G-Cloud 13

Detecting Cyber Security Events Service Definition

Pionen

Contents

1. Introduction..2

Detecting cyber security events .... **Error! Bookmark not defined.**

Security Monitoring .... **Error! Bookmark not defined.**

Proactive Security Event Discovery 3

2. Data Protection...4

3. Using the service 4

4. Provision of the service..6

5. Our experience...7

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 your supply chain to deliver environmental benefits and work towards net zero
- 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, 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.

Security leadership as a service (CISO-as-a-service)

Many smaller organisations cannot afford to appoint a skilled and experienced security leader, such as a CISO. Our managed service provides your organisation with the strategic cyber security insight, expertise and leadership needed to drive a high-impact security programme, and digital resilience.

Service Features

1. Cost effective access to a skilled and experienced cyber leader
2. Advise and support Board and senior executive team
3. Translate cyber security risk to business risk
4. Drive the development of a comprehensive cyber security programme
5. Ensure your organisation complies with relevant laws and regulation
6. Advise on development of organisational cyber security awareness and culture
7. Monitor performance against agreed risk appetite
8. Ensure your organisation's security spending achieves a positive return-on-investment
9. Oversees effective technical security operations
10. Flexible access to further resources and services available on demand

Service Benefits:

1. Make most effective use of scarce budget
2. Gain a impartial view of your security posture and programmes
3. Cyber security advice that is strategic as well as technical
4. Educate your board and senior leaders
5. Drive a culture of security in your organisation
6. Create a joined-up approach to security risk management and governance
7. Discard spending and investments in ineffective products and services
8. Secure best value for money from suppliers
9. Develop your internal cyber security capability
10. Motivate your technology teams

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. 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 guidance.

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 work with Pionen to ensure that the assignment is defined accurately and to a reasonable level of detail, and to facilitate security clearance, where required of Pionen's specialists in accordance with requirements.

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?

[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.

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.

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