Sangfor Incident Response Service Proposal

Make IT Simpler, More Secure and Valuable

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: sales@sangfor.com | W.: www.sangfor.com

Document Details

Name	Sangfor Incident Response Proposal		
Version	V2.0		
ID	SFSS–ICR–P0101		
Author	Sangfor MSS Team	**Issue Date**	30 July 2020
Reviewed By	Sangfor MSS Team	**Review Date**	30 July 2020
Classification	Confidential		
Limited To	· Sangfor Technologies Inc. · Customer/Partner		
Distribution Control	Sangfor Technologies Inc.: CREATE, MODIFY, READ	Customer/Partner: READ	

Disclaimer

This document contains Sangfor Technologies confidential commercial information. By accepting the terms, you agree to keep this document strictly confidential, and not reproduce, transmit or disclose any or all of this document to any person or entity, without prior written permission from Sangfor. If you do not wish to accept the terms, note that disclosure, reproduction and transmission of any or all of this document, in any form, will result in litigation.

Table of Contents

1 Project Background

1.1 Global Security Situation

Continuous popularization and development of the Internet, cloud computing, big data, artificial intelligence and other emerging technologies have made more enterprise service systems open to the Internet. All are increasingly dependent on the Internet. Cybersecurity has become a challenging issue in the Internet age, producing a profound impact on the development of international politics, economy, culture, society, military and other fields. Informatization and economic globalization have propagated, with the Internet integrated into all aspects of social life, profoundly changing people's lifestyles. The information revolution boom era has deeply affected the world at large, sometimes considered a "double-edged sword," as it boosts economic growth at the same rate as it boosts information leakage and security incidents.

2017 witnessed a large-scale leakage of NSA's Equation Group tools, frequent exposure of various loopholes in operating systems and web applications, the widespread outbreak of ransomware attacks in the first half of the year, large-scale prevalence of various mining attacks in the second half of the year, increasing supply chain attacks, and ongoing targeted APT attacks. Explosive cybersecurity events have indicated that the tools used by attackers are highly weaponized. Network attacks driven by personal or national interest are industrialized and organized, and the network attack area is expanding.

With continuous change of cybersecurity capabilities and the gradual strengthening of cybersecurity supervision, security is evolving from a static defense in separate regions, to a constant dynamic confrontation that breaks the boundaries of time and space. The user's security needs have gradually shifted from basic compliance to genuine security protection. On one hand, security technology is constantly innovating. Big data security, threat intelligence, machine learning and cloud security are increasingly used in the security protection systems of government and enterprise. Emerging technologies and relevant knowledge are challenges to existing security management personnel. On the other hand, organizations lack the professional security talent needed to respond to advanced threats and major security incidents in a timely and effective manner.

Looking back upon the international cybersecurity and information security situation of recent years, we find that the overall frequency of cybersecurity incidents is on the rise. Internet giants like Yahoo, Marriott, eBay, Equifax and Target were all were once attacked by ransomware, mining viruses, CPU meltdown/spectre, APT attack persisting for years, zero-day loopholes spread by the dark network, or personal information exposure associated. These security incidents serve as a constant reminder for us to continue to strengthen cybersecurity and information security. In addition, laws and regulation guidelines have been released globally to clarify the relevant responsibilities of network operators from a legal standpoint, that require network operators to conduct security risk evaluation at least once per year. Network operators are obligated to comprehensively investigate deficiencies in cybersecurity and information security and any difficult to detect hidden security hazards with the goal of reducing risks. While meeting the requirements of laws and regulations, operators are also required to clearly understand the current security status of enterprises, assist in making management decisions for enterprises, schedule subsequent risk rectification tasks, reduce the possibility of future security events, and guarantee the secure, stable and sustainable operation of information systems.

1.2 Project Objectives

1.2.1 Understanding in Current Security Situation

1 Gain a deeper understanding of the security situation of the organizational information system, by means of this information security risk evaluation.

2 Determine elements which require security protection in the organization, and prioritize objects based on the identification of these information assets.

3 Determine information security threats faced by the organizational information system, by means of threat identification.

4 Get to know the statistics and distribution of vulnerabilities in the current information system, by means of vulnerability identification.

5 Clearly describe the current security system and the missing security control measures, by means of identification and confirmation of existing security control measures.

1.2.2 Assisting in Management Decision

After risk evaluation and identification is complete, the major risk components will have been identified. Based on the description, quantification and presentation of information security risks, relevant managers of the organizational information system have been educated about strategy and services designed to enhance awareness of information security, improve the level of information security protection, develop a risk control program and eliminate potential security hazards.

1.2.3 Meeting Compliance Requirements

We shall provide professional and efficient security evaluation services for important service applications, identify potential loopholes in advance, handle security problems in a timely manner, prevent security notices from regulatory authorities, and meet all compliance inspection requirements of regulatory authorities.

1.3 Project Benefits

1 Effective asset management and priority sequencing of protected objects is determined.

2 In-depth identification and analysis on the hidden threats, reducing the probability of security events caused by existing security hazards.

3 Full security status and effect of existing security control measures are discovered and analyzed.

4 Based on the results of the security risk evaluation, Sangfor will deliver security hardening and optimization suggestions and subsequent construction schemes, suitable for the unique situation of users, serving as a guide and baseline for all subsequent security updates, empowering users to carry out targeted security protection.

5 Moderate security is advocated. Users judge the acceptability of risks by following risk management principles, avoiding excessive investment for the purpose of pursuing absolute security.

6 An objective and impartial evaluation report, will assist executives in making decisions about subsequent security construction.

7 A balance between efficiency and security is advocated. Efficiency tends to stand in opposition to security. A balance between work efficiency and security requirements will be determined by means of a risk evaluation. The balance ensures efficiency maintains a favorable level while security requirements are met as much as possible.

2 References

The implementation process of the information security risk evaluation complies with relevant policies related to the following international standards or laws and regulations:

1 Information Security Management System Standard (ISO/IEC 27001)

2 Information Technology – Security Technology – Information Security Management Systems – Requirements (ISO/IEC 27001: 2013)

3 Information Technology – Security Technology – Information Security Risk Management (ISO/IEC 27005: 2011)

4 Evaluation Criteria for IT Security (ISO/IEC 15408 CC)

5 Code of Practice for Information Security Management (ISO/IEC 17799/BS7799-1)

6 Concepts and Models for IT Security (ISO/IEC 13335, part 1)

7 NIST Framework for Improving Critical Infrastructure Cybersecurity

8 Information Security Incident Management (ISO/IEC 27035:2011)

9 Information Security Incident Management — Part 2: Guidelines to Plan and Prepare For Incident Response (ISO/IEC 27035-2:2016)

3 Incident Response Service

3.1 Service Definition

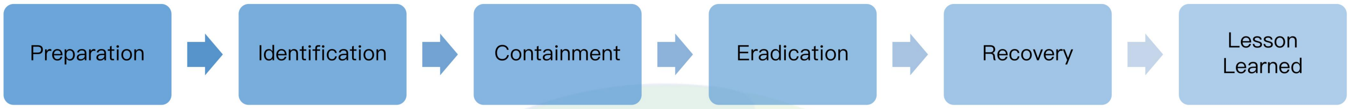
Incident Response is an organized process or phases of methodology that an organization use to response and deal with a security incident or data breach. Any data breach could have potentially significant impacts not only on customer sensitive data, company confidential intellectual property, but time and resources as well. In order to ensure the damages are reduced, incident response is needed for an organization to deal with the security incidents and recover the business from the impacts.

3.1.1 Why Incident Response is Important

- To minimize the risks and impacts when security incident happens
- To ensure business availability when the security incident happens
- To protect business images and reputations

3.2 Service Approach

Incident response is normally broken down into six different phases, as follow:


Preparation → Identification → Containment → Eradication → Recovery → Lesson Learned

a. Preparation

In this phase, Sangfor will assist the organization in preparing for ransomware or APT attacks. Sangfor will identify attack surfaces and vulnerabilities from external point of view. Organization can aware of their current risks and conduct risk mitigation plan. Once the identified risks have been mitigated or reduced, the organization is now prepare for the ransomware attack with minimum impact expected.

b. Identification

When the ransomware or APT attack attempted successfully, Sangfor will provide immediate response, according to the SLA, and identify and determine the following details:

- Ransomware family
- Ransomware type
- Affected date and time
- Entry point

- Kill Chain
- Indicator of Compromise (IoC)
- Triage

These information will be identified and analyzed by Sangfor incident response professional. These information can be collected via many ways, such as firewall logs, event viewers, hidden folders and files, netstat command, running processes and many others. Every steps taken by Sangfor incident response professional will be recorded and screenshot for later documentation purpose. Internet connection and remote support software are required for Sangfor incident response professional to provide remote support.

c. Containment

Containment phase can either be done before identification or during identification. Once the identification of ransomware or APT is completed, Sangfor will provide advise on the containment of the affected machines, in order to minimize the risk of malware lateral movement.

d. Eradication

Once the ransomware or APT had been contained and all the evidences have been collected, Sangfor will assist organization in removing the malicious files.

e. Recovery

Once the ransomware or APT malware have been removed, Sangfor will share the security incident report to organization, which includes weak points identified, vulnerabilities existed in the system, recommendation and best practices. The examples of the vulnerabilities such as dangerous ports (TCP/445, TCP/3389) exposed to Internet, weak password in use, etc. Organization is adviced to follow the recommendation and perform fixing as soon as possible before the next attack occurs.

f. Lesson Learned

This is the most important phase in Incident Reponse where most organization neglected. This is important because this is the phase where organization could further improve their current security posture and prevent future incidents. In this phase, Sangfor will review the external attack surface and conduct external vulnerability assessment in order to identify weak points that could be easily exploited by the attackers. Improvement via lesson learned is important as it not only can avoid future incidents, but it could minimize the risk and impact as well, should a security incident happens again.

3.3 Service Tools

- Sangfor Antibot

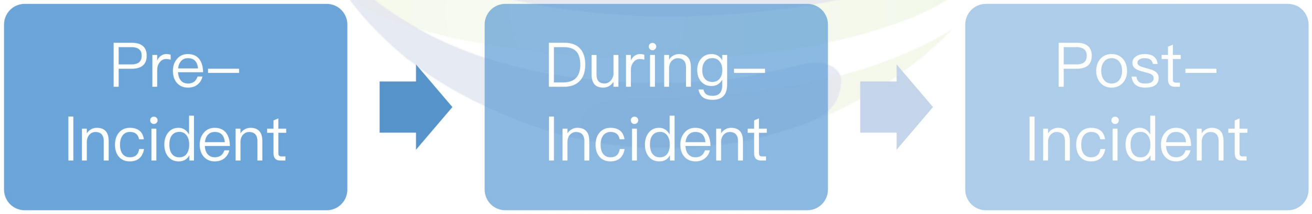
It is a malware killing tool that combines local killing and cloud killing. The tool has a powerful virus database in the cloud that can identify most active virus threats on the existing network; it also has a powerful scanning engine in the local, through static analysis of the program and dynamic virtual execution, so that windows Malware has nowhere to go.

- Sangfor Endpoint Secure

  Core engine of Endpoint Secure, Engine Zero, achieves high detection and low false positive rates by accurately identifying the “DNA” of unknown malware/ransomware based on continuously learning artificial intelligence using multiple techniques such as evolving neural networks and heuristics.

3.4 Service Process

Despite on the packages offered, Sangfor provides a closed-loop solutions to organization. Sangfor separated security incidents into three major phases:



a. Pre-Incident Phase

In pre-incident phase, Sangfor will help the organization to assess the external attack surfaces and vulnerabilities, before the attack occurs. Organization would able to know if existing network architecture, network setup, security practices and security controls are sufficient to defend against ransomware and APT attacks. Attack surfaces, vulnerabilities, weak points and risks are identified before attackers take advantages and exploit on them. Organization is advised to conduct fixing and risk mitigation plan according to the recommendations provided by Sangfor, in order to reduce the risk level to the minimum.

b. During–Incident Phase

Should a ransomware or APT attack successfully, Sangfor incident response team will provide immediate support, within the SLA agreed, to mitigate the incident and minimize the impact.

c. Post–Incident Phase

After the impacted services have recovered and the incident case is closed, the business operation of the organization will be operated as normal. In order to review the protection capabilities of organization against ransomware and APT attack, Sangfor will provide an external vulnerability assessment service and firewall ruleset configuration review in order to ensure new vulnerabilities, weak points and misconfigurations are identified, before the next attack occurs.

3.5 Service Scope

There are three incident response packages offered by Sangfor:

I. Essential Package

- Cover during-incident
  - During-Incident
    - Ransomware Family and Type Identification
    - Kill Chain Determination
    - Entry Point Identification
    - Indicator of Compromise Determination
    - Triage Determination

II. Standard Package

- Cover both pre-incident and during-incident
  - Pre-incident
    - External Vulnerability Assessment
  - During-Incident
    - Ransomware Family and Type Identification
    - Kill Chain Determination
    - Entry Point Identification
    - Indicator of Compromise Determination
    - Triage Determination

III. Premium Package

- Cover pre–incident, during–incident and post–incident
    - Pre–incident
        - External Vulnerability Assessment
        - Attack Surface Identification
    - During–Incident
        - Ransomware Family and Type Identification
        - Kill Chain Determination
        - Entry Point Identification
        - Indicator of Compromise Determination
        - Triage Determination
    - Post–Incident
        - External Vulnerability Assessment
        - External Firewall Ruleset Policies Review

Packages	Essential	Standard	Premium
Pre–incident Scope	–	Yes	Yes
– External Vulnerability Assessment – Attack Surface Identification	–	–	Yes
During–incident Scope – Ransomware family and type identification – Kill chain determination – Entry point identification – IOC and triage determination	Yes	Yes	Yes
Post–incident Scope – External Vulnerability Assessment – External Firewall Ruleset Policies Review	–	–	Yes
Response Time	<2 Hours	<2 Hours	<2 Hours
Assistance Mode	Remote only	Remote /Onsite if necessary	Remote / Onsite if necessary
Incident Response Count	1	1 (recommend 2 times per year for cost–effective package)	1 (recommend 4 times per year for cost–effective package)
Security Incident Report	Yes	Yes	Yes
Vulnerability Assessment Report	–	Yes	Yes
Service Components Health Check **limited to Sangfor product only*	–	–	Yes
Firewall Policies Review Report	–	–	Yes

3.6 Deliverables

I. Essential Package

- Security Incident Report (During–Incident)

II. Standard Package

- External Vulnerability Assessment Report (Pre–Incident)
- Security Incident Report (During–Incident)

III. Premium Package

- External Vulnerability Assessment Report (Pre–Incident)
- Attack Surface Identification Report (Pre–Incident)
- Security Incident Report (During–Incident)
- External Vulnerability Assessment Report (Post–Incident)
- Firewall Ruleset Configuration Review Report (Post–Incident)

3.7 Service Benefits

Precaution is better than cure. Sangfor not only focus on delivering satisfying incident response service to the organization, but Sangfor focus on preventing an organization from being attacked by the ransomware or APT attacks as well.

- **Determination of potential security vulnerabilities**

  The external vulnerability assessment can simulate how an attackers identify the attack surfaces and break in from the outside and eventually center in on a certain threat point and exploit it to produce a threat to the whole network. In this way, the potential security vulnerabilities in the entire system are determined.

- **Security awareness enhancement**

  Any potential vulnerability identified in the external view of an organization may cause "a small leak will sink a great ship". Therefore, the external vulnerability assessment service enables the responsible personnel to effectively eliminate any tiny security defect, thereby reducing the overall security risk.

- **Security skills improvement**

  The user's security skills are improved during the interaction with the test personnel. In addition, the professional vulnerability assessment report provides the user with ideas to solve prevailing security problems.

4 Project Management

4.1 Service Principles

To ensure the normal operation of the information system and the effectiveness of the security risk assessment, the assessment shall strictly abide by the following principles:

- **Standardization**: Strictly comply with relevant national and industry regulations and standards, and implement them with reference to international standards.
- **Service focus**: Security risk assessment mainly focuses on the service provided by the information system, with the service and its data the core for protection. This service-centric policy shall be in effect through all stages of the assessment.
- **Normalization**: Develop rigorous work plans and strictly control personnel, project implementation, quality assurance and time scheduling through normalized project management.
- **Controllability**: Ensure that the tools, methods, and processes used during the safety assessment are in the scope acknowledged by both parties, perform well-established assessment methods in-line with industry security risk assessment standards, and provide the tool software and information resource data with legal rights in project implementation, to ensure that all tools and software are free from ownership and intellectual property disputes, and they are available and reliable.
- **Confidentiality**: Ensure that any confidential data about the users involved will not be disclosed to third parties or individuals, and cannot be used to harm the interests of the users.

- **Minimum impact**: Minimize the impact of the assessment on the normal operation of the system and network, not severely impacting the normal operation of the network system and service applications (including serious system performance degradation, network congestion, and service interruption), and perform backup and emergency measures before the assessment.
- **Interactivity**: Participate in the whole process of project implementation with the users (security administrators, system administrators, general users and other related staff) to ensure the effectiveness of project execution and improve the users' skills and awareness for security.

4.2 Quality Management

At each stage of the project, the project manager will maintain compliance with applicable quality standards, by monitoring and measuring all output (including technical performance, deliverable status and project management status) of the project.

Sangfor ensures that the quality of the project meets specified requirements by the following means:

4.2.1 Standards and Orientations for Quality Control

Standards: The quality control team shall take the contract items as the standards and fairly inspect, supervise and review the work of the project team.

Orientations: Document control, schedule control, integrity control for the service process and response time and quality control for the service request.

4.2.2 Quality Control Team

According to the Sangfor's professional service specifications and contracts, the quality control team shall develop quality control standards before starting the project, which cover the orientations for quality control. Due to the length of time and broad geographical layout of the project, the quality control team shall also consider all unfavorable factors in advance and submit them to the project manager in writing, to ensure the smooth progress of the project.

In the project, the results of the first enhanced service and the regular audit service shall be submitted in document form with the format and text being compliant with the customer's requirements and Sangfor's internal specifications. Quality control keeps all documents under control from this perspective.

In the project start-up stage, the project team shall submit the overall project implementation plan to the quality control team for their records. The quality control team shall supervise and call attention to the project schedule in strict accordance with the implementation plan, analyze and find unfavorable factors that may hinder the project as planned, and submit them to the project manager for coordination and resolution.

The quality control team shall monitor the project implementation process according to the service process specified in the implementation plan, collect customer feedback, and ensure the integrity of the service process.

In the acceptance stage, the project team shall submit the sample project acceptance plan and report to the quality control team. The quality control department shall check and approve the work according to the sample acceptance plan and report, and collect the customer's opinions, to ensure smooth acceptance of the project.

4.2.3 Contract Review

- The requirements of the contract are clear and documented.
- The requirements stipulated in the contract are reasonable and in-line with relevant national laws and regulations, stating appropriate risks and benefits for both parties.
- Any contractual requirements that are inconsistent with the bid or have inconsistent opinions have been resolved.
- The company has the ability to meet the requirements stipulated in the contract.

4.2.4 Process Control

- Three-inspection system

  Each implementation team shall strictly enforce the system covering self-inspection, mutual inspection, and special inspection in the implementation process, to achieve full prevention and eliminate quality issues during implementation. Upon partial or itemized completion, self-inspection shall be first conducted by implementation personnel, and then mutual inspected by the technical director. After passing the mutual inspection, the technical director shall notify the customer's auditor to conduct a special inspection.
- Technical quality notice

  Any serious hazard to the quality of the project shall be reported to the Quality Department of the Company.
- Pre-inspection for the project

Pre-inspection for the project is mainly to inspect or verify the important technical material and sites before or during implementation. The team leader shall inspect or verify the general project sites, and the customer's auditor shall participate and sign off on the inspection results. The project manager, implementation team leader, and customer's auditor shall jointly inspect important sites, and apply for and sign the certificate upon successful inspection.

- Solutions for quality issues

All general quality issues shall be examined and resolved under the organization by the Project Manager Department. Serious quality issues and special project quality issues shall be examined and resolved by competent organizational units under the company QC. Quality issues must be classified as "No approval in three cases (causes unknown, persons in charge and general public uneducated, or no practical preventive measures adopted)" principle. Issues shall be reported to supervisory departments step-by-step in a timely manner according to the relevant state regulations, without delay. The rework for serious quality issues shall be conducted only after special reports are submitted and approved by the Company.

4.3 Project Risk Management

Certain objective risks may exist in the security service. They may impact daily organizational tasks if they are not prevented. Therefore, it is necessary to analyze risks and take countermeasures.

4.3.1 Project Risk Analysis

Certain risks may exist in the implementation process. According to preliminary analysis, the following risks may exist in the security service, including:

- Confidentiality risks

  Security service involves key sites and system facilities. Some sensitive data and even secret data may be exposed during the implementation process. Therefore, confidentiality shall be considered to prevent data disclosure risks.

- Risks caused by testing activities

  The security service targeting key service systems and network systems supporting the service system which require high availability, integrity, and confidentiality. The testing means adopted in security service may be at risk of causing abnormal operation of the service application system, or may introduce malicious codes due to improper use of tools. Therefore, the risks arising from the assessment tools and their use shall be circumvented during the assessment process.

- Technical risks

  Technical issues come from unpredictable errors in certain systems, and may cause extended working time and affect overall progress.

- Time risks

The schedule and actual time for implementation are estimated inaccurately, affecting the progress of the overall work.

- Personnel risks

  The implementer's determination and support for security service affects the progress and quality of the assessment, and the technical competency of the implementer affects the quality of the assessment.

4.3.2 Risk Avoidance Measures

According to the preceding analysis, certain risks may exist in the information security service. Therefore, the measures for avoiding risks shall be worked out before the project is implemented.

- Avoidance of confidentiality risks

  The service provider shall protect the information within the scope of the assessment and the ownership of the Civil Affairs Department. The implementer shall sign a confidentiality agreement when joining the assessment team. Cross-level access to the information requires direct authorization from the project leader. The implementer shall not share the information in a place with an inferior information level. The implementer may not disclose the assessment data, information and results to a third-party without written permission. If the organization requires us to transmit the assessment results by telephone, fax or other electronic or electromagnetic means, specially-assigned persons shall protect and transmit the information in encrypted mode and disclose any security risks of transmission. The implementer shall not disclose any confidential information about the operation, strategy and technology of this security risk assessment team to a third-party. The implementer shall not copy, transmit and disseminate the information belonging to the organization for personal purposes.

- Avoidance of risks caused by testing activities

  The project team has specifically analyzed the impact of each testing measure for risks. In the process of implementation, the testing measures shall be discussed, to carry out response plans and reduce the risks. All technical testing tools shall also be tested strictly before mobilization to avoid faults and hidden issues.

- Avoidance of technical risks

  Get familiar with security service methods, fully understand the features of information systems, strictly standardize operations of the implementer, and carry out joint supervision through multiple supervisors.

- Avoidance of time risk

  Strengthen project planning and management, learn about the progress of the project, analyze, control and adjust resources and reserve time in the plan for adjustment.

- Avoidance of personnel risk

  Before implementation of the project, the project team members shall be trained in operating knowledge, learn about the work flow and risk prevention measures and be informed of and abide by the confidentiality agreement on security.

5 Service Commitment

1 Sangfor shall ensure that the products provided or the tools used are not in violation of national laws and regulations, and will not infringe any patents, trademarks or copyrights of any third-party.

2 Sangfor shall appoint coordinators and project managers to provide reliable services for customers in terms of their specified security services.

3 If the system served by Sangfor suffers an emergency incident, Sangfor shall respond in accordance with the emergency response requirements of the organization within one hour, and deal with any emergency the customer considers urgent within three hours. Immediately rectify any faults requested by the users, including recovery of failed entities, fault diagnosis and event tracking.

4 Sangfor must be authorized by the organization before carrying out the work. Certain high-risk actions or operations shall be supervised by the staff from customer on-site.

5 Sangfor must establish a work team for the project, and the team leader shall be in charge of the project, and shall appropriately increase or reduce the service personnel in special cases.

6 Sangfor staff who participate in the implementation must sign a confidentiality commitment letter. Without the authorization of customer, the staff shall not transmit or disclose relevant information in the process of this assessment in any form.

6 Service Advantages

6.1 Sangfor Security Service Philosophy

Sangfor security service adheres to the "Full Service, Continuous Innovation and Professional Competence" philosophy. It shall ensure the secure operation of customers with premium services, and fully assist customers in all walks of life to demonstrate our value in the service.

In the field of R&D, Sangfor security service BG has a dedicated R&D team, invests in a large number of R&D resources to develop service tools and platforms, and constantly develops new ideas and technologies, making us a leader in the field of security service technologies.

In service delivery, we are committed to building a first-class team of security services experts. We have formulated a standardized service delivery process at a leading worldwide level, to ensure that our security service delivery is always excellent and first-class globally.

6.2 Sangfor Security Service Advantages

- Human-machine intelligence, 24/7 continuous and standardized service
- On-demand experts provide deep threat analysis services
- Precisely matching threat intelligence to the customer's assets, and quickly raising warning messages
- Proactively respond, assist in rectification, and resolve security issues.

6.3 Sangfor Security Service Team

Sangfor Security Service BG consists of the R&D, Delivery, and Marketing teams. Each team participates in each part of the security service. The delivery team members are highly-experienced and have qualifications like CISP, CISSP, PMP, CISA and CCSK.

- **R&D teams**: 100 developers of service tools and platforms, 30 experts in virus analysis, 30 experts in vulnerability analysis, 30 experts in offense and defense research.
- **Delivery teams**: 150 members in the regional professional service delivery team. 100 members in the Changsha Security Operation Center, and 20 experts in the emergency response team at headquarters.
- **Marketing teams**: 30 consultants and 30 marketing specialists.

Back-end capabilities of the Sangfor security service teams are delivered by the Research and Innovation Institute, the Threat Intelligence Lab, and a team of security experts.

6.4 Sangfor Security Service Qualifications

- Network Security Emergency Service Support Unit (State level) under the National Computer Network Emergency Response Technical Team/Coordination Center of China — the highest rating in China,
- Information Security Service Qualification Certificate (Class-A Emergency Response) issued by China Information Security Certification Center — the highest class in China

- Information Security Service Qualification Certificate (Class-A Risk Assessment) issued by China Information Security Certification Center — the highest class in China
- Information Security Service Qualification Certificate (Class-A Security Engineering) issued by China Information Technology Security Evaluation Center
- CS-CMMI5 Certification (the highest level of cloud security capabilities) by the Cloud Security Alliance (CSA)