The Office of the Superintendent of Financial Institutions

Digital Risk Monitoring Service (DRMS)

Annex A - DRMS Statement of Capabilities
Minimum Mandatory Requirements

TABLE OF CONTENTS

1 INTRODUCTION

This Annex provides OSFI's minmim mandatory requirements for the Digital Risk Monitoring Service (DRMS).

2 MINIMUM MANDATORY REQUIREMENTS

2.1 Threat Intelligence

2.1.1 Vulnerabilities and Exposures

a. The DRMS must cover all Common Vulnerabilities and Exposures (CVEs) from the National Institute of Standards and Technology's (NIST's) National Vulnerability Database (NVD) including their Common Vulnerability Scoring System (CVSS) score.

2.1.2 Threat Intelligence

a. The DRMS must provide information on threat actors including (when available) the following:
   i. their common names;
   ii. if they are an Advanced Persistent Threat (APT) their APT number;
   iii. known activities;
   iv. known capabilities;
   v. known Tactics, Techniques and Procedures (TTPs);
   vi. suspected origin;
   vii. suspected motives; and
   viii. targets.

b. The DRMS must provide timelines and details on TTPs used, and impacts of threat events per threat scenario.

2.1.3 Threat Intelligence Collection

a. In support of mass collection of intelligence, the DRMS must use machine learning and natural language processing to collect and structure text content from sources across programming languages and classify them using language-agnostic ontologies and events.

b. The DRMS must have large operational capacity[1].

c. The DRMS must collect intelligence and report on threats on a Global basis[2].

---

[1] Large operational capacity is defined as the capability to observe at least 10,000 network sensors and 15,000,000 end points distributed in at least 50 countries

[2] To demonstrate this capability, the DRMS Contractor must employ at least 700 cyber intelligence analysts distributed in at least 50 countries. The analysts must also be operating in at least 25 languages including:

a. English;
b. French;
c. Russian;
d. Chinese;
e. Arabic;
f. Persian;
g. Korean; and
h. Portuguese.

2.1.4 Experience with Canadian Intelligence Organizations

a. The DRMS Contractor must have recent experience working with the intelligence organizations within at least one of the following Government of Canada organizations:
   i. Canadian Security Intelligence Service;
   ii. Communications Security Establishment;
   iii. FINTRAC;
   iv. Department of National Defence;
   v. Public Safety; or
   vi. Royal Canadian Mounted Police.

2.1.5 Financial Sector Expertise and Industry Focus

a. The DRMS Contractor must be focused on the financial industry with over 250 financial sector clients globally.

b. The DRMS Contractor must have experience providing cyber incidence response to breaches to global financial systems, including the SWIFT banking system.

c. The DRMS Contractor must have demonstrated capability to identify and publish new threat actor groups within the financial (FIN) sector including sufficient evidence where the group is acknowledged and accepted by the cyber intelligence community.

d. The DRMS must group intelligence reports by sector, specifically:
   i. financial;
   ii. insurance; and
   iii. governments.

2.1.6 Indicators of Compromise (IOCs)

a. The DRMS must provide IOCs to OSFI's SIEM (Sentinel).

b. Intelligence related to IOCs must be provided with full context of related entities, including related hashes, IP addresses, CVEs and other relevant information.

c. The DRMS must provide IOCs with a reliability score, detection quality or risk score. Scores must be justified with rationale and dynamic to represent the real-time risk of the IOC.

2.1.7 Technical Sources

a. The DRMS must provide details on threats from technical sources such as WHOIS and Domain Name System (DNS) lookups.

2.1.8 Threat TTPs

a. The DRMS must provide details on threat TTPs including specific procedures, mitigations and detection methodologies per the MITRE ATT&CK3 framework.

2.1.9 Malware

a. The DRMS must provide details about the name, function, characteristics and origin of known malware.

[3] MITRE ATT&CK®

2.1.10 Malware Analysis

a. The DRMS must provide the capability to analyze customer uploaded malware and extract indicators including IP, domain, Mutex, Windows Registry changes and process execution details. It must also provide associated malware family and threat actors.

b. The malware analysis feature must support malware files for common operating systems, at the minimum including Windows, MacOS, and Linux.

2.1.11 Browser Extension

a. The DRMS must provide a browser extension for Google Chrome or Microsoft Edge to scan webpages and analysis of indicators, vulnerabilities and threat actor details present on the webpage. The data and the resulting analysis must be exportable to other tools using JSON files.

2.1.12 Filters

a. The DRMS must allow a user to indicate technologies, operating systems, threat actors and sectors of interest to minimize receiving information on irrelevant threats.

2.2 Dark Web Monitoring

2.2.1 Web Monitoring

a. The DRMS must monitor Surface, Deep and Dark Web sources.

2.2.2 Search for OSFI-specific information

a. The DRMS must allow OSFI to define specific information (text, names and domains) which would indicate breach of OSFI data.

2.2.3 Data Breach Detection

a. The DRMS must provide alerts when suspected breach of OSFI data has been detected, including data type, date/time and source of the suspected breach.

2.3 Fraud Monitoring

2.3.1 Executive Impersonation Monitoring

a. The DRMS must ingest OSFI-defined key individuals[4] and roles against which social media will be analyzed to identify potential fraudulent accounts impersonating those individuals and/or roles.

2.3.2 Credential Monitoring

a. The DRMS must search for OSFI-defined domains (@OSFI-BSIF.gc.ca) to identify and report potential compromise of user credentials and email an alert to the OSFI-defined user whenever breached credentials are identified.

2.4 Common Service Requirements

2.4.1 Language

a. The DRMS must be delivered in English.

b. The DRMS must collect data from multiple languages and automatically translate to English.

2.4.2 Portal Access

a. The DRMS must be accessible via secure links in accordance with:

[4] Example - Executive Biographies (osfi-bsif.gc.ca)

i. https://cyber.gc.ca/sites/default/files/publications/itsp.40.111-eng_1.pdf; and
ii. https://cyber.gc.ca/sites/default/files/publications/itsp.40.111-fra.pdf.

b. The DRMS web portal must not require additional OSFI client-side infrastructure.

c. The DRMS must support Microsoft Edge and Google Chrome web-browsers.

2.4.3 Learning Content

a. The DRMS must provide adequate user documentation including a user manual, query guide and embedded help to facilitate use of the service without the need for dedicated training.

2.4.4 Management of Users

a. The DRMS must provide functionality for an OSFI administrator role to create, modify and delete OSFI user accounts within the tool.

b. The OSFI user role within the DRMS must not have elevated privileges to create, modify nor delete other OSFI users.

2.4.5 Search

a. The DRMS must provide a searchable portal to allow OSFI users to investigate items of interest from the data collected from web sources (paragraph 2.2.1).

b. Query results must contain reference to the source of the information (e.g. Pastebin, Dark Web, Forums, etc.).

c. The DRMS must allow change and customization of query logic.

2.4.6 Content Sanitization

a. Internet-collected content must be sanitized (cached with links inactive).

2.4.7 Dashboards

a. The DRMS must allow a user to compile data to create and save individual dashboards.

b. The DRMS must provide separate dashboards on incidents and threat intelligence.

2.4.8 Reporting

a. The DRMS must allow export of reports in a commonly consumable format (Microsoft Word or pdf) [5].

2.4.9 Export Data

a. The DRMS must allow for the export of query results in Java Script Object Notation (JSON) and Comma-Separated Values (CSV).

b. The DRMS must allow for the export of indicators and associated data as YARA rules.

c. The DRMS must allow query and export data via an Application Programming Interface (API).

[5] Screenshots are not acceptable.

2.4.10 Alerts

a. The DRMS must provide configurable email alerts when there is new information related to pre-defined queries.

b. The DRMS must allow OSFI to create, monitor and automate alerts and report on vulnerabilities and threats, including but not limited to the financial sector.

2.4.11 Availability

a. The DRMS must be available 24 hours per day 7 days per week with service outages not longer than one day per month.

b. The DRMS must provide geographically-dispersed threat intelligence services (SOCs) available 24 hours per day 7 days per week.

2.4.12 Experience

a. The DRMS Contractor must have at least 10 years of experience providing threat intelligence collection and analysis services including tracking of vulnerabilities and IOCs.

2.4.13 Data Collected

a. The DRMS must contain data on threats collected over the past 20 years.

2.4.14 Personal Data Protection

a. If personal data is provided by Canada, the DRMS Contractor must safeguard and encrypt it in accordance with:

   i. https://cyber.gc.ca/sites/default/files/publications/itsp.40.111-eng_1.pdf; and
   ii. https://cyber.gc.ca/sites/default/files/publications/itsp.40.111-fra.pdf.

2.4.15 Data Destruction

a. The DRMS must provide means for an OSFI user to destroy the data they provide to the system.

2.4.16 Timeliness

a. The DRMS must update new threat intelligence data in the portal on the same day they are identified.

b. The DRMS must provide email alerts on the same day they alerts are triggered.

c. The DRMS must provide IOCs to OSFI on the same day they are identified.

2.4.17 Support

a. The DRMS Contractor must provide technical phone support and email support during Business Day Working Hours.

b. The DRMS Contractor must provide support in English.

3 GLOSSARY

This section defines any unusual terms or acronyms used in this document:

Term	Definition
API	Application Programming Interface
APT	Advanced Persistent Threat - An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.[6]
Brand	A public image, reputation, or identity conceived of as something to be marketed or promoted.[7]
Business Day	Canadian Federal Government working day.
CCoE	Cyber Centre of Excellence
Credentials	An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.[8] Example – passwords.
CSD	Cyber Security Directorate
CSV	Comma-Separated Values
CVSS	Common Vulnerability Scoring System
Dark Web	the portion of the internet that is intentionally hidden from search engines, uses masked IP addresses, and is accessible only with a special web browser: part of the deep web.[9]
Deep Web	the portion of the internet that is hidden from conventional search engines, as by encryption; the aggregate of unindexed websites:private databases and other unlinked content on the deep web.[10]
DNS	Domain Name System
DRMS	Digital Risk Monitoring Service, the Contractor's solution encompassing all of the Contractor's infrastructure, hardware, software, and professional services associated with the fulfillment of the requirements stated in this Annex A - DRMS statement of capabilities..
DRMS Contractor	The DRMS Contractor or the software publisher in the case the Contractor is not the software publisher.
Forum	An online discussion site where people can hold conversations in the form of posted messages.[11]

[6] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
[7] Brand Definition & Meaning - Merriam-Webster
[8] Digital Identity Guidelines (nist.gov)
[9] Dark web Definition & Meaning | Dictionary.com
[10] Deep web Definition & Meaning | Dictionary.com
[11] Internet forum - Wikipedia

Functional requirement	defines a function of a system or its component, where a function is described as a specification of behavior between inputs and outputs.[12]
GFCI	Global Financial Centres Index
Indicator	A technical artifact or observable that suggests an attack is imminent or is currently underway, or that a compromise may have already occurred.[13]
IOC	Indicator(s) of Compromise
IRC	Internet Relay Chat
JSON	Java Script Object Notation
NIST	National Institute of Standards and Technology
Non-functional requirement	is a requirement that specifies criteria that can be used to judge the operation of a system, rather than specific behaviours.[14]
NVD	National Vulnerability Database
OSFI	Office of the Superintendent of Financial Institutions
Pastebin	A type of online content-hosting service where users can store plain text (e.g. source code snippets for code review via Internet Relay Chat.[15]
Pdf	Portable Document Format
P2P	Peer-to-peer
Recent	Within the past 3 years.
SDK	Software Development Kit
SOC	Security Operations Centre
Surface Web	Content on the World Wide Web that is available to the general public.[16]
Threat Scenario	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time. Synonym for Threat Campaign.[17]
Tor	The Onion Router
TTP	Tactics, Techniques and Procedures
User	An individual with a defined role using a computer system.
WHOIS	www.whois.com domain lookup.
Working Hours	Normal OSFI working hours: 08:00 to 17:00 ET on Business Days.
XLSX	Microsoft Excel Open XML Spreadsheet

[12] Functional requirement - Wikipedia
[13] indicator - Glossary | CSRC (nist.gov)
[14] Non-functional requirement - Wikipedia
[15] Pastebin - Wikipedia
[16] Definition of surface Web | PCMag
[17] NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments