Contact Sales

# SANS Difference Maker Awards 2020

People and organizations who made a difference in security in 2020.

There is no shortage of publicity around failures in security - constant headlines detailing breaches and vulnerabilities at companies and government agencies. However, what you never hear about are the many organizations who aren't in the news because they have found ways to meet business and mission needs while protecting customer and business data from attackers. There are thousands of security practitioners out there who are quietly succeeding and making breakthroughs in advancing security.

On December 17, 2020, SANS Institute, the global leader in cyber security training and certifications, announced the winners of the SANS 2020 Difference Makers Awards. This prestigious annual awards program honors individuals, teams and groups in the cybersecurity community who have made a measurable and significant difference in security. Through their implementation of security processes or technology, each person has raised the bar in enabling secure business operations and reducing risk.

"In a very challenging year, the 2020 winners are a very diverse group that have used their skills and hard work to overcome obstacles and collectively make the world a safer place," said John Pescatore, SANS Director of Emerging Security Trends. "The Difference Makers range from individual contributors to teams of people, from a Secretary of State to a Biotechnology Threat Focus team to a supply chain security program lead. The common denominator was their willingness and ability to do what SANS calls 'Fight the good fight' in advancing the state of practice in cybersecurity."

Winners will be honored during a virtual awards ceremony on Thursday, December 17, during the SANS 2020 Cyber Defense Initiative online training event. The webcast celebrating the award winners is open to the public - register at https://www.sans.org/webcasts/2020-difference-makers-awards-ceremony-117154 and attend to learn what made their accomplishments so special.

The SANS 2020 Difference Makers Award winners are:

**Frank LaRose, Secretary of State of Ohio**
During these challenging times, Frank LaRose played a proactive and pivotal role in ensuring that election security was a top priority across Ohio. He authorized a statewide rollout of Albert, the MultiState ISAC network monitoring and managing service on-premise for Ohio's Election systems. Frank was part of the team that mandated the CIS Controls be adopted across all County & Elections entities.

**Margaret Latimer, Vice President/Provost -Germantown Campus
and Collegewide STEM Unit at Montgomery College, and Dr. Sanjay Rai,
Senior Vice President for Academic Affairs at Montgomery College**

Montgomery College changed the game for high school and community college students who seek to enter the cybersecurity profession. Their new program, Bachelor of Professional Studies in Applied Cybersecurity (BACS), provides an assured pathway for talented students to launch their careers in cybersecurity.

Margaret Latimer (with the help of previous SANS Difference Maker Joe Roundy) created the program at Montgomery College. Dr. Lai saw the benefits that could be realized and provided critical support from the top, assuring the success of this innovative program.

**Katie Nickels, Director of Intelligence at Red Canary and SANS instructor**

Katie Nickels is a growing leader in the cybersecurity community. Not only is she highly skilled technically, she also has extremely strong communication skills and is dedicated to helping the community. She was one of the principal developers behind the MITRE ATT&CK(R) model, and she is the Program Manager for the Cyberjutsu Girls Academy.

**Jamie Williams, Lead Cyber Adversarial Engineer at MITRE**

Jamie was instrumental in development of sub techniques for the MITRE ATT&CK(R) knowledgebase and has also been a core member of the ATT&CK Evaluations team. Both efforts have been widely used by thousands of cybersecurity professionals to reduce time to detect/respond/restore as well as identify and close gaps in security controls.

**Carrie Roberts, Dynamic Defense Engineer at Walmart**

Carrie Roberts is a highly skilled blue teamer at Walmart and a maintainer of the Atomic Red Team framework, which has been instrumental in helping teams adopt ATT&CK. She also regularly gives back to the community with talks and other volunteer efforts.

**Tom Jennings, USAF 33rd Network Warfare Squadron in San Antonio, Texas**

Tom's contributions to this elite group of defenders over a long period of time has made him a true Difference Maker, most recently as the Deputy Flight Commander, Operations Training of the 33rd - Air Force Computer Emergency Response Team (AFCERT). He has continually championed cybersecurity education and skills advancement, fighting for and managing one of the Cyber Wing's largest training budgets. He led the first- ACD Cyber Range effort through the initial dry run and feedback effort.

**Sean Pruitt, FBI Unit Chief**

Historically, cyber training offered by the FBI was either technical or investigative. As Chief of FBI's Cyber Training Unit, Sean Pruitt realized there was a critical need for a blending of the two after taking command more than three years ago. Using a combination of working groups and input from senior cyber investigators in the field, special mission experts from industry and government, Sean led a team that developed a brand-new series of cyber operations and investigative courses that has become the benchmark within the United States government.

**Dennis Antunes, Cybersecurity Research Analyst at Wells Fargo**

Dennis has six years of tenure on Synack's 1,500-person crowdsourced security testing team, the Synack Red Team (SRT). He is the SRT's top rated SANS-certified penetration tester in 2020 and has been a top performer every year. He has found more than 120 security vulnerabilities so far in 2020 for customers around the world.

**Annie Salem, Third Party Risk Management Program Lead at Mass Mutual**

Annie Salem is the TPRM program lead at Mass Mutual, reporting to the CISO. She was instrumental in re-designing the Mass Mutual 3rd party risk management program. Annie developed their holistic risk model including partitioning Mass Mutual's third-party inventory into eight risk categories based on the classification of data and how it is accessed by whom. Annie was also instrumental in bringing in various AI/ML tools to detect changes in risk posture, which allows MassMutual to focus on those third parties representing the greatest risk to Mass Mutual in real time and on an ongoing basis. Mass Mutual's use of data science, AI and ML to monitor their third-party risk management program has resulted in efficiency gains, requiring less staff for manual processes to more effectively manage and mitigate third-party risk.

**Didier Stevens, Senior Analyst at NVISO**

Didier has spent an enormous effort in creating a library of open-source python scripts to analyze malicious Office documents. The effort he put into those scripts, and the blog posts he is writing on isc.sans.edu, and the time he spends explaining and educating analysts in the effective use of his scripts have helped countless organizations defend against and recover from compromises. His work has been so impressive that SANS has unofficially named one day of the reverse engineering malware class (FOR610), the "Didier Day" as it deals pretty much exclusively with the use of his scripts. Didier has been an Internet Storm Center volunteer handler since March of 2015 and has posted about 360 different times just on isc.sans.edu, often discussing some recent update to his famous scripts.

**BG Paul Stanton, Deputy Director of Current Operations US Cyber Command and John Womble, Training Manager for the US Army Cyber Effects Program**

Starting as far back as 2016, BG Paul Stanton and John Womble played critical roles in the creation and success of Cyber STX, one of the very few live Army exercises that ran in the summer of 2020. This is especially unique as it contained physical elements, in person activities, and travel that all had to be managed during the pandemic.

Without BG Stanton and John Womble's vision to push forward with a plan that involved the whole of CPB's logistics, transportation and cyber teams in this realistic Red on Blue fight, it never would have come to fruition and become the Military's most exciting and realistic CPT Validation exercise in history. John Womble was so intrinsic in the creation of Cyber STX that they named the deep-water port "Camp Womble".

**Jason O'Dell, Director, Incident Management at Walmart**

Jason is an industry leader who embraces large scale cyber education and was an early adopter for team based training and corporate NetWars ranges. Jason has also volunteered to serve as a panelist

for SANS Hackfest Summits and was instrumental in bringing together 70 students for a private Core NetWars Tournament in 2020. Walmart offered this as a "October/Cyber Security month" thank you for key InfoSec professionals, and as a recruiting tool for Walmart Associates considering a transfer into cyber.

### Lee Whitfield, SROC Senior Advisor

During the early stages of the pandemic, Lee Whitfield saw that teens were stuck in quarantine and isolated while learning remotely. He recruited SANS professionals to provide free online training, hands-on activities, and CTFs for a new cyber camp for teens, parents and even instructors. The effort really hit home and the impact on the next generation of Infosec professionals was impressive. Unique material was created and provided to cater to this age group.

### FBI Biotechnology Threat Focus Cell Team, Newark NJ

- SA Scott R. Nawrocki, FBI, BTFC Lead
- SA Tammybeth McHugh, FBI
- Detective Sergeant Anthony Correll, NJ OHSP
- SA Timothy Cho, FBI
- IA Jesus Lopez, FBI
- IA Gerard Martin Jr., NJ OHSP
- IA Christopher Lynam, NJ OHSP
- IA Steven Ford, FBI
- SSA Christian Schorle, FBI Newark Cyber Program Coordinator
- SSA David Miller, FBI Newark CI Supervisor
- Lieutenant Michael Podolak, NJ OHSP CT/CI Lead
- Detective Ed Kelly, New Jersey Office of Homeland Security & Preparedness

The mission of the Biotechnology Threat Focus Cell (BTFC) is to identify, mitigate, neutralize, and share cyber, national security and insider threats to the biotechnology sector. The BTFC is an FBI Newark and New Jersey Office of Homeland Security and Preparedness joint initiative formed in October 2019. Industry partners join Federal and State government during monthly threat exchanges to collaborate, share trends, threat information, and address concerns facing industry.

### The CTI-League

The Cyber Threat Intelligence (CTI) League is an online, global volunteer community of cyber threat intelligence researchers, InfoSec experts, CISOs, and other relevant people within the industry, whose goal is to neutralize cyber threats exploiting the current COVID-19 pandemic. It is essentially an open-source CERT for that community, helping hospitals and health care facilities protect their infrastructures during the pandemic and creating an efficient channel to supply support services.

Established in March 2020, the CTI League grew from 2 users to over 100 volunteers in only one week. In 20 days, more than 1,000 new volunteers joined the league and currently there are more than 1,400 volunteers from almost 80 countries within the league.

Founders: Ohad Zaidenberg, Nate Warfield, Marc Rogers

## Subscribe to SANS Newsletters

Receive curated news, vulnerabilities, & security awareness tips

Your Email...

Select your country

By providing this information, you agree to the processing of your personal data by SANS as described in our Privacy Policy.

☐ SANS NewsBites
☐ @Risk: Security Alert
☐ OUCH! Security Awareness

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Subscribe

## Register to Learn

Courses

Certifications

Degree Programs

Cyber Ranges

## Job Tools

Security Policy Project

Posters & Cheat Sheets

White Papers

## Focus Areas

Cyber Defense

Cloud Security

Cybersecurity Leadership

Digital Forensics

Industrial Control Systems

Offensive Operations

© 2023 SANS™ Institute

Privacy Policy      Terms and Conditions      Do Not Sell/Share My Personal Information      Contact      Careers