Mind the Gap Analysis

Details of CNS Hut3's SANS Top 20 Gap Analysis

www.hut3.net

Benchmark Your Security

Your SANS Top 20 Gap Analysis will review and assess the current policies, technical controls and general governance standards in place that support your IT Environment and Data Security. The review encompasses an assessment of:

1. Governance, policies, processes and standards (including a formal risk assessment)
2. Security architecture
3. Security controls and tools
4. System development lifecycle
5. Operational IT Security
6. Monitoring, Management and Incident Response
7. General Security Awareness & Training

Benefits of a Gap Analysis

With a CNS Hut3 SANS Top 20 Gap Analysis you can:

- Identify clear, practical, strategic measures to protect your business data
- Identify any gaps in your current security programme and objectively prioritise their closure
- Benchmark your security processes and performance against the metrics of a respected industry standard to clearly demonstrate value and on-going improvement to stakeholders

In a Nutshell

The aim is to achieve a gap analysis of your organisation against a best practice security model, in this case the SANS Top 20. This common control set seeks to provide an analysed base on which to build compliance to a multitude of standards such as The Data Protection Act, ISO27001, ISO22301, Cobit, PCI DSS, FCA, SEC, SYSC 3.2.6 etc.). In particular this will be done with a view to industry level analysis, marking your organisation against peers in your sector where possible.

The result: A pragmatic roadmap for closing prevalent security gaps in a risk prioritised order for your organisation.

What is the SANS Top 20

The SANS Top 20 is a prioritised list of critical security controls designed to provide maximum benefits toward improving risk posture against real-world threats. This list of 20 control areas grew out of an international consortium of U.S and international agencies and experts, sharing from actual incidents and helping to keep it current against evolving global cyber security threats. The list is comprised of:

1. Device inventory (authorised and unauthorised)
2. Software inventory (authorised and unauthorised)
3. Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers
4. Continuous vulnerability assessment and remediation
5. Malware defences
6. Application software security
7. Wireless access control
8. Data recovery capability
9. Security skills assessment and appropriate training to fill gaps
10. Secure configurations for network devices (i.e. Firewalls, routers, switches)
11. Limitation and control of network ports, protocols, and services
12. Controlled use of administrative privileges
13. Boundary defence
14. Maintenance, monitoring, and analysis of audit logs
15. Controlled access based on a “need to know” risk rating
16. Account monitoring and control
17. Data protection
18. Incident response and management
19. Secure network engineering
20. Penetration tests and red team exercises