FOR572

ADVANCED NETWORK FORENSICS

The SANS FOR572 Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response course covers the tools, technology, and processes required to integrate network evidence sources into your investigations to provide better findings, and to get the job done faster.

It takes a company 197 days to discover the breach and up to 69 days to contain it. The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years*. Incident Response teams trained to utilize evidence from all kinds of network devices as well as from captured network data itself is critical to identify and mitigate a threat faster.

* IBM The Cost of a Data Breach Report 2023

Fall 2023 Update

The new course update is the result of nearly a year of work coordinating with a dedicated adversary simulation team, enterprise system architects, and investigative experts from across the DFIR spectrum. Students will be prepared to respond to existent adversaries as well as to build baselines of normal activity that allow the proactive identification of malicious activity early in a compromise, before large-scale damage is done.

NEW CONTENT

- A brand new, enterprise-scale attack scenario with a real network built, operated, and attacked by humans to present the most realistic DFIR training scenario in the industry.
- Attendees will see firsthand the artifacts left behind from modern attacker TTPs.
- Viewing specific attacker techniques through the lens of Zeek NSM logs.
- Coverage of recent protocol implementations including HTTP/3, the latest TLS variants, new SMB 3.1.1 features, and more.
- Mail content integrity validation to aid in detecting forged email components

UPDATED FEATURES

- All major tools used in the course updated to their most recent versions for the freshest possible perspective on network forensic casework.
- Virtual Machines running the latest distributions of the SANS SIFT Workstation, SOF-ELK®, and Arkime. While these VMs are uniquely configured to suit FOR572's labs, they are all investigation-ready for casework.
- The latest advertiser tracking technologies and how they can be of use to an investigator.
- Added steps for testing files reconstructed from network traffic to aid in tool and process validation.

LAB REFRESH

- Three brand new labs, and refreshed datasets for other class labs to reflect the latest investigative techniques and enterprise scenarios.
- An entirely new walk-through mini-scenario using proxy logs to identify common malicious insider threat behaviors, including why some may not be cached by most proxies.
- Techniques that allow scaling analytic tools to cover massive evidence sets.
- Methods for decrypting traffic using forward secrecy and HTTP/2 object reconstruction from decrypted samples.
- Bonus content added to each lab and several complete bonus labs that provide added perspectives and approaches to core course content.

Poor or absent cybersecurity training for employees contributes to the great majority of data breaches, between 80% and 88%*.

* Red Canary 2023 Threat Detection Report

"Whether your enterprise is mostly on-premises, all-in on cloud, or a hybrid between the two, your systems are communicating - do you have the perspective and skills necessary to incorporate those network communications into your DFIR investigations? FOR572 lays the foundation for exactly that skill set." – FOR572 course author Phil Hagen

"I feel like the last week has been a massive eye-opener into what extra information I can now use in my forensic investigations." - Will B, FOR572 attendee

GIAC Network Forensic Analyst (GNFA)

FOR572 updates continue to support students seeking to earn the GIAC Network Forensic Analyst (GNFA) credential.

For more information:
sans.org/FOR572

SANS | GIAC CERTIFICATIONS