G-Cloud 13

Protecting against Cyber Attack – Data/System Security & resilience

Service Definition

Pionen

Contents

1. Introduction

Company Overview

Pionen is a UK based organisation, providing Cyber resilience services designed for complex public sector organisations. Specialising in discovery and transformation projects. Your priorities lie at the forefront of our approach. By utilising a variety of methodologies depending on the project requirements, including but not limited to: Prince 2, Waterfall, Scrum, Agile, ITIL, all of which are underpinned with experience of the GDS Service manual. Our teams utilise their expertise against your preferred style of working.

Social Value

Social value is extremely important to Pionen, we not only have goals and targets but are extremely active in our client communities. In line with your own goals around Volunteering; Employability; Family Support; Metal Health and First Call we believe at Pionen, we support the first 4 of these internally for our own staff with a strong emphasis on Diversity and Inclusion (D&I) Strategy and Support for our clients. Operating our own support, continual Mental Health support for teams to provide forums for open discuss and coping strategies. Open forum for D&I to allow our colleagues to share their experience around how to improve the workplace and support better client engagement and interaction, with a strong focus on inclusion through our internal groups.

Fighting Climate Change – Our policy outcome includes effective stewardship of the environment, and is not limited to:

- Working towards net zero
- Working collaboratively with our supply chain to deliver environmental benefits and work towards net zero through renewable energy
- Activities to enhance the natural environment, create green space and improve air quality in the area local to the contract
- Training and education of staff and supply chain on environmental protection and resource use

Overview of the G-Cloud Service

Pionen provide Cyber resilience services designed for complex public sector organisations. Public sector organisations cannot afford to take risks, and we provide pragmatic protection through clear, helpful, attentive approach in plain English.

We believe in clarity, vigilance, pragmatism, empathy and effective values whilst helping you safeguard your critical assets and data.

Helping you and your organisation achieving successful compliance with The Cyber Assessment Framework (CAF) which provides guidance for organisations responsible for vitally important services and activities.

Protecting against cyber attack

Supporting you by identifying, implementing and testing proportionate security measures to protect the networks and information systems from cyber-attack.

Data Security

Verifying that data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on essential functions. Verification of such protection extends to the means by which authorised users, devices and systems access critical data. It also covers information that would assist an attacker, such as design details of networks and information systems.

Understanding Data

Helping you to have a good understanding of data important to the operation of the essential function, where it is stored, where it travels and how unavailability or unauthorised access, modification or deletion would adversely impact organisational operations. Supporting development of policy to allow application to third parties storing or accessing data important to operations.

Data in Transit

Verification that you have protected the transit of data important to the operation of the essential functions. Including the transfer of data to third parties.

Stored Data

Ensuring that you have protected stored data important to the operation of all the essential functions.

Mobile Data

Helping you understand and manage data on mobile devices.

Media Equipment Sanitisation

Support to help you appropriately sanitise media and equipment holding data important to the operation of the essential function.

System Security

Network and information systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to essential functions informs the use of robust and reliable protective security

measures to effectively limit opportunities for attackers to compromise networks and systems.

Secure by Design

Ensuring that security is designed into the network and information systems that support the operation of essential functions. Guiding you to minimise your attack surface and ensure that the operation of the essential functions should not be impacted by the exploitation of any single vulnerability.

Secure Configuration

Show you how to securely configure the network and information systems that support the operation of essential functions.

Secure Management

Enable you to manage your organisation’s network and information systems that support the operation of essential functions to enable and maintain security.

Vulnerability Management

Architect and implement total vulnerability management capabilities. To ensure management of all known vulnerabilities in your network and information systems and achieve full coverage, even in critical systems and CNI.

Resilient Networks and Systems

Helping your organisation build resilience against cyber-attack and system failure into the design, implementation, operation and management of all systems that support the operation of essential functions.

Resilience Preparation

Ensure that you are fully prepared to restore the operation of your essential function following adverse impact. Through design, planning and exercising.

Design for Resilience

Architect the network and information systems supporting your essential functions to be resilient to cyber security incidents. Ensuring systems are appropriately designed, segregated, protected, and available.

Backups

Verify that you hold accessible, secured, current backups of data and information needed to recover operation of your essential functions. Verify that they are regularly tested for robustness and restoration.

Staff Awareness and Training

Ensure all staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the operation of essential functions.

Cyber Security Culture

Support you in the development of a positive cyber security culture. Where all employees and third parties know their security responsibilities and how to action them. Help them to understand that they are all part of the security team.

Cyber Security Training

Ensure that the people who support the operation of your essential functions are appropriately trained and capable in cyber-security. A range of approaches to cyber security training, seminars, awareness campaigns and direct communications are employed.

Service features include:

- Value for Money
- Public Sector delivery experience
- Governance aware stakeholder management
- Technical Acumen (SME)
- Subject Matter Expertise
- Cyber Security Experience
- Best practice implementation
- Independent judgement
- Pragmatic Delivery
- Qualified
- Focused

Service Benefits:

- Client Trust
- Provide Confidence
- Objective Approach
- Consistency and effectiveness
- Proven and Trusted
- Cross department view

Our unique value proposition:

- We have a proven track record of building effective programmes secure by design
- Our qualified team have the most contemporary strategic and technical cyber security knowledge

- We use a tried and tested proprietary process that demystifies public sector cyber security
- We're experienced in working successfully with and within public sector governance
- We work in an empathetic way that focuses on maximising stakeholder comprehension
- We're a consultancy designed specifically for your needs

2. Data Protection

Information Assurance

Pionen is ISO27001 certified as well as achieving and maintain Cyber Essentials. Our resources are multiskilled and qualified in all aspects of information security and solutions. These accreditations and certifications, along with experience in compliance of ISO9000, Sarbanes Oxley, PSN and GDPR/Data Protection Act enable us to provide our clients with the confidence to trust us to safely manage information in line with both internal and external policies and best practice.

Data Back-Up and Restoration

Due to this being a publicly held document, for business security reasons, we can provide the above detailed information upon request. All Pionen data is secured, resilient and recoverable.

Privacy by Design

Pionen operate in a "Secure by Design" approach, which aligns to the legal requirements in the EU General Data Protection Regulations (GDPR) Privacy by design. The protection of citizens' data must be included from the start of the design process of a technology/service. Pionen approach this from the earliest possible opportunity proactively through privacy impact assessment process.

3. Using the service

Ordering and Invoicing

We are flexible in our ordering and invoicing functionality and can fulfil all conventional requirements in this area. We have extensive experience of dealing with a wide variety of invoice formats and will ensure our process are aligned to each individual contract. As standard we would expect a purchase order to be provided for each piece of work which would be invoiced against our accounts receivable department.

Pricing Overview

Pionen offers volume discounts depending on the requirements. Please see our rate card below for a pricing overview.

	Strategy & architecture	Business change	Solution development & implementation	Service management	Procurement & management support	Client interface
1. Follow	400	400	400	400	400	400
2. Assist	500	500	500	500	500	500
3. Apply	600	600	600	600	600	600
4. Enable	750	750	750	750	750	750
5. Ensure/Advise	900	900	900	900	900	900
6. Initiate/Influence	1200	1200	1200	1200	1200	1200
7. Set Strategy/Inspire	1400	1400	1400	1400	1400	1400

Availability of Trial Service

Pionen would welcome opportunities to provide a trial/discretionary/introductory usage of our services which could be made available, such as support to proof of concept or discovery work in order to provide details of scope and magnitude, high level plans to illustrate activities to achieve goals.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

All assignments are tailored with a personalised approach. Therefore, a project plan will provide project specific onboarding and offboarding plans to ensure minimal disruption to the BAU business. Although not an exhaustive list, factors we take into consideration include, knowledge transfer, knowledge libraries, size and sale of the project, timescales, delivery team and locations.

Training

Pionen will undertake knowledge transfer across project disciplines, from technical to management and improvement process to customers as agreed within and during an engagement and/or at the conclusion of the assignment. This could be in the form of seminars, workshops or courseware.

Implementation Plan
Prior to commencement of each service a full implementation plan will discussed with our clients. Our implementation plans are based on your support needs and will be developed to reflect the service requirements.

Service Constraints
Any constraints, risks and opportunity to mitigate these will be highlighted as part of the detailed project plan for professional services that we supply to the public sector.

Service Levels

Service attribute name	Service attribute
Email or ticketing support	No
Phone support	Yes Phone support availability 9 to 5 (UK time), 7 days a week
Web chat support	No
Support levels	Our support levels include on-site, email and telephone assistance, our projects typically employ an account management structure as part of our delivery, support and quality assurance processes.

Financial Recompense Model for not Meeting Service Levels
In line with our Ts&Cs, SLA's will be agreed upon, depending on the nature of the professional services provided.

4. Provision of the service

Customer Responsibilities
To facilitate or validate security clearance, where required of Pionen's specialists in accordance with requirements. To ensure required resource availability and permissions are available to the Pionen team.

Technical Requirements and Client-Side Requirements
Any technical requirements will be discussed as part of the discovery phase / detailed project plan for each project or programme of work.

Development life cycle of the solution

Pionen utilise a variety of methodologies depending on the project requirements, including but not limited to: Prince 2, Waterfall, Scrum, Agile, ITIL, all of which are underpinned with experience of the GDS Service manual. Our teams utilise their expertise against your preferred style of working.

After-sales Account Management

For our professional services, Pionen provides a variety of after sales support which includes a host of MI & reporting, as well as on and offboarding protocols.

Termination Process

Our Ts&Cs in relation to this service have been attached and in line with the Ts&Cs within the GDS framework for the Digital Marketplace.

5. Our experience

Case Studies

We would be delighted to share case studies either related to your request or within a similar size or complexity organisation, we have included an example below;

Protecting HMG from damaging cyberattacks

The Department is the UK's biggest public service department, administering services to around 20 million citizens. With 24/7 reliance on its IT Infrastructure – the largest network of systems in Europe - protection from cyberattack is a top priority.

In May 2017, the global WannaCry ransomware[1] attack caused billions of pounds of damage to over 200,000 computers including the UK National Health Service. The disruption rightly triggered the UK Government to task every department minister with making their systems safe.

The Challenge

WannaCry exploited a weakness in out-of-date Microsoft Windows based hosts, highlighting the importance of regular operating system patch updates. The Departments boundary defence prevented WannaCry getting in, but alarm bells were ringing. What if future ransomware successfully breached the Departments strong boundary defences, reached its target 'endpoint' and was triggered by a user?

With over 50,000 servers and 100,000 laptops running crucial citizen services, the department could not afford to take the risk. They turned to Pionen, experts in endpoint security, to find a solution.

[1] Ransomware is software that encrypts a computer, rendering it useless unless the user pays a cryptocurrency ransom for the decryption key. Ransomware is triggered by a user inadvertently installing it via an email link or USB stick.

The Solution

First, Pionen needed to understand the Departments business requirements – both the functional elements (what the solution would do) and the non-functional elements (how the solution would work with other capabilities). Working collaboratively with the Departments Security Monitoring Teams, they documented a series of use cases – an effective way to capture the functional requirements by describing the step-by-step process each user would go through to achieve a goal.

Pionen then worked through their checklist of standard non-functional requirements to determine the technical constraints, and based on this work, Pionen was confident a commercial-off-the-shelf endpoint security solution would be suitable for the Department.

After assessing available products against the requirements, Pionen compiled a comprehensive compliance matrix with strengths and weaknesses, where the Departments buying team ran a competitive procurement to select from the top three identified vendor platform products. Pionen sat on the evaluation panel, which chose Tanium, a complete endpoint security and management platform.

Pionen then completed the complex design to allow security monitoring across hundreds of segmented networks including different classification levels. The design successfully met all the Departments strict governance standards (based on the Government Security Policy Framework) and was approved by the Design Authority.

In parallel with design, Pionen ran a Business Change Programme. They developed a Future Operating Model, creating and updating all operating processes and initiating training for each identified platform priority user group:

- The Security Monitoring Team responsible for providing assurance overwatch of the Departments infrastructure estate, and administration of their security tooling platforms.
- Digital engineers responsible for providing the IT infrastructure access, and support, for the platform deployment.
- Digital managers providing approval for operational decisions, where stakeholder support is vital to ensuring success in any deployment-at-scale across critical national infrastructure systems.

The first phase of implementation ('Version 1') ran to January 2021, covering over 10,000 servers and critical systems hosted on premises and other large business applications running on Amazon Web Services (AWS). Pionen supported the Digital engineers to resolve technical challenges requiring supplier liaison and design amendment including negotiation with the Design Authority.

Version 2 is underway until December 2022 covering all the Departments AWS and Microsoft Azure services hosted endpoint systems.

The Benefits

The endpoint security project has been a great success within the Department. Tanium now monitors and manages 100% of the on-premises servers and the highest profile cloud hosted business applications, spotting unusual activity through behavioural heuristics, such as unusually high system resource usage, or suspicious application/executables connectivity, invoking potential indicator of compromise rulesets. Invoking response measures if certain conditions are met, such as "quarantine every laptop with x file installed."

The implementation roll-out is on schedule and the Department has not experienced any success-at-scale ransomware or zero-day attacks, including the December 2021 vulnerability in the widely used Java logging library Apache Log4j.

The Department is now considering Version 3, which will provide full coverage of every Departmental laptop and tablet.

The above is an example of one of the many successful Pionen deliveries in Central Government, find out more at www.pionen.co.uk

Clients:

Pionen are currently engaged with the Department of Work and Pensions across a number of complex security deliveries.

In addition, our resources have worked within the following organisations as an example:

- The Home Office
- GCHQ (Tri Agency)
- The Department for Education
- HMRC
- Local Authority
- Police Service
- Fire Service
- NHS
- Lloyds Banking Group
- Barclays

Contact Details

Steve Moran

Client Success Director

01743 296535

steve.moran@pionen.co.uk

-