OnDefend

Cyber Resilience Solutions
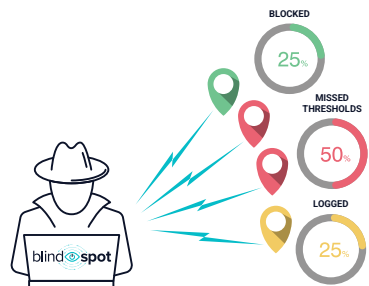
PENETRATION TESTING & RED TEAMING

We deliver advanced network, application, and red team testing services designed to identify exploitable vulnerabilities that could enable adversaries to compromise critical systems, assets, and sensitive data.

ADVANCED TABLETOP EXERCISE

We enhance tabletop exercises with real-world cyber-attack simulations to ensure your internal teams and response vendors can immediately detect, respond to, and effectively investigate an incident when it matters most.

Documentation Review Gap Analysis

- IR Policy
- IR Plan
- IR Playbooks
- Breach Notification Docs
- 3rd Party Retainers

Simulate Attack & Response

- Malware Outbreaks Causing Outages
- System Breach & Data Exfiltration
- Ransomware Threat Actors
- Man-in-the-Middle Attacks
- Or Other Attacks of Your Choice

Powered By BlindSPOT

Leadership Team Tabletop Activities

- Step-by-Step IR Execution
- Find Policy & Protocol Gaps
- Validate Communication & Decisions
- Analyze Impact & Ripple Effects
- Provide Clear Improvement Steps

SECURITY CONTROL VALIDATION

We safely emulate real-world adversary activity in your production environment to continuously assess and confirm your prevention, detection, and response controls are performing as intended, meeting their SLA requirements and delivering quantifiable value.

ATTACK SIMULATIONS

IDENTIFY HIDDEN SECURITY GAPS BY EMULATING REAL-WORLD THREAT ACTOR SCENARIOS ACROSS YOUR ENVIRONMENT.

Ransomware Strains

Supply Chain Threats

Industry Threat Actors

And More...

THREAT DETECTION VALIDATION

ENSURE YOUR SECURITY TOOLS ARE DETECTING AND ALERTING YOUR TEAM EVERY DAY TO REAL-WORLD ATTACK ACTIVITY?

Microsoft Defender

CROWDSTRIKE

SentinelOne

And Others...

THREAT RESPONSE VALIDATION

PROVE YOUR SOC TEAM & RESPONSE VENDORS ARE SWIFTLY RESPONDING TO AND NEUTRALIZING ACTIVE CYBER THREATS.

SOC
Security Operations Center

MSSP
Managed Security Service Provider

MDR
Managed Detection & Response

All Service Offerings

OnDefend

APPLICATION & CLOUD

- ✅ API Testing
- ✅ Application Vulnerability Scanning
- ✅ Cloud Configuration Assessment
- ✅ Desktop Application Testing
- ✅ DevOps Security Consulting
- ✅ Mobile Application Testing
- ✅ SBOM Generation
- ✅ Static Code Review
- ✅ Web Application Testing

ORGANIZATIONAL READINESS

- ✅ Business Continuity & Disaster Recovery Assessment
- ✅ IR Plan Development
- ✅ Policy & Procedure Development
- ✅ Risk Assessment
- ✅ Social Engineering
  - ✅ Phishing
  - ✅ Smishing
  - ✅ Vishing
  - ✅ On-Site
  - ✅ Impersonation
- ✅ Tabletop Exercises (option w/ Attack Simulation)[1]
- ✅ Threat Response Validation (MSSP, MDR, NDR)[1]

NETWORK & INFRASTRUCTURE

- ✅ Active Directory Assessment
- ✅ Breach & Attack Simulations[1]
- ✅ Email Filter Testing
- ✅ Firewall Configuration Assessment
- ✅ IoT Device Testing
- ✅ Network Penetration Testing
- ✅ Physical Security Testing
- ✅ Purple Teaming Exercises[1]
- ✅ Ransomware Defense Validation[1]
- ✅ Red Team Testing
- ✅ VOIP Configuration Assessment
- ✅ Vulnerability Assessment & Management
- ✅ Wireless Configuration Assessment

GOVERNANCE

- ✅ Compliance Consulting
  - ✅ NIST
  - ✅ PCI
  - ✅ ISO 27001
  - ✅ GLBA
  - ✅ SOC 2
  - ✅ HIPAA
  - ✅ CMMC
  - ✅ And More...
- ✅ Certification Readiness Consulting
- ✅ Data Classification & Privacy Consulting
- ✅ Fractional CISO

✉ contact@ondefend.com
🌐 ondefend.com
📞 800.214.2107

[1] **blind spot** is OnDefend's breach and attack simulation solution, which safely emulates specific threat actors revealing an organizations security control failures.