SECURITY FELLOWS PROGRAM

The Insight Security Fellows Program is an intensive, professional training fellowship for systems engineers, software engineers, and data analysts seeking to transition into full-time careers as security engineers, data privacy engineers, and advanced security analysts for leading companies in Silicon Valley. In seven weeks, Fellows gain experience with the tools, skills, and best practices necessary to become leaders in the critical and quickly evolving domain of security.

Your Bridge to a Career in Security

Are you passionate about the security of the internet and the data privacy of people all over the world? Are you looking to transition into a full-time career building robust systems and establishing the future of digital protective services? Do you want a career that leverages your curiosity and problem solving skills in a high-demand field that is central to the success of every company, as well as the underlying infrastructure of the entire internet?

Leading companies are seeking talented engineers and advanced analysts with the knowledge and skills to drive next-generation developments in security, help them secure their systems, ensure their users' privacy, and foster appropriate and ethical use of data. To develop new and valuable technologies in this space, security and privacy engineers not only work with traditional security teams in-industry, but also collaborate with teams across the entire technology stack - data scientists, data engineers, DevOps engineers, and machine learning researchers - to protect company and user assets. The large number of companies moving into this space are competing for a very small talent pool of well-rounded individuals with strong systems experience, coding skills, and security domain knowledge.

The Insight Security Fellows Program is a professional training fellowship that bridges the gap between your current passion for security and a full-time career securing systems, protecting privacy, and performing analyses with new, advanced technologies. This seven week, full-time, in-person program enables systems engineers, software engineers, and analysts to apply their existing skills to the challenging problems of designing, developing, and delivering security products and applications. Fellows learn by pushing the technological envelope in a collaborative and hands-on environment. They receive guidance and resources from industry mentors, leaders of open-source projects, and advisors. Additionally, Fellows gain lifelong access to a network of more than 2,000 Insight alumni, who are now working at over 700 companies. Immediately following the program, Fellows interview for full-time jobs with leading security teams in Silicon Valley. Fellows receive continued guidance and support until they accept a full-time offer to join a top company.

Dropbox

LinkedIn

moz://a

ProtonMail

stripe

Insight Security Fellows Program in a Nutshell:

1. Full-time, seven-week professional engineering fellowship in San Francisco.
2. Tuition-free program, with need-based scholarships and loans available to help cover living expenses.
3. Self-directed and collaborative project development, under the guidance and mentorship of top experts in the field.
4. Rapidly gain knowledge and practical experience with a diverse cohort of talented Fellows, working together on cutting-edge solutions to high-impact problems.
5. Meet top companies, present your work to teams that you're interested in, and interview immediately following the program.

Building Trust into our Digital Lives

Trust is at the core of every successful technology that stands the test of time. Whether these technologies help us work more efficiently, connect us with our friends and family, or simply entertain us, they must be built on a foundation of trust. New features and conveniences may initially attract users, but without the trust of its users, any technology will struggle with adoption in the long-term.

For this reason, trust was a critical consideration during the creation of the internet and the computer systems that power it. In 1984, a decade after the birth of modern operating systems, trust was at the heart of Ken Thompson's Turing Award acceptance speech. The co-creator of UNIX could have celebrated the operating system that would become the backbone to the Linux, Solaris, and OSX systems that power most of the internet today. Instead, he spurred a dialogue on trust in the tech community. With a few lines of well-placed code, he showed how someone could create a nearly untraceable backdoor into any system. His message was powerful: we can't rely on technology alone - we also need to build trust into the technology community.

> *"TO WHAT EXTENT SHOULD ONE TRUST A STATEMENT THAT A PROGRAM IS FREE OF TROJAN HORSES? PERHAPS IT'S MORE IMPORTANT TO TRUST THE PEOPLE WHO WROTE THE SOFTWARE."*

- Ken Thompson, Creator of UNIX, Reflections on Trusting Trust - Turing Award Lecture

In the first decade of the world wide web, those concerns went from theoretical musings to real-world problems. A clever high school or college student was able to create viruses and worms that spread quickly in the newly connected network of users. While these started as innocuous pranks to show off or prove a point, it wasn't long before malware was causing significant damage to businesses and users. While governments scrambled to address these threats with new laws and agencies, there was a real risk that the internet wouldn't be a resource for the safe and trustworthy exchange of information, as envisioned by its creators. To welcome a wider community, the average user had to trust that they could use the internet without sacrificing their security. They had to trust that one bad email attachment wouldn't ruin their computer or risk the valuable work and files it contained.

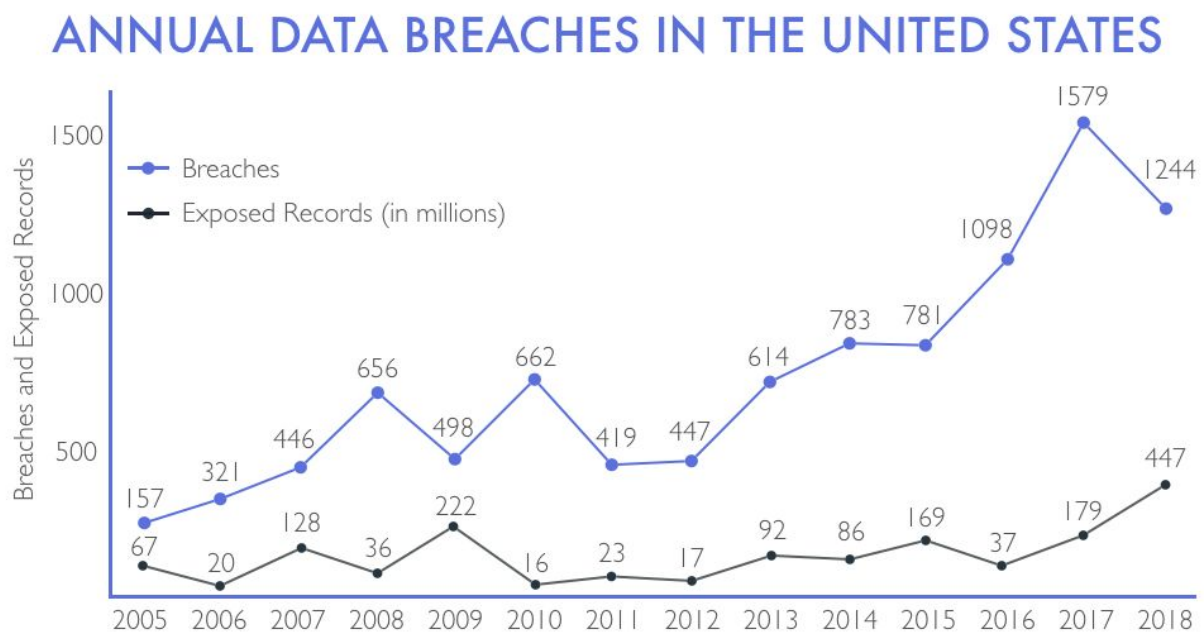
Fortunately, the tech community found solutions to protect the average user. From operating systems to networking protocols, the infrastructure of the internet was improved to offer more robust controls on permissions and mitigate the damage of malware. Along with that focus came a new cybersecurity industry with a variety of roles to look out for users. Security engineers emerged to defend against threats by building more robust systems and securing the infrastructure that powers the internet. Security analysts studied past failures with digital forensics to understand vulnerabilities and prevent future breaches.

In addition to technical solutions, an important and fruitful collaboration developed between the industry and a community of ethical hackers. A relatively small, but passionate, group of "white hats" volunteered their skills to test systems and report issues before malicious actors could exploit them. Software made by humans could never be free of flaws, but a community of thoughtful and watchful engineers helped restore trust in the internet. With this trust, the internet became a place where businesses could exist, and everyday people could feel comfortable using their true identities rather than the pseudonyms and handles that were preferred in the early days of the web. That trust led to the early success of the internet and the technology ecosystem that has grown out of it. People connected to the internet at an exponential rate, and businesses ranging from e-commerce to online banking thrived.

But after the dotcom bubble, a novel business model emerged that led to a fundamental dilemma that the tech community is still wrestling with today. A new set of tech-savvy organizations offered an implicit Faustian bargain: provide users free and revolutionary services - which have radically changed the way we work, communicate, and live together - in exchange for valuable data that can be used to optimize and fund those services.

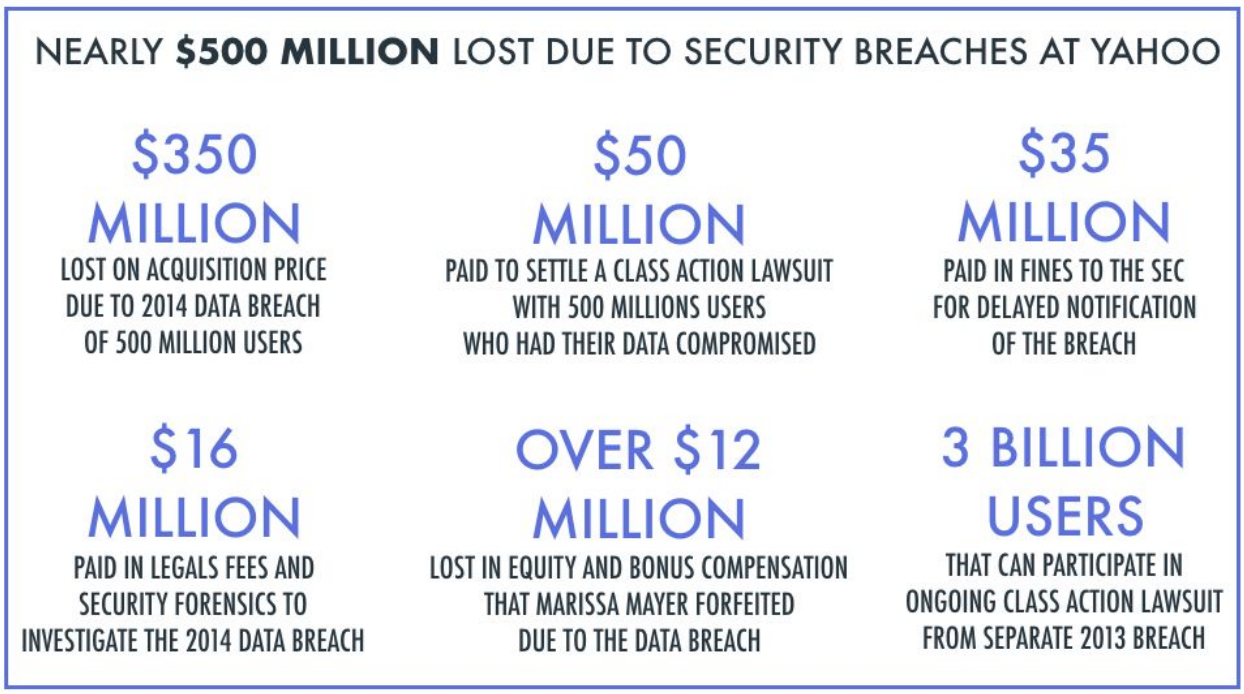
In the past several years, more and more companies have built sophisticated and beneficial products using that data. Much of the internet is built on this new model, including a thriving data and Ad-Tech ecosystem as well as some of the world's most successful businesses. Whether it's the deluge of clickstream data tracked on our favorite apps, or the constant stream from connected devices around us, our data is being collected with the goal of offering services to improve our lives.

But this development of sophisticated products and services that leverage user data brings an ethical obligation that hasn't been fully met. Many teams have been unwilling, or unable, to invest in the necessary security and data privacy needed to match the unprecedented growth they've enjoyed. Many companies have learned this lesson the hard way as their users' data becomes public, and they're the next story on the news. Even with the best of intentions, lax security policies have led to catastrophic problems.



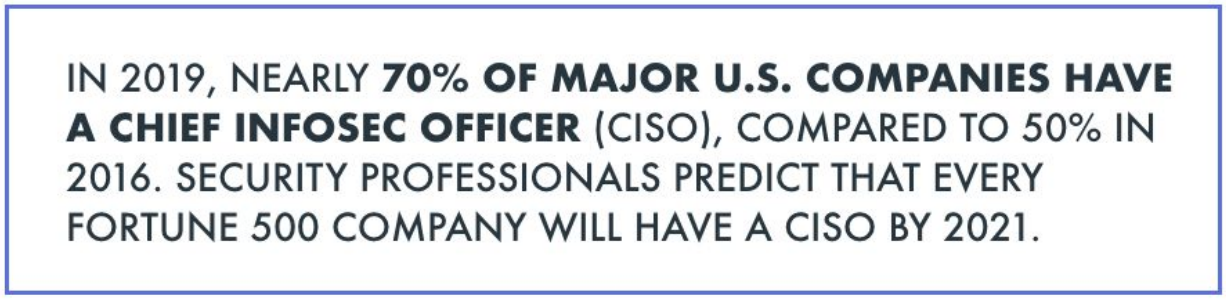
Data breaches have been on the rise since 2005, exposing sensitive information from billions of users. Unfortunately, these numbers represent a lower bound since many breaches go undiscovered and unreported. *Source: Annual reports from the non-profit organization, ITRC, funded by grants from the US Department of Justice.*

Data breaches have affected over 3 billion users, leaking private information to a large black market of personal data like names, emails, credit card numbers and social security numbers. With every breach or data scandal, users are justly questioning the apps, websites, and services that they use every day. We've reached a tipping point where users will no longer tolerate the tradeoff between privacy and free features. They're demanding a more secure internet that they can trust, and they'll take their accounts and data to services that are serious about security and privacy.



Despite an overall rise in value under Marissa Mayer, Yahoo's poor security practices cost them the trust of their users, and heavy financial penalties leading up to the sale to Verizon for a small fraction of its highest market value.

Pandora's box has been opened, and it's unlikely that a new approach could (or even should) supplant the data-driven model of the internet today. Instead, the best companies are realizing that a quality, dedicated security team will be the difference that makes or breaks companies in the long-term. Protecting users and their privacy is becoming a top-tier topic - from boardrooms to engineering stand-ups - as teams prioritize security and data privacy. Just as a strong data team in the last few years was the competitive advantage in understanding and building amazing features, the businesses that will thrive in the years to come will invest in earning the trust of their users.



Source: ISACA and Cybersecurity Ventures Jobs Report

Securing the privacy of our infrastructure, data, and services is one of the defining issues of our time. It's a technical and ethical challenge that touches every aspect of our digital experience. The future of the internet hinges on a new generation of talented and thoughtful security professionals that are deeply dedicated to earning the trust of their users. We must build trust back into our digital lives, or risk the incredible developments of the technologies and services we've built in the past several decades.

New Solutions to New Challenges

While security has always been a challenging field, a number of new developments have forced security engineers to leverage new cutting-edge tools. To meet the needs of customers, teams are utilizing cloud computing, automation, microservices, and container orchestration, which require a qualitatively different approach to security. Long gone are the days when security meant patching software and locking down the network on a single host.

At the same time, advances in data science and machine learning have given a new set of tools to defenders and attackers alike. A single bad actor can leverage widely available tools to take advantage of teams that are unable (or unwilling) to defend their services. Today's security engineers and analysts need to secure the contemporary tech stack, and use a growing set of advanced technologies, like machine learning and data warehouses, to be effective. Specialized startups are emerging to offer security as a service to help smaller startups and enterprises that don't have the internal capacity to defend their data and users.

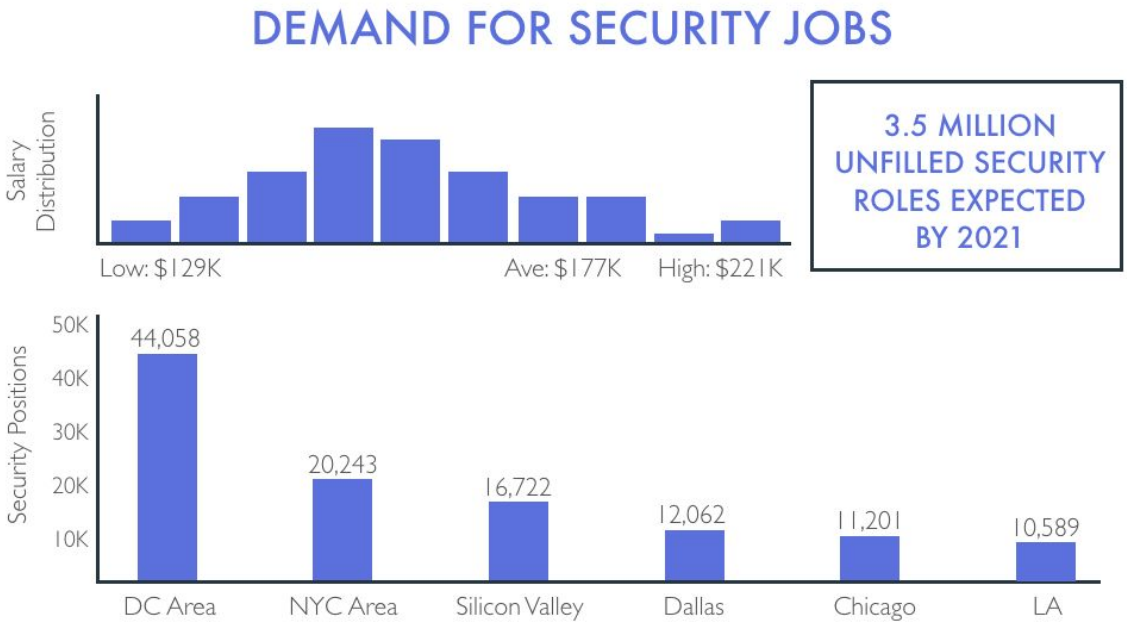
While some engineering teams, in domains like health care and finance, have always worked with data privacy regulations like HIPAA, new regulations like the EU's GDPR and California's CCPA have spurred a movement across the entire industry. These new laws aim to protect users by enforcing fundamental user rights like the ability to delete their data, restricting data access to only those who need it, and the timely removal of older data.

Source: Wall Street Journal and Forrester Research

This has led to new teams within engineering organizations that are dedicated to data privacy and the ethical stewardship of their users' data. These teams ensure that every engineer at their company has the knowledge and tools to build services with data privacy at the forefront. There's often an engineering tradeoff between the easiest way to build a system and what is right for users. Data privacy teams now exist to offset that tradeoff by providing tools that make data privacy easier for everyone.

Beyond preventing data breaches or unwanted access to data, teams are also facing new ethical dilemmas on how to use data. Without careful and thoughtful consideration, algorithms and recommendation systems can inappropriately discriminate against people, risking unintended and damaging effects on their users. Even when data about protected classes are removed before processing, historical biases and problematic issues can persist in the hidden, uninterpretable parameters of the algorithms. These problems are nuanced, and a true solution requires a deep understanding of both data and ethics. To earn the trust of all users, data teams must thoughtfully collaborate with leaders in policy and diversity, as well as the communities they serve.

The need for this advanced set of skills in the field has only exacerbated the shortage of talented security professionals. For years, organizations have tried to invest more in security, only to face a lack of qualified engineers and analysts. Despite urgent calls for more education and training from leaders - from computer science leaders to Fortune 500 executives to the White House - the demand has far outpaced the supply. The mismatch in skills is sharpest in the security roles that require advanced engineering, data, and analytical skills on top of security domain expertise.



The demand for security engineers and analysts has far outpaced the supply of qualified candidates, leading to an average salary over $175,000 in Silicon Valley. Industry experts predict that the shortage will grow to 3.5 million open roles by 2021.
Source: NIST's CyberSeek report, Cybersecurity Ventures job report, and Glassdoor.

This shortage has disproportionately affected the “long tail" of institutions with less access to technical resources, even though many of them still need to protect their users and sensitive data. Unfortunately, this has turned the issue of security into a luxury that most of the world's services, and thus most of the global population, can't afford. Security and data privacy need to be democratized as a service that every person can depend on. Trust should extend to every corner of the world that the internet reaches, including those with governments that don't share a high standard of privacy for their citizens.

But for that to happen, we need to foster a new generation of security engineers and analysts with the necessary expertise and dedication to earn the trust of users. This is the mission of the Insight Security Fellows program.

The Insight Fellowship

In 2012, Insight developed a new model for education: we bring together smart, hard-working, and enthusiastic engineers and scientists who have strong fundamental skills, and enable them to make the transition into a specialized and technical field by gaining hands-on experience with the tools and practices of industry. They learn by building real-world tools, and engage with an extensive network of industry mentors.

Gain Experience through Hands-on Projects

Every Fellow who completes the program will come out of the 7-weeks with strong security fundamentals like penetration testing, networking protocols, software and systems engineering, identity access management and malware defense. Additionally, each Fellow gains an advanced specialization in security by completing a substantial project during the course of the program. These projects are designed to contribute meaningful new features, applications, or technologies for the security ecosystem. Fellows pursue projects that ignite their passion in a self-directed setting, supported by the infrastructure, mentoring, and technical expertise provided by Insight.

The projects vary widely in scope, interacting with different facets and roles in the security and data privacy ecosystem. During project development, Fellows will:

Secure the contemporary tech stack Detect and prevent security vulnerabilities in an interconnected framework that leverages cloud infrastructure, automation, microservices and container orchestration.

Build user-level encryption Design and build distributed data pipelines that enable users to remove their personal encryption keys in a single click, effectively removing access to their data, unless they choose to restore access in the future.

Establish fine-grained "right to be forgotten" Deploy data products and platforms that give users flexible control of their data retention policies, leverage cutting-edge developments like ephemeral encryption keys that automatically enforce data expiration.

End phishing attacks Build services to catch and mitigate the impact of phishing and social engineering attacks by detecting anomalies in user behavior. Contribute to the progress toward ending these damaging attacks, much as we've nearly solved the problem of spam.

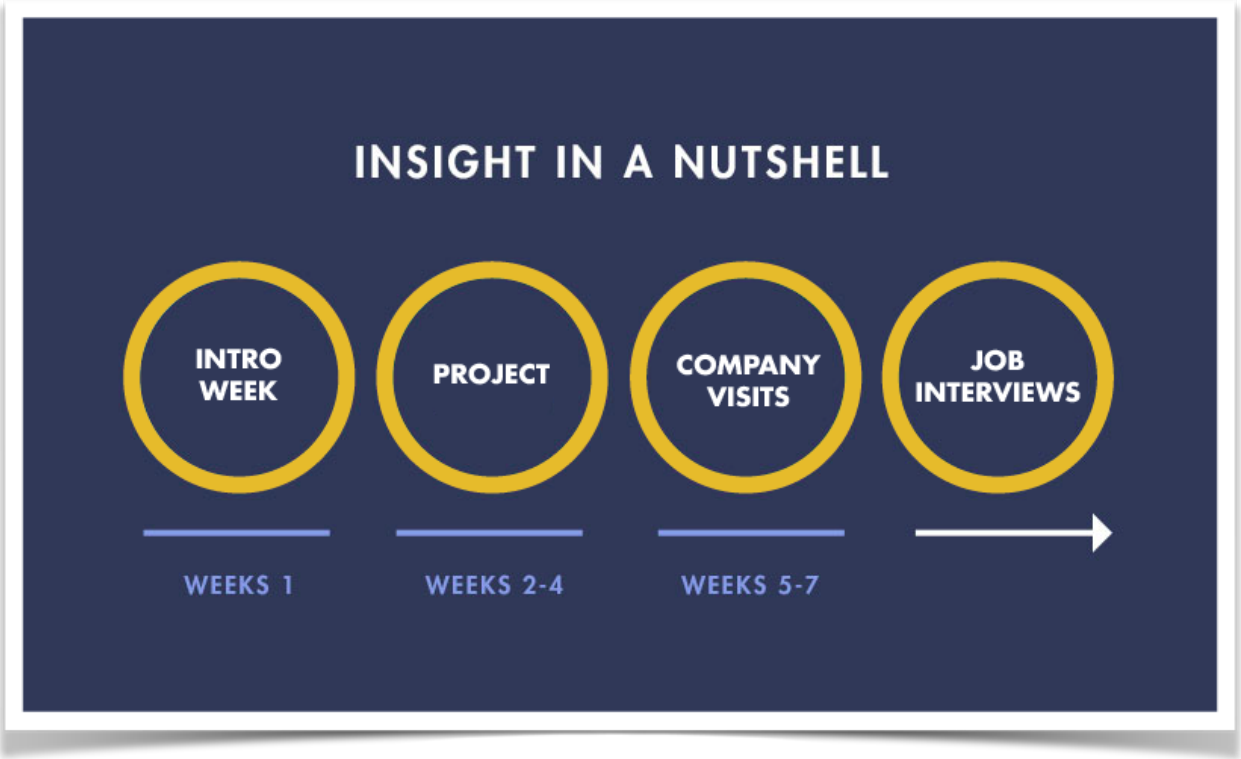
Stop abuse of APIs and websites Develop methods to detect inappropriate behavior like website scraping and API abuse. Apply security forensics at the scale of the most popular services, with hundreds of millions of users.

Prevent eavesdropping on data Leverage new advances like differential privacy and homomorphic encryption to process data for users. These cutting-edge techniques can generate aggregated results while minimizing access to individual data points. Ideally, algorithms can benefit users without anyone (including the data teams, companies, or states with access to the infrastructure) having access to the underlying raw data.

Integrate security into deployments Build security audits into continuous integration so engineers don't deploy code that introduces known vulnerabilities, SQL injection issues, or exposes personally identifiable information. Data privacy and security should be as important as quality code.

Weekly Breakdown of the Program

- **Week 1: Plan the vision** - Learn the security and data privacy landscape, and draft the roadmap to guide your Insight project.
- **Week 2: MVP** - Build a minimum viable product to prototype your project.
- **Week 3: Enhancement** - Iterate the MVP into a functional feature or system, taking into account scaling and deployment considerations.
- **Week 4: Finishing touches** - Complete documentation and your final security improvements. Projects undergo peer review and external security audits by top Silicon Valley partners.
- **Week 5: Professional development** - Polish your project presentation while learning how to optimize your project and integration with new teams.
- **Weeks 6-7: Interview preparation** - Present your project to the teams that you're most excited to work with, and begin preparing for the interviews that will follow.
- **Week 8+: Interview** - Interview with top companies, and join a top security team in Silicon Valley.



Who are the Best Fellows?

The most effective security professionals have a personal drive to secure the internet and protect the privacy of users. They have a passion for understanding the ins and outs of systems, thinking about all failure modes, and then building novel solutions to close vulnerabilities. Although relevant knowledge and nimble technical skills are a general prerequisite for the program, we are looking for Fellows who are extremely curious, highly motivated, love learning across a wide range of fields, enjoy collaborating with other driven colleagues, and are excited about the opportunity to help make a more private and secure world.

The field of security is like a chess match, but the stakes are the most critical parts of a company: the system's infrastructure, the data used to improve services, and the trust of users. But there isn't a set of known pieces on a fixed 8x8 grid - it's an ever-evolving environment, matched up against a series of opponents that are constantly looking for paths to checkmate. The best Fellows will enjoy this type of match, staying several moves ahead of a worthy adversary while considering any missteps.

The field of security requires a unique personality that differs from other technical roles. You must stay calm in difficult situations, plan for the worst while continuing to see the best in people, and understand the importance of collaboration. The only hope of defending against a group of malicious actors is to work on a productive team that is greater than the sum of its parts, and this requires a truly collaborative personality.

There are many paths to Insight, and we're excited to consider any innovative and

knowledgeable applicant, regardless of their background. Successful Fellows may relate to profiles such as:

Systems and Operations Engineers You are an engineer with a knack for systems and a passion to understand how the world works. You're eager to leverage your experience with networking, IT and ops best practices in the domain of security.

Software Engineers You are a general engineer or developer with a passion for security and data privacy. You've worked with production systems, seen security challenges first-hand, and are looking to specialize in this area.

Data Analysts You're an analyst with experience in data and security. You've analyzed data and have experience with scripting, but are looking to learn engineering and security best practices to apply your current skills to security analysis.

Who's involved?

The Insight Security Fellows Program is a professional training fellowship that bridges the gap between engineers and security professionals. We are connecting accomplished Fellows with some of the most innovative companies in the world. Mentors, alumni, and hiring teams for the Insight Security Fellows Program are leaders from:

Collaboration and Mentorship

Though each Fellow will manage their own project based upon their individual interests and abilities, the strength of Insight is rooted in a collaborative environment. Fellows accelerate their learning by working together to solve common problems, and by leveraging the diverse backgrounds of one another and the Insight network. Mentorship comes from the following sources:

- **Company Mentors** - You'll learn about the pain points encountered by teams from leading projects with varying styles, sizes, and sectors. You'll become familiarized with the field's contemporary challenges, and decide which types of teams you want to join.
- **Industry and Project Leaders** - Pioneers at the forefront of the security industry help you learn the best practices and newest tools in the space.

- **Your fellow Fellows** - Grow as part of a team of ambitious software engineers, systems engineers, information technology specialists, and data analysts who share common goals and wield a diverse set of skills to complement and sharpen yours. You will help each other learn by collaborating and working through challenges with your peers in an environment that reflects industrial workspaces and teams.
- **Insight Alumni** - Previous Fellows from our Data Science, Data Engineering, Artificial Intelligence, Health Data Science, DevOps Engineering, Data Product Management, and Decentralized Consensus programs have developed experience in this field, and they provide individualized project guidance and interview practice.
- **Insight Team** - The Insight team offers continuous guidance throughout the entire process. They will help you develop and iterate your ideas, and facilitate your access to the resources and expertise necessary to succeed.

Responsibilities

As an Insight Fellow, you're given the opportunity to learn from the best teams and experts for seven weeks. The program is designed to remove as many obstacles as possible that stand between where you are now, and becoming a successful security professional. However, these benefits come with a few responsibilities:

- Actively and thoughtfully contribute to group activities and sessions during program hours, Mon-Fri from 10AM-6PM. Some days, you will need to stay for mentor and company visits ending as late as 8 or 9PM.
- Take a leave of absence, if applicable, from your current responsibilities (e.g. current employment or studies) in order to participate at Insight. Both the 7-week portion and the subsequent interview process require full-time focus.
- Commit to self-directed learning, tackling a challenging project during the program while giving and receiving constructive feedback.
- Interview for full-time security positions with Insight partners in Silicon Valley upon completion of the program.
- Plan to continue coming into the office during the interview weeks (even when not interviewing) to participate in interview prep sessions with other Fellows.
- Support future Fellows by providing mentorship and guidance once you become a leader in the field.

The guiding principle of Insight is *Fellows first*. We strive to create an environment where you can learn and develop a thriving career in the field of security. In return, we ask that you are fully engaged in the process, and help pass your learning on to future Fellows through alumni mentoring - continuing to make the Insight community stronger.

Benefits

The Insight program is designed to provide all the training, resources, and connections you'll need to effectively transition to a career in security. Here are some of the benefits of becoming an Insight Fellow:

- Guidance and mentorship from industry professionals at every stage of the program, and as you prepare for interviews.
- Fellows pay nothing to participate in the program, thanks to full-tuition scholarships covered by top hiring teams.
- Additional loans and need-based scholarships are also available to help cover living and travel expenses -- our goal is to make sure everyone with the right skills can participate in Insight, regardless of their current financial situation.
- Mentorship from Insight alumni whose experience, at Insight and in their current industry roles, makes them a vital resource for guidance and feedback.
- Personalized matching with top projects and leading companies. We help you figure out which organizations will provide a high-quality fit for you, based on our experience and in-depth conversations with the hiring managers.
- Help navigating the negotiation of final employment terms when companies make you full-time offers.
- Desk space during the program at Insight's headquarter office in Silicon Valley, with full-time access to a library of relevant resources.
- Dedicated cloud computing resources for you to build and maintain your product for the duration of the program.
- Advice from our local staff to help you plan your living arrangements for the duration of the program.
- Perhaps most importantly: an unparalleled professional network of security engineers, data scientists, data engineers, ML engineers, AI researchers, product managers, founders, friends, and acquaintances. Through the program, you will meet and get to know top engineers and scientists who are Insight mentors and alumni, all of whom will be your industry peers. These professional contacts will be an invaluable source of knowledge, advice, career opportunities, and friendship in the years to come.

Applications

Applications are currently open on our website for the first start date of the Insight Security Fellows Program on Monday, September 9th, 2019. We expect high demand, so we encourage you to apply soon for an early decision. If you have any questions please email us at info@insightdatascience.com

To start your application today, visit: https://apply.insightdatascience.com/start