CounterSnipe™

Intrusion Prevention Training

CounterSnipe Systems LLC
http://countersnipe.com

Empowering security engineers to make the most of IDS/IPS systems

CounterSnipe

CounterSnipe Technical Training

Target Audience

This course is directed at those who need to understand not only the advantages that IDS and IPS can bring to an organization but also how to implement and manage a successful deployment. Specific target groups include;

IT Security Architects
Security Operations Managers/Engineers
Network Managers looking to learn about security
Technical Support Engineers
Hands on CISOs
Data Center Managers
Security Analysts
Or anyone else involved with Host or Network security.

Objectives

This hands-on instructor led course is aimed at providing delegates with the knowledge, skills and confidence to utilize both IDS and IPS technologies. This includes focusing not only on operation but also giving an in-site into common threats and attacks that are actively used on the Internet today.

Although most of this course provides knowledge that can be ported between products, it focuses on both the CounterSnipe Security System and the open source Suricata detection engine.

It not only covers usage and configuration of a device but also develops valuable skills in analyzing and deciding whether an attack is a real business threat or falls into one of the following categories.

- False Positives, a false alert on normal operation traffic
- Policy Violations, application usage that does not comply with your security policy.
- Internet white-noise, non-targeted alerts from worms, propagating viruses, etc.
- Non-specifically targeted attacks, Automated scripts launched regardless at blocks of IPs
- Targeted attacks, attempts by a real person to gain unauthorized access to your specific network resources

A good IDS system will present as much information about the attack as possible to the administrator, allowing him to make an informed decision of how to react to the presence of a threat on their network. This is key to the incident response process, and where IPS can provide real value. IPS can remove the required human actions associated with incident response on specified attacks.

Details

- Understanding Intrusion Detection/Prevention Systems
- Understanding Risk Management
- The role of IPS in Information Risk Management
- Traditional Security v Intelligent Security

- Understanding Information Producers
- IDS in Corporate Infrastructures
- Suricata – the Multi Threading Engine
- CounterSnipe Security Software - details
- Deploying and fine tuning active IDS/IPS rule set
- Understanding the problem – examples of different types of security risks with real time data collection depending on the organizational policies.
- Methods of reacting to these problems..possible actions
- The role of Asset Detection in managing IDS events
- Configuring IPS to auto eliminate identified problems
- Creating bespoke signatures and policies.
- Good rule writing.
- Creating and working with rule groups and classifications.
- How to measure the benefits of an NIDS/NIPS
- Securing the entire organization

Duration: 2 Days

Course Fee: Price on request - EX Taxes per person(Min 2)

Maximum Number of Delegates: 10