FortiGuard Penetration Testing Service
Remote Penetration Testing

Bolstered by its long experience in threat analysis and vulnerability research, Fortinet is now providing its own penetration testing service.

Throughout more than 15 years, FortiGuard has been sharpening its skills and tools to become one of the top-notch worldwide cyber security research labs. FortiGuard consists of hundreds of specialists and is credited with over 840 zero-day discoveries – a record unmatched by any other security vendor.

- **Discover Vulnerability**
  Understand current security shortfalls within the network and critical hosts, thereby take appropriate actions to secure them.

- **Get Remediation Advices**
  Received resolution instructions from experienced security experts.

- **Test Incident Response**
  Prepare security team and test existing monitoring tools for real attacks.

**Methodology**
- These services leverage the Open Web Application Security Project (OWASP) to conduct a series of technical assessments on your organization’s security controls to determine the weakness on computer hardware infrastructure and software application.
- Our FortiGuard Pentest Team will apply commercial automated tools to discover unintended services made publicly available by your network and we also apply real world attackers’ methodologies to discover unknown vulnerabilities on the given target.
Features

FortiGuard Pentest Team offers the following remote vulnerability assessment and penetration testing service to the companies who want to know existing security shortfalls in their network. The service conducts technical tests on an organization's assets that typically involve both automated and manual assessments.

External Vulnerability Assessment

To identify vulnerabilities on a system exposed on Internet from an outsider point of view. It includes discovering the public-facing footprint of the company requesting the test.

Web Application Penetration Testing

To assess the risk exposure of a web application, including but not limited to unauthorized access, privilege escalation, exploitation, and data exfiltration. We comply with OWASP Top 10 Application Security Risks when conducting vulnerability assessment on the web application. Customers may want to provide specific accounts to authenticate on the application.

Internal Vulnerability Assessment

To identify vulnerabilities on a system exposed from an insider point of view. In that case, remote access has to be provided with optionally the network architecture.

Mobile Application Assessment

To assess the risk exposure of a mobile application, including but not limited to unauthorized access, exploitation, and data exfiltration. We comply with OWASP Top 10 Mobile Application Security Risks when conducting tests on mobile application.

Deliverables

After the technical phases, we prepare a vulnerability assessment report presenting the potential issues found during the assessment together with risk rankings and recommended remediation procedures. Customers can act on the issues according to severity level set as High, Medium, and Low priority, which is in accordance to Common Vulnerability Scoring System (CVSS) standard.

Order Information

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiGuard Penetration Testing Service</td>
<td>FP-10-PT001-000-00-00</td>
<td>Remote penetration test of 1 web application or 1 mobile application</td>
</tr>
<tr>
<td></td>
<td>FP-10-PT11E-000-00-00</td>
<td>Assess network application vulnerabilities and evaluate Web/Mobile Application security issues conforming to OWASP Top 10 and CWE</td>
</tr>
<tr>
<td></td>
<td>FP-10-PT102-000-00-00</td>
<td>Evaluate Web Application security issues conforming to OWASP Top 10 and CWE</td>
</tr>
<tr>
<td></td>
<td>FP-10-PT108-000-00-00</td>
<td>Remote vulnerability assessment of up to 64 IP addresses</td>
</tr>
<tr>
<td>FortiPenTest</td>
<td>FC-10-FPENT-236-02-DD</td>
<td>FortiPenTest Penetration testing subscription service for detection of critical vulnerabilities in websites / web applications, including those in OWASP top 10. Each subscription covers 10 IP/FQDN</td>
</tr>
</tbody>
</table>