No Theories...

No Cramming...

No Boot Camps...

No Crash Courses...

No Certifications...

No Information Dumps...

No (Web-Based) Lectures...

Hands-On How-To® Training: Threat & Incident Response

How-To Instructions

Real-World Simulations

Hands-On Exercises

Expert Instructors

Small Class Sizes

Tailored Courses

Updated Content

Arsenal of Security Take-Aways

Post-Training Support

Satisfaction Guaranteed

Course Overview:

NetSecurity's **Hands-On How-To® Threat & Incident Response** course teaches incident responders, malware analysts, and forensic investigators the mandatory knowledge necessary to investigate zero-day attacks, data breaches, or perform other live investigations. Students learn how to establish incident response capabilities and prepare their organizations to carry out investigations. The course also provides practitioners the skills needed to excavate and analyze malicious software, resulting from Advanced Persistent Threats and other emerging intrusion techniques. Students learn how to dissect malware and formulate mitigation strategies for preventing future penetration.

The Hands-On How-To Lab Exercises (HOHTLEs) covered in the course incorporate significant real-world experience necessary for delivering world -class results in the field.

NetSecurity Benefits:

Through years of real-world hands-on security and forensics experience, NetSecurity has supported Fortune 500 companies, federal agencies, corporations, and law firms. The benefits of our Hands-On How-To course include:

- Skills to establish and fortify an organization's security, forensics, and incident response capabilities
- Customized private sessions, tailored towards organizations' unique environments
- Detailed step-by-step and how-to instructions
- Instructor-led and student-performed hands-on exercises
- Real-world simulations of forensics challenges
- Seasoned expert instructors with real-world hands-on consulting and training experience
- Arsenal of take-aways (tools, templates, guides, and relevant forensics resources)
- Up-to-date course content, addressing emerging forensics challenges
- Small class sizes ensuring maximum student-instructor interaction
- Vendor-neutral content – covering commercial and freeware tools

Target Audience:

The course is targeted towards technical professionals, including:

- Computer Forensics Investigators
- Law Enforcement Personnel
- Information Security Managers
- Threat/Incident Responders
- Malware Analysts
- IT Professionals
- Cyber Crime Attorneys
- Private investigators
- Compliance Officers
- Auditors

Course Format:

- Interactive presentations by security and forensics expert instructor
- Hands-On How-To Lab Exercises (HOHTLEs) in performing computer forensics and incident response

Course Duration: **3** Days

Course Cost: **USD $3,000.00** (List Price)

Course Objectives:

Upon successful completion of the **Hands-On How-To® Threat & Incident Response** course, each participant will be armed with the knowledge, tools, and processes required in producing computer, formulating incident response strategies and conducting incident investigations, and conducting malware analysis and produce a report that can withstand legal scrutiny.

Course Topics:

NetSecurity's **Hands-On How-To® Threat & Incident Response** course includes in-depth coverage of real-world scenarios and HOHTLEs in the following areas:

• Topics	• Discussion and HOHTLEs
Incident Response Process	• Building Incident Response Capability • Preparation • Incident Readiness Planning • Identification • Containment • Eradication • Recovery • Lessons Learned
Legal Considerations	• Internet Laws and Statutes • Legal Concerns and Privacy Issues • Court Admissibility of (Volatile) Evidence

Evidence Collection	• Volatile Data Collection
	  o Pros and Cons of System Shutdown
	  o Order of Volatility (Memory, Process, Network, Registry)
	• Hard Drive Imaging
	  o Physical Image
	  o Logical Image
	  o Full/Partial Drive Encryption Scenarios
	• Documenting the Cyber Crime Scene
	• Collecting Additional Storage Devices, Sticky Notes, etc.

Evidence Preservation	• Securing the Evidence • Chain of Custody
Preparing Incident Response Tools	• Statically Linked Binaries • Import Library • Incident Response Tools Selection
Hackers' Methods of Maintaining Presence (Persistence Methods)	• Surviving Reboots • Autoruns • Services • Service Host Services • Stubpath • Scheduled Tasks • Windows Firewall
System Compromise Indicators (Quickly Detecting and Confirming Intrusions)	• Firewall, IDS, etc. • Temporary Internet Files • Anti-Virus Logs • Hosts File • DNS Cache • Running Services • Critical Log Files • Network Connections • Memory • Recycled Bin • Hidden and Protected Files

• Topics	• Discussion and HOHTLEs
Volatile Data	• Collection and Analysis on a Live System • Collection and Analysis of Physical and Process Memory • Volatile Evidence in Incident Response • Court Admissibility of Volatile Evidence
Memory Forensics	• Physical Memory Acquisition • Extracting and Examining Processes • Network Connections • Extracting Crucial Artifacts • Windows Registry Analysis • User Activity Reconstruction
Windows Registry Analysis	• Monitoring Registry Changes • System Information • Users Activities • AutoStart Locations
Network Analysis	• Capturing and analyzing network packets • Leveraging IDS/IPs rules and signatures to detect attacks • Analyzing malicious payload in network packets
Forensics	• Timeline Analysis • File Signature Analysis • Hash Analysis
Malware Analysis	• Malware Taxonomy • Malware Threats • Malware Analysis Methodologies • Identifying and Protecting against Malware • Memory-Resident Malware • Memory Imaging Tools/Techniques • Memory Analysis Tools • Static Analysis • Dynamic Analysis • Malicious Document Analysis • Malware Challenges
Cyber Threat Intelligence	• Developing and leveraging threat intelligence to detect, respond, and defeat sophisticated attacks • Automating threat detection and response
Building Incident Response Tool Suite	• Building Trusted Toolkits • Testing the Tools

More information:

For more information about NetSecurity's Hands-On How-To® Training, please contact us at **Training@NetSecurity.com** or call +**1-703-444-9009.**