Sangfor Incident Response (IR) Service Statement of Work

(April 2020)

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 (IR) Service Statement of Work (SOW)		
Version	V1.0		
ID	SFSS-TICR-P0102		
Author	Jeffrey Lee	**Issue Date**	15 April 2020
Reviewed By	Sangfor MSS Team	**Review Date**	15 April 2020
Classification	Confidential		
Limited To	· Sangfor Technologies Inc. · Customer		
Distribution Control	Sangfor Technologies Inc.: CREATE, MODIFY, READ	Customer: READ	

Version Change Record

Modified Date	Version	Description	Modified By
15 April 2020	V1.0	Final Draft	Jeffrey Lee

Disclaimer

SANGFOR

Table of Contents

SANGFOR

1 General Information

Services Performed For:	
Client Name	ABC Company
Client Phone	
Client Email	
Client Mailing Address	
Services Performed By:	
Partner Name	N/A
Partner Phone	N/A
Partner Email	N/A
Partner Mailing Address	N/A
Provider Name	Sangfor Technologies Inc.
Provider Phone	+60 127117129 (7511)
Provider Email	marketing@sangfor.com
Provider Mailing Address	
Date	15 April 2020

2 Purpose of This Document

This Statement of Work (SOW) is issued pursuant to the Consultant Services Master Agreement between ABC Company ("Client") and Sangfor Technologies Inc. ("Contractor"), effective 15 April 2020 (the "Agreement"). This SOW is subject to the terms and conditions contained in the Agreement between the parties and is made a part thereof. Any term not otherwise defined herein shall have the meaning specified in the Agreement. In the event of any conflict or inconsistency between the terms of this SOW and the terms of this Agreement, the terms of this SOW shall govern and prevail.

This SOW, effective as of 15 April 2020, is entered into by and between Contractor and Client, and is subject to the terms and conditions specified below. The Exhibit(s) to this SOW, if any, shall be deemed to be a part hereof. In the event of any inconsistencies between the terms of the body of this SOW and the terms of the Exhibit(s) hereto, the terms of the body of this SOW shall prevail.

SANGFOR

3 Project Details

Project Name	Incident Response (IR)
Project Description	To helps customer in identifying the attack surfaces that could exploited by the malicious actor, get customer in preparing for future attacks, minimizing the impact in case of security incident and assisting in business operation recovery.
Project Schedule	
Location of Work	Remote

4 Contact Information

Client Contact Information	**Primary Point of Contact** Name: Contact Number: Mobile Phone: Email: **Additional Point of Contact** Name: Contact Number: Mobile Phone: Email:
Partner Contact Information	**Primary Point of Contact** Name: Contact Number: Mobile Phone: Email: **Additional Point of Contact** Name: Contact Number: Mobile Phone: Email:

Provider Contact Information	**Sales Manager** Name: Contact Number: Mobile Phone: Email: **Project Manager** Name: Contact Number: Mobile Phone: Email: **Implementer** Name: Contact Number: Mobile Phone: Email: **Additional Implementer** Name: Contact Number: Mobile Phone: Email:

5 Scope of Work

Provider shall deliver the following services:

Service Content	Service Description
Malware Verification	To verify if the malware incident reported belongs to true positives.
Malware Family and Type Determination	To collect the malware information, such as file extension, the ransom demand page, in order to determine its family and its variant version. From there, incident response team able to know if this is belongs to new family or existing family.
Kill Chain Determination	To provide tracebility service by determine the cyber kill chain in order to find out which machine belongs to zero patient, and how many machines are infected
Attack Entry Point Identification	To identify the entry point and the problem source on how the attack came into environment
Collection of Evidences	To collect the evidences, such as date and time occurred, source IP address, attack patterns, etc.., from zero patient machine.
Malware Removal	To assist customer in malware removal process by removing malicious process, malicious files in the machine; then perform verification.
Summary Reporting	To collect all the information and screenshot during the incident response and tracebility process, and summarize them into a report for customer's review.
External Attack Surfaces Assessment	To assist customer in performing external attack surface identification and external vulnerability assessment in order to uncover most possible attack surfaces or vulnerabilities that could be leveraged or exploited by attackers.
External Firewall Ruleset Review	To assist customer in performing firewall ruleset configuration review in order to ensure most of the ruleset are properly in place.

SANGFOR

6 Deliverables

Provider shall provide the following deliverables:

1. Security Incident Report
2. External Attack Surface Assessment Report
3. External Firewall Configuration Review Report

Provider will deliver the documents within 5 working days after the final day of work.

7 Service Approach

Preparation

- To identify external attack surfaces and external weak points that could be exploited by malicious actors
- To assist customer in understand current risks that allow other to take advantage
- To assist customer in risk remediation and risk mitigation plan

Identification

- To identify malware family and type
- To identify chain of infection (kill chain) and source entry point of zero patient
- To determine Indicator of Compromise (IoC) for further actions

Containment

- containment advise to be provided once the identification of malware completed
- To assist customer in minimizing the risk of malware lateral movement / propagation

Eradication

- To remove the malware from infected machines once all evidences have been collected

Recovery

- To assist customer in recovering the business operation

Lesson Learned

- To review the security controls of the customer
- To provide recommendations and long term improvement plan in order to improve overall security status and reduce the chances of being attacked by attacker

8 Client Acknowledgement

The Client will indicate agreement with the content of this SOW prior to the project commencing by signing and returning this page or by email confirmation – either method is acceptable. In agreeing the SOW, the Client acknowledges that this SOW accurately defines the scope of the project and acknowledges its specific responsibilities in this regard detailed in this SOW and in any proposal provided prior to engagement. Once the SOW is agreed upon, subsequent changes to the details of the scope and timescales may be introduced by Contractor and the Client through email exchanges that refer to this SOW, and these changes will be considered to form part of the agreed upon SOW. Note that if this is not agreed prior to the project start date this will involve delays and may incur additional cost.

ABC Company	Partner
Signature: _____	Signature: _____
Name:	Name:
Title:	Title:
Date:	Date:

Sangfor Technologies Inc.
Signature: _____
Name:
Title:
Date: