SANS

The most trusted source for cybersecurity training, certifications, degrees, and research

GIAC CERTIFICATIONS

SANS 2020

Cybersecurity Workforce Development Solutions Catalog

Recruit. Retain. Develop.

- 65+ Training Courses
- 35+ GIAC Certifications
- Aptitude & Skills Assessments
- 8+ Accredited Degree/Certificate Programs

Why Cybersecurity Workforce Development Matters

There are times in history when the demand for professionals with certain skills is high, but the current supply of people with such skills cannot meet it. We currently face such a talent shortage in cybersecurity—and on a global scale. A cybersecurity workforce development plan gives organizations a roadmap for preparing employees with the skills that are in demand, planning for ongoing education/training, and addressing future hiring demands.

The SANS Workforce Development catalog is a resource designed to help you build a strong workforce development plan for your organization. From talent pipeline development through recruiting, to building a cybersecurity team and retention, SANS is your one-stop partner for cybersecurity workforce development solutions.

We are here to help!

Contact your account manager today or email workdev@sans.org to connect with an account manager who can help you create a custom workforce development program for your organization.

SANS has put together a series of free resources on Workforce Development to assist Human Resources (HR), Talent Acquisition, and Recruiting professionals with hiring and retention of cybersecurity personnel. The goal is to provide workforce development managers a community where they can share best practices and will include resources such as private forums, webcasts, posters, and case studies.

In this brochure, you will learn about the following:

For more information, contact workdev@sans.org

SANS Cyber Workforce Development Solutions

For over 30 years, the SANS Institute has been providing intensive immersion training designed to help cybersecurity professionals master the practical steps necessary to defend systems and networks. SANS technical training courses are full of important and immediately useful techniques you can put to work as soon as you return to your office. All SANS courses are developed through a consensus process involving hundreds of administrators, security managers, and information security professionals, and address both security fundamentals and awareness, as well as the in-depth technical aspects of the most crucial areas of IT security.

SANS has helped design and implement workforce development programs for Fortune 500 companies, government agencies, and organizations of all sizes. From recruiting and identifying talent to training your existing teams and providing industry-leading cybersecurity certifications via Global Information Assurance Certification (GIAC), SANS ensures that employees are ready to work on day one.

Implement proven workforce development strategies designed to meet your organization's needs on your schedule.

Validation of Your Security Team's Skills to Clients and Stakeholders

- Justify the cybersecurity skills of your workforce
- Increase opportunities for sales engineers, consultants, and partners

Protecting the Organization's Assets and Intellectual Property

- Protect your customers and brand
- SANS is a trusted training partner of organizations serious about security

Meeting Regulatory Compliance and Risk Protection from Attacks

- Protect citizens and partner nations
- SANS/GIAC credentials are part of the Department of Defense 8140 mandate, which is a requirement for personnel who touch critical systems

Efficiency and Effectiveness of Your Security Teams

- Ensure your security teams can handle security challenges with confidence
- Result: SANS training is a great retention tool for keeping your cybersecurity talent engaged and challenged

Our Workforce Development Solutions Include:

| Aptitude & Skills Assessments | Cyber Immersion Academies | Skills Validation with GIAC Certifications | Over 65 Hands-on Training Courses, Accredited Degree and Certificate Programs |

Why SANS?

100 **OF THE** **FORTUNE 100**
employ cybersecurity professionals **trained by SANS**

Programs reach more than **200,000 SECURITY PROFESSIONALS** **around the world**

Courses available **in over 100 cities** **WORLDWIDE** **or ONLINE**

50,000+ professionals trained each year, **globally**

117,000+ **CERTIFICATIONS ISSUED**

Popular Cybersecurity Career Paths

The extreme shortage of cybersecurity talent has forced companies to take a more creative approach to finding talent. Based on proven programs like the Cyber Immersion Academies (see page 8), SANS has created a training roadmap to help organizations build the cybersecurity skills they need. Below is a sampling of cybersecurity jobs mapped to the courses and certifications necessary to perform these roles. Find more cybersecurity job roles by emailing workdev@sans.org.

Security Analyst

The security analyst role is an entry-level technical position focusing on planning and carrying out security measures to protect an organization's computer networks and systems.

Cyber Leader/Security Manager
NICE Framework Job Role – OV-MGT-001, OV-EXL-001

While still technologists, today's CISOs and other cyber leaders must have business acumen, communication skills, and process-oriented thinking. They need to connect legal, regulatory, and local organizational requirements with risk taking, financial constraints, and technological adoption.

Pen Tester/Exploitation Analyst

This security expert finds security vulnerabilities in target systems, networks, and applications in order to help enterprises improve their security. By identifying which flaws can be exploited to cause business risk, the pen tester provides crucial insights into the most pressing issues and suggests how to prioritize security resources. SANS.edu offers a graduate certificate program in Penetration Testing & Ethical Hacking.

Cyber Defense Operator

A cyber defense operator defends and secures information assets and business systems at an organization. Because traditional counter defenses are no longer effective in stopping malware, viruses, and other advanced attacks, it is a forgone conclusion that targeted organizations will be compromised. Therefore, proactive and layered defensive tactics are needed to stop the adversary and to defend the enterprise. SANS.edu offers a graduate certificate program in Cyber Defense Operations.

Cyber Crime Investigators/Incident Responder

Crime investigators include both "sworn" law enforcement officers and "un-sworn" employees of departments who are dedicated information security investigators. Both are entrusted with the preservation, acquisition, storage, detailed analysis, and clear reporting of digital evidence from many sources. Incident Responders can identify and respond to incidents before they are discovered by clients or customers. SANS.edu offers a graduate certificate program in incident response.

ICS/SCADA Security Engineers

Industrial control systems/supervisory control and data acquisition (ICS/SCADA) security engineers are empowered to understand networked industrial control system environments, monitor them for threats, perform incident response against identified threats, and use knowledge gained from interactions with the adversary to enhance network security and maintain the safety and reliability of operations. SANS.edu offers a graduate certificate program in industrial control systems security.

For more information, contact workdev@sans.org

Identifying New Cyber Talent

When you can't find candidates with the right skills, consider developing the talent you need either from existing employees or from candidates not currently working in cybersecurity. It's not as difficult as it sounds, and there are proven reskilling strategies to guide you along the way. Below are benefits of developing and identifying new, high-potential talent.

Benefits of Developing Your Own Cyber Talent

For Existing Employees:
- Provide a new career opportunity
- Decrease time educating a new employee about the company and policies
- Already a good fit culturally
- Create a deeper sense of loyalty, a benefit for retention

For External Hires:
- Develop specific skills for your organization
- Opportunity to hire a good cultural fit
- Candidate brings expertise and knowledge from another field that can be applied to the new role
- Create a sense of loyalty, a benefit for retention

Students and non-cyber professionals across industries have talent and potential they have yet to discover. Aptitude tools, Capture the Flag exercises, CyberStart, and other competitions are helping young adults and career changers discover their passion and innate aptitude for cybersecurity. Competitions are a unique way of providing participants with a glimpse of what it's like to actually work in cybersecurity while providing an interactive and engaging experience.

A proven method to identify hidden, high-potential cybersecurity talent is through assessment tools. SANS Aptitude assessments have successfully identified thousands of individuals with high potential for success in cybersecurity training programs and ultimately in securing cybersecurity jobs. Learn more about the Assessments on page 10.

Whatever method you use for identifying talent, make sure to set real expectations for your organization and the participants. Once you've found qualified candidates, it's time to get them the hands-on skills and certifications they need for their new career!

"The SANS Institute is renowned and respected for its world-class cyber training. CACI is pleased to team with SANS on this critical workforce development initiative, which will help fill a pressing need for cybersecurity experts in industry and government."

–MIKE MOURELATOS, CACI VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER OF NATIONAL SERVICES

CyberStart Programs and Tools

cyberstart

- **High Schools:** Girls Go CyberStart had 6,647 girls participate in 2018 and over 10,300 girls participate in 2019. Girls Go CyberStart 2020 opened in January 2020.
- **College Students:** Cyber FastTrack had 3,514 participants in 2017 and 10,335 participants in 2019. Over 33% of the registered players in Cyber FastTrack 2019 were female.

CyberStart is an exciting suite of tools aimed at changing the face of cybersecurity for today's young people, presenting it as an engaging and accessible employment option, while also helping government organizations to develop new talent in support of their national cybersecurity capabilities.

CyberStart tools are modular and can be implemented in combinations tailored to an organization's individual needs and requirements, whether they are looking to raise awareness of cybersecurity or inspire the next generation of cybersecurity experts.

Among the elements that SANS offers are:
- Pre-Selection Challenges
- CyberStart Workshops
- Online Game Capabilities
- Capture the Flag Competitions

> **"Many of the girls at my school who participated in Girls Go CyberStart are now interested in looking into cybersecurity for a career. This contest gave them the "why" and the "how to use this knowledge" that they needed to get them extremely excited about computer science.**
>
> **–JEFF, HIGH SCHOOL TEACHER**

SANS has applied gamification principles and game-design techniques in developing CyberStart. The challenges are accessible to those without any pre-existing cybersecurity knowledge and can span various age, difficulty, and skill levels, depending on requirements. The challenges provide context of the day-to-day activities of the modern cybersecurity professional through engaging narratives, tackling everything from Linux to cryptography and programming to forensics.

Help us spark cybersecurity interest for young adults by supporting a SANS CyberStart competition or hosting a program within your organization to attract internal talent to fill the skills gap.

Interested?
Contact cyberstart@sans.org to learn more about the new SANS CyberStart programs (including national competitions) and ways to increase your organization's community and recruitment efforts!

> **"I had no idea what cybersecurity was but after the first few Girls Go CyberStart challenges, I was hooked. Whenever I had a free moment, I was working towards the goal of solving as many challenges as possible. I did not get as far as some of the other girls, but I had so much fun that I realized I had developed a strong interest in cybersecurity—so much so that I would want to go to college for it."**
> **–JADA, HIGH SCHOOL STUDENT**

Cyber Immersion Academies

The Cyber Immersion Academies are a set of immersive training programs that produce high-quality cybersecurity professionals ready to enter information security roles immediately upon graduation. The Academies provide advanced technical training, industry-recognized certifications, and connections to jobs in cybersecurity. The Academies are 100% scholarship-based for qualified participants with an aptitude for cybersecurity who are looking to enter the field.

Academy students come from diverse backgrounds and experiences outside of cybersecurity. Applicants are screened by an aptitude assessment and personal interviews, and only the top candidates are admitted. Once accepted into the program, students begin their training with either CyberStart Essentials or SEC401: SANS Security Essentials Bootcamp Style and GIAC Security Essentials Certification (GSEC). Depending on the type of Immersion Academy, students may take up to three SANS courses and earn the associated GIAC Certifications. Students in the Academy are grouped in cohorts with an assigned mentor, who is a subject matter expert (SME). The mentor and students collaborate to discuss best practices, challenges, and more in terms of cybersecurity tools, certification preparation, hands-on labs, etc. A SANS career placement coordinator also works with students throughout the program to prepare them for the job search and success in employment once they find a position.

Types of Immersion Academies

- VetSuccess Academy
- Women's Immersion Academy
- Diversity Cyber Academy
- Cyber Workforce Academy
- Cyber Reskilling Academy

Ways to Participate

- Create a custom Academy or reskilling program for your organization
- Hire Academy graduates to fill your cybersecurity jobs
- Sponsor Cyber Immersion Academy students
- Please contact cybertalent@sans.org to learn more about engaging these programs!

Employer Benefits

- Access to pre-screened candidates and highly trained, GIAC-certified graduates
- The opportunity to support veterans and diversity in the InfoSec industry
- Create a cybersecurity-focused workforce development or reskilling program specific to your organization's needs

"The Women's Immersion Academy graduate we hired joined the BB&T Cyber Threat Management team and had an immediate positive impact. She has quickly garnered the respect of her teammates, as she is able to apply the skills acquired through the SANS Women's Immersion Academy daily to the benefit of BB&T."
—HARTWELL WATKINS, VP, MANAGER, CYBER THREAT OPERATIONS CENTER AND THREAT INTELLIGENCE, BB&T

Success Stories

Federal Cyber Reskilling Academy

The Federal Cyber Reskilling Academy (FCRA) is an innovative program that offered Federal employees the opportunity for hands-on training in cybersecurity. This reskilling effort was part of the Administration's commitment to developing a Federal workforce of the 21st century, as outlined in the President's Management Agenda and the recent Government Reform Plan. Through a strategic partnership comprising the U.S. Department of Education, the Office of Management and Budget, and the CIO Council, the program launched in November 2018.

The FCRA identified employees within the U.S. government who had never worked in IT but who had high aptitude and a passion for cybersecurity, and then provided training to allow them to master core skills so they can transition into vacant technical cybersecurity positions within the government. The FCRA achieved the following:

- Over 1,500 people applied for the first cohort. All eligible applicants were then invited to take take the SANS CyberTalent Aptitude Assessment.
- 30 individuals were selected to take part in the immersive three-month training program.
- All 30 completed the foundational training course, SANS CyberStart Essentials.
- 29 participants completed the SEC401 course, with an extraordinary 96% success rate on the GSEC certification.
- 28 participants completed the SEC504 course, with an extraordinary 93% success rate on the GCIH certification.

The FCRA successfully demonstrated the ability to reskill employees into cybersecurity professionals by identifying hidden internal talent—specifically employees who had no formal IT training or work experience. It made a measurable increase in cybersecurity workforce development and can serve as a model for other organizations.

Cyber Immersion Academy Graduates

- **Hannah McDaniels** is a retired U.S. Air Force Captain and was laid off from her HR role prior to enrolling in the SANS Women's Academy. She excelled in her courses, earning the GSEC, GCIH, and GCFE certifications, leading to her former employer rehiring her as a Lead IT Security Incident Response Analyst.

- **Chris Harper** is a former Army medic who specialized in telemetry and had a lifelong interest in IT. He was accepted into the SANS Cyber Workforce Academy, where he earned both the GSEC and GCIH certifications and then landed a cybersecurity job with an employer partner upon graduation.

- **Serenity Smile** previously worked as an Administrative Assistant and discovered her passion for cybersecurity due to her son's interest in coding and IT. She pursued multiple open source courses prior to acceptance into the Diversity Cyber Academy. She earned the GSEC, GCIH, and GCIA certifications and recently accepted a cybersecurity position with Target.

For more information, please visit sans.org/cybertalent

CyberTalent Assessments

The SANS CyberTalent Assessments include eight online tools that quickly and effectively provide managers the insights they need to:

- Improve their ability to identify the best job candidates
- Develop more effective workforce development plans
- Increase the productivity of training investments

There are currently eight CyberTalent Assessments:

- InfoSec Aptitude
- CyberTalent Enhanced (CTE)
- Cyber Defense
- Penetration Testing
- Digital Forensics
- Application Security
- Industrial Control Systems
- InfoSec Management

Simple and Convenient to Use
Most assessments are 60 minutes in duration

Online Platform
Access assessments results and reporting online. Assessments are valid for 12 months from activation.

How CyberTalent Assessments Improve Talent Management

1 Recruitment
Identify candidates with high potential or advanced skills.

2 Retention
Keep top talent you have. Improve professional development plans.

3 Performance
Maximize organizational effectiveness & workforce development.

Get a Free Demo!
sans.org/cybertalent/free-demo/

"The Cyber Defense tool has been great, and we have used it for almost all of our hires on the Security program we support. Also, we have used it to baseline current employees. So far it has been wonderful."
–MIKE SCHMIDT, TALENT ACQUISITION LEAD, TRIUMPH ENTERPRISES, INC.

Training for Cyber Job Roles and Tasks

SANS offers more than 65 courses that build hands-on skills in security essentials, cloud security, monitoring and detection, security management, secure development, penetration testing, and digital forensics to ensure your cybersecurity team has the right skills for your organization. All of our instructors are active security practitioners, bringing their extensive knowledge and real-world experiences directly to the classroom. Their passion for the topics they teach shines through, making the SANS training experience—both live and online—dynamic and effective. **View our full course catalog at sans.org.**

Degree and Certificate Programs

The SANS Technology Institute offers graduate and undergraduate programs at the cutting edge of cybersecurity. For working professionals, the college offers a Master of Science in Information Security Engineering and job-specific graduate certificate programs in cybersecurity engineering, cyber defense operations, incident response, industrial control systems security, and penetration testing and ethical hacking. The undergraduate certificate in Applied Cybersecurity provides foundational knowledge and skills for college students who want to enter the field and workers seeking to transition into cybersecurity roles.

Incorporate these programs into your organization's tuition reimbursement program to further enhance employee development opportunities. **See all accredited degree programs at sans.edu.**

Skills Validation with GIAC Certifications

GIAC Certifications, known for the highest standard of cybersecurity credentialing, aligns with SANS training and ensures mastery of specific job skills and in-depth abilities across critical focus areas. GIAC-certified professionals validate that they're not only knowledgeable but have actionable skills to get the job done. GIAC exams featuring CyberLive, VM-based practical testing, extend GIAC's dedication to measuring hands-on cybersecurity abilities.

"The decision to take five days away from the office is never easy, but so rarely have I come to the end of a course and had no regret whatsoever. This was one of the most useful weeks of my professional life."
–DAN TRUEMAN, NOVAE PLC

For more information, contact workdev@sans.org

Justifying Workforce Development Investments

Let SANS help you build a workforce development program to fit your organization's goals and budget! Whether it is protecting your organization's infrastructure or meeting regulations, we have a solution. Training is a key element of employee retention, satisfaction, and team morale, especially in a highly competitive marketplace. We can help you create a reskilling program for current employees as well as provide strategies for future hiring needs. According to the Employee and Engagement Survey from the Society for Human Resource Management (SHRM), 40% of employees rated job-specific training as very important to their satisfaction, followed by professional development at 36%.

Our team of training portfolio advisors will help you get the best return on a workforce development plan. Below are a few best practices leading organizations are using to justify the expense of developing a cybersecurity talent roadmap.

Business Development Budgets

Security is often looked at as a cost, but it can also be utilized to bring in revenue. Investing in security training and certification for your team as you do infrastructure builds a strong security posture and provides confidence among your partners and clients. Examples where skills validation through SANS training and GIAC Certifications can bring revenue to the organization include:

- **Project Bids** – GIAC Certifications separate your organization from the competition by demonstrating your commitment to security and privacy.
- **Sales Job Roles** – GIAC Certifications validate the skills of your sales engineers and other client-facing positions.
- **Consultants** – GIAC Certifications validate the skills of your cybersecurity team members and instill clients' confidence.
- **Tech Channel Partners** – SANS training validates the cybersecurity skills of your affiliates. Open doors of opportunity knowing that your channel partners are endorsed with the high-level skills your clients require, reducing the risk of high-visibility breaches.

Tuition Reimbursement

If your organization offers tuition reimbursement for employees, these funds can be used to create a reskilling plan. Employee benefits may be a tax benefit for the employer while helping retain top talent. Some employers require that these benefits go through an accredited body. The SANS Technology Institute can meet such requirements with our Master's Degree, Undergraduate, or Graduate Certificate Programs. SANS Technology Institute is accredited through The Middle States Commission on Higher Education (sans.edu).

"SANS courses were selected due to their overlap with our core business, and because they offer the biggest "bang" for our buck when it comes to developing new employees quickly."
–JASON NICKOLA, PULSAR SECURITY

Hiring Budgets

While primarily used for new talent, hiring budgets can also be used to reskill current employees who demonstrate an aptitude in cybersecurity. Retraining employees not only creates a strong sense of loyalty, but it also makes your team more effective and efficient while keeping hiring costs down. Using CyberTalent Assessments during internal and external recruiting can decrease the cost of a bad hire by testing skills and aptitude before you make an offer and investment.

Risk Management Budgets

The Ponemon Institute's 2019 Cost of a Data Breach Report states the global average cost of a data breach is $3.92 million, a 1.5 percent increase from the 2018 study. An estimated 2 million cyber attacks in 2018 resulted in more than $45 billion in losses worldwide as local governments struggled to cope with ransomware and other malicious incidents. Training can save you money and help lower your probability of an attack. While training is not the only means to protect your organization from attacks, without the right talent it is impossible to develop the right processes in protecting your assets. For example, organizations that both formed an incident response team and extensively tested saw a $1.23 million savings over organizations who had neither.

Reskilling/Upskilling Current Staff

- The cost of one new skilled cybersecurity hire is 10–25% of first-year salary or $8,000–$35,000.
- Upskilling two existing staff will likely eliminate one new hire. If you spend $12,000 on training and certification, you may save more than $100,000 for a single hire.
- Reskilling/Upskilling current staff increases talent retention and job satisfaction.

Meeting Regulatory Compliance

Organizations are always getting scrutinized for their cyber risk profile! A perfect example is the DoD's new Cybersecurity Maturity Model Certification (CMMC) Initiative, which requires 100% of all DoD contractors to obtain third-party certifications on cybersecurity compliance. With the transition from self-disclosure to an external auditor to ensure cybersecurity compliance, contractors can expect to see an increase in enforcement litigation for failure to comply with the cybersecurity regulations. We can create training programs that will help your organization become complaint in specific areas and give you peace of mind while saving you from external monetary penalizations.

For more information, contact workdev@sans.org

SANS Cyber Team Seals

In 2020, SANS will introduce SANS Cyber Team Seals. These seals will demonstrate your organization's commitment to protecting data and assets, verify your team has the knowledge and hands-on skills to handle advanced cybersecurity threats, and will set you apart from competitors during the bidding process.

SANS Cyber Team Seals will assure stakeholders that your team has verifiable, hands-on cybersecurity skills. The Team Seals can be included in proposals, bids, stockholder reports, presentations, collateral, and communications, including social media and emails.

SANS Cyber Readiness Team Seal
Validation of Mission Based Security Teams

This seal demonstrates your team's top-notch skills. At least 80% of your team must be GIAC certified to meet the SANS Cyber Readiness Team requirements. Create a training roadmap to build your team's skills and prove to stakeholders that your team has what it takes to protect their assets and manage their projects. Roadmaps are designed by our training advisors and subject matter experts to meet your enterprise goals.

workdev@sans.org

SANS Cyber Immersion Academy Seal
Building the Next Generation of Cybersecurity Professionals

The SANS Cyber Immersion Academy Seal is for organizations that develop their own internal employees, recruit new professionals, and encourage diversity within their organization. This seal designates an organization's commitment to clients, cybersecurity, and their employees.

sans.org/cybertalent

Contact workdev@sans.org to learn
more about the SANS Cyber Team Seals!

How We Can Help Your Organization

SANS has a series of training advisors ready to help build your customized workforce development program and meet your organization's goals. We are here to research your past efforts, learn your goals/pain points, and utilize best practices within the cybersecurity training, certification, and higher education industries. As the global leader in cybersecurity workforce development, only SANS can offer such a full suite of workforce development solutions from assessments to validation through our GIAC Certifications and SANS.edu degree programs. By leveraging practitioners within cybersecurity, we understand what is needed in the real world, including the skills needed to meet your organizational goals.

Our training advisors are supported by our subject matter experts internally and the SANS faculty in their specialized skill domains. We can offer detailed course descriptions along with demos to make sure we are building a program that meets your organizational goals. We also have a program management system to track your investment and each student's training journey. As your workforce development partner, we offer value add-ons including webcasts, posters, product solutions, a community forum, free content, and access to subject matter experts.

Five Ways to Partner with SANS for Workforce Development Solutions

1 Suite of Workforce Development solutions – Aptitude & Skills Assessments, 65+ courses, 35+ GIAC Certifications

2 A Program Management system to track your investment and student's training journey

3 Provide Managerial Value Adds – access to faculty, forums, and leadership content

4 Organizational Value Adds – premier access, key client benefits, free tools, and content

5 Mapping job tasks using best practices learned from organizational roadmaps, Academies, and industry-leading cybersecurity schools

Our goal is to give you the best return on your workforce development investment.

"SANS training is a central pillar of our training paths for both new and seasoned employees, and I have no doubt that it will remain so moving forward."
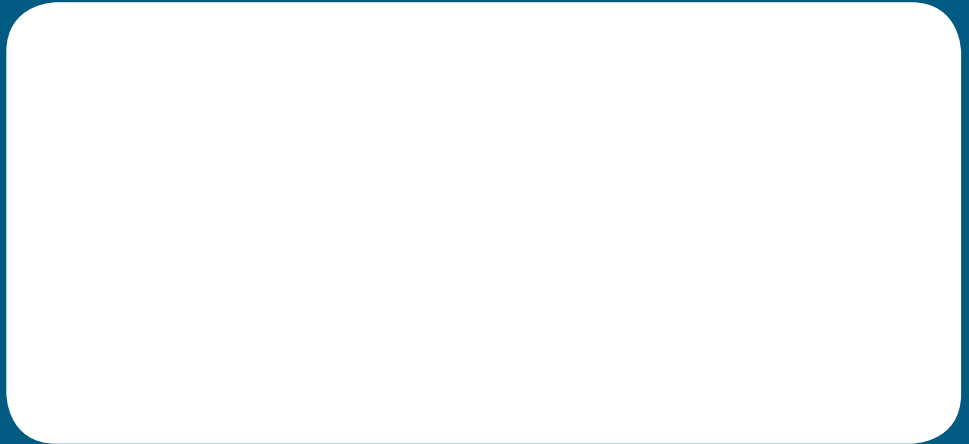–JASON NICKOLA, PULSAR SECURITY

For more information, contact workdev@sans.org

SANS

5705 Salem Run Blvd.
Suite 105
Fredericksburg, VA 22407

The most trusted source for cybersecurity training, certifications, degrees, and research

AFCEA
Corporate Member

As the leading provider of information defense, security and intelligence training to military government, and industry groups, the SANS institute is proud to be a Corporate Member of the AFCEA community

Resources for CyberTalent Managers
For more information, contact **workdev@sans.org**.

SANS has put together a series of free resources on Workforce Development to help Human Resources, Talent Acquisition, and Recruiting professionals with the hiring and retention of cybersecurity personnel. Our mission is to provide CyberTalent Managers a home where they can talk and share best practices amongst each other. Some of those free resources include:
- Webcasts, Posters, Case Studies
- Private Community Forum for CyberTalent Managers to Connect with Each Other
- Examples: Checklist of Job Roles, Hire/Retain for a SOC, Privacy Info

Join the **SANS** community to enjoy **exclusive resources.**
Go to **sans.org/join** to sign up today!

Newsletters

NewsBites
Twice weekly summary of the important news relevant to cybersecurity professionals

OUCH!
Security awareness newsletter for the everyday computer user

@Risk
A reliable weekly summary of exploits, attacks, and information on newly discovered vulnerabilities

Webcasts

Ask The Experts
Current and timely on relevant topics

Analyst
Whitepaper and survey results

What Works
Experiences on resolving specific security issues

Tool Talks
Commercial talks can be utilized to solve real-world security problems

Other Resources

- Infosec Reading Room
- Top 25 Software Errors
- 20 Critical Controls
- Security Policies
- Security Posters
- Intrusion Detection FAQs
- Security Glossary
- 20 Coolest Careers