G-Cloud 13 Source Code Control Ltd
Service Definition Document

1 Introduction

This is a service definition document for our G-Cloud External Threat Scanning Service. Below you will find information about how to use this document and what the document contains. It is important you read this introduction section to get the best experience from this document and ensure you find the information you need quickly and easily.

1.1 Document Sections

This document has the following sections:

Section 1 - Service Information contains essential information about our service, the functionality, security, and brief aspects of pricing.

Section 2 - G-Cloud Alignment Information details how our services and company aligns with the G-Cloud buying process and provides typical information to help you understand how to buy, configure and consume our services, and how to leave our services should the need arise.

Section 3 - About Our Company and Our Services provides information specific to our company and how we can solve the problems faced by customers in the public sector.

Section 4 - Appendices provide supplementary service information that explain the functionality and benefits in greater detail. Also covered is how to search for and select the service(s) on G-Cloud and how to differentiate services of this kind when comparing across suppliers.

1.2 How to Use This Document

This service definition document is an active document which means you can click on the links we provide to move around the document viewing only those specific sections you are interested in during the different phases of your G-Cloud buying process. There are also links to enable you to return to this section to speed up the reviewing process.

Contents

Table of Contents

2 Service Information

2.1 Section Introduction

In this section, we describe our External Threat Scanning service. You will find information about our service functionality. We describe the functionality in a way that should be understood by people familiar with this kind of service. However, we have also provided links to more detailed guidance if you need assistance with the terminology and benefits that this/these service(s) can provide if you are not that familiar with services of this kind.

2.2 Overview and Assurance

The Source Code Control External Threat Scanning Service is a SaaS based service which scans an organisation's domains from the outside and reports on vulnerabilities. In addition, the customer can provide keywords which are then compared with chatter on forums and on the dark web to attempt to pre-empt malicious acts.

The service provides a dashboard of issues and action items as well as alerts to the existence of credible threats.

2.2.1 Service Functional Capabilities

The service provides real-time digital footprint discovery that reveals attack surfaces, vulnerable systems, data leaks, brand infringement and executive impersonation.

The attack surface discovery focuses on identifying possible entryways into the organisation and potentially exposed external assets, shadow IT and forgotten systems, which can be exploited by malicious actors. Once the attack surface is determined vulnerabilities are mapped to the assets and the associated exploits are ranked based on criticality.

Data breach monitoring is one of most important functionalities of the service as it allows organisations to apply real-time detection of intellectual property, personal data or financial information which have been leaked, with background information, description and impact analysis. With this information companies can plug the gap and avert any further reputation and financial damage. This will also ensure compliance with regulatory policies concerning data management.

Impersonation and infringement intelligence allows organisations to protect their brand integrity and to avert business disruptions from phishing and social engineering attacks. The service will identify all online entities that are masquerading a company's digital profile, assets, products and brand, based on the domain name provided for the scan.

Recommendations and remedial actions are provided for each associated risk and exposure, so that organisations can react quickly and activate the necessary resources to close the exposed security gaps.

If you require additional information, please follow this link to our detailed service functionality in Appendix 1.

Return to Table of Contents

Return to Service Information

2.2.2 Service Non-Functional Capabilities

Dark Web exposure gives organisations visibility into hacker conversations and suspected fraudulent activities from the dark web for any match of domain provided for the scan and ancillary info, such as email ID, PII/CII data etc. This allows companies to be among the first to know if their data has been exposed and this allows them to take swift action that will correct the security gap.

Risk and Hackability scores provided in the analysis allows organisations to gain insight into their risk postures and to understand their overall digital risk. With every action taken to mitigate the vulnerabilities discovered with the service the score updates and this allows organisations to monitor their security progress over a period of time.

Return to Table of Contents

Return to Service Information

2.2.3 Information Assurance

Information Assurance (IA) concerns the protection and risk management of information and information systems. It is built on five key principles designed to help ensure the integrity, availability, authenticity, confidentiality and non-repudiation of information and information systems.

To maintain customer confidence and avoid regulatory sanctions, businesses must demonstrate their commitment to information assurance. The service provides the details the organisation needs to achieve compliance with the latest regulation and standards.

Our service is hosted in AWS cloud platform. Security accreditations include ISO 27001:2013 and ISO 14001:2015. Annual penetration tests are conducted.

Return to Table of Contents

Return to Service Information

2.3 Security

Source Code control is a registered data processor with the ICO office and has the UK Cyber Essential accreditations.

We have SC level approved staff and Non-Police Personnel Vetting (NPPV) Level 2 Qualifications

Customer data is stored securely in a SaaS platform, with full role-based access control (RBAC) access as required.

We do not request particular PII or other privacy relevant data from our customer. For the best results we only request information about the hard-/software assets and corporate details such as company name, domain(s), email domains etc.

Our data gathering in publicly available sources, returns possible customer and PII/privacy related data, which is already exposed. Our services allow detailed tracking of the origin of the data and outline possible reasons for the data leakage. Access of this data is controlled by the user-specific authentication model within our platform, which allows and supports a selective and fine-grained access definition.

Any access controls used to authenticate and control access to data/services is through authentication based-upon registered users/passwords and can optionally be extended by 2FA and IP whitelisting.

[See Appendix 4 for further guidance].

Return to Table of Contents

Return to Service Information

2.3.1 Secure Encrypted Connection from the Client to the Application

In order to access the application, the following secure connections are being established:

SSL technology: Secure Socket Layer technology is implemented at the transport layer and allows the web browser and web servers to communicate over a secure connection. In this secure connection, the data is encrypted before being sent and is then decrypted upon receipt and before processing. Both the browser and the server encrypt all traffic before sending the any data.

Our service is available as SaaS applications, accessible either via browser or via API-integration. Either of these connections are secured with TLS based RSA 2048-bit encryption.

As stated in **chapter 2.3: Security**, Access of confidential data is controlled by the user-specific authentication model within our platform, which allows and supports a selective and fine-grained access definition. Any access controls used to authenticate and control access to data/services is through authentication based-upon registered users/passwords and can optionally be extended by 2FA and IP whitelisting.

Return to Table of Contents

Return to Service Information

2.4 Backup/Restore and Disaster Recovery Provision

The service is hosted in AWS environment. The infrastructure is spread across multiple Availability Zone (AZ) which is in Mumbai and Japan. The switch is automatic in case the primary AZ goes down. Recovery Time Objective (RTO) and Recovery Point Objective (RPO) will be 30 minutes. That is, both the maximum acceptable delay between the interruption of service and restoration of service and also the maximum acceptable amount of time since the last data recovery point is 30 minutes. In case the entire region of AWS Japan goes down, then the RPO and RTO of AWS will apply.

Return to Table of Contents

Return to Service Information

2.5 Technical Requirements

The following browser and versions are supported:

→ 64-bit Mozilla Firefox: 45.8 Extended Support Release and later.
→ 64-bit Microsoft Internet Explorer with Microsoft Edge mode enabled: V11.0, Edge 38.14393 and later.
→ 64-bit Google Chrome: Latest
→ Safari: Latest

The interface is available both in English and Japanese language.

Return to Table of Contents

Return to Service Information

2.6 Browsers

List of browser compatibility capabilities are mentioned in chapter **2.5 Technical Requirements**.

Return to Table of Contents

Return to Service Information

2.7 Service Pricing

The price of the service is £10,950 per annum for the subscription and ten keywords included. Additional keywords can be added in batches of twenty-five and each set of twenty-five keywords would cost an additional £500.

For on-boarding a customer the service requires an active domain name and ten keywords representing brand names, product names, employee names etc. These keywords will be externally monitored for potential security threats and dark web chatter.

The keywords used can be changed as frequently as required by the customer, during the duration of the subscription.

2.7.1 Service Provision Pricing

Service Provisioning pricing is included in the service charges (section 2.7).

2.7.2 On-Boarding Charges

All on-boarding charges are included in the service charges (section 2.7).

2.7.3 Off-Boarding Charges

n/a

2.7.4 Termination Charges

n/a

2.7.5 Training Charges

There is no training available for this service.

2.7.6 Consultancy Charges

Consultancy charges are included in the service charges (section 2.7)

2.7.7 Other Charges

n/a

3 G-Cloud Alignment Information

Here we provide information for sections that help you comply with the requirements set out by G-Cloud.

3.1 On-Boarding and Off-Boarding Processes

[Return to Table of Contents](#)

[Return to G-Cloud Alignment Information](#)

3.1.1 On-Boarding

For on-boarding a customer the service requires an active domain name and ten keywords representing brand names, product names, employee names etc. These keywords will be externally monitored for potential security threats and dark web chatter.

[Return to Table of Contents](#)

[Return to G-Cloud Alignment Information](#)

3.1.2 Off-Boarding

Customer's data will be disposed of, from the DeTCT platform. All report copies related to customer's data will be deleted.

[Return to Table of Contents](#)

[Return to G-Cloud Alignment Information](#)

3.2 Service Management Details

[Return to Table of Contents](#)

[Return to G-Cloud Alignment Information](#)

3.2.1 Technical Boundary

Any access controls used to authenticate and control access to data/services is through authentication based-upon registered users/passwords and can optionally be extended by 2FA and IP whitelisting

[Return to Table of Contents](#)

[Return to G-Cloud Alignment Information](#)

3.2.2 Support Boundary

Administrative HTTPS and SSH traffic to the management interface and support channels can be restricted to specific IP ranges.

[Return to Table of Contents](#)

3.2.3 User Authorization and Roles

The service is provided by the Source Code Control team and the customer is alerted to any issues via email and test alerts. Direct access to the portal is available on request.

There is therefore just the one role which is that of user contact who will provide and keep up to date the "keywords".

Return to Table of Contents

Return to G-Cloud Alignment Information

3.2.4 General Support details

Incidents are reported to Source Code Control team via email, Monday through Friday between 9 AM and 5 PM (excluding legal holidays). Source Code Control team to escalate to vendor. Source Code Control team works with the vendor to resolve the issue.

Return to Table of Contents

Return to G-Cloud Alignment Information

3.3 Service Constraints

The support of service is available Monday through Friday between 9 AM and 5 PM GMT (excluding legal holidays)

Return to Table of Contents

Return to G-Cloud Alignment Information

3.3.1 Planned Maintenance

Customer will be notified of any planned maintenance no later than 24

hours in advance.

Return to Table of Contents

Return to G-Cloud Alignment Information

3.3.2 Emergency Maintenance

In case any emergency occurs such as disruption of service, customers will be notified at the as soon as possible.

Return to Table of Contents

Return to G-Cloud Alignment Information

3.4 Service Levels

n/a

3.4.1 Award of Service Credits

Service credits are not offered for this service.

3.4.2 Payment of Service Credits

 n/a

3.4.3 Financial Recompense

n/a

3.5 Training

There is no training provided for this service.

3.6 Invoicing Process

To order the Eternal cybersecurity threat scanning Service from Source Code Control, please contact us at g-cloud@sourcecodecontrol.com.

A purchase order will be required prior to the work commencing. An invoice will be provided on completion of the report either by presentation or email distribution.

3.7 Termination Terms

The customer acknowledges that it has purchased the Services for the Minimum Period and any Renewal Term(s), as defined in the Certificate or Order Summary.

The term of Agreement will be 1 year. However, the Client shall have option to revisit on pricing terms at the end of each year by providing 30 days prior notice before end of the first year.

Return to Table of Contents

Return to G-Cloud Alignment Information

3.8 Data Extraction/Removal Criteria

The only data extraction the service requires are domain names, company name and supplied keywords.

Return to Table of Contents

Return to G-Cloud Alignment Information

3.8.1 Data standards in use

n/a

Return to Table of Contents

Return to G-Cloud Alignment Information

3.8.2 Consumer generated data

The service provides an end result of generated data that reveals attack surfaces, vulnerable systems, data leaks, brand infringement and executive impersonation.

Return to Table of Contents

Return to G-Cloud Alignment Information

3.8.3 Data extraction

There are pre-defined reports within the tool and the information can be exported to PDF format.

Return to Table of Contents

Return to G-Cloud Alignment Information

3.8.4 Price of extraction

No extra charges due.

Return to Table of Contents

3.8.5 Purge and Destroy

Customer data will be deleted upon termination of service

3.9 Data Processing and Storage Locations

All the data processing will be stored in AWS platform in Mumbai and Japan.

3.10 Data Restoration/Storage Migration
n/a

3.11 Customer Responsibilities

The customer is responsible for:

→ Initiating the work by contacting g-cloud@sourcecodecontrol.com.
→ Agreeing a kick-off call.
→ Providing a valid purchase order.
→ Providing payment in line with the purchase order.
→ Providing company name, domain name and list of keywords.

Source Code is responsible for:

→ Maintaining the service and calculations in line with industry current practice
→ Guiding the customer through the process
→ Securely handling the customer data
→ Performing accurate calculations
→ Ensuring the customer understands the calculations used
→ Creating the reports in the appropriate formats
→ Delivering the reports in an understandable manner during the delivery of findings
→ Invoicing.

3.12 Details of any Trial Service Available

A trial of up to 7 days can be provided to the customer. A request can be made to g-cloud@sourcecodecontrol.com

3.13 Government Policy Alignment/Compliance

n/a

3.13.1 ICT Greening Policy Compliance

n/a

3.13.2 ICT Strategy Policy Compliance

n/a

3.13.3 Website Accessibility and the Equality Act (W3C Compliance)

n/a

3.13.4 EU Cookie directive

n/a

4 About Our Company and Our Services

In this section you will find details about our company and what we do.

4.1 About Us - Source Code Control

Source Code Control is an open-source software and cloud economics specialist consultancy. Leveraging proven skills in application modernization, licensing, FinOps and discovery, the team provides a range of services, including evaluations for cloud transformation, cyber security, and software component evaluations.

Return to Table of Contents

Return to About Our Company and Our Services

4.2 Why Choose Us?

As independent advisories, our customers can have confidence in our recommendations as we do not sell third party software, ensuring all recommendations are genuine. As a result, we have a diverse client portfolio, ranging from NHS England and Wales, FTSE 100 companies, medical device manufacturers, specialist software companies and in the highly secure military software. We provide more services around these topics than any other consultancy in the market, with a proven track record as subject matter experts.

Return to Table of Contents

Return to About Our Company and Our Services

4.3 Why Choose Our Services?

Browse our LinkedIn profiles or on https://sourcecodecontrol.co/about/ and you will see a team brimming with industry experience. We have worked on both the vendor side and the customer side, so we understand what you need. Our services are designed to empower you with information in a usable format based on accurate data.

Wherever possible, our services are fixed cost. This gives you the confidence to buy, knowing exactly what you are getting in return.

While our brand may not be the most widely recognised in the market we have deep niche skills and understanding. Many of the cloud's biggest players use our staff to deliver the complex part of their consultancy services.

Return to Table of Contents

Return to About Our Company and Our Services

4.4 Our Service Portfolio (other services on G-Cloud)

Cloud Sustainability Service – A consultancy service to help you calculate the impact of adopting cloud services on your carbon footprint. We can help you benchmark your on-

premises IT devices in terms of CO2 equivalent and then estimate the reduction / what that looks like in the cloud.

Cloud Optimisation Service – A consultancy service aimed at assessing your public IaaS cloud subscriptions for: potential cost savings; security issues; missing best practices and configuration documentation.

Return to Table of Contents

Return to About Our Company and Our Services

4.5 How to Buy Our Services

We can provide example reports and arrange short introductory presentations over video call, to explain and answer any questions.

To make a purchase, simply contact us at: g-cloud@sourcecodecontrol.com.

Return to Table of Contents

Return to About Our Company and Our Services

4.5.1 The Award Process

n/a

Return to Table of Contents

Return to About Our Company and Our Services

4.5.2 Pricing Our Services

n/a

Return to Table of Contents

Return to About Our Company and Our Services

4.5.3 Sample Order Forms
  n/a

Return to Table of Contents

Return to About Our Company and Our Services

5 Appendices

5.1 Appendix 1: Detailed Service Functionality

The service provides real-time digital footprint discovery that reveals attack surfaces, vulnerable systems, data leaks, brand infringement and executive impersonation.

The attack surface discovery focuses on identifying possible entryways into the organisation and potentially exposed external assets, shadow IT and forgotten systems, which can be

exploited by malicious actors. Once the attack surface is determined vulnerabilities are mapped to the assets and the associated exploits are ranked based on criticality.

Data breach monitoring is one of most important functionalities of the service as it allows organisations to apply real-time detection of intellectual property, personal data or financial information which have been leaked, with background information, description and impact analysis. With this information companies can plug the gap and avert any further reputation and financial damage. This will also ensure compliance with regulatory policies concerning data management.

Impersonation and infringement intelligence allows organisations to protect their brand integrity and to avert business disruptions from phishing and social engineering attacks. The service will identify all online entities that are masquerading a company's digital profile, assets, products and brand, based on the domain name provided for the scan.

Recommendations and remedial actions are provided for each associated risk and exposure, so that organisations can react quickly and activate the necessary resources to close the exposed security gaps.

Dark Web exposure gives organisations visibility into hacker conversations and suspected fraudulent activities from the dark web for any match of domain provided for the scan and ancillary info, such as email ID, PII/CII data etc. This allows companies to be among the first to know if their data has been exposed and allows them to take swift action that will correct the security gap.

Risk and Hackability scores provided in the analysis allows organisations to gain insight into their risk postures and to understand their overall digital risk. With every action taken to mitigate the vulnerabilities discovered with the service the score updates and this allows organisations to monitor their security progress over a period of time.

5.2 Appendix 2: Benefits of Service Functionality

The benefits of service functionality allow companies to be among the first to know if their data has been exposed and allows them to take swift action that will correct the security gap.

The service will identify all online entities that are masquerading a company's digital profile, assets, products and brand, based on the domain name provided for the scan.