H3C Security Expert Service Specification

1. Service Overview

H3C Security Expert Service is an expert support service that includes consultation and technical support services derived from customers' requirements for software deployment of H3C security products, security management system, operation and maintenance system and technical system construction. It can help customers build a security system.

H3C has a wealth of experienced technical experts, relying on advanced service management concepts and unique software and hardware tools, working closely with customers' technical staff and IT managers to address the needs of customers based on product-based technical services, in infrastructure and data, providing professional and standard technical services at all levels of the business.

H3C can flexibly organize service content for customers according to their actual needs, and provide on-site technical support and remote technical support.

2. Service Content

H3C Security Expert Service includes two aspects:

- Software deployment service for H3C security products
- Security consulting and technical support service

The service content includes but is not limited to the following contents, and can be freely combined according to the actual needs of customers.

2.1 Software deployment service for H3C security products

Security product software deployment services is a service project designed by H3C to help customers ensure the deployment quality of security products and give full play to the utility of products. In the process of product software debugging and deployment, H3C will dispatch senior project product experts to provide services such as security product software deployment plan review, software debugging and deployment, and on-site training etc., to help customers successfully complete the task of security product deployment.

Security product software deployment services includes technical solution design, software deployment and on-site training, excluding hardware to be put on shelf.
2.1.1 Technical solution design

The technical manager shall write the Technical Implementation Plan of security Products according to customer requirements, clarify the key technical points and difficulties needed in the deployment of security products, and be responsible for the technical feasibility of the deployment of security products. Based on its maturity, the technical manager decides whether to submit the technical proposal to the product support engineer for review.

The role of technical manager can be the front-line post-sales engineer of the representative office or the post-sales engineer of the agent. The agent engineer is responsible for basic security gateway products, such as firewall &VPN, application control gateway and intrusion prevention system, the technical proposal writing etc. And the front-line post-sales engineer of the representative office can be responsible for the review. For other multi-service security gateway and security application layer products, the technical proposal should be written by the front-line post-sales engineers of the representative office. After the technical solution is output, the technical manager will choose whether to submit the technical solution to the product support engineer for review based on the maturity of the solution (the maturity is judged by the coverage of typical configuration materials).

Note: Multi-service security gateway refers to M9000 series, security application layer products include load balancing products, Web application firewall, webpage tamper-proof, operation and maintenance audit system, database audit system, vulnerability scanning system, abnormal flow cleaning system, data leakage prevention system, security isolation and information exchange system, etc.

2.1.2 Software deployment

The software engineer is responsible for the debugging and deployment of software which is usually the technical engineer of the representative office.

According to the customer's business requirements and technical solutions, the software engineer writes the Security Product Configuration Implementation Plan and the configuration scripts, defines the configuration steps, and provides the recovery plan for cutover failure. For security product configuration implementation with high risk, the software engineer should submit the configuration implementation plan to the product support engineer for review. The product support engineer is responsible for demonstrating the feasibility of the configuration, identifying the defects and deficiencies in the deployment scheme, and reviewing the configuration script to give the optimal configuration suggestions.

After the configuration implementation plan is confirmed, the software engineer and the customer reserve the time of equipment cutover and on-line, and carry out the equipment on-line in accordance with the Security Product Configuration Implementation Plan. During the cutover process, the software engineer is responsible for product function test and fault location.

2.1.3 On-site training

In the process of equipment debugging, the technical manager will provide on-site training to the technical personnel of the client, so that the technical personnel of the client can understand the configuration, common problem handling and daily maintenance.
2.2 Security consulting and technical support

Security consulting and technical support service includes consultation and technical support services derived from the construction requirements of the customer's secure management system, operation and maintenance system and technical system.

Customers can flexibly customize the service content:

<table>
<thead>
<tr>
<th>Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security program consultation</td>
<td>In the process of daily security project construction, it involves information classified security protection, boundary scheme, security reinforcement, security planning and other related scheme design. The security consulting experts of H3C can participate in the scheme preparation process, and provide security related professional suggestions to improve the professionalism and competitiveness of the scheme.</td>
</tr>
<tr>
<td>Security management system</td>
<td>The information security management system is established by defining the scope and policy, business analysis, risk assessment, design, implementation and other stages, according to the relevant international, national or industrial security management system standards, based on the business risk method.</td>
</tr>
<tr>
<td>Security emergency management</td>
<td>For all kinds of information security incidents at all levels, from the perspective of emergency management, the information security emergency management system is established for organizations through the preparation of emergency plans and guidance of emergency drills, and is constantly improved and enhanced.</td>
</tr>
<tr>
<td>Industry security dynamic tracking</td>
<td>A monthly security situation report shall be provided, including emergency security event notice, security vulnerability notice, security early warning notice and security suggestions. In case of high-risk loopholes and emergencies, corresponding security notices will also be provided. &lt; monthly regular push, monthly security research report &gt; At the beginning of each month, the latest security information, security vulnerability situation, critical vulnerability examples, security highlights of this month and H3C security solutions will be released to the public &lt; major security incidents, follow up in the first time &gt; In view of the major security incidents in the field of cybersecurity at home and abroad, H3C security experts will follow up in the first time, and push relevant precautions and solutions to users.</td>
</tr>
<tr>
<td>Security support at critical time</td>
<td>Provide on-site security services during major meetings and holidays. The guarantee service mainly includes the following: On site monitoring: during the meeting, our company will send security experts with rich experience in security attack and defense to</td>
</tr>
</tbody>
</table>
Security leakage and penetration test

Provide users with remote or on-site penetration test or vulnerability scanning services according to specific needs, and output test reports and repair suggestions.

Security code testing

Provide on-site code test service for users according to specific requirements and output test report and repair suggestions.

Security risk assessment

Provide users with relatively fast and moderately reduced security risk assessment services according to the specific situation and output the risk assessment report and rectification suggestions.

Security awareness training

According to difference of training personnel, such as management personnel, operation and maintenance personnel, ordinary employees, etc., provide training including security awareness training, security attack and defense training, security management training, security operation and maintenance training and policy and regulation training.

Emergency response service for security incidents is a security service provided to meet the needs of enterprises in case of security incidents and urgent problem-solving. In case of hacker intrusion, system collapse or other security events that affect the normal operation of business, the H3C security experts will make emergency response to the security events in the first time, so that the network application system of the enterprise can resume normal operation in the shortest time, help the enterprise to find the source of intrusion, and recover or reduce economic losses for the enterprise.

After handling the emergency response to the security incident, we will provide a detailed emergency response report, which will restore the invasion process and provide the corresponding solutions.

Emergency response: during the meeting, when the target website is attacked by hackers, the on-site personnel on duty immediately analyze, detect, suppress and deal with the intrusion event, find the source of the intrusion and restore the normal operation of the system, and then provide an emergency response report, in which the intrusion process will be restored and corresponding solutions will be given.

enter the user's site, to assist the user in on-site security watch of the target website, and to conduct real-time monitoring and log analysis of the security situation of the website.

Emergency response to security incidents

Provide users with relatively fast and moderately reduced security risk assessment services according to the specific situation and output the risk assessment report and rectification suggestions.

Security awareness training

According to difference of training personnel, such as management personnel, operation and maintenance personnel, ordinary employees, etc., provide training including security awareness training, security attack and defense training, security management training, security operation and maintenance training and policy and regulation training.