# CASP, Part 8 of 9: Incident Response

page 1

**Meet the expert:** David Bigger is the lead trainer at Bigger IT Solutions. He has been information technology for a little over 20 years and has been training all over the US. He has worked with companies like US Military, Lockheed Martin, General Dynamics, Dominos Pizza, University of Utah and Expedia

**Prerequisites:** This course assumes that the student has familiarity with information technology and basic networking. The student should also be familiar with basic security concepts, whether through the CompTIA Advanced Security Practitioner Parts 1-6 or outside study. No scripting or “hacking” experience is required.

**Runtime:** 01:01:56

**Course description:** What happens when things go horribly awry? That’s where incident response comes in, allowing you to take control and figure out the best solution to remedy the problem. Take an in-depth look at incident response, its best practices, and some methodologies and tools you can use, including the how, who and when aspects of the incident. Additionally, take a deep dive into the incident in a forensically sound manner making sure any evidence isn’t tampered with and could still be admissible in court. Though this course won’t make you a forensic investigator, it will give you a better understanding of the process so you can make sure you’re making the best decisions when handling an incident. This course is part of a series covering the CompTIA Advanced Security Practitioner (CASP).

**Course outline:**

**Incident Response**
- Introduction
- Incident Response
- Preparation
- Detection and Analysis
- Incident Analysis
- Documentation
- Incident Prioritization
- Incident Notification
- Containment, Eradication, and Recovery
- Evidence Gathering
- Identify the Attackers
- Eradication and Recvery
- Recovery
- Post-Incident Activities
- Lessons Learned
- Summary

**Incident vs. Event**
- Introduction
- Incident vs. Event
- Incident
- Events
- Summary

**Forensics**
- Introduction
- Forensics
- Computer Forensics
- Computer Forensics Readiness
- First Responder
- First Responder Tasks
- First Responder Continued
- Summary