

Session T3 – Auditing in a Windows Environment

By Nicholas Green

Topic Summary

This session will introduce you to auditing a Windows environment. It will cover an introduction to the major elements of the Windows Server NT/2000/2003 security architecture and provide you with an approach to auditing a Windows environment. You will learn about Active Directory including, trees and forests, domains and organizational units, user and group administration, user rights and privileges and the delegation and control of administrative authority. You will learn about the security and configuration settings available in Windows, the use of Group Policy to apply security configuration settings to users and how Windows auditing can be implemented. You will explore key settings to secure Windows servers. You will review some of the differences between the different versions of Windows Server and how they can affect security. You will learn techniques for collecting audit evidence for Windows audits and how to take advantage of the array of free tools to perform more effective audits.