

Session #S21

Name:	Michael Smith
Presentation Title:	How to Protect from Malicious Code – Using Honeynet and Darknet Technology as Part of a Compliance Program
Abstract:	
<p>The purpose of this presentation is to explain and demonstrate methods for improving an organizations' security posture as it is related to untargeted malicious code. I will show why this is important and how measurable success can be achieved with minimal resource investment. The specific methods that I will be examining are the creation of an Incident Response (IR) toolkit and the deployment of a honey net and/or dark net.</p> <p>The participant will learn more about:</p> <ul style="list-style-type: none"> • The importance of Configuration Management (CM) and sound engineering practices to security • The ways that honey net technologies could be valuable to your organization and how they can be a part of a greater compliance solution • How to detect possible malicious code on your network • What to do if you discover malicious code on your network 	
Target Audience:	
<p>Intermediate-Advanced Security First line managers and direct contributors</p>	
COBIT Objectives:	
<p>DS3 Manage Performance and Capacity DS5 Ensure Systems Security ME1 Monitor and Evaluate IT Processes ME2 Monitor and Evaluate Internal Control</p>	
Speaker Bio:	
<p>Mr. Smith has more than ten years of experience in the field of Information Security. He has provided security consulting services to state, local, and federal governments as well as many commercial clients across multiple verticals. He has achieved various industry certifications throughout his career, such as the PMP and CISSP. He has published articles about honeynet and darknet technologies and is currently doing research related to malicious code detection. Most recently Mr. Smith has worked as the Senior Manager to design and manage the operation of the Multi-Sate Information Sharing and Analysis Center Security Operations Center (MS-ISAC SOC).</p>	