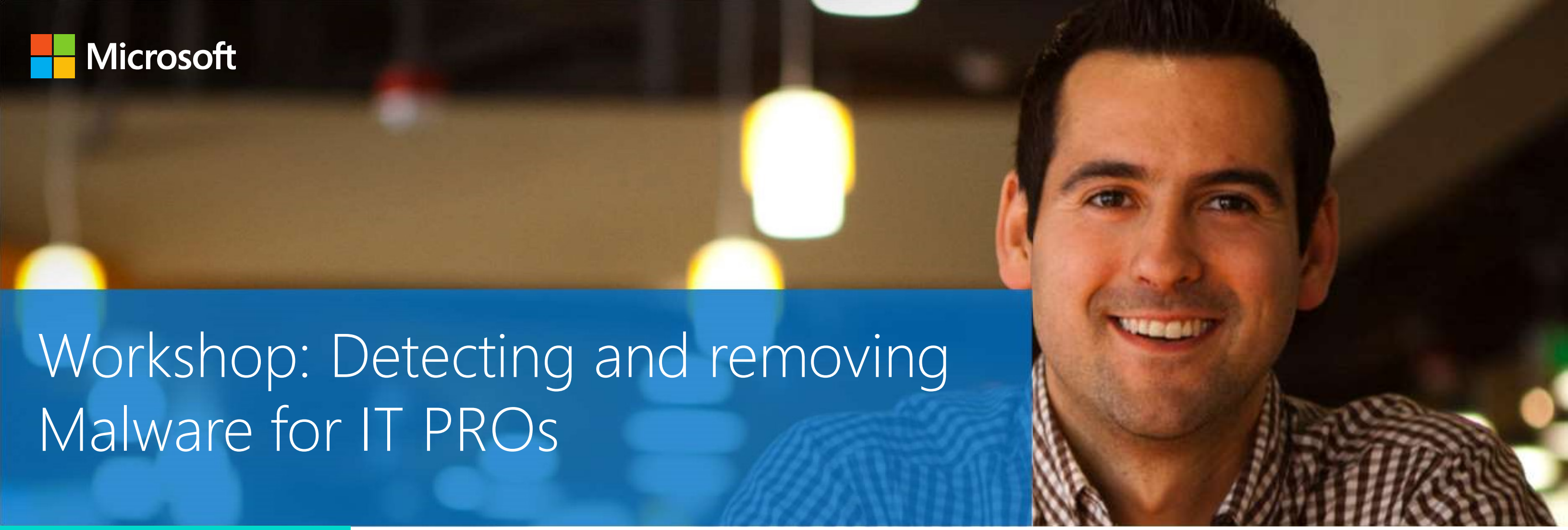
Microsoft



Workshop: Detecting and removing Malware for IT PROs

Premier Workshop

Target Audience:

This Workshop is an advanced Workshop and is targeted for System Administrators and Security Professionals working on Windows Infrastructure.

The basic concepts and know-how of the product will not be covered in this course, and it is expected that attendees will already possess that knowledge.

Overview

Detecting and removing malware for IT PROs gives the techniques and tools needed to identify and remove malware on Windows environments. The course is delivered via PowerPoint presentation, live demos, and "capture-the-flag" labs.

This workshop is focusing on IT PROs, while some PowerShell understanding would be helpful, developer skills are neither a prerequisite nor will we use debugging technologies. Tools used will be mainly Windows on-board functionality as well as the Sysinternals Suite.

Key Features and Benefits

Each group of modules is organized by scenario and is designed to provide participants with in-depth expertise, tools and hands-on experience of how to use advanced techniques to detect and remove malware.

Technical Highlights

After completing this course, you will be able to:

- Understand how malware enters and explores your infrastructure
- Know effective approaches to detect and identify malware
  - Static analysis
  - Dynamic analysis
  - Post-mortem analysis based on Eventlogs

Syllabus

This workshop will take place for two full days:

Module 1: Introduction to Malware

- Malware Categories
- Next Generation Malware
- Forensics vs. Incident Response

Module 2: Malware Analysis

- Analysis Overview
- Static Analysis
- Dynamic Analysis

Module 3: Post-mortem Analysis: Detecting Malware using Eventlogs

- Introduction and Prerequisites: Windows Security Auditing, configuring a Baseline, Windows Eventlog Forwarding
- Analyzing Windows Security Eventlog
- AppLocker Audit Mode
- Monitoring Registry Usage
- Monitoring PowerShell Usage
- Monitoring using Sysmon
- Filtering for suspicious activities

Microsoft

This data sheet is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY