Schneider Digital Statement of Work

Cybersecurity Testing R&D 2020
Vendor I , France
Start Date : 01 May 2020

CONTRACTUAL REFERENCE

This Statement of Work (SOW) is being executed pursuant to the Master Services Agreement between Schneider Electric USA, Inc, ("Schneider Electric" or "SE" or "Client") and Vendor I ("Supplier" or "Vendor I") dated June 28, 2018 (the "Master Agreement"). Any terms not defined herein shall have the meaning set forth in the Agreement.

Signature of this SOW by Supplier and Schneider Electric will constitute acceptance of the terms of this SOW. Supplier acknowledges and agrees that the SOW cannot be modified without Schneider Electric's prior written consent. Therefore, any provisions of this SOW that Supplier deletes, amends or modifies in any way, without Schneider Electric's prior written consent, will be null, void and have no effect.

SPONSORS

Schneider Digital Executive Sponsor: Joseph SPIRO
Schneider Digital Project Manager/Owner: Tim DAVIES

Supplier Executive Sponsor: Joe Harrison
Supplier Project Manager: Anderson Barnes

TERM AND TERMINATION

This SOW is effective as of the signature date unless otherwise noted here and is valid until December 31, 2020. Termination of this SOW will be pursuant to the terms for termination of a SOW as defined within the Agreement including the Termination for Convenience clause.

PURPOSE

Background

As of June 2019, the vulnerability threat has continued to grow and Schneider Electric needs to take proactive steps to secure its R&D sites along with the corresponding intellectual property. Risk quantification analysis has identified worst case potential loss or damage estimates ranging from 780M to 6.8B Euros across Schneider Electric. Recent outbreaks of exploits have raised the awareness of cyber risk and the need to improve Schneider Electric's security posture/position. In addition to hardening of SE defenses, Schneider Electric must also work to enhance preparedness for response and recover during a Security Incident to minimize disruption to the business and assure continuity of Schneider Electric's operations.

Vendor I performed a first mandate for Schneider Electric Digital to assess the cybersecurity posture of four (4) R&D sites leveraging a "red team" approach. Under this SOW, Vendor I will continue the work to assess additional SE R&D sites.

Objectives

The services under this SOW will establish the Cybersecurity vulnerabilities of the major SE R&D hub sites. Cybersecurity Testing will use state-of-the-art intrusion vectors and techniques to evaluate the vulnerabilities of the computer resources located at the selected sites. The results of the Cybersecurity Testing will be a report of the discovered vulnerabilities as well as the remediation recommendations.

To enable delivery of the services under this SOW, the parties will collaborate for the project “Cybersecurity Testing” on the operational scope described in this SOW (the “Project”).

SCOPE & APPROACH

SCOPE

In-Scope

The following Services are covered under the scope of this SOW (“the project”):

Phases of the Project	Description
Work Package 1. **Preparation**	**Deliverable 1:** Design document with the agreed attack scenarios to be performed during the Cybersecurity Testing
Work Package 2. **Cybersecurity Testing**	**Deliverable 2**: Site 1 - Final report after Cybersecurity Testing completion **Deliverable 3:** Site 2 - Final report after Cybersecurity Testing completion **Deliverable 4:** Site 3 - Final report after Cybersecurity Testing completion **Deliverable 5:** Site 4 - Final report after Cybersecurity Testing completion

Out-of-Scope
Driving remediation to identified vulnerabilities.

The list of selected sites for intervention shall be agreed between the Parties at the start of the engagement.

APPROACH

The methodology described below will be utilized for the two work packages of the project. This methodology will be repeated for the 4 R&D sites in the scope of this SOW:

WP1 (Work Package 1) – Preparation:

- Preparation: Confirm the scope and prepare the audit field work with documentation and tools to support the execution.
- Define Approach: Define execution details for WP2 and validate the technical scenarios that will be executed during the fieldwork
- Validation: Ensure agreement on the overall approach that will be applied for all the sites included in the scope of this SOW and for future potential Cyber Testing

WP2 – Cybersecurity Testing (To be executed for each in scope site):

- Reconnaissance: Gather relevant OSINT (Open Source INTelligence) to assess the R&D site digital footprint (IT assets), identify any collaborators credential leaks, and classified and/or sensitive information. This based on the physical address details, and a list of past/ongoing R&D projects only, and to prepare the next phases of the testing.
- External penetration testing: Perform penetration tests to identify vulnerabilities on the R&D site selected assets accessible from the Internet.
- [For one site] POC Spear phishing: By leveraging intelligence from previous phase, craft, send, and monitor phishing emails targeting few employees of the site (typically 3 employees), with the objective to either still their credentials and/or deliver fake malware / code to beacon back.
- USB Drops: Supplier will provide the Schneider Security team with code to beacon centrally, that Schneider will put on USB keys to be dropped in building entrances and lots. This to identify who plugged which USB key into which computer.
- Wi-Fi assessment: Perform an on-site assessment to list the Wi-Fi networks around the Schneider site to identify any shadow/rogue access point and try to break into the Schneider Corporate Wi-Fi networks.
- Internal penetration testing: By playing the internal threat (fraudulent user/partner) and being provided access to the network, perform penetration testing to lateralize and gain access to the site IT/OT assets.
- Reporting: Document and present identified vulnerabilities, attack scenarios and recommendations.

TIMELINE

DUE TO THE CURRENT COVID 19 OUTBREAK IT IS EXPRESSLY ACKNOWLEDGED THAT THE TIMELINE BELOW IS AN ESTIMATE:

- WP1 (deliverable 1) – One month after the contract signature
- WP2 (deliverables for the 4 sites) – By redefined deadlines at the beginning of the project
- Milestone Dates are listed in the diagram below:

SERVICES & DELIVERABLES

The Deliverables under this SOW follow in the table below:

Deliverable	Deliverable Description	Deliverable Format	Completion Criteria	Completion Date
Work Package 1. Preparation	**Deliverable 1:** Design document with the agreed attack scenarios to be performed during Cybersecurity Testing	Schneider Digital approval of the Cyber Testing scenarios	MS PowerPoint	T0+1 month
Work Package 2. Cybersecurity Testing	Assessment reports of cybersecurity controls in place at each testing site which identify vulnerabilities and provide recommendations for improvements: **Deliverable 2**: Site 1 - Final report after exercise completion **Deliverable 3:** Site 2 - Final report after exercise completion **Deliverable 4:** Site 3 - Final report after exercise completion **Deliverable 5:** Site 4 - Final report after exercise completion	Schneider Digital acceptance of approval of the Cybersecurity Testing reports	MS PowerPoint	By T0+7 months (end of engagement)

DELIVERABLES & ACCEPTANCE CRITERIA

For any Deliverables under this SOW, the following conditions apply, together with the conditions set out in Appendix A:

- All deliverable reviews will be performed against the Specifications set out in this SOW together with any requirements set forth in the Agreement.

- No deliverables can be deemed as accepted by Schneider Electric until Schneider Electric confirms its acceptance in writing, except as detailed in Appendix A.
- For deliverables specified under this SOW, if the deliverable does not meet the acceptance criteria specified in this SOW, the effort to get the deliverable to the expected quality level is the Supplier's responsibility.
- Schneider Electric reserves the right to return for correction, within the review period, any Deliverables that do not meet the Specifications set forth in this Statement of Work.
- Supplier shall fix any defects within a reasonable time period as agreed between the Parties.
- See Appendix A for the standard Deliverable Acceptance language. If the Agreement (MSA) states different Deliverable Acceptance language, place it in Appendix A.

ASSUMPTIONS

1. Availability of relevant stakeholders which includes the Schneider Digital project resources, on-site digital risk resources & site security resources.
2. Availability of required documentation for in scope products and organizations.
3. Availability of results of past product security reviews (e.g. penetration tests).

RESPONSIBILITY MATRIX

Supplier Responsibilities:

- Establish a regular status reporting and meeting schedule.
- Communicate with SE in a timely manner if data quality challenges or delays in obtaining information will impact the Supplier's ability to execute the assessment as defined in this SOW.
- Communicate with SE in a timely manner if fees are anticipated to exceed the upper limit of the fee estimate and the reasons for such.
- Oversee the quality of the assessment and ensure it is executed in accordance with the terms of this SOW.
- Provide written report to include summary of procedures performed, relevant findings/observations, and recommendations for potential changes/enhancement to the contracts and procurement and asset management processes.
- Notify SE immediately, outside of the regular status reporting time agreed, should the Supplier have findings which it deems to impact the scope of its work.

SE Responsibilities:

- Provide Supplier with timely access to relevant data, documentation, personnel, and required access to the Information System(s).
- Provide timely input regarding the Supplier's queries raised and subsequently confirm the go-forward approach.
- Provide timely feedback on the reporting deliverables.

SOW GOVERNANCE

All issues and disputes will first be worked out between the **respective project leads**. If a resolution can't be reached between the project leads, no longer than two (2) weeks from the initial documentation of the issue or dispute, the issue or dispute will be escalated to the **executive sponsors** for resolution.

If a resolution can't be reached at the executive sponsor level, the issue or dispute will be worked out according to the terms and conditions of the Agreement.

Any alternative process for managing issues and disputes should be documented in this section and mutually agreed between the Parties.

All issue and dispute documentation, available to Schneider Electric and the Supplier, will be stored in a Schneider Electric Box folder or similar Schneider Electric controlled document repository along with any resolutions.

MEETINGS & REPORTING

All meeting and other project related documents will be stored in a Schneider Electric Box folder or similar Schneider Electric controlled document repository, accessible by both Schneider Electric and the Supplier.

Vendor I will participate in the following Meetings :

- Weekly status update
- Quarterly Steering Committee

Vendor I will provide the following Reports:

- Summary Report for each R&D site which includes a presentation of the report for each site.

SCHNEIDER ELECTRIC DELAYS

- Schneider Electric will exercise due diligence and will ensure that factors beyond the control of Supplier, such as Schneider Electric delays and failure to fulfill Schneider Electric responsibilities, do not interfere with Supplier's ability to complete the Services.
- Schneider Electric shall notify Supplier of any such factors that may cause delays in the completion of tasks or changes to the Statement of Work, and both Parties will mutually determine required modifications to this Agreement.

CHANGE ORDERS

Any proposed changes to this SOW, including scope changes, must be documented in a written Change Order.

No Change Order modifying this SOW will be effective unless it is in writing and signed by both Parties.

PRICE AND PAYMENT SCHEDULE

Specify the type of contract: Fixed Fee

Total Value of SOW:

Type of Cost	Cost (Euros)
Services	190,000

Travel	0
Total	190,000

In accordance with the terms and conditions of this SOW, Schneider Electric agrees to pay to Supplier on a fixed fee basis a total fee amount of **190 000 €** (excluding taxes).

The Parties expressly agree that the services under this SOW ("the Project") will be provided on a fixed fee (not to exceed basis) and all Services and Deliverables within the Project shall be delivered in accordance with the terms of this SOW. Any work not specified in this SOW must be identified and mutually agreed in a Change Order to this SOW that must be signed by both Parties.

Commercial effort for additional Cybersecurity Testing (extended scope)

Vendor I will deliver the in scope Cybersecurity Testing "Red Teaming" exercise over the 4 following sites:

1. Grenoble (FR),
2. Monterrey (MX),
3. Bangalore (IN),
4. Andover (US).

PAYMENT TERMS

- Payment terms are as per the Agreement.
- The Parties agree that for the services under this SOW, Supplier shall issue invoice(s) to SCHNEIDER ELECTRIC USA directly in EURO (€), which shall pay such invoice to Vendor I .
- Fees shall be invoiced in accordance with the Billing Schedule set out below:

Invoicing Date	Currency	Amount
At acceptance of Deliverable 1	Euros	38 000 €
At acceptance of Deliverable 2	Euros	38 000 €
At acceptance of Deliverable 3	Euros	38 000 €
At acceptance of Deliverable 4	Euros	38 000 €
At acceptance of Deliverable 5	Euros	38 000 €

- All Supplier travel costs are included in the Fees.

TRAVEL GUIDELINES

- All Supplier travel requires written pre-approval from Schneider Electric. All travel will be booked aligned with SE travel guidelines. All travel disbursement related costs will be invoiced based on actual costs incurred.

COMPLIANCE

Supplier certifies that Supplier will comply with all relevant regulations, laws, rules, statutes or other legal and regulatory obligations as it pertains to the delivery of this SOW, and related activities.

Supplier ensures that its personnel will comply with written policies and procedures of Schneider Electric communicated to it in advance while on-site at Schneider Electric's facilities and while accessing any system or equipment of Schneider Electric whether on-site or remotely.

CONFIDENTIALITY

All Confidentiality terms from the Agreement, and any applicable Non-Disclosure Agreement, currently in effect between the Parties, shall apply.

AGREEMENT DEVIATIONS

- For the avoidance of doubt, the terms and conditions of the MSA take precedence over this SOW unless explicitly listed in this section and mutually agreed between the Parties.
- All deviations from the governing MSA should be included in this sub section and must be reviewed and approved by Schneider Electric Legal before this SOW is signed.
    - Due to the nature of the services, Customer provides Supplier the ability to access and conduct the security tests according to the Penetration Testing Mandate contained in Appendix C of this document. Schneider Electric undertakes to sign the Penetration Testing Mandate in the format provided in Appendix C herein, which shall be an integral part of this SOW.

SUPPLIER RESOURCE LOADING

Supplier's resource loading for this SOW follows in the table below:

Consultant Name (N/A under French MSA)	Consultant Title/Role	Work Location (City / Country)	Is resource a sub-contractor? If yes, from what company? (Yes / No)	Is resource a former SE, employee? (Yes / No)	Has resource been assigned to SE as an independent contractor within the past 12 months?	Rate Per Day (€)	Total days	Total Cost* (€ VAT exluded))
N/A	Partner	Paris, France	No	No	No	2650	2	5 300 €
N/A	Manager	Paris, France	No	No	No	1690	15	25 350 €
N/A	Senior Consultant	Paris France, or Located in the site in scope	No	No	No	1350	28,5	38 350 €
N/A	Consultant	Paris, France or Located in the site in scope	No	No	No	1150	100	115 000 €
Totals							**145,5**	**184 000 €**
Totals with discount							**145,5**	**184 000 €**

PRIMARY WORK LOCATION(S)

Supplier Work Locations:

- Paris La Défense, France

DATA PROTECTION & PRIVACY

Each Party will process professional contact details and adequate information from employees or other representatives of the other Party in the framework of a customer-supplier relationship and for the purpose of performing this SOW. In doing so each Party, as a Data controller, shall comply with applicable laws on the protection of personal data, including the EU General Data Protection Regulation ("GDPR").

Based on the nature of the services to be completed by Supplier under this SOW, the following shall apply: *pls check the applicable box*.

☒ Attach Completed DPA Annexures 1 - 3 (as applicable) to Appendix B to this SOW if Supplier will engage in Processing activities related to Personal Data as Processor with Schneider Electric as Data Controller (Processing, Personal Data, Data Controller each as defined under GDPR) in its performance of the SOW.

☐ Supplier hereby declares that Supplier will not engage in Processing activities related to Personal Data as Processor with Schneider Electric as Data Controller (Processing, Personal Data, Data Controller each as defined under GDPR) in its performance of the SOW.

APPENDICES

List of Appendices:

- Appendix A – Deliverable Acceptance (as applicable to this SOW)
- Appendix B – Data Privacy Regulation Addendum (as applicable to this SOW)
- Appendix C – Penetration Testing Mandate
- Appendix D – Scale up Discounting Tiers

IN WITNESS WHEREOF, the parties hereto have executed this Statement of Work.

SOW SIGNATURE

Vendor I	Schneider Electric Industries SAS
Name:_____	Name:_ _____
Signature: _____	Signature: _____
Title: Partner, Cyber Services_____	Title: _____
Date: _____	Date: _____