Service Plans: Infrastructure

ISE's methodology focuses on assets and adversaries in order to best harden systems. Understanding that not all assets, adversaries or systems should be treated the same, ISE accordingly offers varied service plans. These tiered offerings are scaled to meet the profile of needs for a given system.

The below checklist helps our customers determine the best evaluation tier with which to proceed.

- See below to map the characteristics of your system to the most appropriate assessment tier.
- See reverse for the services that are included with each assessment tier.

MOST SECURE

SYSTEM CHARACTERISTICS	TIER III	TIER II	TIER I
ASSET VALUE			
Low	✓	✓	✓
Medium		✓	✓
High			✓
ATTACK TYPE			
Untargeted attacks	✓	✓	✓
Targeted attacks		✓	✓
Advanced attacks			✓
Insider attacks			✓
ADVERSARY SKILL			
Low	✓	✓	✓
Medium		✓	✓
High			✓
ADVERSARY TYPE			
Casual Hacker	✓	✓	✓
Hacktivists		✓	✓
Organized Crime			✓
Nation State			✓
ATTACK SURFACES			
WAN-facing servers/services	✓	✓	✓
Data centers	✓	✓	✓
Internal servers/services		✓	✓
End-systems		✓	✓
Vendor-connected networks		✓	✓
Partner-connected networks		✓	✓
Email		✓	✓
Rouge devices		✓	✓
Wireless LANs		✓	✓
VOIP systems		✓	✓
Employees (social engineering)		✓	✓
Remote employee access			✓
Remote vendor access			✓
Mobile devices			✓
Malicious peripherals			✓
Embedded systems			✓
Others/custom			✓
Physical trespass			✓
Physical theft			✓

Tier III: Best suited for scenarios involving low value assets and low skill adversaries. Scope focuses primarily on known attacks against the front-end.

Tier II: Best suited for systems that access medium-to-high value assets and/or are targeted by medium-to-high sophistication adversaries.

Tier I: Best suited for critical systems that access high value assets or are targeted by sophisticated adversaries. This level of review considers entire system scope, including the back-end and possibly source code.

MOST SECURE

ASSESSMENT DELIVERABLES	TIER III	TIER II	TIER I
SCOPE			
Front-end	✓	✓	✓
Back-end			✓
ASSESSMENT TASKS			
Policy Testing (Social Engineering)	✓	✓	✓
Rouge Device Identification	✓	✓	✓
Security Policy Review	✓	✓	✓
Configuration Assessment		✓	✓
System Hardening		✓	✓
Security Policy Development		✓	✓
Network Architecture Review			✓
Vulnerability Assessment			✓
Penetration Testing			✓
Defense-in-depth Strategy			✓
Insider Threat Assessment			✓
Long Term Security Planning			✓
ASSESSMENT DEPTH			
Implementation-level assessment	✓	✓	✓
API-level assessment		✓	✓
Design-level assessment			✓
Policy-level assessment			✓
OTHER SERVICES			
Private confidential report	✓	✓	✓
Public report		✓	✓
Threat intelligence advisories		✓	✓
General consulting		✓	✓
Iteration hardening consulting		✓	✓
Virtual Chief Information Security Officer (vCISO)		✓	✓
Presentation of results			✓
Incident Response Guarantee			✓
Training			✓
PRICING OPTIONS			
Lump Sum	✓	✓	✓
Monthly		✓	✓
Custom Rate			✓

DOMAIN EXPERTISE:

- Cryptanalysis
- Protocol Analysis
- Documentation Review
- System Architecture
- Network Architecture
- Authentication
- Digital Rights Management
- Content Protection
- Vendor Awareness
- Network & System Awareness
- Policy Review
- Policy Development
- Long Term Planning
- Trust Modeling & Verification
- Defense-in-depth Strategy
- Insider Threat Assessment
- Fuzzing
- Hacking
- Source Code Review
- Vulnerability Assessment
- Penetration Testing
- Malware Analysis
- Configuration Assessment
- Rouge Device Identification
- System Hardening
- Policy Testing
- Social Engineering
- Design Verification