# Statement of Requirement (SoR)

## *Purpose*

*This document is for new Extra-Mural (EMR) Contracts. Use the Request for Contract Action (RCA) Guidance for EMR page on WikiD when filling out this SoR and a supporting RCA. Please seek assistance if desired from Commercial or your Divisional Procurement Representative.*

*This document is supplier facing and the RCA is an internal document. Please delete non-essential grey text before issuing externally/ to suppliers.*

| | |
|---|---|
| **Reference Number** | **RQ0000012774** |
| **Version Number** | **0.2** |
| **Date** | **05/07/2022** |

| **1.** | **Requirement** |
|---|---|
| **1.1** | **Title** |
| | **Orchestrated Cyber Deception Demonstrator using Virtual Machine Introspection** |
| **1.2** | **Summary** |

|  |  |
|---|---|
|  | [REDACTED – DEFENCE] The aim of this activity is to further explore the viability of Virtual Machine Introspection (VMI) as a means to deceive malicious activity on virtualised hosts. This will be focused on enhancing a pre-existing Xen-based deception virtual hypervisor to facilitate user testing at a later stage<br>The approach will further develop the deception-oriented hypervisor to utilise multiple CPU cores and mature the pre-existing deception concepts to minimise methods to bypass them. This approach will enable multiple deception concepts to be utilised on individual VMs. This approach will also develop additional deception concepts targeted at deceiving and disrupting Cobalt Strike activity. The approach will ensure this concept can be orchestrated by other tooling via the standardised Open Command and Control (OpenC2) framework [1]. |
| **1.3** | **Background** |

Current cyber deception approaches typically rely on deceiving adversaries either before they gain access to internal networks and/or during the lateral movement phases of an intrusion. When deception is utilised, it is typically at the network level – once a malicious actor gains access to an individual host, current deception measures are often limited. What measures are available often contaminate hosts with tell-tale signs of their presence (logs, suspicious processes, or inconsistent decoy data which stands out), or may be bypassed through modified Tactics, Techniques and Procedures (TTPs).

Virtual Machine Introspection (VMI) allows for the monitoring of the runtime state of process and application issued system level instructions in virtual environments. In the past this has been utilised for software debugging, forensics and for controlled inspection of malware execution. One of the advantages of this approach is that it does not leave obvious signs of its utilisation on the individual host, making it harder to detect. As VMI allows for monitoring (and where necessary, manipulation) of low level requests from applications and processes to the underlying system kernel, it should be possible to manipulate these in order to feed intentionally erroneous data back to the source, potentially deceiving the adversary utilising it. If such activity could be coordinated with other Defensive Cyber tooling, this provides an opportunity to manipulate and gather threat intelligence on adversaries whom have penetrated defended networks, as well as a means to hinder their further progression.

The aim of this task is to provide software development resources to further develop a pre-existing Xen-based hypervisor using VMI for deception. This work shall include developing new deception concepts targeted at explicitly deceiving and/or disrupting Cobalt Strike activity within a Windows virtual environment. This work also requires further development on several pre-existing deception concepts to minimise methods for a theoretical adversary to bypass or otherwise not encounter them. This development activity will require utilising pre-existing VMI-libraries and APIs (such as LibVMI [2] and DRAKVUF [3]) to develop the deception concepts. On the core hypervisor itself, additional work to enable multiple deception concepts to be utilised against individual VMs will need to be undertaken. Integration of multi-core processing for the underlying hypervisor is needed. Additional work is also needed to ensure these deception concepts can be orchestrated remotely via the OpenC2 standard.

Successful completion of this task will enable future research (including testing against human participants) on the technical maturity and usability of this approach by cyber operators.

| 1.4 | **Requirement** |
|---|---|

| | |
|---|---|
| | This will be a **8** month EMR activity, contracted through the Digital Marketplace (Lot: 1 Digital Outcomes). **Estimated contract start date is the 01/09/2022**, with final delivery date stated to be no later than 01/04/2023. [REDACTED – DEFENCE] Software development will be managed using an Agile approach (e.g. Scrum) and prioritisation of tasks will be managed via a backlog accessible to the supplier and Dstl. This backlog shall be provided by the supplier within 20 working days of contract award. The project backlog will constitute a visible record of current and future progress towards achieving the overall aims of this task.<br>The supplier will work with a Technical Partner (TP) from the Authority for regular interactions.  The supplier shall prepare and issue a project management plan and provide it to the Authority within 20 working days of contract award. The supplier will be required to host a start-up and planning meeting with the Authority. This will be utilised to discuss the backlog for the task and allow the Authority to context on how it intends to utilise and exploit the software developed from this task. The supplier shall provide a brief on their capabilities and working ethos. Minutes from this meeting will be captured by the supplier and delivered to the Authority.<br>The supplier must utilise a pre-existing custom Xen hypervisor provided by the Authority which has been developed as part of a prior development activity. This codebase alongside relevant documentation will be provided within 30 days working days of contract award.<br>As part of this work the supplier will be required to undertake a period of familiarisation and testing in order to understand how pre-existing deception concepts need to be extended. This will allow for the identification and subsequent development of this concepts to minimise adversary methods of bypassing.<br>The development of deception concepts targeted at hindering Cobalt Strike activity may require an initial scoping study to understand the type of activity generated by Cobalt Strike over an attack life cycle. Given the timescales this may be required to occur concurrently with other development activity.<br>The development of additional deception concepts must utilise the LibVMI [1] and/or DRAKVUF [2] software libraries/APIs to facilitate introspection against target VMs. These deception concepts must be written in C or Python programming languages. No specific coding styles or standards are mandated, although guidelines outlined in Joint Service |

Publication (JSP) 188: Documentation of Software In Military operational Systems, should be followed unless otherwise agreed with the Authority.

Any new deception concepts created and/or by the supplier must be able to run on supported versions of Debian-based Linux operating system (>= Ubuntu 18.04 LTS) and should avoid any closed-source, proprietary, software dependencies where possible (unless otherwise stated by the Authority). The deception concepts will be targeted at userspace processes running in Windows 10 VMs. Agreement from the Authority is required prior to integrating any other additional third party software libraries.

Some prior work has already been undertaken in the development of the OpenC2 API. However the supplier must further extend this to ensure the deception concepts can be properly orchestrated to facilitate increased automation. As such the supplier may be required to engage with the OpenC2 community to clarify appropriate syntax for deception actions within this standard.

The supplier must make source code available to the Authority over the course of the contract period. This shall be achieved via the use of a private git repository, hosted by the supplier and accessible over the internet. The approach taken by the supplier will be detailed by the supplier in the proposal submitted in response to this requirement. The Authority requires access to unstable incremental updates and stable builds (for example post-sprint) of the source code for internal testing. Instructions for compiling and deploying the code are required. On conclusion of the task, source code and any compiled file must be provided.

The supplier will be required to demonstrate work undertaken to stakeholders at a Dstl site. On conclusion of the task, the supplier shall attend a close down meeting. The supplier will provide a brief summary of the activity undertaken, identifying any relevant lessons.

## References

[1] Organization for the Advancement of Structured Information Standards, “Open Command and Control (OpenC2),” Organization for the Advancement of Structured Information Standards, 12 05 2022. [Online]. Available: https://openc2.org/. [Accessed 23 05 2022].

| | |
|---|---|
| | [2] LibVMI project, “LibVMI: Simplified Virtual Machine Introspection,” Github, 2021. [Online]. Available: https://github.com/libvmi/libvmi. [Accessed 10 05 2021].<br>[3] DRAKVUF project , “DRAKVUF,” DRAKVUF project , 12 03 2021. [Online]. Available: https://drakvuf.com/. [Accessed 04 05 2022].<br>[4] M. Tarral, “KVM-based Virtual Machine Instrospection,” Github, 2021. [Online]. Available: https://github.com/KVM-VMI/kvm-vmi. [Accessed 10 05 2021]. |
| **1.5** | **Options or follow on work** *(if none, write ‘Not applicable’)* |
| | Not applicable under DOS Framework. |

| **1.6** | **Deliverables & Intellectual Property Rights (IPR)** | | | | | | |
|---|---|---|---|---|---|---|---|
| **Ref.** | **Title** | **Due by** | **Format** | **TRL*** | **Expected classification (subject to change)** | **What information is required in the deliverable** | **IPR DEFCON/ Condition**<br>*(Commercial to enter later)* |
| *D – 1* | *Project Management Plan* | *T0+20 days* | *Report (.pdf)* | *n/a* | *[REDACTED – DEFENCE]* | *Document outlining how the supplier intends to address aims of task, key milestones, any requirements, etc.* | *[REDACTED – DEFENCE]* |
| *D – 2* | *Initial Project backlog* | *T0+20 days* | *Excel (.xlsx) or agreed alternative* | *n/a* | *[REDACTED – DEFENCE]* | Record of current and future progress towards achieving the overall aims of the task | *[REDACTED – DEFENCE]* |
| *D – 3* | *Kick-off meeting* | *T0+20 days* | *Presentation (.pptx)* | *n/a* | *[REDACTED – DEFENCE]* | *Presentation to discuss but not limited to:*<br>• *Project Management Plan*<br>• *Preliminary backlog.*<br>• *Software Development Capability*<br>• *Commercial aspects.*<br>• *Review of deliverables.* | *[REDACTED – DEFENCE]* |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | *• Initial Risks/issues.*<br>*• GFA/GFI requirements and supplier performance* | |
| *D – 4* | *Kick-off meeting minutes* | *T0+1 month* | *Report (.pdf)* | *n/a* | *[REDACTED – DEFENCE]* | Record of discussions of the kick off meeting. | *[REDACTED – DEFENCE]* |
| *D - 5* | *Progress report* | *T0+2 month* | *Report (.pdf)* | *n/a* | *[REDACTED – DEFENCE]* | summarise the results of work done during the period covered and shall be in sufficient detail to comprehensively explain the results achieved; | *[REDACTED – DEFENCE]* |
| *D - 6* | *Progress report* | *T0+3 month* | *Report (.pdf)* | *n/a* | *[REDACTED – DEFENCE]* | summarise the results of work done during the period covered and shall be in sufficient detail to comprehensively explain the results achieved; | *[REDACTED – DEFENCE]* |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| *D - 7* | *Progress report* | *T0+4 month* | *Report (.pdf)* | *n/a* | *[REDACTED – DEFENCE]* | summarise the results of work done during the period covered and shall be in sufficient detail to comprehensively explain the results achieved; | *[REDACTED – DEFENCE]* |
| *D - 8* | *Progress report* | *T0+5 month* | *Report (.pdf)* | *n/a* | *[REDACTED – DEFENCE]* | summarise the results of work done during the period covered and shall be in sufficient detail to comprehensively explain the results achieved; | *[REDACTED – DEFENCE]* |
| *D - 9* | *Progress report* | *T0+6 month* | *Report (.pdf)* | *n/a* | *[REDACTED – DEFENCE]* | summarise the results of work done during the period covered and shall be in sufficient detail to comprehensively explain the results achieved; | *[REDACTED – DEFENCE]* |
| *D - 10* | *Progress report* | *T0+7 month* | *Report (.pdf)* | *n/a* | *[REDACTED – DEFENCE]* | summarise the results of work done during the period covered and shall be in sufficient detail to comprehensively explain the results achieved; | *[REDACTED – DEFENCE]* |
| *D - 11* | Demonstration event | *T0+8 Months* | Demonstration | *n/a* | *[REDACTED – DEFENCE]* | Demonstration of modified and additional deception concepts in use against Cobalt | *[REDACTED – DEFENCE]* |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | Strike. Exact format of demonstration subject to discussions with suppliers | |
| *D - 12* | Final delivery of Source Code | *T0+8 Months* | | TRL5 | *[REDACTED – DEFENCE]* | All source code generated in support of this task packaged alongside software dependencies. | *[REDACTED – DEFENCE]* |
| *D - 13* | Instructions of building, deploying and operating deception concepts. | *T0+8 Months* | document | n/a | *[REDACTED – DEFENCE]* | Instructions detailing how to deploy deception concepts into suitable environment. Depending on approach taken by supplier this may be limited to deception concept examples, web front-end and API or include a full deployment process for integrating VMI and QEMU modifications into a target OS. | *[REDACTED – DEFENCE]* |
| *D - 14* | Final Technical Report | *T0+8 Months* | Report (.pdf) | *n/a* | *[REDACTED – DEFENCE]* | Final technical report detailing work done, technical design of concepts and API, issues identified with technical approach, possible follow on tasks | *[REDACTED – DEFENCE]* |

***Technology Readiness Level required**

*Notes- IPR should be inserted / checked by commercial staff before sharing with the supplier(s) to ensure accuracy.*

| | |
|---|---|
| **1.7** | **Standard Deliverable Acceptance Criteria** |
| | All Reports included as Deliverables under the contract e.g. Progress and/or Final Reports etc, must comply with the Defence Research Reports Specification (DRRS) which defines the requirements for the presentation, format and production of scientific and technical reports prepared for the MOD.<br>Interim or Progress Reports: The report should detail, document, and summarise the results of work done during the period covered and shall be in sufficient detail to comprehensively explain the results achieved; substantive performance; a description of current substantive performance and any problems encountered and/or which may exist along with proposed corrective action. An explanation of any difference between planned progress and actual progress, why the differences have occurred, and if behind planned progress what corrective steps are planned.<br>All Reports shall be free from spelling and grammatical errors and shall be set out in accordance with the DRRS Statement of Requirement above. Failure to comply with the above may result in the Authority rejecting the deliverables and re-questing re-work before final acceptance. |
| **1.8** | **Specific Deliverable Acceptance Criteria** |
| | Kick-off Meeting minutes shall provide a record of discussion of the kick off meeting and shall be delivered as a .docx formatted document. This will be reviewed by the Authority with a 5 working day acceptance period.<br>Monthly Progress / interim reports shall summarise (not detail) work undertaken over the course of the month (including the outcomes of any sprint activity), risks to progress, opportunities and issues related to delivery. These shall be delivered as a .PDF file. These will be reviewed by the Authority with a 5 working day acceptance period.<br>Any and all code developed for the deception concepts shall be packaged alongside software dependencies (relevant VMI libraries), where permissible, required to run the deception concepts. These will be reviewed by the Authority with a 10 working day acceptance period.<br>Technical report detailing work done, technical design of concepts and API, issues identified with technical approach, possible follow on tasks. The technical details shall be sufficient to permit this shall be delivered as a .PDF file. These will be reviewed by the Authority with a 10 working day acceptance period. |

| 2. | Quality Control and Assurance |
|---|---|
| **2.1** | **Quality Control and Quality Assurance processes and standards that must be met by the contractor** |
| | ☒ **ISO9001** (Quality Management Systems)<br>☐ **ISO14001** (Environment Management Systems)<br>☒ **ISO12207** (Systems and software engineering — software life cycle)<br>☐ **TickITPlus** (Integrated approach to software and IT development)<br>☒ Other: **(Please specify below)**<br>Compliance with TickIT*plus* is desirable, but not mandatory. Where applicable, the supplier should comply with guidance set out in Joint Service Publication (JSP) 188: Documentation of Software in Military Operational Systems. |
| **2.2** | **Safety, Environmental, Social, Ethical, Regulatory or Legislative aspects of the requirement** |
| | N/A |

| | | |
|---|---|---|
| **3.** | **Security** | |
| **3.1** | **Highest security classification** | |
| | **Of the work** | *[REDACTED – DEFENCE]* |
| | **Of the Deliverables/ Output** | *[REDACTED – DEFENCE]* |
| **3.2** | **Security Aspects Letter (SAL)** | |
| | Yes<br>If yes, please see SAL reference- *Enter iCAS requisition number once obtained* | |
| **3.3** | **Cyber Risk Level** | |
| | N/A | |
| **3.4** | **Cyber Risk Assessment (RA) Reference** | |
| | *[REDACTED – DEFENCE]*<br>If stated, this must be completed by the contractor before a contract can be awarded. In accordance with the Supplier Cyber Protection Risk Assessment (RA) Workflow please complete the Cyber Risk Assessment available at https://suppliercyberprotection.service.xgov.uk/ | |

| **4.** | **Government Furnished Assets (GFA)** |
|---|---|
| GFA to be Issued - Yes<br>• **Source code repository** containing VMI Deception hypervisor developed in previous phase will be provided. (Includes previous deception concepts, Web front-end, OpenC2 API, Custom Xen build).(?)<br>• **Final technical report from supplier** for previous Phase | |

| 5. | Proposal Evaluation criteria |
|---|---|
| 5.1 | **Technical Evaluation Criteria** |
|  | *[REDACTED – DEFENCE]* |
| 5.2 | **Commercial Evaluation Criteria** |
|  | *[REDACTED – DEFENCE]* |