

ABOUT AURORA

Aurora Information Solutions, Ltd. is a technology company specializing in cybersecurity. Our team consists of fellows from renowned universities, PhD holders, and certified professionals such as CISSP and CISP. The company focuses on cutting-edge global technologies in areas including system security, web security, mobile security, blockchain security, big data applications, security threat intelligence, and AI security. Through technological innovation, AI empowerment, and big data-driven approaches, Aurora provides technical services and customized security solutions to its clients.

TEAM STRENGTHS

Led by world-class experts, specializing in APT protection and vulnerability discovery, a cybersecurity pioneer serving global Fortune 500 companies and critical infrastructure sectors.

Elite Cybersecurity Team

Our team is composed of highly skilled professionals, led by distinguished Fellows and a PhD specializing in cryptography, cybersecurity, and blockchain technology. Over 70% hold CISP certification, with certain members possessing CISSP, OSCP, and CWE credentials. Each member brings over 10 years of experience.

Top-tier Technical Capabilities

The Aurora Security Team specializes in advanced APT (Advanced Persistent Threat) attack prevention and vulnerability mining technology. The team has built an exclusive cyber threat intelligence platform, monitoring the 9 major APT organizations around the world. In addition, with strong AI R&D capabilities, the team has successfully developed advanced security tools such as AI attack chain prediction system and Web3 detection engine module, providing innovative and efficient solutions for network security.

Extensive practical expertise

Aurora has successfully provided top-tier security services to over 500 enterprises and institutions, including critical sectors such as Fortune 500 companies, military industry, aerospace, government entities, finance, energy, healthcare, aviation, teleco, and education. The team has extensive experience in securing critical national infrastructure, having participated in national-level network protection operations 7 times and receiving multiple public commendations from military-industrial and public security authorities.

SERVICES HIGHLIGHT

Crypto Security Assessment

Oversee Web3 security, safeguarding crypto asset and blockchain systems

Cyber Threats Intelligence

Digital asset analysis, threat monitoring & optimized security strategies.

Vulnerability Assessment & Pen Test

A vulnerability management, discovery, analysis, remediation, and continuous monitoring.

Security Risk Assessment Security Audit

Comprehensive protection of information assets, ensuring security and compliance.

Security Operations Management

Comprehensive cybersecurity reports, with dedicated customer managers.

Cybersecurity Awareness Training

Customized security training and drills to enhance defense capabilities.

Incident Management & Forensic

Incident handling and analysis, instant emergency response.

Custom Solution For Enterprises

AURORA WEB3 SECURITY SUITE

CONTACT US
contact@aurorait.com.hk

The Aurora Web3 Security Platform is a professional and comprehensive cybersecurity solution designed specifically to protect decentralized applications (DApps) and their associated digital assets within the Web3 ecosystem. The platform includes the following five core functions:

Aurora AI
Web3
Assistant

On-Chain
Monitoring

Smart
Contract
Auditing

Web3 Threat
Intelligence

Security
Knowledge
Base

AURORA SERVICES LIST



Information Security Consulting Service

Provide expert guidance to improve an organization's security, including risk assessments, strategy and policy development, and recommendations to protect systems, data, and networks from threats.



Security Risk Assessment Service

Evaluate system security in accordance with international standards (e.g., ISO/IEC 27001), covering assets, architecture, devices, vulnerabilities, and applications, with remediation recommendations to mitigate risks.



Advanced Penetration Testing

Simulate real-world attack techniques to identify vulnerabilities in networks, systems, and applications, assess the current security posture, and highlight the need for vulnerability remediation.



Vulnerability Scanning

To identify and address security vulnerabilities in hosts, networks, and applications using a database-driven approach, generating comprehensive reports and remediation recommendations.



Source Code Auditing

To examine website source code and architecture, identify security vulnerabilities, and deliver secure coding guidelines, precise vulnerability localization, and remediation recommendations.



App security testing services

To identify internal security risks in applications through expert-led penetration testing, providing detailed security analysis and actionable improvement recommendations.



Security Hardening Service

Regularly inspect the secure operation of the customer's system, identify potential risks, and provide technical and managerial improvement suggestions, with a standard cycle of once per quarter.



Security Inspection Service

Regularly inspect the secure operation of the customer's system, identify potential risks, and provide technical and managerial improvement suggestions, with a standard cycle of once per quarter.



Security Incident Response Service

To providing instant technical support during a security incident in an information system, aimed at controlling impact, identifying causes, and offering solutions, including attack traceability and digital forensics.

CLIENTS & PARTHNNERS

