CYBER SECURITY ASSESSMENTS

Minimize the risk of company and customer data breaches with full-service vulnerability assessment, policy implementation and training.

OES Lancer offers three (3) Tiers of service and a menu of concierge add-on support. Each tier of service offers an unmatched level of excellence from initial consultation to post-assessment reporting and briefing.

TIER 1: ALPHA TEAM

Personnel Interview
Security Assessment
Reporting
Briefing

TIER 2: BLUE TEAM

Personnel Interview
Security Assessment
Baseline Development
Patch Configuration
Reporting
Briefing

TIER 3: RED TEAM

Personnel Interview
Threat Assessment
Legal Authorization
Penetration Testing
Baseline Development
Patch Configuration
Reporting
Briefing

ADD-ON/SUPPORT: GREEN TEAM

Remediation
Policy Development
Patch Configuration

Vulnerability Assessments & Solutions
Security Awareness Training
IT Manager Security Training

Tiered services can be offered on a monthly, quarterly, semi-annual or annual basis. When these services are requested on a regularly-occuring schedule, OES Lancer is able to provide clients with a better picture of the total security posture of the company’s system over time.

TIER 1: (ALPHA TEAM) NETWORK VULNERABILITY ASSESSMENT

SCOPE

Tier 1 provides limited vulnerability assessment with a maximum of 40 hours and of 250 IP addresses. This scope includes scans of 1 set of enterprise services (email and multiple domain controllers). Personnel interviews limited to 6 people identified in the organization. Based on these boundaries, we can create samples of devices by group and provide confidence levels based on determined sample sizes. We scan network switches and routers for vulnerabilities and findings from Security Technical Implementation Guide's (STIG).

Tasks

- **Initial Consultation**
  - Identify priorities
  - Identify business processes
  - Educate leadership
  - Identify personnel to be interviewed
  - Obtain access permissions to perform scans
  - Establish sample sizes based on scope
- **Personnel Interview**
  - Identify and classify information assets
  - Interview and perform cyber security evaluation
  - Understand business processes
- **Security Assessment**
  - Internal vulnerability scans operating inside your business's firewall (for example, sample size of 20% of networked IP addresses)
  - Check existing security packages and software patching policies
  - Scan systems against Security Content Automation Protocol specifications
  - Scan enterprise services (domain, mail, database, etc.)
  - Check switches and routers
  - Assess current security posture
    - Assess policies
    - Assess procedures
    - Assess security knowledge
    - Assess baseline security
    - Report and Briefing
  - Meet with leadership and technical personnel
  - Provide compliance report and results of cyber security evaluation
- **Quarterly Scan**
  - Recognize significant network changes, new system component installations, topology changes, firewall rule mods, product upgrades.

TIER 2: (BLUE TEAM) CORPORATE VULNERABILITY ASSESSMENT

SCOPE

Tier 2 provides complete vulnerability assessment with a maximum of 160 hours of service and sampling on 1,000 IP addresses. The goal is to assess all systems in the organization.

Tasks

- **Internal Scans**
    - Internal vulnerability scans operating inside your business's firewall (sample of 20% of networked IP's)
- **Initial Interview**
    - Identify priorities
    - Identify business processes
    - Educate leadership
    - Identify personnel to be interviewed (Understand business process)
    - Obtain access permissions to perform scans
- **Personnel Interview**
    - Identify and classify information assets
    - Interview and perform cyber security evaluation
    - Understand business processes
- **Threat Assessment**
    - Check existing security packages and software patching policies
    - Scan systems against Security Content Automation Protocol specifications
    - Identify Vulnerabilities on the following:
        - Operating Systems
        - Database Applications
        - Open Source Software
        - Network Devices
        - Wireless Devices
        - Virtualization Infrastructure
        - Mobile Operating Systems (optional)
    - Identify outdated software on workstations and servers
    - Identify installed software and highlight deviances from baseline
    - Perform external scan to check firewall posture
    - Scan servers and perform checks of publicly accessible systems (web applications)
    - Document legacy or custom systems that depend on outdated packages and understand linkages to other systems
    - Check Active Directory permissions and Group Policy Objects
    - Check switches, routers, firewalls, intrusion detection and prevention systems
- **Remediation**
    - Establish security baseline to address vulnerabilities
    - Ensure patching policy is correctly configured
- **Report and Briefing**
    - Meet with leadership and technical personnel
    - Provide compliance report and results of cyber security evaluation
    - Detail vulnerabilities and remediation for each vulnerability
    - Provide recommendations for way-forward within context of risk management framework

TIER 3: (RED TEAM) ATTACK AND PENETRATION

SCOPE

Tier 3 provides complete vulnerability assessment with a maximum of two months.
Tasks

- **Targeting & Exploitation (customer sets the scope)**
  - Technical and infrastructure data
  - Employee data (SSN, PII, PHI, Financial information)
  - Customer Data (SSN, PII, PHI, equity accounts, credit info, bank info, supplier data)
  - Partner Data
  - Cloud services account data
  - Company Proprietary info (Trade secrets, R&D data, source code)
  - Human assets: divulge information (key personnel, executives)
  - Establish legal authorization
- **Reporting**
  - Detailed reports outlining:
  - Back doors
  - Audit logs
  - 'Captured information'

REMEDIATION

SCOPE

Remediation provides comprehensive vulnerability mitigation services based on the results of a Vulnerability Assessment (such as from Tier 1, from a la carte services, or from Tier 2).
Tasks

- **Remediation**
- **Understand business processes**
- **Mitigate vulnerability findings**
  - Provide fixes
  - Document business need and accept risk
  - Test new security baselines on subset to ensure business needs are met
  - Work with customer to test server security baselines in testing enviroment
  - Deploy updated security baselines to production environment
- **Network & Application**
  - Update baseline security posture
    - Provide & install security policies
    - Deploy baseline security configurations on systems
    - Deploy baseline security configurations on the network
  - Secure web applications
  - Secure web services
- **Operating System**
  - Update Service packs
  - Update Group policies
  - Update Security templates
  - Update Configuration baselines

POLICY DEVELOPMENT (GREEN TEAM)

SCOPE

Policy Development customizes and delivers security policies to the customer using industry best practices to ensure that users, infrastructure, and the organization are protected.

TASKS

Policy Development

- Understand business processes
- Develop and update policies and procedures
  - Computer Use Policy
  - Acceptable Use and User Agreement
  - Cyber security Training Brief
  - Security Handbook
  - WAN Diagram (Logical Architecture)
  - Access Control Standard
- Deliver documents to management

USER SECURITY TRAINING (GREEN TEAM)

SCOPE

User Security Training provides instruction and presentation of completion certificates that educate the information system users on the policies and on general cyber security practices.

TASKS

User Security Training

- Establish training schedule
- Prepare instructional material customized to organization's policies
- Conduct training class for group of users
- Certify users on understanding of material
- Deliver certifications to management