SC MAGAZINE

AWARDS 2016

Honored in the U.S.

Entry Kit

scmagazine.com/awards

Entry rules and information

Who can enter?

The 2016 SC Awards U.S. is open to all information security vendors, service providers and professionals.

Vendors and service providers that offer a product and/or service for commercial, government, educational, nonprofit or other industries can enter the Trust Awards (formerly Reader Trust Awards) and Excellence Awards categories, which relate to products, services and/or information security companies. Entrants should be executing work in North America.

Information security professionals from end-user companies can enter into the Professional Awards categories, which honor teams and individual CSOs/CISOs working in North America. This means NO vendors or service providers that sell IT security-related products or services to private and public organizations qualify for these categories and SHOULD NOT ENTER. If vendors or service providers do enter they will be disqualified after editorial review of entrants in these categories and will receive NO REFUND of related entry fees. It is acceptable and, indeed, encouraged for vendors and service providers to nominate their thought-leading customers. After all, the Professional categories have been created to honor the accomplishments of their end-user customers.

Other Professional Awards categories relate to both professional certification providers and those professional advancement companies that offer training on various information security issues to end-user companies. These, too, should be based in North America.

Entry requirements and qualification questions

Each category requires that you answer a set of questions in order to qualify your nomination. Please see each category for the full list of qualifying questions. Answer these completely.

Be sure that your product or service is a fit for the categories in which you are nominating, as *SC Magazine* reserves the right to eliminate a product or service from consideration if our editorial team and/or judges find that the offering is inappropriate for that category.

Also, if you are entering multiple categories, you should offer unique answers for each. That is, avoid copying and pasting the same answers for each category you enter as this may yield a negative response from our judging panels.

Online nomination submission

Each nomination must include:

- Answers prepared for the qualification questions for each nomination and
- Nomination fee (online payment required): Visa, MasterCard, American Express.

Once you have prepared your nominations, please visit our website, awards.scmagazine.com, to submit your nomination.

Finalist notification

Finalists will be announced online on our website, scmagazine.com, in December 2015. Winners will be announced at the 2016 SC Awards U.S. Gala to be held on March 1, 2016 in San Francisco.

Questions

Please contact Anna Jurgowski, events coordinator, at 646-638-6015 or via email at anna.jurgowski@haymarketmedia.com.

Sponsorship opportunities

For information on sponsorship opportunities for the 2016 SC Awards U.S., please contact Mike Alessie at 646-638-6002 or via email at mike.alessie@haymarketmedia.com.

Terms and conditions

The mission of the 2016 SC Awards U.S. is to honor the achievements of companies and information security professionals striving to safeguard businesses, their customers and critical data in North America. Information security products and services nominated for the Trust Awards, therefore, should be available for sale to U.S. and Canadian organizations, as well as provide both customer service and support to users in these countries. Competitors are voted on by end-users, readers and vendor-neutral judges. After averages for each category are tallied, finalists and winners are decided. Results are completely independent. Financial/advertising considerations play no part in the results. That is, no one can "buy" a win by advertising, partnering or working with *SC* and its various team members!

Judging information

Trust Awards

(formerly Reader Trust Awards)

Finalist and winners in these categories are chosen by IT security professionals from the *SC Magazine* readership who have been invited (and vetted) by the *SC* editorial team to participate as part of a judging panel for this particular group of awards. Members of this panel, which will be made up of approximately 100 professionals, primarily are from end-user organizations. They are invited and chosen to participate as judging panelists for the Trust Awards categories based on their industry expertise and background. Typically, they lead information security divisions, play roles in implementing information security policies and plans for their organizations, and/or have in-depth knowledge or experience with testing, deploying or managing IT security products/services. They represent a cross-section of *SC*'s audience – which is comprised of information and IT security personnel at large, medium and small enterprises from all major vertical markets, including financial services, health care, government, retail, education and other sectors. Having volunteered their time and, most importantly, their knowledge of and experience with the contenders in these categories, these industry professionals are tasked with carefully considering each of the competitors in relation to the categories for which they entered. To reach their decision, not only will they review the materials provided by entrants, but also will consider whether the product or service in each category actually is the most effective in helping companies address the problems for which the product or service was designed. They also are asked to consider the functionality, manageability, ease of use and scalability of the product or service, as well as the customer service and support provided for it. Too, they have been encouraged to peruse any applicable product reviews that *SC Magazine* has published in the last year to help in making their final decisions, along with any other relevant industry and/or analyst reports. They also may suggest that certain entrants be moved between categories if they deem them unsuitable for one but appropriate for another.

After the judging panels' decisions are in, *SC Magazine*'s product reviews team steps in to review the finalists in each to ensure, yet again, that they accurately jibe with the category for which they entered. In the event that a particular product or service is not an appropriate fit for a category, the product reviews team and VP of editorial will convene to make a final decision on whether it should remain in the running. (No refunds will be provided if a product is eliminated for failing to meet the criteria for the category to which it was submitted.)

Excellence Awards

Winners in this category are decided by a second expert panel of judges. These judges are hand-picked by *SC Magazine*'s editorial team for their breadth of knowledge and experience in the information security industry. Our judges come from all walks of life – from end-user companies to the analyst and consulting communities to academia. Many are practicing and former chief security officers from the private and public sectors who also may have been honored themselves at SC Awards galas in previous years. Not only are judges advised to review the materials provided by entrants, they also are asked to check out any applicable research or analyst reports, as well as product reviews appearing in *SC Magazine*. There will be one winner chosen per category.

Professional Awards

With the exception of the Editor's Choice Award recipient within this category, winners in the Professional Awards category will be decided by an expert panel of judges. Like the Excellence Awards, not only are judges advised to review the materials provided by entrants, they also are asked to review any applicable research or analyst reports, product reviews by *SC Magazine*, and/or any additional documentation/input provided by *SC Magazine* and/or other Haymarket Media publications. In some cases, the panel may be offered further insight or additional notes from *SC Magazine*'s editorial team members who may decide to interview or already have interviewed contenders. There will be one winner chosen per category.

*KEY INFO

Deadline for nominations: Sept. 18, 2015. Nominations submitted after Sept. 18 will be considered late and will incur a late fee. **Late nominations:** Late entries will be received until Sept. 25, 2015. However, all nominations received after Sept. 18, 2015 will incur a penalty of $145 per entry.

Nomination entry fees:
Trust Awards (formerly Reader Trust Awards) and Excellence Awards categories: $335 per entry.
Professional Awards categories: $240 per entry.

Judging information

Editor's Choice Award

Based on feedback from *SC Magazine*'s editorial team, its Editorial Advisory Board, readers and other sources, a small list of contenders for this designation is created internally. Those considered for this award can be industry bodies, professionals, companies or products.

The award winner is decided by the VP of editorial for *SC Magazine* and announced at the SC Awards Gala on March 1, 2016. This award enables the editorial team to pay homage to those individuals or entities that are making a positive impact on the industry as a whole.

Interested in judging?

To be considered as a judge for the 2016 SC Awards, please click here and complete the application form by Aug. 24, 2015. After this date, applications will be reviewed and judges chosen by the editorial team to participate on the Trust Awards panel. If some applicants seem more appropriate for the second judging panel, which is responsible for deciding Excellence and Professional categories, they will be considered for inclusion by the VP of editorial.

Please understand that judging for the SC Awards is a serious commitment, requiring all panelists to devote some time to evaluate submissions fairly and objectively so that IT security solutions and services providers, industry leaders and their teams can be recognized and honored for their exemplary work and contributions to the wider field. We do expect a healthy interest from our *SC* audience to participate, but submitting an application does not guarantee a spot as a judge.

Click on a category to jump to that section

Entry rules & information

Judging information

Trust Awards

Excellence Awards

Professional Awards

Trust Awards

Click on a category to jump to that section

Entry rules & information

Judging information

Trust Awards

Excellence Awards

Professional Awards

Categories & requirements

Best Advanced Persistent Threat (APT) Protection

An advanced persistent threat (APT) product and/or service provides real-time detection of and protection against intruders gaining access to an enterprise environment to stealthily extract high-value information assets from targeted organizations in manufacturing, financial, national defense and other industries. Tactics used by cyber thieves launching these attacks often allow their activities to go undetected for indefinite periods of time. This is because an APT intruder must continuously rewrite code and employ sophisticated evasion techniques to accomplish their primary goals. One technique that is commonly used by an APT intruder is spear phishing, a type of social engineering, to gain access to the network through legitimate means. Then, these tricky intruders are ready to harvest valid user credentials (especially administrative ones) and move laterally across the network, installing backdoors at will. These backdoors provide the APT attacker unlimited opportunity to install bogus utilities to create a "ghost infrastructure" for distributing malware that remains hidden in plain sight. While these types of attacks are difficult to identify, the theft of data can never be completely invisible. To find and stop these intruders, an APT product or service must have a unique set of features and functions specifically for addressing APT mitigation. Contenders entering this category should provide real-time network traffic analysis of new and unknown malware; block data exfiltration attempts in real-time (including but not limited to web, email, file, FTP, DNS, or other critical systems and related applications); provide content and/or behavioral analysis; offer an integrated cloud-based dynamic threat intelligence distribution infrastructure; and offer advanced evasion technique (AET) detection and/or prevention functionality. Central administration and management and secure remote management capabilities also are musts.

Best Behavior Analytics/ Enterprise Threat Detection

A still somewhat-emerging category, these products focus on detecting insider threats, targeted attacks and other fraudulent activities by examining human behaviors, sussing out patterns that are then analyzed through the application of algorithms and statistical analysis to detect anomalies that may indicate threats of loss or compromise to organizations' critical data. Offerings in this space are also referred to as so-called "user behavior analytics" products by analyst company Gartner.

Best Cloud Computing Security Solution

These technologies are deployed to protect data and/ or applications in a cloud environment. They may also protect the cloud computing infrastructure itself. Cloud computing security concerns are numerous for both providers and their customers – and include security and privacy worries, compliance issues and legal/contractual problems. Solutions or services in this category can provide for the protection of data or applications in the cloud, protection for traffic flowing between companies and their cloud service providers, policy management and encryption capabilities, privileged user access and controls or more.

Click on a category to jump to that section
Entry rules & information
Judging information
Trust Awards
Excellence Awards
Professional Awards

Best Computer Forensic Solution

Products in this category fall into two sub-categories: network and media. The network tools must be exclusively intended for forensic analysis of network events/data. If the product is a SIEM with forensic capabilities, it should be placed in the SIEM category. Media tools cover just about all other non-network forensic tools, including those tools that collect data from media over the network and live forensic tools. This also includes specialized forensic tools that are not intended to analyze network data.

Best Database Security Solution

Protecting its critical information is the number one priority for many organizations. An integral component of this is to secure corporate databases. Entries here should include solutions that help customers safeguard mission-critical database environments. Features of these offerings can run the gamut – from encryption to access management to logging and monitoring. Be sure to explain the specific ways the solution protects these corporate crown jewels and the features present to ensure exposures are mitigated.

Best Data Leakage Prevention (DLP) Solution

Products in this category include those that help organizations safeguard their intellectual property and customers' critical data persistently – inside and outside the company. Network-based and endpoint data leakage prevention products will be considered. Products should prevent data from unauthorized exit from the network, or protect data on the endpoint – whether the endpoint is connected to a network or not. Products typically are policy-driven and should include scanning of all data, regardless of protocol or application leaving the network, and/or keep track of peripherals, such as removable storage and attached to the endpoint – reporting that inventory to a central location or administrator. All entrants should have the capability of being managed by a centralized administrator. Those products considered part of this category include: network DLP products, which are typically gateways; those products protecting only endpoints; and hybrid products that operate at both the gateway to the network and at the endpoint. Specifically for endpoint DLP, traffic should be monitored and encryption should be available.

Best Email Security Solution

Email security addresses the ability to exchange email messages with assurance, as well as the ability to filter email messages based on content, source or other criteria. Solutions should ensure the privacy of sensitive messages, limit the repercussions of email forgery, and manage other aspects of safeguarding email within the organization. These products are enterprise-centric and should have, but are not required to have, some form of centralized management. They may include spam filters, junk mail filters, malware filters, unauthorized content (sometimes called "extrusion protection" or "data leakage protection"), phishing and other types of undesirable content. However, these are not simply anti-spam filters. These email security products should be evaluated on their effectiveness, manageability, non-intrusiveness, ease of use and other factors that impact the implementation of this type of product in the enterprise environment. They typically provide features such as email encryption, digital signatures, automatic shredding of messages and attachments, and more.

Best Fraud Prevention Solution

Given the reliance on the internet by consumers from all walks of life to conduct any number of retail, banking or other transactions, fraud prevention solutions have become critical. Tools nominated in this category strive to minimize online privacy and security problems that could lead to fraud and, therefore, impact both the company and the customer. Still an evolving area of information security, there are a slew of solutions and services available that could qualify for consideration in this category – from authentication and enhanced encryption solutions to secure web communication or malware-detection offerings.

Categories & requirements

Best Identity Management Solution

Products in this category address the identity management lifecycle in an enterprise environment, including password management, user provisioning and enterprise-access management

Best Managed Security Service

These offerings provide a turnkey approach to an organization's primary technical security needs. These offerings can either be a co-located device at the client organization facility, or can be a completely outsourced solution where the application to be protected would reside at the vendor's data center.

Best Mobile Security Solution

More and more employees are using smaller and smaller devices with loads of applications to access corporate data. Some examples include iPhones, iPads, Android devices, BlackBerries and more. Products in this category deal with not only a collapsing perimeter, but also consumer-owned and -controlled devices being used to get at corporate resources. At a minimum, these devices likely will require strong endpoint security, point-to-point encryption and more. This is a broad category. If your product is used to secure this type of small device/handheld, it may fit. Security can be for data at rest in the device itself, secure access to data in the enterprise, and encryption for data in motion between the enterprise and the device. It also includes anything from hard disk encryption solutions and tools that track lost mobile devices to USB/thumb drive security solutions.

Best Multifactor Solution

Products here provide enhanced security to end-users or devices by offering credentials for access to an authenticator or authentication server. Software and hardware that specializes in the biometric authentication of users is also included here. These solutions may use a tangible device (something you have) for authentication and knowledge (something you know) for authentication. For biometrics, the solution provides identification and authentication using any of the following methods: finger/thumb print/retinal scan/voice recognition/hand/palm geometry/facial recognition.

Best NAC Solution

Protecting host-based computing platforms and network resources from threats that are brought in by employees, vendors, contractors and guests involves a numbers of solutions and policies. From anti-virus and firewalls to IDS/IPS solutions, the products in this category run the gamut. However, to control access to network resources at the endpoint, the tools companies often rely on are network access control (NAC) products. These solutions can be used to validate the existence of certain security measures and validate that they are properly configured and up to date. They also can validate the existence of current OS patches and can be used to manage the complexity associated with overseeing permissions and authorizations for various groups of users. Most will integrate with a common directory structure, some will provide local authentication capabilities, while others will match something on the endpoint – such as an agent or MAC address – to the authentication before allowing access to the protected network resources.

Best Risk/Policy Management Solution

These products measure, analyze and report risk, as well as enforce and update configuration policies within the enterprise, including but not limited to network, encryption, software and hardware devices. Contenders' products should offer a reporting format that covers the frameworks of multiple regulatory requirements, such as Sarbanes-Oxley, Gramm-Leach-Bliley and other acts and industry regulations. As well, this feature should be network-centric, providing reporting to a central administrator and allowing for companies to centrally manage the product.
So, overall, entrants' products should be enterprise-centric; collect data across the network, including threats and vulnerabilities; report associated risk, endpoint configuration, enforcement, auditing and reporting; provide remediation options (but are not exclusively patch management systems); and, finally, offer centralized reports based on regulatory requirements and local policies.

Click on a category to jump to that section
Entry rules & information
Judging information
Trust Awards
Excellence Awards
Professional Awards

Best SIEM Solution

GSecurity information and event management (SIEM) tools are used to collect, aggregate and correlate log data for unified analysis and reporting. Typically, these tools can take logs from a large number of sources, normalize them and build a database that allows detailed reporting and analysis. While forensic analysis of network events may be a feature of a SIEM, it is not the only feature, nor is it the primary focus of the tool.

Best UTM Security Solution

Given the continuous convergence of the market, we've decided to retire some categories this year and integrate a number of individual categories from previous years into this unified threat management (UTM) category. The former categories – Best Enterprise Firewall, Best Intrusion Detection System/Intrusion Prevention System Product, Best IPsec/SSL VPN, Best Anti-Malware Gateway and Best Web Content Management – are now integrated here. As formerly, contenders in the UTM security category should take an "in-depth" defense approach. Entrants should have an integrated, multifunction endpoint/UTM offering – not a single-function product. These products typically aggregate a wide variety of threat data into a single unified tool. Many organizations define those threat categories as anti-malware, content management, IDS/IPS and spam filtering, along with firewall/VPN. Entrants should meet this minimum functionality and can include anti-malware gateway, anti-spam gateway and anti-phishing gateway, as well as provide web content filtering for laptops, desktops and, optionally, servers that blocks or filters objectionable websites and content.

Best Vulnerability Management Solution

These products perform network/device vulnerability assessment and/or penetration testing. They may use active or passive testing, and are either hardware- or software-based solutions that report vulnerabilities using some standard format/reference.

Best Web Application Solution

Application firewalls inspect the body of packets and restrict access to legitimate application traffic while blocking access to other parts of the operating system. They typically use deep-packet inspection, provide logging and reporting, block real-time traffic, provide alerting capabilities and auto-update features, perform web caching, provide content filtering, offer web-based access to reporting and/or logging, protect traffic from reaching the underlying operating system, and filter application traffic to only legitimate requests.

Qualification questions

(150-word maximum on each response)

- How does this product/service answer the specific market need or application for which it was designed and is being nominated?
- How does this product/service significantly differ from its competitors?
- What are the business and technical advantages to enterprises or SMEs investing in this product/service?
- What is this product's/service's total cost of ownership? Is it possible that some of your customers find that scalability issues, management of updates/configurations and more, increase costs associated with deployment of your solution/service?
- If applicable, what is the frequency of updates to the product/service?
- How has this product/service helped customers to meet/surpass corporate budgetary expectations?
- How does this product/service show a sound business benefit and/or return on investment? That is, how is it enabling customers and their businesses?
- What is the market share for the sales of this product?
- This year, we're giving competitors the opportunity to provide an optional informational video about their entries. Your video (two-minute-maximum) should explain to us why your product should win the particular category you are entering, detailing things like what the solution does, what makes it stand out from competitors, how many customers and what types of customers currently use it and why, etc.

Click on a category to jump to that section

Entry rules & information

Judging information

Trust Awards

Excellence Awards

Professional Awards

Categories & requirements

Excellence Awards

Click on a category to jump to that section

Entry rules & information

Judging information

Trust Awards

Excellence Awards

Professional Awards

Categories & requirements

Best Security Company

Nominees should be the tried-and-true, longer-standing companies which have been offering products and services to customers for at least three years. Nominations can come from all sectors. Areas that will be accounted for in the judging process include: product line strength, customer base, customer service/support, research and development, company growth and solvency, innovation and more.

Rookie Security Company of the Year

Nominated companies should be new to the IT security field – offering an initial, strong, flagship product that is within two years of its initial release. Nominees can come from any IT security product/service sector and will be continuing efforts in further product development, customer growth and overall fiscal and employee growth. Please note in your submission the launch date of your initial flagship offering. If this initial offering or any of your other products have been on the market for longer than two years, please do not submit a nomination in this category.

Qualification questions (150-word maximum on each response)

- How strong is the company's customer base and continued customer growth?
- Does the company have a strong product/service portfolio? Explain.
- Does the company offer strong customer service and support for the products/services it supplies? How?
- Is the company engaged in compelling research and development efforts that will lead to continued innovation? How?
- How well is the company meeting its overall mission and vision? In what ways?
- How is the company using its products and services to help enable/strengthen its customers' business?
- Are customers seeing a benefit in using your products/services to differentiate from the competition? That is, are customers finding market value in touting the use of your company's product/service?

Additional support

- Please attach three testimonials from clients, along with contact details, should the judges choose to follow-up. Testimonials should explain why the nominee is best qualified to win this category.

Best SME Security Solution

This includes tools and services from all product sectors specifically designed to meet the requirements of small- to midsized businesses. The winning solution will have been a leading solution during the last two years, having helped to strengthen the IT security industry's continued evolution.

Best Enterprise Security Solution

This includes tools and services from all product sectors specifically designed to meet the requirements of large enterprises. The winning solution will have been a leading solution during the last two years, having helped to strengthen the IT security industry's continued evolution.

Best Regulatory Compliance Solution

Nominated solutions should help organizations comply with specific regulatory requirements demanded of companies in the health care, retail, educational, financial services and government markets. Solutions should help customers meet mandates noted in such legislation as *HIPAA, SOX, GLBA*, FISMA, or in guidelines noted by the likes of the FFIEC or the PCI Security Standards Council. Nominees must be prepared to offer references of customers who are engaged in, or have already completed, real, fully fledged deployments, and should be ready to address specific questions posed to them during the judging process.

Qualification questions (150-word maximum on each response)

- How strong is the customer base and continued customer growth for this product/service?
- Does the company offer strong customer service and support for this product/service? How?
- What is this product's/service's total cost of ownership? Is it possible that some of your customers find that scalability issues, management of updates/configurations, and more, increase costs associated with deployment of your solution/service?
- If applicable, what is the frequency of updates to the product/service?
- Are efforts underway to continue developing and strengthening this product/service? What do these efforts entail?
- Overall, how well is this product/service meeting the needs of its customers?
- What is the market share for the sales of this product/service?
- How is the company using its products and services to help enable/strengthen its customers' business?
- Are customers seeing a benefit in using your product/services to differentiate themselves from the competition? That is, are customers finding market value in touting the use of the company's product/service?
- This year, we are giving competitors the opportunity to provide an optional informational video about their entries. Your two-minute-maximum video should explain to us why your product should win the particular category you are entering, detailing things like what the solution does, what makes it stand out from competitors, how many customers and what types of customers currently use it and why, etc.

Additional support

- Please attach three testimonials from clients, along with contact details, should the judges choose to follow-up. Testimonials should explain why the nominee is best qualified to win this category.

Best Customer Service

Support as well as service of products and assistance sold are critical components of any contract. For many organizations that seek out help from information security vendors and service providers, the aid they receive from customer service representatives is crucial to the deployment, ongoing maintenance and successful running of the technologies they've bought and to which they have entrusted their businesses and sensitive data. For this new category, we're looking for vendor and service providers that offer stellar support and service – the staff that fulfilled its contracts and maybe even goes a little beyond them to ensure that organizations and their businesses are safe and sound against the many threats launched by today's savvy cybercriminals.

Qualification questions (150-word maximum on each response)

- Do you offer installation documentation, online manuals, user-oriented manuals and/or any supplemental documentation needed for your customers to implement and manage the product/service successfully? (Which ones do you offer?)
- Are the various forms of documentation associated with the product/service understandable and effective?
- What customer service and support is standard with product/service purchase?
- Do you offer customers telephone support? Do customers pay additional fees for this? How much more?
- Do you offer customers web-based downloads? Do customers pay additional fees for this? How much more?
- Do you offer customers online forums or FAQs sections? Do customers pay additional fees for this? How much more?
- Can customers get additional on-site help whenever needed? Do they pay additional fees for this? How much more?
- Do customers get on-site help in deploying the solution/service? How long is this available to them? Do they pay additional fees for this? How much more?
- Is there anything unique or special you'd like to call out about your customer service and support offerings? Would you say these help to differentiate you from competitors?

Additional support

- Please attach three testimonials from clients, along with contact details should the judges choose to follow-up. Testimonials should explain why the nominee is best qualified to win this category.

Best Emerging Technology

What cutting-edge technologies with some innovative capabilities are bursting onto the scene to address the newest information security needs facing organizations? This new category welcomes both new vendors and old pros looking to provide products and services that look to help shape the future by addressing fast-evolving threats through the creation of these types of offerings. Solutions should have just hit the market in the last six to 12 months, and entries should have some customers available who can act as references. The company should also have an office in North America and provide ready support and service to customers in this country.

Qualification questions (150-word maximum on each response)

- What segment of the market does this new product/service address? What threats does this product/service deal with and why do you consider this to be critical in today's environment?
- How do the features and capabilities of this product/service tackle organizations' newest information security needs?
- How strong is the customer base and continued customer growth for this product/service?
- Does the company offer strong customer service and support for this product/service? How?
- What is the total cost of ownership of this product/service? Is it possible that some of your customers find that scalability issues, management of updates/configurations, and more, increase costs associated with deployment of your solution/service?
- If applicable, what is the frequency of updates to the product/service?
- Are efforts underway to continue developing and strengthening this product/service? What do these efforts entail?
- Overall, how well is this product/service meeting the needs of its customers?

Additional support

- Please attach three testimonials from clients, along with contact details should the judges choose to follow-up. Testimonials should explain why the nominee is best qualified to win this category.

Professional Awards

Click on a category to jump to that section

Entry rules & information

Judging information

Trust Awards

Excellence Awards

Professional Awards

CSO of the Year

Contenders should include those who work for end-user companies only. No vendor CSOs will be considered. Nominees are the cream of the crop, having spearheaded a viable IT security program, gained the support of their company's executive leaders, as well as their colleagues, and helped – through their indefatigable efforts – to propel the CISO/CSO position to a footing of influence within their organization and the corporate world as a whole. Specific projects and undertakings, as well as over-arching security programs to propel these various goals, should be noted. Nominees should be prepared to answer further questions during the judging process, offer at least two references, and be open to holding confidential interviews with members of the *SC Magazine* editorial team, if warranted.

***Please note:* Professionals who work for an IT security vendor, IT reseller or IT consultancies are not eligible for this category.**

Qualification questions (150-word maximum on each response)

- How has the CISO/CSO developed and managed a strong IT security team?
- By what means has the CISO/CSO gained the support of corporate leaders and colleagues?
- How has the CISO/CSO helped to propel his/her position to a footing of influence within the organization and the corporate world as a whole?
- How has the CISO/CSO helped to strengthen the influence of the department in meeting business initiatives and goals?
- How has the CISO/CSO strengthened end-user and customer awareness of IT security threats and safeguards?
- In what ways does the CISO/CSO continue to better the expertise of internal IT security?
- What steps is the CISO/CSO taking to better position risk management/information security planning as business enabling? That is, how is she/he educating the rest of the company to understand that security is just as integral to the business' success and profitability as any other traditional division's function?

Additional support

- Please attach three testimonials from clients, along with contact details, should the judges choose to follow-up. Testimonials should explain why the nominee is best qualified to win this category.

Categories & requirements

Best Security Team

Contenders should only include teams from end-user companies that have executed and are managing exceptional and strong security programs, which they have built from virtually non-existent ones. The team should have successfully established and implemented an integral and/or innovative/cutting-edge component of their security program, and should have spearheaded various areas of support for its success, such as strong end-user awareness training, good configuration management, and more.

***Please note:* Professionals who work for an IT security vendor, IT reseller or IT consultancies are not eligible for this category.**

Qualification questions (150-word maximum on each response)

- How has the security team developed and managed itself within the corporate environment?
- By what means has the security team gained the support of leaders and colleagues?
- How has the security team helped to propel the CISO/CSO position to a footing of influence within the organization and the corporate world as a whole?
- How has the security team strengthened the influence of its department in meeting business initiatives and goals?
- How has the security team strengthened end-user and customer awareness of IT security threats and safeguards?
- In what ways does the security team continue to better the expertise of internal IT security?
- What steps is the security team taking to better position risk management/information security planning as business enabling? That is, how are they educating the rest of the company to understand that security is just as integral to the success and profitability of the business as any other traditional division's function?

Additional support

- Please attach three testimonials from clients, along with contact details should the judges choose to follow-up. Testimonials should explain why the nominee is best qualified to win this category.

Best IT Security-Related Training Program

This category is targeting companies and organizations that provide end-user awareness training programs for organizations looking to ensure that its employees are knowledgeable and supportive of the IT security and risk management plans. It also is considering those training companies or organizations that provide programs for end-user organizations' IT security professionals to help them better address components of their IT security and risk management plans, such as secure coding, vulnerability management, incident response/computer forensics, business continuity/disaster recovery, etc.

Programs usually entail training and education by outside industry experts who may hold various seminars, hands-on classes, etc. and recommend additional activities that further support training sessions, such as exercises or simulations to test the soundness of plans, email campaigns, online tests on certain IT security topics, etc. Entrants should include companies and organizations that offer such training without the requirement or need to secure any particular professional certification.

Programs typically are unrelated to the attainment of industry-specific professional certifications. For these companies, "Best Professional Certification Program" is the most appropriate category to enter.

Qualification questions (150-word maximum on each response)

- How is the professional training organization helping to educate and strengthen the knowledge of the IT security professional and/or corporate end-user?
- How does the training program differentiate itself from other offerings?
- How well is the program honing security skills or enhancing security-related knowledge and awareness? Explain.
- How are offerings enhancing end-user awareness and training or enabling end-user companies' IT security professionals to strengthen risk management plans that may address areas such as business continuity, incident response, secure coding, etc?

Additional support

- Please attach three testimonials from clients, along with contact details, should the judges choose to follow-up. Testimonials should explain why the nominee is best qualified to win this category.

Categories & requirements

Best Professional Certification Program

Programs are defined as professional industry groups offering certifications to IT security professionals wishing to receive educational experience and credentials. Entrants can include organizations in the industry granting certifications for the training and knowledge they provide.

Qualification questions

(150-word maximum on each response)

- How is the certification organization helping to educate and strengthen the knowledge of the IT security professional?
- How does the certification program differentiate itself from other offerings?
- How well is the certification program meeting the needs of the IT security professional? Explain.

Additional support

- Please attach three testimonials from clients, along with contact details should the judges choose to follow-up. Testimonials should explain why the nominee is best qualified to win this category.

Best Cybersecurity Higher Education Program

This category includes the best cybersecurity undergraduate or higher education program which currently has a cybersecurity degree program. These are for schools throughout the United States. Qualification is based on the quality of instruction, programs and how well these prepare students for the marketplace.

Qualification questions

(150-word maximum on each response)

- How is your program helping to educate and strengthen the knowledge of students so that future IT security professionals will be able to create robust risk management plans for their employers and stay on top of all the threats?
- What innovative offerings or educational opportunities does your program include that should entice students into a profession where additional help is needed to fill the growing demand for IT security executives?
- In what other ways does the program differentiate itself from other university offerings?
- Is the program currently an NSA and Department of Homeland Security National Center of Academic Excellence in IA Education (CAE/IAE) or CAE in Research?

Additional support

- Please attach three testimonials from clients, along with contact details, should the judges choose to follow-up. Testimonials should explain why the nominee is best qualified to win this category.

Editor's Choice Award

Based on information culled from *SC Magazine* events, through research conducted by the *SC Magazine* editorial team for various features and news articles, and conversations with and feedback from readers, analysts, vendors and the Editorial Advisory Board of *SC Magazine*, this award is given to a group, person, company or product at the discretion of *SC Magazine*'s VP of editorial.