DISC INFOSEC // AI ASSESSMENT + SITE CARE

Your AI is live. Your site is your shop. Who's answering for either?

Security assessments for AI infrastructure, agents and applications, plus Site Care for the websites your business runs on. Built for SMBs and for firms that sign their work: founders, agencies, research and consulting teams.

THE PROBLEM

Most small firms didn't design their AI stack; it piled up. A model API in the website, an agent with inbox access, a plugin installed to solve last Tuesday's problem. Each one works, and each one opens a door **nobody has checked**. Meanwhile the website, your storefront, has no one on call when it goes down or gets compromised.

HOW WE TEST

Authorized, scoped testing with an AI-driven offensive toolkit. Automation gives breadth; a senior practitioner verifies every finding, so you get **real risk, not scanner noise**.

`Claude Guide for Pentesting` `Burp Suite Pro + Burp AI` `Microsoft PyRIT` `CyberSentinel-AI` `CyberStrike` `Metatron` `PentestCode` `SecureSecSuite` `SecSuite` `Xalgorix` `PenTestSwarmAI`

WHAT WE ASSESS

01
Infrastructure
Cloud configuration, IAM and service accounts, containers, secrets, model and package supply chain.

CIS Controls · NIST CSF 2.0

02
Agents
Tool permissions, excessive agency, memory poisoning, MCP server trust, third-party skills and plugins.

OWASP Agentic Top 10

03
Applications
Direct and indirect prompt injection, RAG data leakage, API authorization, STRIDE threat modeling.

OWASP LLM + API Top 10

04
Governance
Control alignment so fixes also hold up in customer due diligence and regulatory review.

ISO 42001 · AI RMF · EU AI Act

SITE CARE

Your site is your shop. Nobody's on call for it. We are.

One flat monthly fee. Patching, uptime and malware monitoring, tested backups, incident response, a monthly report and small fixes included.

$249
per site / month

$299
one-time audit + hardening

$2,490
annual prepay, 2 months free

$199
per site from the 3rd site

WHAT YOU GET

- Risk-ranked findings, every one verified by a human
- Remediation items ready to assign to an owner
- A plain-language executive brief
- A roadmap from "it works" to "it's defensible"

WHY DISC INFOSEC

Led ShareVault through **ISO 42001 Stage 2 certification on the first attempt** and authored their MCP Governance Standard. Enterprise background across KPMG, IBM and Intel/McAfee FoundStone. **CISSP · CISM · ISO 42001 & 27001 Lead Implementer · PECB Authorized Training Partner.**

Book a 30-minute scoping call.

Tested by AI. Verified by a human. Answered for every month.

calendly.com/hd-deurainfosec
hd@deurainfosec.com · (707) 998-5164 · deurainfosec.com