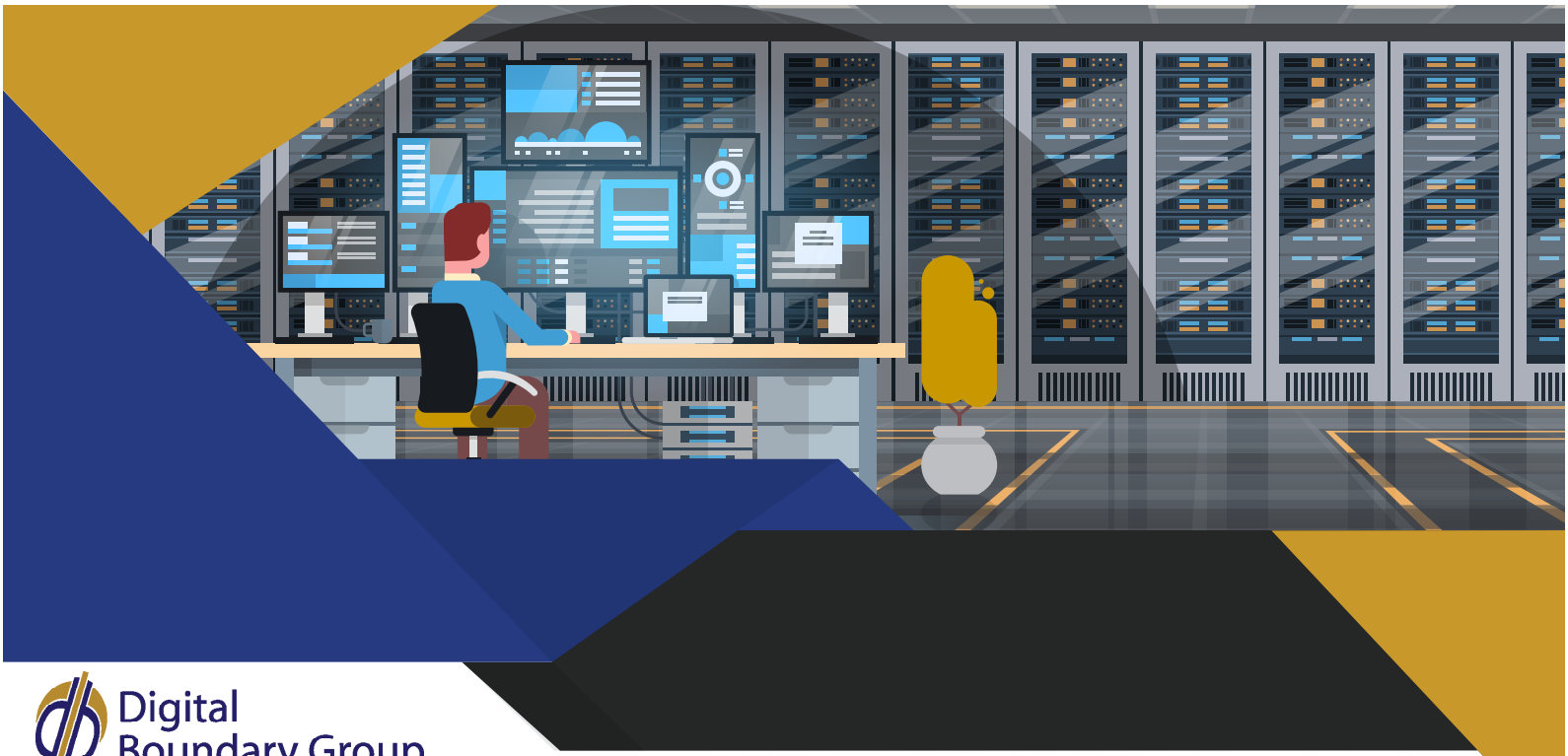


Digital Boundary Group

SIEM TUNING by LIVE FIRE

SIEM TUNING by LIVE FIRE is a platform used to simulate common post-compromise attacks. It is used to evaluate the ability of an organization's SIEM solution to receive, properly analyze, and alert the internal security team of a simulated active security breach. Unlike traditional testing, it takes an integrated approach to assess information security defenses by combining multiple testing strategies into a comprehensive offensive

TWO STEP APPROACH

To obtain the best results, we apply a two-step process: configuration auditing, and threat simulation.

PHASE ONE
Configuration Auditing

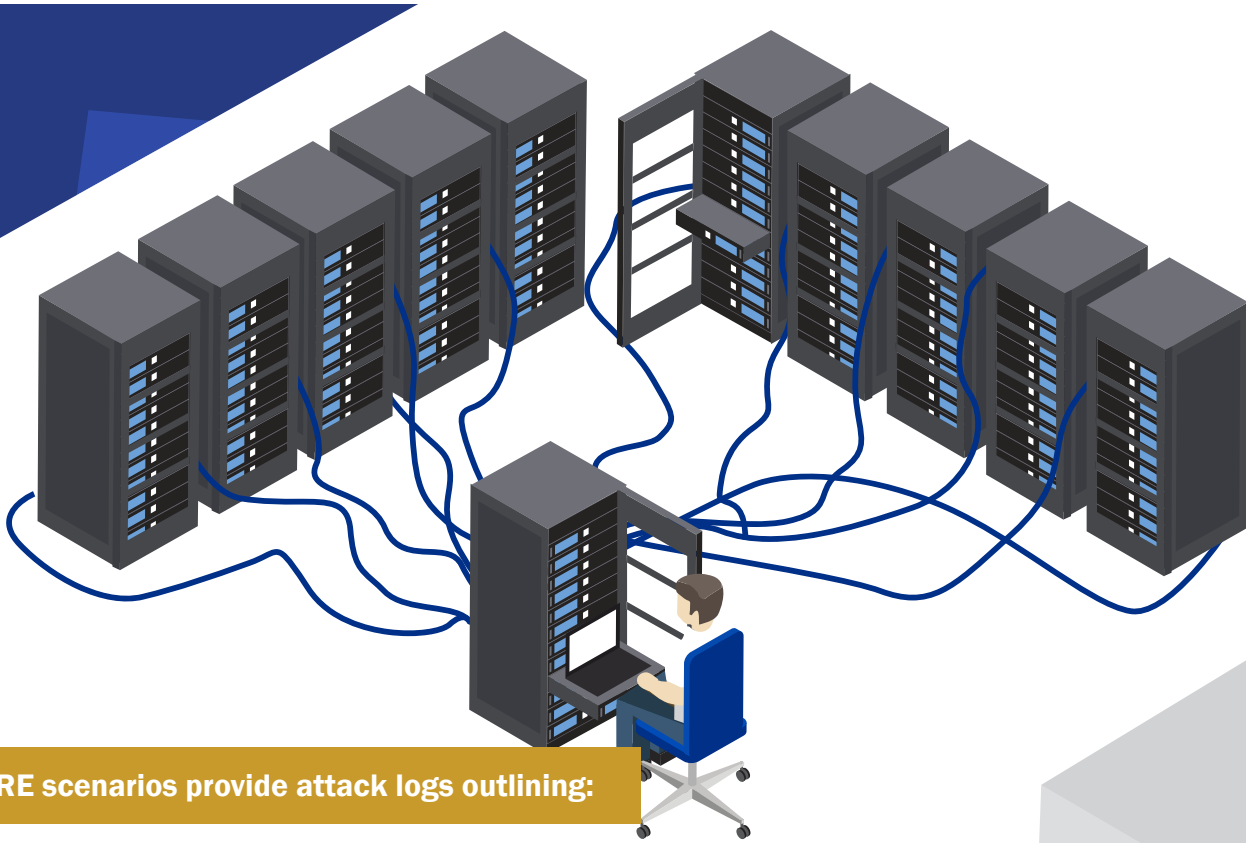
- Verify audit settings Microsoft Active Directory
- Audit Policy
- Sensor Placement
- Log Forwarding
- Review SIEM rules & log sources
- Forward simulated events directly to SEIM by becoming a log source

PHASE TWO
Threat Simulation

- Reconnaissance and situational awareness mapping
- Active Directory enumeration
- Exploitation and system compromise
- Data exfiltration
- Command and control – remote access persistence

UNBIASED TESTING

SIEM TUNING by LIVE FIRE gives your company the opportunity to assess your outsourced security service provider or internal incident response team.



SIEM TUNING by LIVE FIRE scenarios provide attack logs outlining:

- Attack ID
- Attack Description
- Start and Stop Times
- Target(s) Information
- Source Information (hostname, IP address, service information, etc.)

THREAT CATEGORIES

- Situational Awareness
- Privilege Escalation
- System Management and Manipulation
- Defense Evasion (Endpoint Security and Configuration Audit)
- Lateral Movement
- Account Lockout and Disruption
- Data Collection and Exfiltration
- Command and Control

SAMPLE ATTACKS

- Identification of default, weak and/or commonly guessed credentials
- Enumeration of user accounts, computers, and policies from within Microsoft Active Directory
- Password guessing over network devices and port scanning for services identified primarily in remote code execution and other nefarious exploits
- Identification of critical systems from enumeration of privileged groups and organizational units
- Process injection and privilege escalation
  File modification to simulate ransomware

PRICING

Subject to confirmation of scoping