Centre for Defence Enterprise

Cyber Defence: Securing Against the Insider Threat

Competition launch: Wednesday 27 November 2013

Competition closes: Thursday 9 January 2014 at 1700 hrs

The Centre for Defence Enterprise (CDE) proves the value of novel, high-risk, high-potential-benefit research sourced from the broadest possible range of science and technology providers, including academia and small companies, to enable development of cost-effective capability advantage for UK Armed Forces and national security.

Proposals for funding must be submitted by **1700 hrs on Thursday 9 January 2014** using the Centre for Defence Enterprise Portal. Please mark all proposals for this themed competition with **"Cyber Defence"** as a prefix in the title.

- **Technical queries** should be sent to cybersecurityCDE@dstl.gov.uk. Please see guidance on using this facility under the 'CDE proposal submission process' section.
- **General queries** (including how to use the Portal) should be sent directly to CDE at cde@dstl.gov.uk or by phone on +44 (0)1235 438445.

CDE: www.science.mod.uk/enterprise
Dstl: www.dstl.gov.uk

SBRI Government challenges. Ideas from business. Innovative solutions.

[dstl]

Defence Science and Technology Laboratory

Ministry of Defence

Cyber Defence: Securing Against the Insider Threat

Background

The 2010 Strategic Defence and Security Review (SDSR)[1] sets out the threat to the UK's Cyber Security

"The risks emanating from cyber space (including the internet, wider telecommunications networks and computer systems) are one of the four Tier One risks to national security (set out in the National Security Strategy). These risks include hostile attacks upon the UK from other states, potential shortcomings in the UK's cyber infrastructure, and the actions of cyber terrorists and criminals. But cyber space also creates opportunities for the UK Government and British businesses, which will derive benefits from the protection that effective cyber security measures bring to the UK economy. These threats and opportunities are likely to increase significantly over the next five to ten years, as our dependence on cyber space deepens."

SDSR Page 47, Section 4.C.1

The Programme and Delivery Directorate (PDD) at the Defence Science and Technology Laboratory (Dstl), is responsible for the planning, formulation and delivery of the overall Science and Technology (S&T) research requirement for UK defence and security, as directed by the Ministry of Defence's (MOD) Research and Development (R&D) Board. Dstl are running this CDE call on behalf of MOD.

The cyber programme is part of the PDD within Dstl and supports the implementation of the National Cyber Security Strategy[2] across defence. This involves inter-disciplinary research across the physical, information and human sciences domains into the evolution of cyberspace and its influence on human behaviour. Its goal is to deliver the capabilities needed by UK MOD to train, exercise, rehearse and conduct military operations in cyberspace in the same way that it does on land, sea and in the air. The cyber programme also works across government to address the capabilities needed to secure the UK's broader interests in cyberspace.

Cyber Defence

The MOD cyber research programme, in partnership with other government departments, seeks to enable freedom to operate across all environments by finding ways to defend all of Her Majesty's Government (HMG) digital assets. The cyber defence research programme is responsible for developing new and novel methods to secure MOD's systems, communications and platforms. The MOD enterprise infrastructure is large and varied covering 70+ countries with 1200 UK Sites, 800,000 IP addresses and 225,000 Users. Additionally, MOD has a wide variety of platforms, which are increasingly interconnected and reliant on cyber capability to function. MOD's operational infrastructure has consequently a large attack surface, which presents a substantial challenge to defend from ongoing attacks from capable adversaries.

One of the key potential threats to the MOD cyber assets is the abuse of legitimate credentials, either by individuals or malware. The Global Corporate IT Security Risks 2013[3] survey identifies employee activity (deliberate or malicious) as one of the main causes of incidents which lead to leakage of sensitive data. The

[1] The Strategic Defence and Security Review 2010
[2] The National Cyber Security Strategy
[3] The Global Corporate IT Security Risks 2013 Survey

2013 US State of Cybercrime Survey[4] identified that over 50% of respondents to the survey had experienced an insider incident within the last 12 months. The cyber insider threat continues to grow and has the potential to have a severe operational impact on MOD and HMG. These consequences could include a loss of capability, resources and the potential for reputational damage.

Technology challenge

This CDE themed competition seeks proof-of-concept research proposals for detecting cyber insider threats using host-based solutions, focused on securing MOD digital assets against the abuse of legitimate credentials. This can result in users accessing areas they are not entitled to, carrying out unauthorised alteration of logs or audit traces, running unauthorised programmes or scripts, unauthorised copying or transferring of files or data, activating or changing parameters of Real Time Operating Systems (RTOS) and other activities.

To address these scenarios, MOD is looking for novel and innovative host-based solutions utilising both technology and social science to detect and characterise anomalous and abnormal behaviour. For the purposes of this competition, a host is defined to include all end-user client devices (including those deployed on platforms) and covering their device memory, configuration, audit and logs. A platform is any military structure or vessel, such as a submarine or an aircraft carrier. These platforms are generally complex entities constructed of many parts (system of systems including bespoke infrastructure), for example, the Type 45 Air Defence Destroyer[5].

MOD's challenge is real, with many bespoke platforms that require protection from the abuse of legitimate access. One way to do this is by using a solution deployed at end points. This could include an element of hardware to interface with bespoke systems, for example, a ship's plant. These systems can supplement detection using widely deployed standard protection measures, such as Intrusion Detection Systems (IDS).

In order to detect abnormal behaviour on MODs digital portfolio, this competition covers a wide scope including the study of behavioural and socio-technical indicators, and the novel application of heuristics to indicate regular pattern of life and identify and characterise anomalous user behaviour. The prime focus of this competition is to identify and test novel proof-of-concept solutions to detect anomalous behaviour on the host, however, some consideration should be given to scaling detection on user client devices and the enterprise backend services that would be required. Any tool developed under this competition should also allow for gathering situational awareness from the user client devices, for example by aggregation, acumination, association and attribution of misuse from associated data. While this competition is looking for host-based solutions, there is potential for any tool developed to enable innovative statistical analysis and detection of anomalous behaviour centrally in a cloud system (ie a large database and memory requirements that exceed the host capability), providing a level of pre-processing is undertaken on the host to reduce bandwidth requirements.

Anomalous or abnormal behaviour includes that which is significantly different to the standard user behaviour for a given credential set. As an example, indicators of change in behaviour might include, but need not be limited to, aspects such as:

- changes in access patterns (ie where and when the user accesses the system)
- change in type and frequency of access of files, locations, systems, networks, platforms etc
- alterations in aspects such as dwell time on systems or locations
- changes in programmes executed
- changes in network traffic to/from the host
- alteration of logs or audits etc
- differences in use of language, typing patterns etc

[4] The 2013 US State of Cybercrime Survey
[5] Tyoe 45 Destroyers

- transferring large numbers of files/data onto or off the host
- activities or changes that have an unusual or “out of band” time and/or frequency element.

The monitoring of anomalous behaviours should be done for each credential set (ie routine behaviour should be described for each user, rather than generically by role), as different users with the same access might interact with hosts in a different manner. This will require understanding the baseline for regular behaviour for each individual set of credentials and to be able to account for regular variations for those credentials (eg diurnal, seasonal, familiarity, aging) as well as change of user role (role-based credentials might transfer between individuals when the role is handed over). Suppliers should note that baseline behaviour on MOD networks is not necessarily stable – for example, operational or exercise deployments often mean the behaviour of personnel will potentially change dramatically and any proposed solutions need to be able to account for this level of complexity.

To reduce user and administrator burden, a high level of sensitivity and specificity will be key for successful concepts. It is anticipated that approaches combining multiple (preferably orthogonal) indicators to provide a higher level of confidence in any classification are more likely to be funded. Given the significant number and variety of users on MOD systems, suppliers should be cognisant that even small improvements in the false positive and false negative rate of any approach will have an impact on real systems and be of substantial benefit to those who monitor those systems.

Proposals from potential suppliers should look to identify not only that anomalous behaviour might be taking place, but to characterise this behaviour, for example as malware, illegitimate users or legitimate users and the potential risk to MOD digital assets by the activities. The detection of this threat will enable MOD authorities to respond to protect systems and deter attackers, for example, by physical, procedural and technical controls such as reduction in permissions and privileges and other incident response activities. Proposals should also consider the ability to prioritise different occurrences of anomalous behaviour to help direct the response to any potential threat.

Dstl is especially interested in approaches that cover the entirety of MOD’s digital portfolio, bearing in mind that MOD’s platforms and systems are increasingly cyber enabled and connected. Suppliers also need to account for the fact that MOD has a wide range of non-standard hardware, software and protocols in use across its estate. This estate includes next generation technology as well as legacy (hardware and software) systems, using bespoke protocols. Tools and techniques that could potentially cover a wide range of these assets will be of substantial interest and approaches that address aspects beyond the typical TCP/IP network traffic will be more likely to be funded. However, approaches should not cause the user to have to alter their normal behaviour pattern in any way and should make use of existing hardware.

Bidders should also consider, as part of their proposal, suitable metrics to measure success of their approach. This should cover aspects including, but not limited to: computational burden of the method; time to detection of anomalous behaviour; sensitivity and specificity of detection; applicability of approaches across MOD’s digital assets etc. Bidders are free to add additional metrics to this list to demonstrate the benefits of their approach. Being able to demonstrate the success of methods against these types of metrics will increase the likelihood of future funding to further develop the selected approach.

Proposals submitted to this CDE competition should demonstrate the applicability and potential of the methods suggested, including a demonstration against exemplar data chosen by the bidder. Bidders should note that Dstl will not provide test data or hardware/software at this stage. Any tool or software developed under this competition should utilise open standards and tools wherever possible and should avoid proprietary software tools as much as possible. The output of this proof-of-concept stage should provide sufficient confidence to Dstl that the ideas are worth pursuing, allowing further development, refinement and testing against more realistic data and situations.

Please note this CDE competition is focused on the detection of anomalous behaviour by users with legitimate credentials. Proposals that focus on preventing unauthorised access or on securing legitimate credentials will not be considered under this CDE competition as these aspects are covered elsewhere.

What we want

This competition will fund innovative studies and proof-of-concept demonstrators at low to medium technology readiness levels (TRL 1-4)[6] of high technological risk but with high potential benefit, where these demonstrate the highest quality and align with our stated needs of improving the provision of cyber defence.

Proposals must include:

- a clear description of what is novel in the proposed solution and the potential impact of the solution on operational capability
- a clear statement of the programme of work that would be carried out and the outputs (deliverables) the work will deliver
- a technical proof-of-concept demonstrator
- a development plan beyond the initial proof-of concept phase (ie if an initial concept demonstrator is funded and is successful, how might this be taken forward in future)
- success metrics for the approach (ie a clear description of how you will demonstrate your approach is beneficial)
- an initial test plan against a relevant exemplar data set the bidder either owns or has access to (bidders will need to demonstrate why any data set they propose to use would be relevant to the task).

Given the interest in socio-technical indicators and baselining for anomalous behaviour, we would be interested in proposals that seek to collaborate and partner with other like-minded organisations – especially those collaborations that bring physical and social sciences expertise together. Whilst any proposal can be from single organisations or individuals, Dstl would like to see collaboration from parties that may have similar ideas, and also collaboration with, but not limited to, existing MOD suppliers to increase the likelihood of exploitation. In the past, academic institutions who have partnered with industry suppliers have been particularly successful at having their proposals funded and exploited by MOD.

What we don't want

Dstl will not fund proposals that:

- utilise existing heuristic methods without extension or expansion
- restrict their scope to not include the detection of abuse of legitimate credentials (including by malware)
- add substantial computational burden or require substantial additional hardware to be installed
- expand the threat surface
- are based on existing commercial products
- have already been considered within the military community
- do not include some form of demonstrator (ie are limited to a paper study)
- offer solutions which solely protect personal computation devices
- offer solutions which are solely based on a black-box implementation (ie without suitably detailed technical explanation of how the mechanism works).

[6] A description of Technology Readiness Levels can be found in the Acquisition Operating Framework

Exploitation

Proposals seeking funding under this competition must include an initial “proof-of-concept” stage of around 3-5 months in duration. Following successful demonstration of the proof-of-concept approaches, there is the potential for them to be demonstrated on a deployed cyber situational awareness development environment. They may also be trialled with operational customers, to enable informed decisions when procuring future MOD infrastructure enterprise solutions.Further development of successful proposals will only be considered after the successful end of the “proof-of-concept” period. To get the most out of successful proposals, Dstl expert advice will be provided on how best to co-ordinate with existing or planned MOD systems including engagement across government and the supply base. Suppliers should note that Dstl will not provide data sets to support the development, testing or refinement of proposed projects at this initial stage and suppliers must either supply their own, or utilise access to relevant third party data sets to demonstrate the applicability of the concept demonstrators. The most promising tools and techniques are highly likely to be developed further, but Dstl does not commit to fund any follow on work as a result of any contracts placed via this CDE competition.

Invitation for CDE proposals

This competition will be supported by presentations given at the launch seminar on 27 November 2013. These will be available to download at:
http://www.science.mod.uk/events/event_detail.aspx?eventid=263

Proposals are invited from industry and academia in the UK and overseas for research that can demonstrate a proof-of-concept to meet one or more of the challenges for "**Cyber Defence: Securing Against the Insider Threat**".

There is no cap on the value of proposals and all proposals will be considered, but it is more likely at this early stage of innovation that a larger number of lower value proposals (eg £50k—£150k) will be funded than a smaller number of higher value proposals. Overall, Dstl has up to £1M available to fund novel and innovative concept demonstrators under this competition.

As stated above, proposals should focus on a short, sharp, proof-of-concept phase – typically, but not exclusively, 3-5 months in duration – with deliverables completed within FY 2014-2015. Proposals should include a descriptive scoping for a longer programme demonstrating potential exploitation of successful ideas, but must be clearly partitioned with a costed proof-of-concept stage which is the focus of this CDE competition. Proposals for further work beyond the proof-of-concept stage will only be considered after the proof-of-concept stage has successfully delivered, using the understanding gained to make an informed decision.

For this initial proof-of-concept phase, proposals should avoid any reliance on research that involves human participants as this would require MOD ethics approval.

Proposals will be assessed by subject matter experts from MOD, Dstl and wider government (notably the security and intelligence research and development community) using the MOD Performance Assessment Framework (PAF). Deliverables from contracts will be made available to Technical Partners and subject to review by UK MOD and the output will be shared with the government security and intelligence research and development community.

Dstl will be available to provide advice and/or guidance via an appointed Technical Partner throughout the project and provide the interface with MOD and wider government community.

Dstl does not commit to fund any follow on work as a result of any contracts placed via this CDE competition, but more promising ideas will be considered for further funding where appropriate.

CDE proposal submission process

Key dates

- 27 November 2013 Competition launch event
- 11 December 2013 Post-launch webinar
- 9 January 2014 Competition close at 1700 hrs.

Proposals for funding must be submitted by 1700 hrs on Thursday 9 January 2014 using the CDE Portal. Proposals must be clearly marked with "Cyber Defence" as a prefix in the title.

Please plan the timeline for submitting your proposal carefully. If you have not used the CDE Portal before you will need to become familiar with the guidance, including how to open an account starting with the Quick Start Guide.

Other information and guides are available on the CDE website:

- general CDE advice: www.science.mod.uk/engagement/cde/working_with_cde.aspx
- contract & IPR guidance: www.science.mod.uk/engagement/cde/funding_contracts.aspx
- on using the Portal: www.science.mod.uk/engagement/the_portal.aspx. The Portal is optimised for proposals based on physical sciences and engineering and we are aware that proposers sometimes struggle to adapt to using it with social science based proposals. The key points (rather than the detailed questions) that are sought under the main headings still apply and further advice can be obtained from CDE.

Common errors in preparing and submitting a proposal include:

- **character limit** – there is a limit of 1000 characters in each individual descriptive paragraph within the proposal; when completed they must be added to the document; additional paragraphs can be added if 1000 characters is insufficient.
- **it is a web-based tool** – please save your work regularly to avoid 'time-outs' that lose work.
- **attachments fail** – They must be Word 97-2003 format, portrait format, should have generous margins with no material overhanging the margin and a max size of 1 MB. Please note that attachments should only be used for supplementary information, the main points of your proposal should be written into the online form. Care should also be taken to make sure that attachments are placed in the relevant section (e.g. technical information should not be attached to the commercial section).
- **failing to properly submit** - **publish is not the same as submit**. You have **not** completed the submission process if your proposal is at the FINAL/PUBLISHED stage (in the status and published status columns respectively); CDE has no sight of the proposal at this stage. To complete submission you need to press 'submit' under the 'Tasks' column. This changes the status of your proposal to 'SUBMITTED'; it will then change (normally after a few days, often sooner) to 'RECEIVED' indicating that the proposal has been accepted by CDE for assessment.

For a proposal to be accepted for assessment:

- the standard terms and conditions of CDE must be unequivocally accepted
- there must be at least one deliverable against which payment can be made
- the commercial section of the proposal must be completed.

Please do not leave submission of your proposal until just before the deadline. Past experience has shown that the Portal becomes heavily loaded near the competition close resulting in slow operation (up to one hour to publish rather than a few minutes) and that, with the pressure of the deadline, mistakes are made that mean proposals are not submitted or accepted.

All proposals and content placed on the Portal must be UNCLASSIFIED.

Queries and help

As part of the proposal preparation process, queries and clarifications are welcomed:

- **Technical queries** about this specific competition should be sent to cybersecurityCDE@dstl.gov.uk. **Capacity to answer these queries is limited in terms of volume and scope. Queries should be limited to a few simple questions or if provided with a short (few paragraphs) description of your proposal, the technical team will provide, *without commitment or prejudice*, broad yes/no answers. This query facility is not to be used for extensive technical discussions, detailed review of proposals or supporting the iterative development of ideas. Whilst all reasonable efforts will be made to answer queries, CDE and Dstl reserve the right to impose management controls when higher than average volumes of queries or resource demands restrict fair access to all potential proposal submitters.**

- **General queries** (including how to use the Portal) should be sent directly to CDE at cde@dstl.gov.uk.