

Cloud Environments Security Testing

Protect your cloud environments from misconfigurations, data exposure and advanced threats.

[Contact Us](#)

Cloud Environments Testing

Secure your cloud to uncover risks before attackers do with our customized testing options:



Automated Cloud Configuration Review

- Automated scanning with industry-standard tools to identify misconfigurations and vulnerabilities.
- Price: €600 + €300/additional day | Duration: Minimum 2 days for 500 resources + additional days for extended scope.
- Get a full analysis of detected vulnerabilities with expert advice on remediation.



Comprehensive Cloud Configuration Review

- Combines automated scanning with manual analysis to uncover deeper issues not detected by tools. Includes IAM analysis, storage security, networking configuration review, encryption checks, and logging/monitoring validation.
- Price: €900 + €300/additional day | Duration: Minimum 3 days for 500 resources + additional days for extended scope.
- Receive an in-depth report with detailed misconfigurations, risk assessment, and tailored remediation steps.

[Order Now](#)[Explore Service Details](#)

Automated Cloud Configuration Review

Comprehensive Cloud Configuration Review

Prerequisites

Cloud Account (Read-only), API/CLI Access

Test Type

Automated

Actions

Identify and Report Misconfigurations

Used Tools

Prowler, ScoutSuite

Covered Vulnerabilities

Identity & Access Management

- Check for weak password policies, missing MFA, inactive accounts, unused groups, root.

Compute & Networking

- Verify secure instance metadata service (IMDSv2), restrictive security groups, HTTPS for load balancers.

Storage & Databases

- Check for public buckets, encryption at-rest, logging enabled, and restricted database exposure.

Logging & Monitoring

- Confirm CloudTrail/Activity logs, GuardDuty/Defender enabled, logging on CDN/WAF.

Application & Serverless

- Automated checks for secrets in Lambda/Functions and public API exposure.

Cloud Account (Read-only), API/CLI Access, Web Console Access

Automated and Manual

Identify, Validate, and Report Misconfigurations with Business Impact

Prowler, ScoutSuite, AWS CLI, Azure CLI, Manual Policy & Console Analysis

Everything from Automated Review plus:

Identity & Access Management

- Full IAM/Entra ID review, least-privilege validation, privilege escalation detection, guest/conditional access restrictions

Compute & Networking

- Review VPCs, subnets, firewall rules, VPN access, cross-account trust, and workload-specific risks

Storage & Databases

- Manual validation of encryption key management, customer-managed keys, advanced DB authentication (IAM, Entra ID), versioning & recovery settings

Logging & Monitoring

- Validate central logging, custom alerting for critical actions, compliance with CIS/NIST monitoring standards

Application & Serverless

		Manual review of IAM execution roles, API Gateway access control, and secret management practices
Reporting	Findings with remediation guidance.	Prioritized risks, escalation paths, compliance mapping, and tailored remediation plan.
Duration	2 days minimum for 500 resources (+additional days for extended scope)	3 days minimum for 500 resources (+additional days for extended scope)
Price	€600 + €300/additional day	€900 + €300/additional day

Order Now

Order Now

Step-by-Step Process

- 1. Order Service Request**

The client orders a "Service Request" by completing the contact form, providing the details of the resources in scope, a brief project description, and contact information.
- 2. Scope Review & Kick-Off (if applicable)**

We review the Service Request and, if necessary, schedule a 30-minute kick-off meeting to discuss the effort estimation, project timeline, and details regarding the in-scope resources. For Black-Box tests, we can proceed directly to the next step.
- 3. Contract and Payment**

Once the details are agreed upon, we send the client a contract and invoice. After the contract is signed and payment is received, we begin the testing phase.
- 4. Testing Execution**

Our expert team conducts a combination of automated and manual tests, simulating real-world attack scenarios to uncover vulnerabilities and assess security posture.
- 5. Report Delivery**

Upon completion, you'll receive a comprehensive report detailing identified vulnerabilities, their severity levels, and actionable recommendations to enhance your security.

Subscribe to our newsletter

Email address

Submit

Contact

Email: office@ethicsec.com

Socials: [in](#)

Contact Us