



SIG² G-TEC SANS Top 20 Consensus Research Initiative

Steven Sim Kok Leong
Team Lead / Principal Investigator
SIG² G-TEC SANS Top 20 Consensus
Research Project

steven@security.org.sg



About SIG²

- Special Interest Group in Security and Information inteGriTy (SIG²)
- Information Technology Security (ITSec) society in Singapore and South Asia.
- Participated in and contributed actively to major National ITSec initiatives.
- Initiatives to consolidate Singapore as the regional hub for ITSec.
- Setup of G-TEC (Garage for Technical Excellence and Collaboration) and first independent security test lab in Singapore and Asia-Pacific.
- Embarked on plan to build ITSec Career roadmap that focused on ITSec continuing education and building baseline for ITSec professionals through Centre for Competency.
- More details can be found at: <http://www.security.org.sg>



Agenda

- Objectives
- Why is this list important?
- Rough guide to consensus process
- Call for participation
- Looking for more Information?



Objectives (1)

- SANS Top 20 Consensus for 2004 wrote:

“The Top-20 is a consensus list of vulnerabilities that require immediate remediation. It is the result of a process that brought together dozens of leading security experts. They come from the most security-conscious government agencies in the UK, US, and Singapore; the leading security software vendors and consulting firms; the top university-based security programs; many other user organizations; and the SANS Institute.”



Objectives (2)

- Represent consensus voice from local IT security community
 - Defining the list
 - Defining the ranking of list
 - Defining how vulnerabilities should be mitigated
- Increase SIG² visibility



Why is this list important? (1)

- Many VA solutions rely on this list
 - Qualys SANS Top 20 scan
 - <https://sans20.qualys.com/>
 - nCircle IP360
 - http://www.ncircle.index.php?s=news_press_2004_1102
 - Counterpane
 - <http://www.counterpane.com/pr-sans.html>
- More details
 - <http://www.sans.org/top20/tools.pdf>



Why is this list important? (2)

- Reliance by organizations on it as first vulnerabilities to patch in a risk assessment exercise.
- An inappropriate list would increase the security risk of devices relying on it.



Rough guide to consensus process (1)

1. Nominate new SANS Top 20 vulnerabilities
(All participants)
 - Identify which vulnerabilities are still relevant from SANS Top 20 for previous year
 - Identify whether this is an accurate picture of threats for now and coming months, etc.
2. Voting / Ranking these vulnerabilities
(All participants)
3. Develop expert commentary
(Development team)
 - Nature of threat
 - Identification
 - Subsequent mitigation/remediation



Rough guide to consensus process (2)

4. Collation and initial compilation
(Editorial team)
5. Proof read, validation and review
(Editorial team) [multiple cycles]
 - Independent verification of content
 - Verify for grammatical errors
 - Review for quality assurance
6. Proof and review by SANS Executive
7. Public release



Call for participation

- Join the SIG² SANS Top 20 Consensus Research Team
 - <http://www.security.org.sg/gtec/sanstop20/subscribe.html>
- Team benefits
 - Make your voice heard
 - Peer recognition
- Team details
 - <http://www.security.org.sg/gtec/sanstop20/team.html>



Looking for more Information?

- SIG² SANS Top 20 Research Team
 - <http://www.security.org.sg/gtec/sanstop20>
- SANS Top 20 Consensus
 - <http://www.sans.org/top20>