2025 COURSE UPDATE

FOR508

Advanced Incident Response, Threat Hunting, and Digital Forensics

FOR508 is the most complete incident response and threat hunting course on the market. It teaches the advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT state-sponsored adversaries, financial crime syndicates, and ransomware operators. An emphasis on developing analytical skills and anomaly detection is in the DNA of the course, ensuring that learned skills are transferable to any network and any security tool stack.

76% of organizations report seeing "living off the land" (LOTL) techniques in nation-state attacks, highlighting the ongoing need for behavior-based detection and deeper analysis of attacker tradecraft. Source: SANS Threat Hunting 2025 Survey Results

Spring 2025 Update

The Spring 2025 update to FOR508 delivers a wide-ranging refresh of core content, with major upgrades to credential theft coverage, enhanced threat hunting material, and updates that address evolving attacker tradecraft—including "living off the land" (LOTL) techniques—and support the growing demand for in-house expertise in today's complex enterprise environments.

NEW CONTENT

- Includes new insights into threat hunting methodology, cyber threat intelligence integration, and modern use of the MITRE ATT&CK® framework.
- New content for explaining the threat hunting process, C2 frameworks, common file hiding techniques (misspelling, homoglyph, etc.), malicious use of third-party software (including remote access and file sharing), and DLL-hijacking techniques.
- Deeper coverage and explanations on the use and abuse of "named pipes" by adversarial C2 frameworks.
- Added discussion of Microsoft Entra ID integration and its impact to on-prem logging.
- New content added for detecting malicious Windows drivers (aka "LOLdrivers") via memory analysis techniques.

UPDATED FEATURES

- Major enhancement to the course's credential theft material, designed to better emphasize core concepts such as the difference between authentication and authorization, while expanding coverage of modern techniques like coercion attacks, relays, and delegation abuse.
- Added illustrations to demonstrate log anomalies caused by common credential attacks.
- New visualizations were added to illustrate how Windows logs events across different systems during credential use, helping students better understand the distributed nature of authentication and authorization.
- Increased coverage of lateral movement techniques including lesser-known but highly relevant techniques like Remote Registry and DCOM abuse attacks
- Updated guidance for memory acquisition and hibernation file processing tools.

LAB REFRESH

- Updated memory analysis labs, featuring the latest versions of the advanced memory forensics tools MemProcFS and Volatility 3.
- Brand new Windows 11 "SIFT" virtual machine preloaded with a wide range of processing and analysis tools for student use during the class--and beyond.
- Added a custom Windows Services for Linux (WSL) distribution for processing forensic evidence with the Plaso timeline analysis suite of tools.

GIAC Certified Forensic Analyst (GCFA)

61% of respondents cite skilled staffing shortages as a primary barrier to success, emphasizing the critical need for advanced training like FOR508 to build in-house expertise in threat detection, incident response, and investigative techniques. Source: SANS Threat Hunting 2025 Survey Results

For more information:
sans.org/FOR508