ultraviolet

AI SECURITY SERVICES

Enable AI-Led Growth, Without Expanding Enterprise Risk.

Every major enterprise is integrating AI into core operations. But AI doesn't just increase productivity. It concentrates privilege, expands attack surface, and automates risk. If your AI systems are secured the same way as legacy software, you are blind to the most dangerous behaviors.

UltraViolet Cyber provides security services scross the AI lifecycle, combining strategy, threat modeling, adversarial testing, monitoring, and training to support secure AI adoption.

OUR AI SECURITY OFFERINGS

AI PROGRAM STRATEGY & GOVERNANCE

Establish the governance, policies, and operational practices required to securely adopt AI. Gain visibility into your AI risk posture and a clear roadmap for implementing security controls across development, deployment, and ongoing operations.

Key Capabilities

☑ AI security maturity assessments

☑ Governance and policy development

☑ AI risk and control frameworks

☑ Build vs. buy security advisory

AI THREAT MODELING

Identify how adversaries could exploit your AI systems before they are deployed. Map attack paths across models, prompts, APIs, agents, and data pipelines to uncover risks such as prompt injection, model manipulation, and data leakage.

Key Capabilities

☑ AI system architecture risk analysis

☑ LLM application attack path mapping

☑ Agent and workflow risk modeling

☑ Security control design recommendations

AI PENETRATION TESTING

Adversarial testing that simulates how attackers target AI-enabled applications before they reach production. Evaluate prompt injection, jailbreak attempts, sensitive data exposure, guardrail enforcement, and model misuse across models, APIs, and integrations.

Key Capabilities

☑ Prompt injection and jailbreak testing

☑ Sensitive data extraction and leakage scenarios

☑ AI model and guardrail validation

☑ API, integration, and workflow security testing

AI INSTRUCTOR-LED TRAINING

Practitioner-led training that equips development and security teams to build and operate AI systems securely. Learn how to apply secure development practices across the AI lifecycle, from model design and data handling to deployment and operations.

Key Courses

☑ Principles of AI/ML Security

☑ Threat Modeling for AI/ML Systems

☑ Security Champions Workshop for AI Teams

REAL-WORLD RESULTS

Customer: Global Fintech
Industry: Financial Services
Location: North America

Goals:

- Assess the security of new AI tools used by employees for research, advisor preparation, and financial analysis
- Understand prompt injection, jailbreak, and data extraction risks
- Test across Web app, API, and LLM platform integrations

Key Outcomes:

☑ Advanced AI security findings delivered to the development team

☑ Security controls strengthened before broader rollout

☑ Additional AI applications added to the testing roadmap

> **"As we expanded internal AI capabilities, we needed validation that our controls were working. UltraViolet provided that assurance."**
>
> **CISO**
> Multinational Independent Investment Firm

WHY ULTRAVIOLET CYBER

Built by Operators
Founded by former U.S. intelligence community operators, UltraViolet brings offensive DNA to defensive strategy. We don't just know how to detect threats, we know how attackers think.

Full Lifecycle Coverage
From pre-breach validation to post-breach containment, we integrate continuous testing and continuous defense into one unified model.

Outcomes, Not Alerts
Our customers don't measure success in alert volume. We focus on verified threats, real-time containment, and business impact.

Proven Federal & Commercial Expertise
Trusted by DHS and Fortune 500 enterprises alike, UltraViolet delivers operational rigor with agile execution.

Flexible Engagement Models
Whether co-managed, fully outsourced, or embedded, we adapt to your team, your tech stack, and your mission.

START WITH AN AI SECURITY PROGRAM ASSESSMENT

Understand your current AI security posture, benchmark it against peer organizations, and receive a clear, prioritized roadmap for strengthening governance, engineering controls, and runtime protection.

Continuously Assess. Consistently Defend.

ultraviolet

UltraViolet Cyber is a leading platform enabled unified security operations company providing a comprehensive suite of security operations solutions. Founded and operated by security practitioners with decades of experience, the UltraViolet Cyber security-as- code platform combines technology innovation and human expertise to make advanced real time cybersecurity accessible for all organizations by eliminating risks of separate red and blue teams. By creating continuously optimized identification, detection and resilience from today's dynamic threat landscape, UltraViolet Cyber provides both managed and custom-tailored unified security operations solutions to the Fortune 500, Federal Government, and Commercial clients. UltraViolet Cyber is headquartered in McLean, Virginia with global offices across the U.S. and in India

443.351.7630 / info@uvcyber.com / in UltraViolet Cyber / 𝕏 ▶ @uv_cyber