Manage metrics for Prod Security adoption
- Develop new patterns for Threat Modeling and Security Reviews
- Focus on "Shift-Left" initiatives, supporting Marqeta's Product Engineers

What We're Looking For

- Hands on development in Python, GoLang, Java and/or NodeJS
- Experience with IaaC tooling incl but not limited to Terraform or Helm
- Knowledge of AWS Fundamentals
- Experience coordinating Security initiatives in cross-functional settings
- Background in Application Security, incl experience with SAST, DAST, and SCA

- Experience with Software Engineering Development Workflows, including flavors of CICD
- Ability to map a path forward and drive a project to completion
- Experience with Developing close partnerships with Product Engineers
- Solid grasp of full-stack engineering: front-end/backend, API and service architecture design, web infrastructure and distributed systems
- Pro-Social Behavior
- Excellent communication and collaboration skills
- Employ strong collaboration patterns and enjoy creating positive cross-team dynamics
- Understand ownership and support positive outcomes
- Remain constructive under pressure, with a flexible working style

Nice to have

- Experience building reliable, scaleable software - preferably with SaaS systems
- Experience deploying Golang and Java services at scale
- Knowledge of Identity and Access Management best practices and protocols, such as OAuth, OpenID Connect, SAML, MFA, and SCIM
- Firm understanding of OWASP Top 10, Application Security tooling, and Content Security Policies
- Experience in Payments or Financial Services

Benefits And Perks

- Flexible time off – take what you need
- Retirement savings program with company contribution
- Employee insurance premiums paid 100% + coverage for dependents and pets
- Family forming benefits including fertility support and up to 20 weeks Parental Leave
- Free therapy sessions, financial coaching, and a Wellness stipend
- Monthly stipend to support our hybrid work model
- Equity in a publicly-traded company
- Bi-annual “Hack Week” to support and reward innovation

Security Partner, Emerging Areas

Meta United States Remote 2 days ago 63 applicants

- https://www.linkedin.com/jobs/view/3092827141/

Full-time

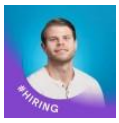
10,001+ employees · Internet Publishing

10 connections · 24 company alumni · 6 school alumni

See how you compare to 63 applicants. Try Premium for free

- Actively recruiting

Meet the hiring team



Phillip Reese
2nd
Talent Acquisition Leader at Meta - Come build community!
1 mutual connection
Message

Security Partners acquire a deep understanding of one or more areas of Facebook's expanding portfolio and partner with engineering and product leaders to ensure that security is correctly designed into their products and operations. This might be securing end-to-end messaging encryption, protecting next-generation gaming and media services from exploitation, validating a secure boot process and certificate storage, infusing security into SoC hardware designs, creating security programs for new product innovations and much more. The ideal candidate will share our passion for solving complicated business and security problems, while minimizing friction and maximizing productivity and impact. This is a technical role, requiring both deep and broad technical knowledge across a range of security disciplines. This is also a leadership role that will be making recommendations to leadership on resourcing, roadmaps and processes. The ideal candidate will need to be adept at communicating at the highest levels of the organization, presenting arguments based on data, and representing Facebook's security team at the CISO level.

Security Partner, Emerging Areas Responsibilities:

- Discover needs and drive security solutions across one or more of Facebook's business units

- Represent Security organization in product strategy and roadmap development with PMs, TPMs and Engineers
- Build deep relationships with product and engineering leaders
- Drive security risk decisions, initiatives, and influence technical architecture
- Act as the primary liaison between the product and engineering teams, and the Facebook security team
- Develop and maintain deep industry expertise in the assigned areas

Minimum Qualifications:

- 10+ years experience in information security
- Technical experience across security disciplines
- Experience communicating risks and roadmaps to senior leadership
- Experience building relationships with stakeholders and business leaders
- Experience with international standards for audit and data protection
- Self-motivated and work well in ambiguity
- Customer facing experience

Preferred Qualifications:

- Strong domain experience in one or more of the following fields: web application security and OWASP, mobile application layer security, distributed infrastructure, consumer devices, or production hardware

Security Partner Strategist, ATO on AWS - Security and Compliance Acceleration

Amazon Web Services (AWS) United States Remote 1 week ago 16 applicants

-

Full-time

10,001+ employees · IT Services and IT Consulting

6 connections · 3 company alumni · 7 school alumni

See recent hiring trends for Nike. Try Premium for free

- Actively recruiting

Job Summary

DESCRIPTION

We are seeking a qualified candidate to help forge new cloud computing capabilities and accelerate customer success in regulated markets across the globe. Are you a knowledgeable and customer-driven security and compliance professional with a strong aptitude for building business relationships and supporting go to market activities? If you answered yes to the above, this position may prove a good fit for you.

As an AWS Security Partner Strategist you will have the exciting opportunity to shape and deliver joint strategies between Amazon Web Services and regional security and compliance partners. You will be the primary point of contact and subject matter expert in a given region, necessitating a fundamental to strong understanding of regulatory requirements across the public, financial, and healthcare sectors. You will have day-to-day interactions with partners, internal customers, and external customers to support both the growth of our program as well as execute on our primary purpose of simplifying and accelerating regulatory compliance on AWS. The ultimate goals for the role include growing customer adoption of AWS through partnership with qualified AWS partners, and building organizational competency and momentum within AWS Security and AWS Sales leadership.

You will also be responsible for awareness and education of security and compliance requirements, processes, and tools for the AWS sales field and partner channel. The ideal candidate will possess strong communication skills that will enable them to engage and interact with cross-functional AWS teams, partners, and customers. Additionally, the candidate must have a self-driven attitude and affinity to solving problems with little direction.

Here at AWS, we embrace our differences. We are committed to furthering our culture of inclusion. We have ten employee-led affinity groups, reaching 40,000 employees in over 190 chapters globally. We have innovative benefit offerings, and we host annual and ongoing learning experiences, including our Conversations on Race and Ethnicity (CORE) and AmazeCon (gender diversity) conferences. Amazon's culture of inclusion is reinforced within our 14 Leadership Principles, which remind team members to seek diverse perspectives, learn and be curious, and earn trust.

Our team also puts a high value on work-life balance. Striking a healthy balance between your personal and professional life is crucial to your happiness and success here, which is why we aren't focused on how many hours you spend at work or online. Instead, we're happy to offer a flexible schedule so you can have a more productive and well-balanced life—both in and outside of work.

Our team is dedicated to supporting new members. We have a broad mix of experience levels and tenures, and we're building an environment that celebrates knowledge sharing and mentorship. We care about your career growth and strive to assign projects based on what will help each team member develop into a better-rounded professional and enable them to take on more complex tasks in the future.

A day in the life

As an AWS Security Partner Strategist you can expect to meet and recruit partners to join and support our program. This includes frequent meetings with prospective partners detailing the program, regularly occurring meetings with partners that support our program regionally, and supporting customers, either indirectly through our partners or directly, in meeting their regulatory compliance obligations across the financial services, healthcare, and public sectors. You can also expect to attend conferences and marketing events where you may be asked to speak publicly, join panel discussions, and/or support promotional booths.

About The Team

Our team is dedicated to supporting new members. We have a broad mix of experience levels and tenures, and we're building an environment that celebrates knowledge sharing and mentorship. We care about your career growth and strive to assign projects based on what will help each team member develop into a better-rounded professional and enable them to take on more complex tasks in the future.

Basic Qualifications

- 5+ years experience operating in a role related to international security and compliance, such as security or compliance auditing, public policy, business development with a security and compliance focus, or related role.
- Maintain at least one internationally recognized cybersecurity certification, to include but not limited to CISSP, CISA, CISM, CEH, or Security+.
- Completed Bachelor's degree from an accredited college or university, or 10+ years working in security and compliance role.

Preferred Qualifications

- Deep understanding of regulatory requirements in a given global region (Asia, Latin America, European Union)
- Target orientated, ambitious, creative, customer focused
- Self-starter with highly developed interpersonal skills and organizational skills
- Ability and willingness to travel both regionally and internationally, potentially up to 25%
- Fluency in second language
- Ability to create and execute integrated lead generation campaigns using tactics that include live and/or virtual events, webinars, email, organic social, paid media and sales insights.
- Manage incoming leads and distribute across geographical/industry leaders
- Conduct initial prospects calls with customers to identify and qualify opportunities
- Meet with prospective partners to determine suitability in joining our program
- Generate interest and provide vision of our security portfolio to potential customers
- Strong presentation skills and the ability to articulate complex concepts to cross functional audiences.
- Strong written and verbal communications skills are a must, as well as the ability to work independently
- Highly self-motivated and entrepreneurial
- Comfortable operating in an ambiguous environment where a specific set of steps for success is yet to be defined

Manager of Information Security Partnerships

BetterUp San Francisco, CA Remote 1 week ago 59 applicants

- https://www.linkedin.com/jobs/view/3114645666

Full-time · Mid-Senior level

501-1,000 employees · Business Skills Training

1 company alumni · 1 school alumni

See how you compare to 59 applicants. Try Premium for free

- Actively recruiting

Meet the hiring team

Bryan Payne
2nd
Information Security Executive
4 mutual connections
Message

Let's face it, a company whose mission is human transformation better have some fresh thinking about the employer/employee relationship.

We do. We can't cram it all in here, but you'll start noticing it from the first interview.

Even our candidate experience is different. And when you get an offer from us (and accept it), you get way more than a paycheck. You get a personal BetterUp Coach, a development plan, a trained and coached manager, the most amazing team you've ever met (yes, each with their own personal BetterUp Coach), and most importantly, work that matters.

This makes for a remarkably focused and fulfilling work experience. Frankly, it's not for everyone. But for people with fire in their belly, it's a game-changing, career-defining, soul-lifting move.

Join us and we promise you the most intense and fulfilling years of your career, doing life-changing work in a fun, inventive, soulful culture.

If that sounds exciting—and the job description below feels like a fit—we really should start talking.

The Information Security Partnerships team at BetterUp brings the human touch to enabling the business through security. Members of this team help bridge the gap between security and other business domains (such as sales, human resources, information technology, software engineering, and more) to keep everyone aligned on how to best grow the business while keeping risk in check. This team also runs our security training and awareness programs.

What You'll Do

As the manager of this team you will set the strategic vision and work to bring the vision to life using your skills in hiring, mentorship, and empathetic leadership. You will set the tone for how security partnerships operate at BetterUp. Sometimes this will be hands-on as you build relationships across the business. Other times you will lead through your team by helping them build partnerships while they grow in their own career.

If you have some or all of the following, please apply:

- Experience as a people manager in the information security domain
- Experience as a security partner, security architect, or another related technical security role working with software engineering or information technology teams
- Communication skills that you can adapt as needed for working with individual contributors, executives, and everyone else in the organization
- Exceptional grit and a willingness to work in a fast-paced startup setting
- Eager to contribute to the BetterUp mission

We know that the best candidates often come from non-traditional backgrounds. If you are excited about this opportunity and feel that it could be a good fit, we'd encourage you to apply regardless of how many boxes you check from the above list. We'd love to get to know you before making a decision!

Benefits

At BetterUp, we are committed to living out our mission every day and that starts with providing benefits that allow our employees to care for themselves, support their families, and give back to their community.

- Access to BetterUp coaching; one for you and one for a friend or family member
- A competitive compensation plan with opportunity for advancement
- Medical, dental and vision insurance
- Flexible paid time off
- Per year:
    - All federal/statutory holidays observed
    - 4 BetterUp Inner Work days (https://www.betterup.co/inner-work)
    - 5 Volunteer Days to give back

    - Learning and Development stipend
    - Company wide Summer & Winter breaks
- Year-round charitable contribution of your choice on behalf of BetterUp
- 401(k) self contribution

Gusto Security Partner Engineer (L4+)

About the role:

The Security Partner role will work with product and engineering leads to design products and features with the safety and privacy of our customers in mind. This role will be focused on building long-term relationships between the Product Security team and internal stakeholders across the company. Secondarily, there is opportunity to drive security processes as well as building and integrating security tools.

The Product Security team helps Gusto move faster, securely. We're a team of engineers who work to enable other teams to build products as quickly as possible while continuing to protect our customers. We support developers in shipping secure code by building security tools and services, providing security training and expertise, and advocating for best practices in authentication, authorization, and safe data handling across the company.

Here's what you'll do day-to-day:

- Design processes for security reviews, threat modeling, and partnering with product engineering teams.
- Work with product teams to design safe features to protect our customers.
- Provide detailed security advice and risk assessment.
- Develop long-term relationships with product development and engineering teams.

Here's what we're looking for:

- 5+ years of experience in information security, especially application / product security / security partnerships.
- Ability to work with engineers to balance security risks, customer privacy, and business needs.

- Experience building software. We primarily use Ruby, JavaScript, Python, and Kotlin.

Our customers come from all walks of life and so do we. We hire great people from a wide variety of backgrounds, not just because it's the right thing to do, but because it makes our company stronger. If you share our values and our enthusiasm for small businesses, you will find a home at Gusto.