

SecureIdeas

professionally **evil**[®]

2026

Services Catalog



Professionally evil, hands-on
offensive security testing
and advisory services



CREST Accredited



CMMC Level 1
Compliant



PCI Associate PO

Table of Contents



Who We Are	3
How We Price	4
PETaaS® Credits	5
Network Penetration Testing	6
Internal Penetration Test	6
External Penetration Test	7
Application Pentesting	8
Web Application Penetration Test	8
Mobile Application Penetration Test	9
API Penetration Test	10
Adversarial Simulation	11
Red Team Engagements	11
Social Engineering	12
Physical Security Testing	12
Specialized Testing	13
Wireless Network Testing	13
OT Penetration Test	14
Embedded Systems Penetration Test	14
Assessment & Advisory	15
Security Assessments	15
Tabletop Exercises	16
Advisory Services	16
Contact	17

ABOUT

Who We Are



Secure Ideas is a boutique offensive security consulting firm that helps organizations identify vulnerabilities and weaknesses across their applications, infrastructure, networks, and systems. Every engagement is hands-on, expert-led, and manual. We don't rely on automated scans dressed up as findings.

Our consultants have been the ones on-call when a server went down, shipping code under deadline, and keeping operations running while implementing security mitigations. That background shapes everything we deliver: accurate findings, practical recommendations, and reports that give your team clear, prioritized actions.

9

State Offices

15+

Years in Business

85

NPS Score

INDUSTRIES WE SERVE



Healthcare



Legal



Military



Nonprofit



Automotive



Manufacturing



Finance



Technology



Insurance



Energy



Utilities



Retail

STANDARDS & FRAMEWORKS

OWASP

HIPAA

GLBA

PCI DSS

MEMBERSHIPS

OWASP | ISSA | ISACA | InfraGard

TEAM CERTIFICATIONS

AWS Academy

AZ 900

CC

CEH

CISM

CISSP

CPSA

CySA+

GAWN

GCFA

GCIH

GCIA

GPEN

GWAPT

ISO 27001 LA

OSCE

OSCP

OSWP

PCSE



PRICING

How We Price



Two pricing models designed for different buying preferences. Choose per-project simplicity or the flexibility of prepaid capacity.

Flat Fee

\$340/hour

\$2,720/day

Each engagement is individually scoped and priced based on days of effort and number of consultants. Every project is documented in a standalone statement of work.

BEST FOR

Organizations that prefer to evaluate and approve engagements on a per-project basis.

POPULAR

PETaaS® Credits

\$2,520/credit

1 Credit = Up to One Full Day of Expert Work

Purchase credits upfront and deploy them across any combination of services as needs evolve. Minimum 25 credits.

- ✓ Apply to any effort-based service
- ✓ Reallocate as priorities shift
- ✓ Advisory support at no additional cost
- ✓ Transition between models anytime

PETAAS® VOLUME DISCOUNTS

Discount	Credits	Investment Range
5%	30 – 49	\$71,820 – \$117,306
10%	50 – 89	\$113,400 – \$201,852
15%	90+	\$192,780+

The discount is applied to the invoice in which the volume tier is attained.



PRICING

Professionally Evil Testing as a Service®



PETaaS® credits program is designed around one principle: **flexibility**. Rather than locking into a rigid engagement structure, credits allow you to purchase capacity upfront and deploy it across any combination of services as your needs evolve throughout the contract period.

There are *no predetermined tiers or fixed monthly allocations*. Secure Ideas works with you to determine the right number of credits based on your anticipated testing goals, compliance requirements, and budget, with a minimum purchase of 25 credits. From there, credits can be applied to any effort-based service Secure Ideas offers, including penetration testing, security assessments, architecture reviews, corporate training, tabletop exercises, and more.

This structure is intentional. Security programs don't operate on a fixed schedule, and testing needs shift as environments change, new applications are deployed, compliance deadlines approach, or incidents require rapid response. The credits model provides the ability to respond to those shifts without renegotiating scope or contracts for each individual engagement.

As the relationship matures, Secure Ideas also provides advisory access to help plan how to allocate credits strategically across the contract period, ensuring your testing program stays aligned with your priorities. *Advisory support is built into the credits program at no additional cost.*

Transitioning Between Models: We understand that security needs change over time and flexibility is paramount. Given this understanding, you can transition between service models at any point during the contract by purchasing the difference in credits. Any outstanding credits will have their expiration reset to align with the new purchase date, and the credit discount will continue to apply.

SERVICES

Network Penetration Testing

Evaluates the security of an organization's internal and external infrastructure, systems, and services. Testing focuses on identifying vulnerabilities, misconfigurations, and attack paths from the perspective of a threat actor operating either inside or outside the network perimeter.

Internal Penetration Test

Evaluates internal network security from the perspective of a threat actor who has already gained access. Consultants identify vulnerabilities, misconfigurations, and attack paths that could allow privilege escalation, lateral movement, or access to sensitive data and critical systems.

Active Directory

Network Segmentation

Credential Hygiene

Privilege Escalation

Broadcast Protocols

File Shares & Databases

ENGAGEMENT MODELS

Assumed Breach

Begins with a defined foothold.
Focuses on post-compromise activity: lateral movement, privilege escalation, and access to critical assets.

Threat-Led

Modeled around threat intelligence and adversary behaviors. Aligned to MITRE ATT&CK. Relevant for TIBER, CBEST, and DORA frameworks.



Deliverable: Detailed report documenting vulnerabilities, attack paths, and actionable recommendations to prioritize remediation.

Type	Scope	Flat Fee	Credits
Small	≤100 hosts / 3 Class C	5d / \$13,600	5 / \$12,600
Average	≤500 hosts / 1 Class B	8d / \$21,760	8 / \$20,160
Large	≤5,000 hosts / 100 Class B	13d / \$35,360	13 / \$32,760
Enterprise	5,000+ hosts / 100+ Class B	25d / \$68,000	25 / \$63,000

External Penetration Test

Evaluates internet-facing infrastructure from the perspective of a remote attacker with no prior internal access. Identifies and attempts to exploit vulnerabilities across your external attack surface, including web servers, mail gateways, VPN endpoints, DNS, cloud services, and other publicly exposed assets.

- Web Servers
- Mail Gateways
- VPN Endpoints
- DNS Infrastructure
- Cloud Services
- Publicly Exposed Assets

ENGAGEMENT MODELS

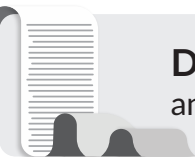
- Standard External

Comprehensive assessment of all internet-facing IP ranges, hosts, and services.
- OSINT & Attack Surface

Maps your full external footprint: forgotten assets, cloud resources, leaked credentials, metadata.
- Cloud-Focused

Targets externally accessible cloud resources across AWS, Azure, and GCP.
- Perimeter Evasion

Tests bypass of firewalls, IPS, WAFs, and email gateways using evasion techniques.



Deliverable: Detailed report documenting vulnerabilities, methods used to discover and exploit them, and actionable recommendations to reduce external risk.

Type	Scope	Flat Fee	Credits
Small	≤10 live hosts	3d / \$8,160	3 / \$7,560
Average	≤100 live hosts	5d / \$13,600	5 / \$12,600
Large	≤1,000 live hosts	10d / \$27,200	10 / \$25,200

Application Pentesting

Evaluates the security of web, mobile, and API-based applications and their supporting infrastructure. Testing is performed against the application layer itself, focusing on how the application behaves when it is used in ways the developers did not intend.

Web Application Penetration Test

Manually tests web applications for vulnerabilities that automated scanners frequently miss, including business logic flaws, authentication and session management weaknesses, authorization bypass conditions, and data handling issues. Guided by the OWASP Testing Guide and OWASP Top 10.

Business Logic

Authentication

Authorization

Session Management

Input Validation

Data Handling

ENGAGEMENT MODELS

Authenticated

Tests across user roles for privilege escalation, access control enforcement, and session management weaknesses.

Unauthenticated

Evaluates the attack surface from the perspective of an external attacker with no valid credentials.

Single-Page App (SPA)

Targets modern front-end frameworks (React, Angular, Vue) where significant logic executes in the browser.

Pre-Release / SDLC

Tests in staging or pre-production environments. Findings formatted for development teams to act on quickly.



Deliverable: Detailed report with step-by-step reproduction instructions for development teams and actionable recommendations to remediate findings.

Type	Scope	Flat Fee	Credits
Small	Single purpose, one role, up to 5 dynamic pages	5d / \$13,600	5 / \$12,600
Average	1-2 roles, 5-50 pages, payment/app boundaries	8d / \$21,760	8 / \$20,160
Large	Complex, multi-role, 50+ dynamic pages	13d / \$35,360	13 / \$32,760



Mobile Application Penetration Test

Examines the full mobile ecosystem: the application on-device, its supporting backend services, and the communication channels between them. Covers local data storage, API communication, authentication, session management, and device-level features. Guided by the OWASP MASTG and Mobile Top 10.

Local Data Storage

API Communication

Authentication

Session Management

Binary Protections

Inter-Process Communication

ENGAGEMENT MODELS

iOS

Keychain, ATS, URL schemes, Universal Links, binary protections, data leakage through backups and logs.

Android

Content providers, intents, shared preferences, WebView, certificate pinning, external storage exposure.

Backend API

Server-side APIs using the mobile client as the attack interface. Auth tokens, authorization, input validation.

Cross-Platform

React Native, Flutter, Xamarin, Cordova. Bridge-layer vulnerabilities, bundle exposure, and platform security control leveraging.

Reverse Engineering & Tampering

Evaluates resilience against decompilation, hardcoded secrets, obfuscation effectiveness, and repackaged binaries interacting with production services.



Deliverable: Report documenting vulnerabilities across the application, backend services, and communication channels, with actionable recommendations.

Type	Scope	Flat Fee	Credits
Small	Single role, limited API, basic data flows, single platform	5d / \$13,600	5 / \$12,600
Average	2-3 roles, standard auth, core API, single platform	8d / \$21,760	8 / \$20,160
Large	Multi-role, extensive API, payments, both platforms	13d / \$35,360	13 / \$32,760

API Penetration Test

Tests RESTful APIs, SOAP web services, and GraphQL endpoints directly, independent of any front-end application. Evaluates authentication and token handling (OAuth 2.0, JWT, API keys), authorization enforcement, input validation, rate limiting, and data exposure in API responses.

- OAuth 2.0 / JWT / API Keys
- Object-Level Authorization
- Mass Assignment
- Injection
- Rate Limiting
- Data Exposure

SUPPORTED API TYPES

RESTful

Standard HTTP-based APIs with endpoint and parameter testing across all methods.

SOAP

XML-based web services with WSDL analysis and message-level testing.

GraphQL

Query depth, introspection, batching attacks, and schema-level authorization testing.



Deliverable: Detailed report with reproduction steps formatted for development teams and actionable recommendations to harden the API.

Type	Scope	Flat Fee	Credits
Small	Simple RESTful, small endpoint count, no role differentiation	4d / \$10,880	4 / \$10,080
Average	Moderate complexity, 2-3 roles or replay protection	8d / \$21,760	8 / \$20,160
Large	Complex, multiple endpoints, multiple roles, replay protection	10d / \$27,200	10 / \$25,200

Adversarial Simulation

Evaluates an organization's detection and response capabilities by simulating realistic threat actor behavior. Unlike traditional penetration testing, these engagements are objective-based: Secure Ideas operates as a simulated threat actor while your security operations team works to detect and contain the activity.

Red Team Engagements

Simulates a realistic adversary operating against your environment with predefined goals such as accessing sensitive data, compromising critical systems, or establishing persistence. Grounded in the MITRE ATT&CK framework and real-world adversary behaviors. Every engagement operates under defined rules of engagement, including scoping boundaries, escalation procedures, and regular coordination touchpoints.

Initial Access

Command & Control

Privilege Escalation

Lateral Movement

Persistence

Objective Achievement



Deliverable: Detailed report with all red team activity logged, identifying gaps in defensive controls, security monitoring, and incident response, with actionable recommendations.

Type	Scope	Flat Fee	Credits
30-Day	Focused simulation. Recon, initial access, limited lateral movement.	15d / \$40,800	15 / \$37,800
60-Day	Multi-phase, multi-vector. Phishing/vishing, persistence, purple team.	25d / \$68,000	25 / \$63,000
90-Day	Full-scope APT simulation. Extended stealth, multi-vector, exec briefing.	35d+ / \$95,200+	35+ / \$88,200+

Social Engineering

Tests whether personnel can recognize and resist manipulation attempts commonly used by real-world threat actors to gain initial access, harvest credentials, or extract sensitive information. Each campaign is designed in coordination with the client to establish scope, approved techniques, target populations, and success criteria.

ENGAGEMENT FORMATS

Phishing

Targeted emails with spoofed login pages and weaponized attachments. Tracks delivery, open, click-through, credential submission, and reporting.

Vishing

Live phone calls using pretexting scenarios to manipulate targets into disclosing information or granting system access.

Smishing

SMS-based social engineering targeting mobile workforces and BYOD environments. Tests link clicks and information disclosure.

Pretexting & Impersonation

Detailed scenarios impersonating vendors, IT support, new employees, or executives across multiple communication channels.



Deliverable: Final report with detailed metrics, examples of successful and unsuccessful attempts, and recommendations to improve security awareness training.

Pricing: \$340/hour | \$2,720/day | 1 credit per day | Scoped per engagement.

Physical Security Testing

Controlled physical intrusion attempts using tailgating, badge cloning, lock bypass, dumpster diving, and social engineering of on-site personnel. Every engagement operates under clearly defined rules of engagement, including approved facilities, restricted areas, escalation procedures, and a letter of authorization carried by all testers.

Tailgating

Badge Cloning

Lock Bypass

Dumpster Diving

On-Site Social Engineering



Deliverable: Final report with all access attempts documented with photographs and detailed narratives, identifying gaps in physical controls and personnel awareness.

Pricing: \$340/hour | \$2,720/day | 1 credit per day | Scoped per engagement.

Specialized Testing

Addresses environments and technologies that require distinct expertise beyond traditional IT penetration testing, including industrial control systems, embedded devices, and wireless infrastructure.

Wireless Network Testing

Assesses the security of wireless infrastructure including encryption strength and protocol configuration (WPA2/WPA3), authentication mechanisms (802.1X, PSK, captive portals), rogue access point detection, client isolation and network segmentation, and susceptibility to deauthentication, evil twin, and relay attacks.

WPA2 / WPA3

802.1X

Rogue Access Points

Client Isolation

Evil Twin

Deauthentication

EXTENDED PROTOCOL TESTING

Bluetooth

Pairing, discovery, and data interception.

Zigbee

Network key extraction and replay.

Z-Wave

Controller pairing and command injection.

LoRa

Transmission security and data exposure.



Deliverable: Detailed report documenting vulnerabilities with actionable recommendations to harden wireless infrastructure.

Type	Scope	Flat Fee	Credits
Essentials	1 SSID or ≤ 100 users. Config and testing only.	3d / \$8,160	3 / \$7,560
Small	1 SSID or ≤ 100 users. +1-day architecture review.	6d / \$16,320	6 / \$15,120
Average	≤ 2 SSIDs, ≤ 300 users. +1-day architecture review.	8d / \$21,760	8 / \$20,160
Large	≤ 3 SSIDs, ≤ 500 users. +2-3 day architecture review.	13d / \$35,360	13 / \$32,760

OT Penetration Test

Evaluates the security of systems that monitor and control physical processes in industrial environments, including ICS, SCADA, PLCs, and other specialized equipment. Tests patch management, access controls, network segmentation, and privilege escalation potential while exercising extreme care to avoid disrupting active production systems.

- ICS / SCADA
- PLCs
- Patch Management
- Access Controls
- Network Segmentation
- Legacy Systems

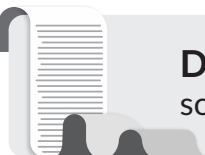


Deliverable: Report documenting vulnerabilities across the OT environment with actionable recommendations.

Embedded Systems Penetration Test

Examines the security of specialized computing devices built into larger products and systems, from medical devices and automotive components to smart home devices and industrial equipment. Testing includes hardware inspection, firmware extraction and analysis, communication interface security, and identification of hardcoded credentials or vulnerabilities.

- Hardware Inspection
- Firmware Extraction
- Debug Ports
- Communication Interfaces
- Hardcoded Credentials



Deliverable: Report documenting vulnerabilities across hardware, firmware, and software components with actionable recommendations.

OT & EMBEDDED PRICING

Type	Scope	Flat Fee	Credits
Simple	Web applications	5-8 days \$13.6K-\$21.8K	5-8 \$12.6K-\$20.2K
Moderate	Thin clients on client-provided workstations/servers	8-13 days \$21.8K-\$35.4K	8-13 \$20.2K-\$32.8K
Complex	Application software + embedded device	13-18 days \$35.4K-\$49K	13-18 \$32.8K-\$45.4K
Highly Complex	Multiple software, devices, and peripherals	18-24+ days \$49K-\$65.3K+	19-24+ \$45.4K-\$60.8K+

Assessment & Advisory

Cooperative, non-adversarial engagements in which Secure Ideas works alongside your team to evaluate the design, configuration, and controls across your technical environment. Unlike penetration testing, these are consultative reviews focused on understanding where gaps exist between your current state and security best practices.

Security Assessments

Analysis performed through documentation review, technical configuration review, and structured interviews with IT and security staff. Interviews are conducted via phone or video conference, typically 60 to 90 minutes per session, focusing on design decisions, operational procedures, and control implementation.

ASSESSMENT TYPES

Architecture & Design

Network segmentation, data flow, trust boundaries, and defensive architecture.

Policy & Procedure

Documented policies assessed against NIST CSF, ISO 27001, or CIS Controls.

Configuration & Hardening

Systems evaluated against CIS Benchmarks and vendor-specific hardening guides.

Cloud Security

IAM, network controls, storage, logging, and resource exposure across AWS, Azure, or GCP.

Compliance Readiness

Current state evaluated against PCI DSS, HIPAA, SOC 2, CMMC, or NIST 800-171. Findings mapped directly to relevant controls with a prioritized remediation roadmap.



Deliverable: Detailed report with findings, vulnerabilities, and practical, prioritized recommendations to close gaps and improve security practices.

Type	Scope	Flat Fee	Credits
Assessment	Architecture, configuration, policy, and controls review	6-11 days \$16.3K-\$29.9K	6-11 \$15.1K-\$27.7K

Tabletop Exercises

Structured exercises that evaluate how various roles within your organization respond to cyber incidents. Secure Ideas provides a dynamic learning experience designed to engage active participation from all attendees.

EXERCISE TYPES

Executive

Risk management and business objective discussions with legal, communications, and HR representatives.

Technical

Root cause analysis, investigation procedures, and operational response with technical teams.

ENGAGEMENT MODELS

Template-Based

Pre-generated scenarios tailored to your organization. Multiple scenarios explored during a 1-2 hour event.

Custom-Designed

Collaboratively built scenario specific to your environment with significant pre-event planning.

Type	Scope	Flat Fee	Credits
Template	Pre-generated scenarios, moderately customized	3 days \$8,160	3 \$7,560
Custom	Collaboratively built, significant pre-event planning	6-8 days \$16.3K-\$21.8K	6-8 \$15.1K-\$20.2K

Advisory Services

On-demand access to senior security consultants for guidance outside the scope of a formal testing engagement. Covers security architecture questions, remediation guidance, incident triage, tool selection, and policy development.

- Architecture Guidance
- Remediation Support
- Incident Triage
- Tool Selection
- Policy Development

Pricing: \$340/hour | \$2,720/day | 1 credit per day | Available standalone or included at no additional cost with PETaaS® credits.



Secure Ideas

professionally **evil**[®]



866.404.7837



sales@secureideas.com



secureideas.com



Scan to schedule
a conversation



CREST Accredited



CMMC Level 1
Compliant



PCI Associate PO