THE Human Sensor PROGRAM

"SEC464 brings awareness to people with various levels of understanding in IT Security including risks, exploits, and vulnerabilities. Everyone will gain something out of this course."
-Larry Lee, Columbia University

SANS
SEC464

Hacker Detection for Systems Administrators

with CONTINUING EDUCATION

There are just not enough well-trained network security professionals to meet the daily onslaught of cyber criminal and cyber-terrorist activities. This is an important challenge for organizations because perimeters are routinely being breached, allowing attackers to roam through networks for weeks or months on end without being discovered. This program addresses this challenge.

SANS

For more information:
HumanSensor@SANS.org
www.sans.org/human-sensor
US +1 646 257 5875
UK +44 779 257 9875

It took just a modicum of skill using tried-and-true hacking techniques for criminals to pull off the record-setting data breach of the retail chain TJX in 2007 – and then top that by stealing even more data from payment card processor Heartland Payments System in 2008.

Once the bad guys got inside each company's firewall, they were able to extract a steady stream of data in each case for more than a year. [They] allegedly used mundane hacking techniques to extract some 94 million records from TJX, parent of TJ Maxx and Marshalls, over the course of at least eight months, and 130 million records from Heartland over 14 months.

"They stayed inside the network chucking stuff out of the window, and nobody noticed, much less tried to stop them," says Michael Lloyd, chief scientist at network security firm RedSeal.

-Lastwatchdog.com

A new defensive approach is needed. SANS has developed this unique training program for systems and network administrators which has been embraced by many leading US organizations. **Sandia National Labs, NASA, the State of Texas, and many of the leading US Universities** have trained hundreds of sysadmins in the program.

> "The reason that we're losing in the computer security battle is many key players, who should be the first line of defense, don't have the time to know their networks, let alone the types of attacks and abnormalities that should provide warning signs."
>
> -John Strand, Course Author

The Human Sensor Program **gives systems administrators tools and techniques** to illuminate evidence of potentially malicious activity on their systems and teaches them how to look deeper to determine whether the problems they see are real. It turns them into Human Sensors for malicious activity in their organizations and **teaches them how to work effectively with their organization's security professionals** to resolve these problems.

> "Coming from a system administration background, now in a security role I really wish I would have had a class like this available then. I am recommending all of our system administrators take this course. It would help overall security operations in our organizations."
>
> -Curt Shaffer, Synaptek Corporation

This class will close the distance that seems to exist between many security professionals and the systems administration staff they work with every day. **Many times sysadmins don't even understand what it is that security professionals want them to do.** They don't appreciate the possible consequences of doing or not doing what the security professionals are requesting. This class will better equip sysadmins to bridge this divide. And, while not the primary goal, the class will also help sysadmins to better prepare for security audits.

> "The course provides 'quick wins' and key tools without being overwhelming or information overload."
>
> -Timothy Kotoski, The Kemtah Group

This class is designed to help the systems and network administrators of an environment understand what it is that they need to do to meet security and audit requirements so they can get back to doing their job of keeping that environment running.

John Strand, Course Author

For more information:
HumanSensor@SANS.org
www.sans.org/human-sensor
US +1 646 257 5875
UK +44 779 257 9875

Who Should Attend?

This program provides a two-day introductory class followed by a continuing education program. It is tuned directly to the interests of system administrators and establishes a clear entry career path from sysadmin to security professional. It is not designed for trained security professionals.

Organizations really benefit from this innovative SANS program when they train a significant percentage of their sysadmin staff. Further, by taking this class through the SANS Onsite program, the organization benefits from the certified SANS instructor's ability to focus the discussion on the specific needs of the organization.

CONTINUING EDUCATION

Quarterly Threat & Tool Briefings

Good training needs to be continuous and needs to build upon the core learning objectives from the two-day class. In this way students can leverage and apply what they have learned in class to real-life situations as they arise. The Human Sensor Program, therefore, **includes a minimum of four Quarterly Threat & Tool Briefings during the 12 months following the two-day class.** These are included as part of the initial training fee.

These Quarterly Briefings highlight the newest attack vectors. They also demonstrate how the information provided in each briefing, together with the tools and techniques they learned in class and in previous Quarterly Briefings, can be adjusted to target the latest attack vectors. It's like having your own personal education coach for sysadmin security.

This is hands-on training that is fresh and relevant. Only students who have entered the Human Sensor Program will have the option to continue the Quarterly Threat & Tool Briefings through payment of an annual fee once they have completed their first 12 months of continuing education.

Topics Covered in this Course

- Why bad things happen to good systems administrators: Five common mis-configurations and mistakes that lead to a system being compromised
- Security methodology and thought process in daily systems administration activities
- A sysadmin's view of what matters in systems architectures
- Security monitoring: Not knowing makes the auditors and hackers happy
- The hard part – knowing what is normal for Windows and Unix systems
- The harder part – knowing what is abnormal for Windows and Unix systems
- Hardening Windows and Unix systems is easier than you thought
- Command line kung fu for Unix and Windows
- Understanding network traffic for systems administrators
- Malware: Why it is still effective in your environment

> **"Great foundational material for system administrators to establish a relationship with their information security team."**
> -Jeff Wickmam, Thrivent Financial for Lutherans

Pricing Schedule

- **Class Title:** SEC464: Hacker Detection for Systems Administrators
- **Class Length:** Two-day class PLUS *vLive Quarterly Threat & Tool Briefings*
- **Catalog Pricing:** $2,195 per student Initial Training Fee
  (Includes one-year subscription to *vLive Quarterly Threat & Tool Briefings*).

  $495 per student for one-year subscription to *vLive Quarterly Threat & Tool Briefings*
  (Includes access to all course updates and modules via SANS OnDemand and any periodic Web-based attack updates).

Participating organizations pay an Initial Training Fee for the Class and the first year of *vLive Quarterly Threat & Tool Briefings* based on the number of Systems Administrators that the organization chooses to train. This is then followed by an Annual Subscription Fee for the *vLive Quarterly Threat & Tool Briefings* per System Administrator. Training delivery has three options: live SANS OnSite training, SANS v-Live! training, and SANS OnDemand training. These options can be combined.

Special Pricing for Multiple Students

Number of Students per Class [1]	Initial Training Fee Per Class of Students (This includes one year subscription to *SANS vLive! Quarterly Threat & Tool Briefings* for each student) [2]	Annual Subscription per Class of Students for *SANS vLive! Quarterly Threat & Tool Briefings* for Year Two [3]
Up to 25 [4]	$46,000 – equivalent to $1,840 per student	$12,000 – equivalent to $480 per student
Up to 50 [5]	$82,000 – equivalent to $1,640 per student	$22,000 – equivalent to $440 per student
Up to 100 [6]	$149,000 – equivalent to $1,490 per student	$40,000 – equivalent to $400 per student
Up to 250 [7]	$300,000 – equivalent to $1,200 per student	$87,500 – equivalent to $350 per student
Above 250	Call for pricing	Call for pricing

Pricing information is in US Dollars.

Notes:

[1] Recognizing individuals may be in multiple locations and/or need training at different times, courses can be taken in a combination of formats including OnSite, vLive! and OnDemand.

[2] Customer has one year from date of agreement to complete the initial training.

[3] Includes access to all course updates and modules via SANS OnDemand and any periodic Web-based attack updates. Access to *vLive! Quarterly Threat & Tool Briefings* is granted only to students who have participated in the SEC464 2-day class. Repeat attendance at instructor-led classes via On-Site or vLive! is not included in subscription.

[4] Includes one SANS instructor-led On-Site or vLive! session for SEC464.

[5] Includes up to two separate SANS instructor-led OnSite or vLive! sessions for SEC464.

[6] Includes up to three separate SANS instructor-led OnSite or vLive! sessions for SEC464.

[7] Includes up to five separate SANS instructor-led OnSite or vLive! sessions for SEC464.

> *"This course provides cutting edge security topics for both Windows and Unix and bridges the gap between cyber security professionals and system administrators. The hands on exercises reinforce the course content and demonstrate how attacks can happen and how to stop them and most importantly gives the systems administrator the knowledge to know what is normal and abnormal on their systems."*
>
> -Jeremy Baca, Cyber Security Technologies,Sandia National Labs

SANS

For more information:
HumanSensor@SANS.org
www.sans.org/human-sensor
US +1 646 257 5875
UK +44 779 257 9875