Learnsoft
ENTERPRISE TRAINING

Cyber Security – Security Onion

Length: 4 Days

COURSE CONTENT

1. Network Security Monitoring (NSM) methodology
2. Security Onion Installation
3. Configuration
    a. Setup Phase 1 - Network configuration
    b. Setup Phase 2 - Service configuration
    c. Evaluation Mode vs Production Mode
    d. Verifying services
4. Analyzing Alerts
    a. Replaying traffic
    b. Squert
    c. Sguil
    d. Kibana
        i. Hunting with Kibana
        ii. Create custom dashboards in Kibana
    e. Pivoting between interfaces
    f. Pivoting to full packet capture
5. Bro
    a. Introduction
    b. Bro Programming Language
    c. Bro-IDS
    d. Bro Logs
    e. Bro Scripts
    f. Bro Intel Framework
6. Production Deployment
    a. Advanced Setup
    b. Master vs sensor
    c. Node types - Master, Forward, Heavy, Storage
    d. Command line setup with sosetup.conf
    e. Architectural recommendations
    f. Sensor placement
    g. Hardening
    h. Administration
    i. Maintenance
7. Tuning
    a. Using PulledPork to disable rules
    b. BPFs to filter traffic
    c. Spinning up additional Snort/Suricata/Bro workers to handle higher traffic loads