ORACLE
Advanced Customer Services

Oracle Managed Security Penetration Testing Service

Oracle Managed Security Penetration Testing Service for PaaS and IaaS is designed to identify and validate vulnerabilities of internet-facing web application environments on Oracle Cloud. This service helps customers reduce security risks and costs by enabling them to identify vulnerabilities before they are exploited by cybercriminals.

STAY AHEAD OF CYBERCRIMINALS

Today, most organizations face the risk of sophisticated hacker attacks and have implemented layers of defensive mechanisms to prevent unauthorized access and exploits.

However, increasing threat sophistication and proliferation of malicious actors can make it more challenging for companies to protect their internet-facing web applications and defend against cyberattacks.

VALIDATE SECURITY DEFENCES THROUGH SIMULATED ATTACKS

Oracle Managed Security Penetration Testing Service helps identify and demonstrate vulnerabilities of customers' internet-facing web applications and helps enable them to reduce risks through:

- Experienced Oracle Ethical Hackers that simulate attacks combining unique skills with sophisticated automated scanning tools alongside human engineered attack vectors
- Thorough Penetration Testing Process based on reliable industry standard recommended practices and methods coordinated by an Oracle Security Service Manager from start to end
- Comprehensive scan and analysis report providing information about security risks found, severity ratings, and remediation recommendations

Penetration Testing Phases and Activities Include:

PHASE	DESCRIPTION
Planning	**Pre-Engagement Scoping and Requirements Gathering** An Oracle Security Service Manager works with the customer to agree on the service scope: • Gather information about the target environment along with any customer-mandated regulatory, policy or risk management requirements • Agree on the scope and goals of the test • Gain the written approval from the customer's security point of contact

Key Features

- Experienced security engineers simulate a real-world attack
- Proactive detection and validation of web application security vulnerabilities
- Security assessment and analysis report with details about findings, severity ratings, and remediation recommendations
- Dedicated Security Service Manager to coordinate service delivery

Key Business Benefits

- Reduced risk of malicious attacks and incidents
- Actionable remediation recommendations designed to help meet security needs
- Unique security service and proven technical solutions help unload in-house resources
- Improved efficiency of risk management programs at predictable costs

ORACLE

Discovery	**Information Gathering and Vulnerability Scanning** Oracle security specialists use a combination of various tools[1] to map assets and services that are part of the target environment and identify potential vulnerabilities associated to those running services.
Attack	**Penetration Testing Execution** Oracle Ethical Hackers conduct penetration tests based on the scope and information identified in the planning and discovery phases: • Simulate actions of a competent and motivated hacker from the public internet • Use publically available tools[2] and manual testing • Conduct dictionary attacks to augment the ability to gain access to accounts. This activity can be restricted depending on the customer's need to resolve issues like application or operating system account lockouts • Ethical Hacking Team will only attempt to test for unauthorized access to the environment and data contained therein and will not update, delete or insert any data or make any configuration changes as part of this phase
Reporting	**Report of Findings Creation and Presentation** The Oracle security specialists team presents the results of the penetration test: • Create a detailed report of findings including information on all the tests conducted, security risks found, severity ratings, and remediation recommendations • Conduct a service delivery review meeting with the customer's security point of contact to present the outcome, and discuss the remediation recommendation

Related Products

- Oracle Cloud

Related Advanced Customer Services

- Oracle Managed Security Web Application Vulnerability Assessment
- Oracle Managed Security Vulnerability Assessment (Infrastructure)
- Oracle Managed Security Web Application Firewall Service
- Oracle Managed Identity Cloud Service
- Oracle Managed Security Operations Center for Cloud

WHAT MAKES ORACLE ADVANCED CUSTOMER SERVICES UNIQUE

Oracle Advanced Customer Services has many years of experience with implementing Oracle security products and services, and in securely managing security for customer environments in Oracle Cloud. The broad portfolio of managed security services can help customers minimize security risks in their Oracle Cloud web applications.

[1]Tools used may include but are not limited to Nmap, Socat, Burpsuite pro, Nessus, Qualys, WebInspect, Paros, CrypTool, HTTPLiveHeaders, and sqlmap

[2]Tools used may include but are not limited to WebScarab Proxy, Medusa, Hydra, CrowBar, Metasploit, publicly available exploit code, Oracle-authored tools

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com/acs.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/advanced-customer-services

Integrated Cloud Applications & Platform Services