skillsoft
global
knowledge™

FOCAL POINT - AUTOMATED NETWORK DEFENSE

Course Code: 100219

Learn how to defend large-scale network infrastructures by building and maintaining IDS/IPS and mastering advanced signature-writing techniques.

Cyber threats are increasing at an alarming rate every year and the ability for organizations to defend against full-scale, distributed attacks quickly and effectively has become much more difficult. An Intrusion Detection/ Prevention System (IDS/IPS) affords security administrators the ability to automate the process of identifying attacks among the thousands of connections on their network, provided the system is properly configured and the signatures are well written.

This course teaches how to defend enterprise infrastructure at scale using a combination of tools and platforms such as IDS/IPS, firewalls, and SIEMs. Configuring and tuning these systems properly maximize their effectiveness at catching and stopping threats while reducing alert fatigue for analysts and responders. Students learn to identify gaps in coverage, write basic and complex signatures, manage rule sets for optimization, use chain rules to detect multistage events, and implement decoding and fingerprinting capabilities to overcome evasion techniques.

What You'll Learn

- Explain the benefits and limitations of different security technologies (IDS/IPS, firewalls, VPNs, web proxies, etc.)
- Identify optimal platform deployment and gaps in coverage
- Write basic and complex IDS signatures to identify malicious traffic flows, and tune them to reduce false positives
- Use reassembly and pre-processing engines to automatically reconstruct streams of network data prior to analysis
- Apply decoding and other tools to overcome attacker evasion techniques
- Implement automated fingerprinting of encrypted traffic flows to detect anomalous or malicious flows

Who Needs to Attend

- Incident Responders who need to understand and react to IDS alerts
- Network Defenders seeking to automate threat detection

- IDS administrators who wish to improve their signature writing skills
- Security Operations Center Staff seeking to automate traffic analysis
- Penetration Testers looking to reduce their network visibility

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 5/8/2025 10:56:50 PM