June 2025 | Business Value White Paper, sponsored by SANS Institute

The Business Value of SANS

David Clemente
Research Director,
European Security, IDC

Leonardo Freitas
Research Manager,
European Skills Practice, IDC

Ladislav Kinda
Consultant,
Business Value Strategy Practice, IDC

THIS PDF USES HYPERLINKS

Table of Contents

BUSINESS VALUE HIGHLIGHTS

Click any link and look for the ➤ symbol on the corresponding page. Use the Return to Highlights button to return this page.

£38,998
annual additional value per SANS-trained staff member

£733,044
fraud damages and costs avoided annually

4.2 times
faster to identify threat

51.6%
faster threat response

43.8%
faster threat remediation

£661,338
external cybersecurity investment avoided annually

36.8%
longer employment tenure for SANS-trained staff

Executive Summary

In today's rapidly evolving cybersecurity landscape, organisations must prioritise the development and enhancement of their security capabilities to protect sensitive data and maintain regulatory compliance. SANS training has proven a critical component in achieving these goals, offering comprehensive, hands-on training that addresses technical gaps, improves incident response capabilities and supports career pathing and skill development.

SANS training is designed to provide cybersecurity practitioners and the organisations they support with the knowledge necessary to enhance their security posture, reduce incidents and improve staff productivity. IDC conducted research that demonstrates the value and benefits for organisations using SANS training to achieve improved cybersecurity outcomes, optimise security operations and enable business growth.

Based on a series of in-depth interviews and a specialised Business Value methodology, IDC calculated that interviewed SANS customers achieved an annual average value of £2.64 million per organisation and £38,998 per SANS-trained staff member by:

- **Enhancing employee skills and fostering cohesive teamwork:** Creating a common language among staff for better collaboration.
- **Improving incident detection, response and remediation capabilities:** Equipping employees with advanced skills for faster threat management.
- **Reducing system downtime and accelerating deployment timelines:** Implementing efficient security controls and processes.

- **Lowering the incidence of security incidents and regulatory findings:** Achieving better compliance and fewer audit findings.
- **Achieving better annual business results over time:** Boosting productivity and efficiency among cybersecurity teams.

Organisations reported significant improvements in overall environment security, incident reduction and staff productivity, highlighting the substantial financial impact of investing in SANS training.

Situation Overview

While it was once possible to be a cybersecurity generalist, those days are gone. Security has become an increasingly specialised field, where one can focus their career on one domain – for example, cloud security – and spend much of their time inside subsegments of that domain. This specialisation has occurred for many reasons, but a core one is that enterprise technology requirements have evolved significantly over the past 20 years.

The rise of distributed computing – and a 'cloud-first' approach for many organisations – has created substantial new commercial opportunities. It is now trivial for remote workers to connect to corporate networks from anywhere in the world (this often holds true for malicious actors as well). Industrial equipment can be connected to the internet, where owners/operators and trusted third parties can monitor and modify it, with benefits including more effective preventative maintenance and less downtime.

These changes not only bring greater efficiency but also greater complexity. And while some of this complexity can be automated or abstracted away, skilled security practitioners will remain essential to understanding and securing these environments.

According to IDC's *Global Skills Survey* (September 2024), cybersecurity is one of the two most in-demand skill areas in information and communications technology worldwide, trailing only AI, which has seen a sharp rise in demand over the past three years. Furthermore, security skills take substantial time to develop and have a relatively short lifespan, requiring a lifelong learning approach for professionals.

This is where cybersecurity training and skills come into play. Security expertise is necessary in many different places across an enterprise, first of all in the security team to enable core tasks of building and running the organisation's security tools and processes. But it is also necessary in other teams, including IT, software development, audit, compliance, legal and supplier management.

For practitioners, security training is essential to (a) adequately understand the fundamentals of their areas of specialisation and (b) maintain and update this knowledge over time as their areas of specialisation evolve.

As security technologies and underlying risk management methods evolve, the ways professionals build and sharpen their skills must keep pace and serve as a bridge between theory and practice to cater to these novel upskilling needs.

Beyond upskilling IT professionals, companies need to better align learning and development with their technology strategies. IDC's *Worldwide IT Training MaturityScape 2023* found that only 7.4% of organisations take an optimised approach, directly linking training to technology adoption plans. This alignment improves the relevance of training programmes and increases support for training budgets across the organisation.

To reach a more strategic view of training, companies need support to assess the return on investment of their learning and development spending and convey a clear message to C-level executives that upskilling pays off in the longer term. This paper will sidestep the much-debated topic of a shortage of security practitioners (the opposing view holds that the shortage is not of practitioners but instead of employers willing to offer adequate remuneration). Instead, it will emphasise the benefits of security training for both enterprises and practitioners, particularly at higher levels of skill and specialisation.

SANS Training Overview

Founded in 1989 and headquartered in North Bethesda, Maryland, the SANS Institute is a global provider of cybersecurity training, certification and research. The organisation delivers educational programmes and resources to support cybersecurity professionals at various stages of their careers.

The SANS Institute operates internationally, with regional offices in the United States, United Kingdom, Singapore and Dubai, as well as representatives in multiple countries. Past and current customers include over 40,000 organisations, from government agencies, private sector companies and academic institutions across multiple continents.

SANS offers a wide portfolio of over 85 courses covering areas such as cyber and network defence, penetration testing, digital forensics, incident response, industrial control systems security, cloud security and compliance. Instructors with practical industry experience develop and update the curriculum, and courses cater to a wide range of skill levels, from introductory to advanced.

SANS training is available through several formats:

- **In-Person Events:**
  Instructor-led sessions at global locations
- **Live Online:**
  Real-time virtual classes
- **On-Demand:**
  Self-paced online modules with interactive labs and assessments
- **Private and Group Training:**
  Customisable programmes for organisations, delivered virtually or on-site
- **Cyber-Ranges and Security Awareness:**
  Practical skill-building and human risk management exercises

The SANS Institute administers the Global Information Assurance Certification (GIAC) programme, which offers over 40 cybersecurity certifications. Additionally, the SANS Technology Institute provides accredited undergraduate and graduate degree programmes in cybersecurity.

In recent years, SANS has expanded its curriculum to address new areas such as cloud security, AI and operational technology security. The organisation has also developed workforce initiatives and scholarship programmes to support the cybersecurity skills gap. SANS continues to publish research and surveys on cybersecurity trends and participates in collaborative exercises with industry and government partners.

The Business Value of SANS

IDC's research involved interviews with a diverse range of organisations, including those in manufacturing, financial services, insurance and more. These organisations vary significantly in size, with employee numbers ranging from 1,500 to 350,000 and revenues from £481 million to £80 billion. This diversity showcases the scalability of SANS training. The ability of SANS to cater to such a wide range of industries and organisational sizes demonstrates its flexibility and adaptability. Organisations from different sectors and with varying levels of complexity in their security needs have successfully implemented SANS training, highlighting its universal applicability.

The average number of employees among the interviewed organisations is 73,300, with an average revenue of £19.9 billion (**Table 1,** next page).

TABLE 1

Firmographics of Interviewed Organisations

Firmographics	Average	Median
Number of employees	73,300	20,000
Number of IT staff	17,300	2,200
Number of cybersecurity staff	1,250	110
Revenue per year	£19.9B	£6.5B
Verticals	Utilities (2), Insurance, Investment, Financial Services, Banking, Professional Services, Manufacturing	
Countries	United States (4), United Kingdom (2), Germany, Belgium	

n = 8; Source: IDC Business Value In-Depth Interviews, April 2025

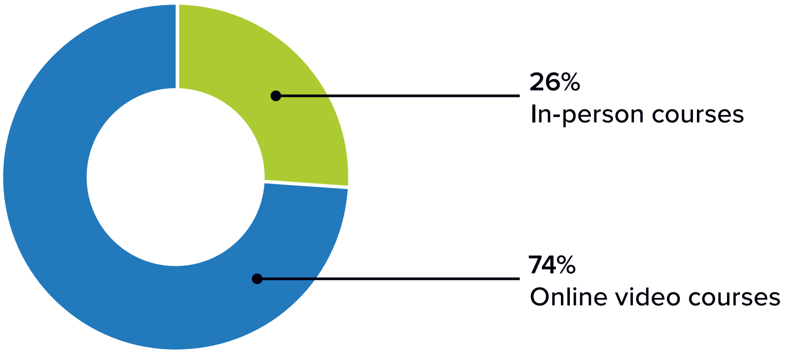
Most of the interviewed organisations preferred online training for its flexibility, but some still saw value in in-person training delivery for hands-on experience and direct interaction with instructors (**Figure 1**). This preference for online training aligns with the need for scalable and accessible training solutions, especially in a post-COVID-19 world. However, the value of in-person training remains significant for those seeking more interactive and immersive learning experiences.

Organisations also noted that the quality of the training content was a decisive factor in selecting SANS.

FIGURE 1

SANS Training Delivery Method

(Percentage of usage)



n = 8; Source: IDC's Business Value In-Depth Interviews, April 2025

Choice and Use of the SANS Institute

Interviewed organisations chose SANS as their training provider for several reasons. Companies used SANS to comply with regulations, attracting and retaining talent. They integrated SANS into career pathing initiatives, offering skills for advancement. Additionally, they preferred SANS for its hands-on training, focusing on practical skills. This made SANS a preferred choice for improving workforce capabilities and meeting industry standards.

Insurance:
'Before SANS training, our security posture was reactive, with limited incident response capabilities, siloed knowledge, heavy reliance on vendor solutions and specific team members. We also faced technical gaps, such as limited forensic skills, longer incident resolution times, higher false positive rates and costly vulnerability remediation.'

Manufacturing:
'We comply with NIS2, DORA and other regulations requiring job-specific staff training. We also follow NIST CSF. While compliance training isn't mandatory, it's an option we use to attract and retain talent.'

Financial Services:
'Starting with a team re-organisation last year, our organisation committed to career pathing to create advancement opportunities. Recognising the need for training to support this initiative, we chose SANS training for its proven value. This decision aimed to pair training with career pathing, offering employees the necessary skills for advancement.'

Utilities:
'Our main focus was to provide hands-on training where employees could interact with the keyboard and learn practically applicable skills, rather than just high-level conceptual training.'

Business Value of the Qualified Benefits of SANS

SANS training significantly enhances employee skills across various sectors, making employees more versatile and ensuring a baseline of knowledge through certification. It fosters cohesive teamwork by creating a common language among staff, improves the maturity of cybersecurity teams, reduces false positives and enhances incident investigations.

Additionally, SANS helps retain experienced cybersecurity staff by offering in-person training and career-relevant certifications:

Professional Services:
'With SANS training, our employees are more deployable and were equipped with diverse skill sets, increasing their chances of being selected for various engagements. It also establishes a baseline of knowledge, ensuring accountability and competence through certification.'

Manufacturing:
'One of the most important benefits of SANS training is that it creates a common language among the trained staff and background in response and processes, ensuring cohesive teamwork. Without it, teams would be fragmented.'

Utilities:
'The maturity our cybersecurity teams achieved thanks to SANS training helped reduce false positives as well as increased effectiveness of investigating other potential incidents. That's how trained cybersecurity staff reduces the impact or the number of security incidents.'

Investment:
'SANS training enhances skills, directly improving our security posture. Retaining seasoned cybersecurity staff is challenging, but offering certifications and in-person training helps them build their skill set and stay with the firm.'

When asked about the overall organisational impact of SANS training, IDC learned how SANS has proven highly beneficial across various areas, leading to improved incident detection, efficient security controls, reduced system downtime and faster deployment timelines. Enhanced incident response performance facilitated transitions to cloud infrastructure and fewer cybersecurity findings during audits are among the key benefits.

Organisations have achieved substantial financial benefits by leveraging SANS training to enhance their security capabilities and reduce risk:

Insurance:
'SANS training has resulted in cybersecurity avoidance and incident frequency reduction. Meantime to detect the incident has improved, security controls implementation efficiency has improved, systems downtime has reduced. Deployment timelines have improved.'

Utilities:
'We measure incident response performance by detecting within 1 minute, responding within 10 minutes and closing within 1 hour. We're well within these metrics; SANS training is a big part of that. SANS training contributes a significant role in our well-educated workforce's success.'

Banking:
'Training with SANS was a significant advantage for us, especially as we moved part of our infrastructure to the cloud. Initially, we lacked cloud security knowledge and contracted a third party for help. After training, our team identified and addressed critical security gaps, leading to improved risk assessments and configurations. The training proved highly beneficial, helping us advance our security posture.'

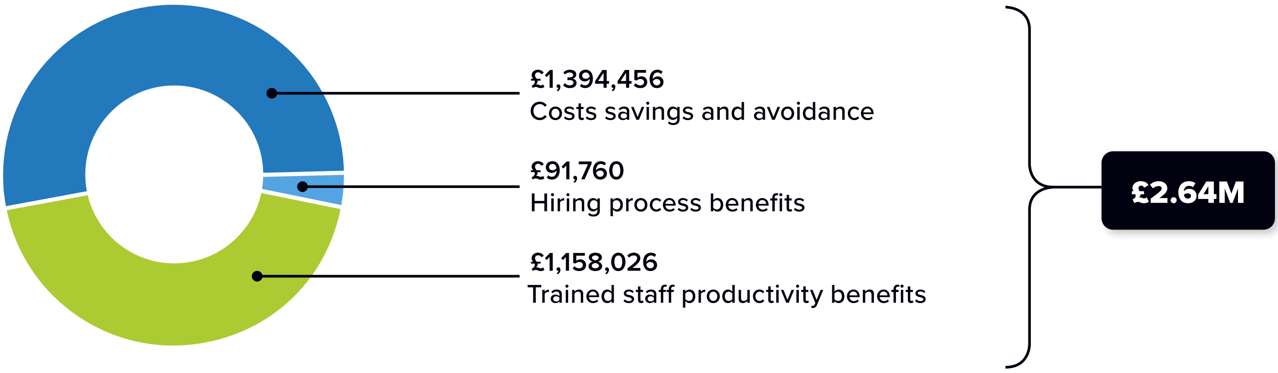
Insurance:
'We've achieved 60% fewer cybersecurity findings during regulatory audits and improved third-party risk management. Our teams enhance vendor security assessments, cloud provider security, contract requirements and compliance monitoring, better navigating audits and managing insurance partner risks, thanks to SANS training.'

The average annual benefits per organisation amount to £2.64 million (**Figure 2**), and per trained staff member, they are £38,998 (**Figure 3,** next page). These benefits, which the following text presents and explains in detail, include cost savings, productivity gains and hiring process improvements. Organisations highlighted the importance of SANS training in achieving cost savings and avoiding external cybersecurity costs.

FIGURE 2

Average Annual Benefits per Organisation

(£ per interviewed organisation)



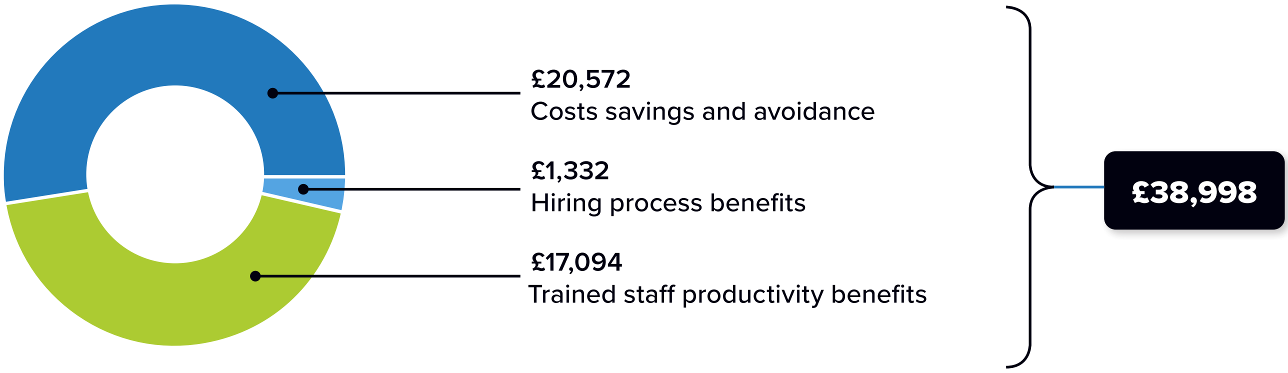
n = 8; Source: IDC's Business Value In-Depth Interviews, April 2025

The average annual additional value per trained staff member equals £38,998 (**Figure 3,** next page). This figure highlights the individual impact of SANS training on staff productivity and effectiveness. SANS-trained staff members contribute to improved security operations, faster incident response and better compliance with regulatory requirements. The training not only enhances their technical skills but also boosts their confidence and job satisfaction, resulting in higher productivity and reduced turnover. Organisations have found that investing in SANS training for their employees leads to substantial returns in terms of both financial benefits and overall security improvements.

FIGURE 3

Average Annual Benefits per One SANS Cybersecurity or Compliance Trained Staff Member

(£ per interviewed organisation)



n = 8; Source: IDC's Business Value In-Depth Interviews, April 2025

Cybersecurity and Compliance Staff Benefits

SANS training fosters open-mindedness and proactive advisory roles, accelerating project delivery and enhancing security implementations. It enables teams to proactively advise on new projects, reducing friction and saving time, and helps teams realise the potential of proper controls, preventing unnecessary project challenges.

The training also enhances compliance efforts and helps manage regulatory risks:

Banking:
'SANS training helps cybersecurity teams become more open-minded, realising that many things are possible with proper controls. This understanding prevents unnecessary project challenges and promotes effective implementation.'

Financial Services:
'SANS training makes the team more informed, enabling them to proactively advise on new projects. This reduces friction and accelerates project delivery, saving a month or two on six major revenue-generating projects.'

Utilities:
'About a year ago, our average time to detect and resolve threats was approximately 1.5 hours. Today, we've managed to reduce this time to 30 minutes or less, significantly speeding up our threat detection and resolution process.'

Professional Services:
'Especially within government services, individuals with these certifications act as force multipliers. Out of 100 people, I invest in 30–40 for SANS certifications, enabling them to become key personnel who can help others learn and apply the knowledge and data.'

SANS training boosts cybersecurity team efficiency, adding significant value through additional productive time. SANS training helped these organisations add 24% additional productive time for SANS-trained cybersecurity staff, and the value of additional productive time was £0.93 million (**Table 2**). These productivity gains demonstrate the significant impact of SANS training on cybersecurity operations. Organisations also noted that SANS training helps improve the efficiency of cybersecurity teams and enhances their ability to manage security incidents.

TABLE 2

Cybersecurity Teams Productivity with SANS

Productivity	Before SANS	With SANS	Difference	Benefit
FTEs	52.3	**64.8**	12.5	24%
Value of additional productive time	£3,869,090	**£4,797,716**	£928,626	24%

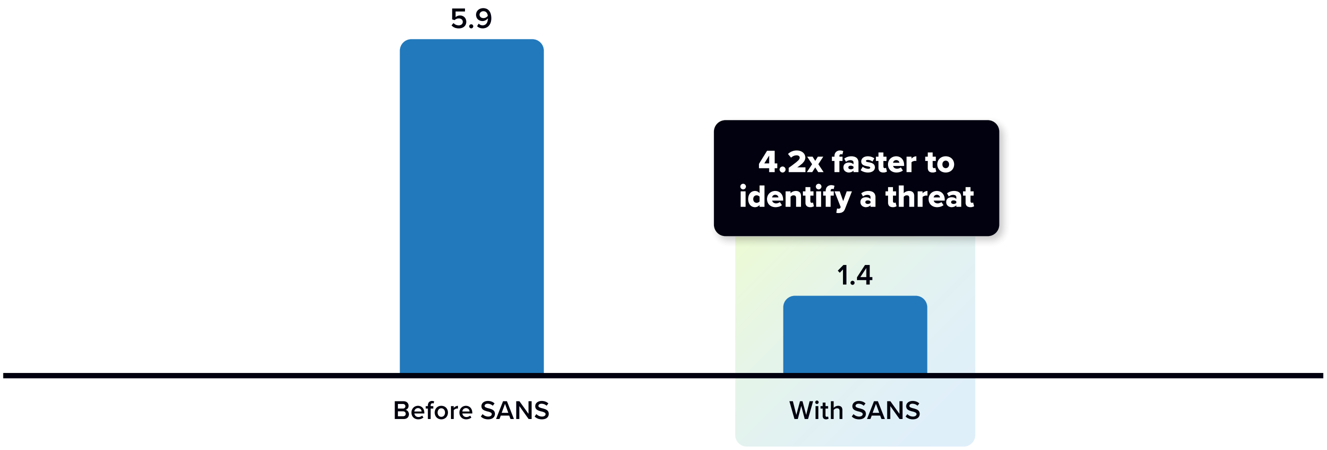
n = 8; Source: IDC Business Value In-Depth Interviews, April 2025

SANS training enables faster threat identification, significantly reducing the time required to detect potential threats. The average time to identify threats decreased from 5.9 hours to 1.4 hours, making threat detection 4.2 times faster (**Figure 4,** next page). This improvement highlights the effectiveness of SANS training in enhancing threat identification capabilities. Organisations also mentioned that SANS training helps improve the accuracy and speed of threat identification.

FIGURE 4

Threat Identification Benefits

(Hours)



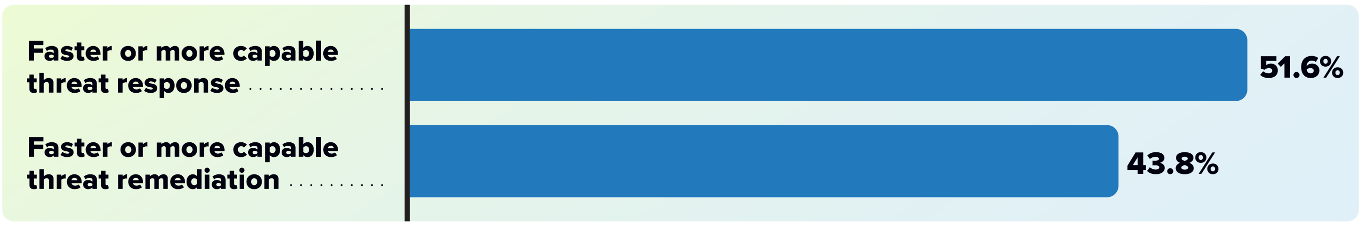
n = 8; Source: IDC's Business Value In-Depth Interviews, April 2025

Improved threat response and remediation capabilities make teams more efficient and effective. SANS training resulted in a 51.6% faster threat response and a 43.8% faster threat remediation (**Figure 5**). These improvements underscore the value of SANS training in enhancing cybersecurity threat management. Organisations also noted that SANS training helps reduce the time required to respond to and remediate threats.

FIGURE 5

Cybersecurity Threat Management with SANS

(Percentage improvements in selected areas)



n = 8; Source: IDC's Business Value In-Depth Interviews, April 2025

SANS training contributes to an overall reduction in cybersecurity incidents, enhancing organisational security and risk management. Organisations reported an 8.8% overall reduction in cybersecurity incidents attributable to SANS training. Organisations also emphasised the importance of SANS training in reducing the frequency and impact of security incidents. An insurance organisation noted that: *'By integrating SANS training, we build security into our digital insurance products, make risk-based decisions and align security with our road map. This includes long-term security development, governance and managing third-party insurer and broker risks, which has been crucial since DORA's implementation.'*

SANS training enhances compliance team productivity, adding value through additional productive time. SANS training of compliance team members translated into a 20% improvement in the equivalent productive time they were able to deliver to their organisations, and the value of additional productive time was £229,400 (**Table 3**). Organisations also noted that SANS training helps improve the efficiency of compliance teams and enhances their ability to manage regulatory risks.

TABLE 3

Compliance Teams Productivity with SANS

Productivity	Before SANS	With SANS	Difference	Benefit
FTEs	15.5	**18.6**	3.1	20%
Value of additional productive time	£1,147,000	**£1,376,400**	£229,400	20%

n = 8; Source: IDC Business Value In-Depth Interviews, April 2025

Cost Savings and Avoidance with SANS

SANS training helps organisations avoid significant external cybersecurity costs and fraud damages annually. Organisations reported avoiding £661,338 in external cybersecurity costs and £733,044 in fraud damage each year (**Table 4,** next page). These cost savings demonstrate the financial benefits of investing in SANS training. Organisations also mentioned that SANS training helps reduce the costs associated with external cybersecurity services.

TABLE 4

Cost Savings and Avoidance with SANS

Cost Savings and Avoidance	Difference
External cybersecurity costs avoided annually	**£661,338**
Fraud damage and costs avoided annually	**£733,044**

n = 8; Source: IDC Business Value In-Depth Interviews, April 2025

Employee Satisfaction Benefits with SANS

SANS training boosts employee satisfaction, retention and career development, making staff more marketable and valued. It leads to increased technical staff satisfaction, improved career development satisfaction, enhanced job role confidence and a rise in perceived organisational investment.

Employees see SANS training as an investment in their productivity and personal value, enhancing job satisfaction and retention:

Insurance:
'SANS training is perceived as an investment in employees' skills, making them more marketable and improving retention. We've observed a 30% increase in technical staff satisfaction, a 50% improvement in career development satisfaction, a 40%–50% boost in job role confidence and a 50% rise in perceived organisational investment.'

Financial Services:
'Employees see SANS training as an investment in their productivity and personal value, enhancing job satisfaction and retention. Despite higher-paying offers, some employees see the value of the training and stay with our organisation. This commitment to their development fosters trust and directly impacts job satisfaction.'

Professional Services:
'I would say that those who have taken the SANS training have more opportunities because they're more of a Swiss army knife. It affects their ability because of the variety or knowledge of training, they can talk on so many topics, they are more valued or more wanted than someone without that ability.'

Manufacturing:
'For young cybersecurity professionals starting their careers, SANS offers the best value in terms of establishing a common training culture. SANS provides a level of consistency and quality that is often lacking in other training programmes, including recognition of quality across companies and industries.'

SANS training extends the average tenure of cybersecurity staff, reducing turnover and associated hiring costs. The average tenure for SANS-trained staff increased by 36.8%, reducing the need for new hires and associated costs (**Table 5**). This extension in tenure highlights the retention benefits of SANS training. Organisations also mentioned that SANS training helps improve employee retention and reduces turnover.

TABLE 5

SANS-Trained Employees Tenure and Hiring Savings Benefits

Cybersecurity Staff Hiring Savings	Before SANS	With SANS	Difference	Benefit
Average tenure for cybersecurity staff (years)	4.40	**6.10**	1.63	**36.8%**
Total costs associated with a new hire	£29,008	**£29,008**	N/A	N/A
New hires per year	11.80	**8.60**	3.17	26.9%
New hires costs per year	£341,362	**£249,602**	£91,760	26.9%

n = 8; Source: IDC Business Value In-Depth Interviews, April 2025

SANS training fosters innovation, making employees more creative and effective problem solvers. Organisations reported that SANS-trained employees are, on average, 26% more innovative compared to their non-SANS-trained counterparts. This increase in innovation demonstrates the positive impact of SANS training on employee creativity and problem-solving abilities. Organisations also noted that SANS training helps improve employee innovation and problem-solving skills. Further, a utilities organisation spoke to IDC about the positive effects of SANS training for its employees: *'SANS training makes employees more creative and effective problem solvers. They design and engineer solutions that are more elegant, cost-effective and relevant to the business.'*

Investment and Benefit Analysis of SANS Training

SANS training delivers substantial benefits within a one-year period, with significant returns on investment. The average organisation in the researched data set spends £501,276 on SANS training to receive benefits amounting to £2.64 million, resulting in a benefit of £2.15 million in a given year (**Table 6**). This analysis highlights the immediate financial returns of investing in SANS training, demonstrating its effectiveness in enhancing the efficiency and productivity of cybersecurity and compliance teams.

Organisations noted that SANS training helps achieve quick and impactful improvements in security posture, staff productivity and cost savings, making it a valuable investment for enhancing organisational security and compliance capabilities.

TABLE 6

One-Year Investment and Benefit Analysis

Investment and Benefit Analysis	Per Organisation	Per SANS-Trained Cybersecurity and Compliance FTE
Benefits	£2,644,168	£38,998
Investments	£501,276	£7,326
Difference	**£2,142,892**	**£31,598**

n = 8; Source: IDC Business Value In-Depth Interviews, April 2025

Challenges/Opportunities

In the security industry, SANS is on the premium end of the training market. This is reflected both in the high level of education offered by instructors (many of whom are leading experts in their area of specialisation) and in pricing.

A key challenge for SANS is maintaining its premium positioning in the market even as some buyers prefer training that is delivered through self-paced, online video courses (a method that many organisations would perceive as less premium than in-person training, and which does not necessarily yield the same business value).

Conversely, the IDC study found that organisations selecting SANS as their cybersecurity training provider reported a variety of tangible and intangible benefits. These outcomes suggest that high-quality cybersecurity education delivered by experienced professionals can positively influence employee skills and overall organisational performance. This offers SANS a strong opportunity to focus on, given its premium approach.

Of course, the willingness to invest in premium training depends on customers recognising the value and importance of ongoing, comprehensive security education and the benefits that SANS brings to the table compared to its competitors. Proving the value of training is not unique to cybersecurity, and this has been a challenge across the broader IT learning and development industry.

In addition, while the cybersecurity training market is highly competitive, SANS offers programmes suitable for professionals at different career stages and for organisations with diverse security upskilling needs. SANS's training portfolio is well-positioned to cater to a diverse range of professionals and company sizes, which provides the company an advantage over more niche competitors.

Conclusion

This IDC study clearly demonstrates that SANS training delivers substantial and measurable business value across a wide range of industries and organisational sizes. Organisations that invest in SANS training report significant improvements in cybersecurity outcomes and operational and staff efficiency.

On average, each SANS-trained staff member contributes an additional £38,998 in annual value, while organisations realise, on average, £2.64 million in total value per year – far exceeding the cost of investment. Faster threat detection and response, reduced system downtime, improved compliance outcomes and enhanced employee satisfaction and retention drive these gains.

SANS training also fosters innovation, strengthens team cohesion and supports long-term career development, making it a strategic asset in addressing the cybersecurity skills gap. The research highlights that high-quality, hands-on training – delivered by experienced practitioners – can transform cybersecurity teams into proactive, high-performing units. As cybersecurity threats grow in complexity and frequency, the ability to upskill staff effectively and efficiently becomes a critical differentiator. SANS's comprehensive, flexible training model positions it as a premium provider capable of meeting evolving enterprise needs. For organisations seeking to enhance security capabilities while achieving strong returns on training investments, SANS training offers a proven, impactful solution.

Appendix: Methodology

IDC used its standard Business Value/ROI methodology for this project. This methodology gathers data from organisations using SANS training.

Based on interviews with organisations using SANS training, IDC performed the following process to establish the return on investment of SANS training:

1. **IDC gathered quantitative benefit information during the interviews** using a before-and-after assessment of the impact of using SANS training.
2. **IDC created a complete investment profile based on the interviews:** investments go beyond the initial and annual costs of using SANS training and can include additional costs related to migrations, planning, consulting and staff or user training.
3. **IDC established the value of the average annual benefits derived from SANS training** by comparing the researched total investments and the value of the sum of the discrete benefit areas.

IDC bases the payback period and ROI calculations on several assumptions, which are summarised as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and manager productivity savings. For this analysis, based on the geographic locations of the interviewed organisations, IDC has used assumptions of an average fully loaded salary of £74,000 per year for IT staff members and an average fully loaded salary of £51,800 per year for non-IT staff members. IDC assumes employees work 1,880 hours per year (47 weeks x 40 hours).
- Because IT solutions require a deployment period, the full benefits of the solution are unavailable during deployment. To capture this reality, IDC prorates the monthly benefits and subtracts the deployment time from the first-year savings.

Note: all numbers in this document may not be exact due to rounding.

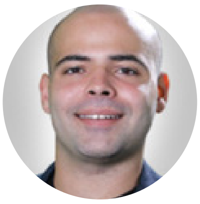
About the IDC Analysts

David Clemente

Research Director, European Security, IDC

Dave Clemente is a research director in IDC's European Security practice, with a focus on security services (including managed services and professional services). He is a research professional with more than 15 years of experience in cybersecurity, including in think tanks, professional services and market analysis.

More about David Clemente



Leonardo Freitas

Research Manager, European Skills Practice, IDC

Leonardo Freitas leads IDC's European IT Talent for AI, Cybersecurity, Cloud and Digital Business Success theme, focusing on IT talent, skills development, skills mapping and identification of key competences in core areas of technology. He has a background in research and consulting, with more than 10 years of experience in technology, ICT, public sector transformation and FMCG.

More about Leonardo Freitas

Ladislav Kinda

Consultant, Business Value Strategy Practice, IDC

Ladislav Kinda is a consultant in the IDC Business Value Strategy practice team. Kinda conducts customised business value research and consulting projects for clients across various technology domains. His primary focus is assessing the return on investment from their adoption of enterprise technologies. Kinda's research delves into how organisations leverage digital technology solutions and initiatives to enhance efficiency and drive business growth.

More about Ladislav Kinda

Message from the Sponsor

SANS | GIAC CERTIFICATIONS

SANS Institute is the world's most trusted and largest provider of cybersecurity training and certification for professionals across government and commercial sectors.

SANS offers over 85 expert-led courses through in-person, virtual and OnDemand formats. Its affiliate, GIAC, validates hands-on skills with more than 50 technical cybersecurity certifications. The SANS Technology Institute, a regionally accredited subsidiary, offers bachelor's and master's degrees, graduate certificates and an undergraduate certificate in cybersecurity.

SANS also supports the global InfoSec community with free resources such as research reports, webcasts, podcasts and the Internet Storm Center– an early warning system for cyber threats. Powered by a network of experienced practitioners, SANS advances the mission of improving cybersecurity readiness worldwide.

Learn more at www.sans.org

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

idc.com in @idc X @idc