Nominate Now: Deadline is July 6, 2012

The 25 Most Important Cybersecurity Innovations of 2012

If more organizations were to follow the lead of those that are most effective in cybersecurity, countless cyber attacks could be stopped, huge amounts of sensitive information could be kept out of malicious hands, and hundreds of millions of dollars wasted on ineffective cybersecurity measures could be saved. The effective organizations have found innovative methods and products that use existing security technology to greatly reduce cyber risk at significantly lower cost than their peers. The launch of the National Cybersecurity Innovation Awards in 2011 by White House Cyber Coordinator Howard Schmidt marked the first systematic recognition of those leaders and what they have accomplished (view the 2011 award winners https://www.sans.org/press/2011-national-cybersecurity-innovation-awards.php).

The 2012 National Cybersecurity Innovation Awards will recognize 12 more innovations than last year's program and will reach out even further into the cybersecurity community. Executives from 40 major companies will help identify innovators, whose achievements will then be reviewed by a prestigious and trusted panel of judges who know what actually works. In all, there will be 25 awards for proven innovation and 10 more awards for promising innovations.

The winners will be featured at a special plenary session at the National Cybersecurity Conference in October 2012. By presenting their innovations and lessons learned along the way, these award-winning professionals will help others follow in their footsteps. Substantial web and press coverage will serve to disseminate their innovations as widely as possible.

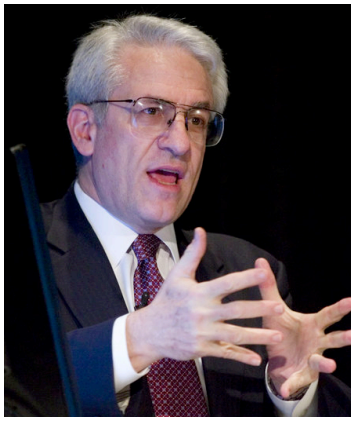
The Judges

During **Tony Sager's** 34 years at the National Security Agency, he headed the Systems & Network Attack Center, oversaw all Red and Blue Team projects, created and headed security product evaluation teams, helped guide the agency's top talent development programs, served as founding director of the Vulnerability Analysis & Operations Group (comprised of 700 of the NSA's top technical cybersecurity specialists serving the defensive mission), and was the Chief Operating Officer for the Information Assurance Directorate. He is also well known as a national advocate for open security standards such as the Security Content Automation Protocols (SCAP).

Sameer Bhalotra served as White House Sr. director for cybersecurity, where he led the national identity management and continuous monitoring initiatives. He built a bipartisan budget consensus to fund pilot cybersecurity programs and add $200 million to enable the Department of Homeland Security and other agencies buy the necessary tools to implement continuous monitoring across government. Bhalotra has also served as the principal cybersecurity staffer for the Senate Intelligence Committee, which oversees the cyber budgets of the National Security Agency and the other intelligence agencies. He has comprehensive knowledge of advanced cybersecurity requirements and tools. He has a PhD is in applied physics from Stanford University.

Asheem Chandna is the dean of venture capitalists who invest in cybersecurity companies. While he was vice president of business development and product management at Checkpoint in the 1990s, the company grew from $10 million to $550 million in revenue. He was personally responsible for launching the era of virtual private networks. As a partner at Greylock since 2003, he has helped create and grow multiple security technology businesses to market-leading positions, and successfully merged several into larger companies. He also serves on the panel of judges for the Wall Street Journal Global Technology Innovation Awards.

Alan Paller is director of research at SANS. He oversees the international 20 Critical Controls Project, efforts to identify the best tools for continuous monitoring using the 20 Critical Controls, the Internet Storm Center, and the annual selection of the Seven Most Dangerous New Attack Patterns. He has testified before the U.S. Senate and House. He was named by President Bill Clinton to the National Information Assurance Council, and named by the federal CIO Council as the 2005 Azimuth Award winner – a singular lifetime achievement award given to the one person outside government who has done the most to improve federal information technology. In 2010, the Washington Post named Alan one of "seven people worth knowing or knowing about in cybersecurity."



Criteria

We recognize that innovation in the delivery of cybersecurity can take many shapes. We are looking for ideas big or small that have resulted in tangible improvements in risk reduction on a large scale.

Nominees will be assessed based on three broad criteria:

- *Cybersecurity impact* – The project team and tool(s) being nominated should have contributed to the prevention, control, or mitigation of cyber attacks through significant improvements in the quality of the technology and processes being deployed.

- *Innovation and creativity* – The nominee should have applied imaginative and pioneering approaches to overcome difficult challenges to deploying and perfecting cybersecurity defenses. *Innovation* is not the same as *invention*. Even simple ideas applied in creative ways to overcome real-world challenges can be considered innovative.

- *Scale* – The nominee's innovation should be at scale or suitable to be implemented at scale within the nominee's agency or enterprise and in other large enterprises in the United States and possibly around the world.

Categories

Preliminary list, subject to review:

- Continuous monitoring, with particular emphasis on automated monitoring of the 20 Critical Controls
- Advanced targeted attack defenses and discovery
- Mobile device management
- Cloud security innovation
- Authentication and Identity management
- Effectively changing the culture to enable rapid security improvement
- Other technology-based innovations

Tips for Nominators

Following are some tips for those wishing to submit nominations:

- Nominations must represent an innovative approach to cybersecurity that has demonstrated impact.
- Nominations will be reviewed by a panel with broad expertise and a track record in identifying innovations. However, these reviewers may not be deep experts in your area of cybersecurity. So ideas should be described in clear language with explanations of any technical jargon unique to your area of cybersecurity.
- Documentation of the innovation's impact does not need to be sent with the initial nomination form. However, credible evidence supporting the validity of a project or sufficient proof of innovation and impact may be requested at a later date. We will need to validate claims prior to determining the final award winners.
- Nominators should review the policies, guidelines, terms, and conditions associated with this award.

Submitting Your Nomination

Please complete the online form and email it to ncia@sans.org

Nominations will be accepted through July 6, 2012 at 11:59 PM Eastern Daylight Time