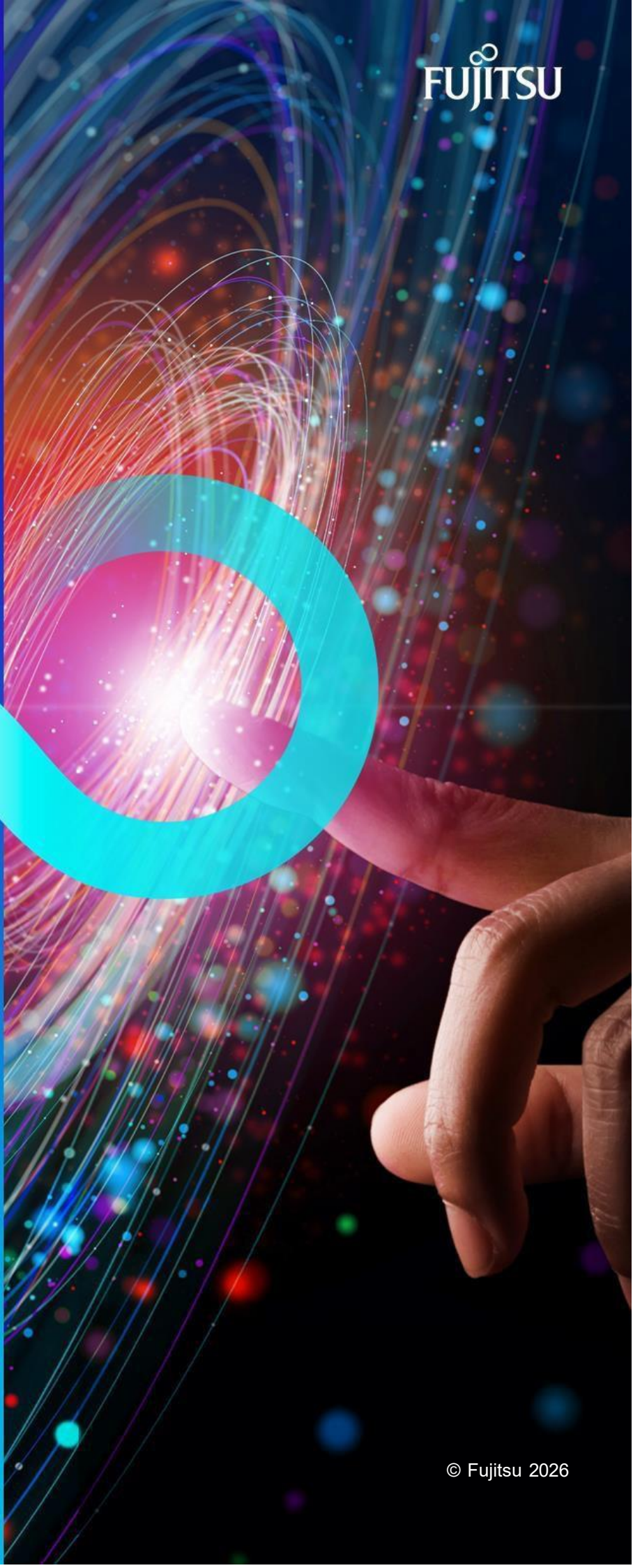
Service Definition

Threat and Vulnerability Management



G-Cloud 15

Contents

Managed Security Services

Fujitsu is a proven security partner with 40 years of demonstrable capability in providing intelligent security solutions to organisations across both private and public sectors including FTSE250 companies operating in highly complex and regulated environments.

Fujitsu's security professionals are trusted advisors with the expertise to enable organisations to prepare for and respond to cyber security incidents effectively and efficiently. Fujitsu also provides guidance on the appropriate security controls to protect organisations, ongoing management of cyber security capabilities on behalf of customers, undertakes 24x7 security monitoring from its Advanced Threat Centre and UK Security Operations Centres (SOCs).

Fujitsu integrate market leading security technologies and expert professional services to support the assessment of risk, define requirements, provide technical and service design and security architectures, as well as ensuring effective deployment, operation, and management of our Managed Security Services (MSS). Fujitsu also provides predictive cyber threat intelligence services and threat response services, underpinned by security orchestration, automation, and response (SOAR), which provide timely and expert response services to mitigate the impact of potential and actual security incidents for our customers. Fujitsu services are aligned to NIST Cyber Security Framework core functions of Identify, Protect, Detect, Respond and Recover.

Figure 1: Cybersecurity Framework

As a global security and service integrator, Fujitsu provides security and resiliency consultancy services across the full delivery lifecycle. These services are seamlessly integrated within the operational, service and security framework within customer organisations, with our services perceived as an extension of our customers' security capability.

Fujitsu's relationships and close links with UK Government, national cybercrime agencies, academia, and our strategic technology partners, enables Fujitsu to achieve service intimacy with our customers. Fujitsu works with HMG Departments to support them to implement many of the security measures required to protect their information, technology, and digital services/assets to meet their SPF, National Cyber Security Strategy and Minimum Cyber Security Standards obligations.

In line with HMG requirements, Fujitsu holds Cyber Essentials and Cyber Essentials Plus certifications and design, build and manage ISO 27001:2013 certified frameworks for HMG where data is classified OFFICIAL through to SECRET and above. Fujitsu has a large pool of SC and DV cleared UK personnel and has experience of designing, building, and maintaining governance and security to deliver service offerings at OFFICIAL, SECRET and ABOVE SECRET classifications.

Why Choose Fujitsu

With Fujitsu's Managed Security Services, your security needs are underpinned with market-leading security technologies and professional services expertise. We assess risk, define requirements, provide technical / service designs, and ensure effective deployment and operation. Additionally:

- Fujitsu provide essential security capabilities to our Public Sector customers, supporting their drive to protect information assets in the face of emerging strategic and operational business challenges
- We are a critical component of our customers' approach to regulatory and legislator demands, helping them to manage their information security risks flexibly and effectively
- Fujitsu has been supplying computing and communications services to Government for many years, and pioneered the use of shared services in Government
- As one of the world's most experienced ICT providers, Fujitsu is combining innovation with responsible business practices to transform business and create a better future for everyone

Confidentiality and Integrity

Securing data when stored, accessed, or transmitted remains a top priority for organizations everywhere. As compliance demands increase, along with the potential penalties for failure, it's critical to keep your house in order. However, knowing exactly which controls to apply and where can be a headache.

Fujitsu's services provide you with the ability to protect your sensitive data and assets by examining data and controlling who and what can access these valuable assets. This increased visibility results in the ability to apply appropriate levels of control.

Fujitsu's has broad portfolio of industry leading network and endpoint security controls that enhances an organisations information security posture through continuous monitoring and the management.

Strategic Technology Partners

Fujitsu has strategic relationships with several global security vendors and has expertise in the definition, provision, design, implementation, test, integration, and operation of these technologies into a cohesive service.

Fujitsu actively monitors developing technologies and develops a roadmap of technologies which are relevant to the mass market and to specific industries.

Fujitsu recognise HMG clients need to leverage existing investments, reduce complexity, reduce cost, evaluate options (i.e. Open Source) and ensure that Partners can meet HMG support needs (assurance, focus, etc.). In principle, Fujitsu focus on building and managing mutually beneficial partner relationships with key security vendors to drive project outcomes, improved service/contract management and enhanced resilience (support). Fujitsu maintain a portfolio of security technology partners that reflect our comprehensive managed and professional services capabilities.

Security Portfolio

Fujitsu has an extensive portfolio of technology, consultive and managed services that include and compliment those described later in this document.

Figure 2: Security Portfolio

Scope

Overview

Today we operate in an environment that is constantly threatened by cyber-attacks. Increasingly attackers are now performing multistage incursions that exploit vulnerabilities, social engineering, data theft and spear-phishing techniques to create a persistent threat that is advanced, zero-day, and targeted.

Regular publicity serves to highlight the frequency and impact of these advanced threats to organisations with analysts estimating that:

- There is now over 1.4 billion pieces of malware programs out there.
- 560,000 new pieces of malware are detected every day.
- Every minute, four companies fall victim to ransomware attacks.
- Trojans account for 58% of all computer malware.

People, process, and technology must now come together to protect individuals and organisations from Cyber-attacks.

Detecting and containing these advanced threats requires a coordinated approach that utilises multi-layer countermeasure solutions to create a unified, proactive, and vigilant approach that provides security controls at all levels.

Visibility is key to preventing, detecting, and containing a security threat, and, without complete visibility, harmful threats are left unchallenged. This means organisations are exposed and need to re-examine their exposure to reputational challenges and their ability to respond to potential crises.

Threat and Vulnerability Management

Fujitsu provides you with a suite of complementary services to reduce your organisation's attack surface and, with context-rich intelligence, proactively predict, detect, and manage active cyber threats, and respond more effectively to cyber incidents. Threat and Vulnerability Management Services can be subscribed to individually or in combination to meet requirements.

The services are:

- Vulnerability Management
- Security Information and Event management (SIEM)
- Security Orchestration, Automation and response (SOAR)
- Cyber Threat Intelligence (CTI)
- Managed Detection and Response (MDR)
- Incident Response (IR)

Managed Detection and Response (MDR)

As already stated, detecting, and containing the ever increasing number and advanced nature of threats requires a coordinated approach that utilises multi-layer countermeasure solutions, to create a unified, proactive, and vigilant approach providing security controls at multiple levels.

Visibility is key to preventing, detecting, and containing these threats, and, without complete visibility, harmful threats can remain unchallenged for an extended dwell time. Fujitsu MDR provides this visibility to reduce the Mean Time to Detect (MTTD) validated threats and the Mean Time to Respond (MTTR), with a blend of tooling, service, process, and our expertise.

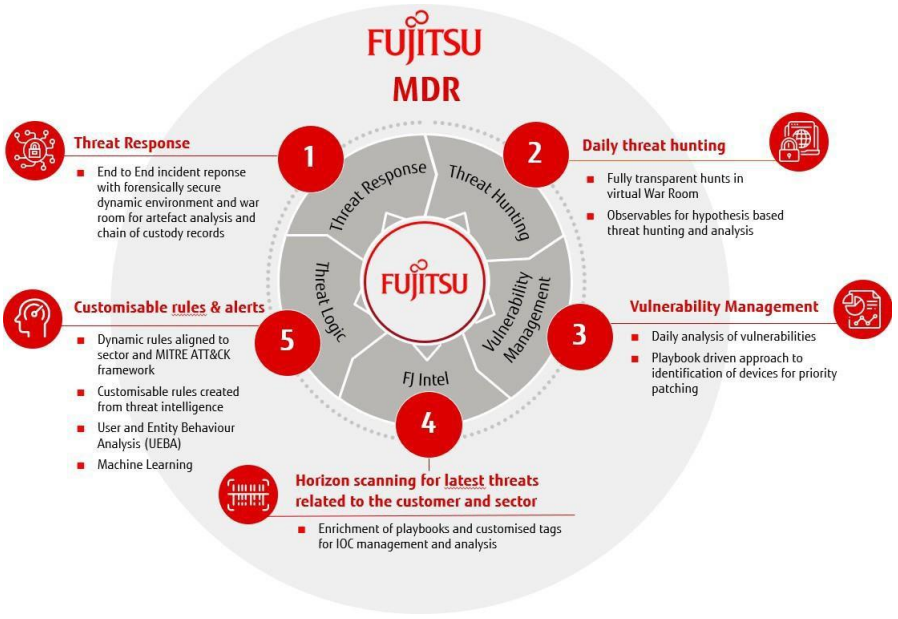


Figure 6: Managed Detection and Response

Fujitsu consultants map your journey to a full MDR service, identifying the appropriate phases to deploy and integrate the various security and data sources from across the environment, along with the orchestration and automation of detection and response activities.

The service includes:

- 24x7 security monitoring
- 24x7 SOC Cyber Analyst support
- Commercial and in-house targeted threat intelligence
- Continuous development and tuning of analytic rules, use cases and playbooks
- Detection of unknown attacks using behaviour analytics
- Detections mapped to MITRE ATT&CK Framework
- XDR platform
- Actionable data provided via dashboards and reports
- Human led investigations
- Incident handling and response

Forensically secure incident response environment

- Virtual war rooms for evidence capture and collaboration
- Fully developed environment for out of band incident management

Service reviews and continuous improvement planning

By selecting Fujitsu MDR, you can benefit from:

- Significantly reduced the time to detect from potentially 200+ days to just minutes, dramatically reducing the potential impact of an incident.
- Improved security posture and resilience to potential attacks
- Identify, contain, and remediate against otherwise unseen, sophisticated threats through threat hunting.
- Respond to threats more effectively and restore assets to a known good status through orchestrated response and managed remediation.
- Redirect your staff from reactive and repetitive incident response work toward more strategic projects.

Vulnerability Management

Fujitsu's Vulnerability Management Services specifically target your relevant assets, proactively assessing and then maintaining intelligence regarding their risk of exposure and status. The enables you to know how secure your enterprise really is and where to prioritise resources to address any issues or concerns.

By effectively managing this risk, vulnerability management protects your reputation and revenues. This happens in five key stages:

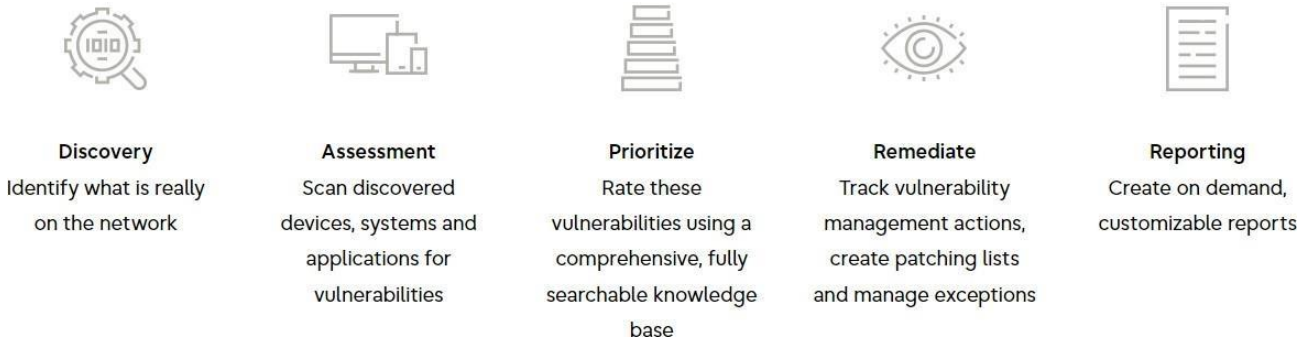


Figure 4: Vulnerability Management

Benefits of this service include:

- Discover assets and vulnerabilities present within your environment(s). Assets can include Servers/Workstations/Network Appliances and Applications
- Support organisational assessment against compliance objectives such as PCI-DSS (Payment Card)
- Enables assessment against Centre for Internet Security Benchmarks (infrastructure) and OWASP Top 10 (application). This supports focussed remediation.
- Highly scalable service to meet the needs of all sizes of organisation.
- Cloud SaaS, appliance or VM deployment options to suit every infrastructure requirement.
- 24x7 monitoring of the infrastructure and services.
- Scalable and tailored solutions to meet the organisation’s specific requirements.

Security Information and Event Management (SIEM)

Protecting your business from threats, compliance violations and operational issues is an ongoing process. It requires broad visibility, continuous monitoring, automated behavioural analytics, intelligent countermeasure capabilities as well as ongoing adaptation to new and evolving issues and threats. The pivotal part of that process is having the ability to correlate what is happening and create actionable intelligence.

With Fujitsu's Security Information and Event Management (SIEM) Services, we provide you with the core components for the collection and detection. Enabling response, and remediation of security incidents in addition to enabling retrospective analysis to support security investigations and compliance requirements.

Our service offers a variety of features, which can include the following depending upon the services purchased:

- Integration and collection of a wide range of customer environment standard log sources, with custom log source integration available upon request.
- Protect of heterogeneous environments by including on-premises, hybrid and cloud infrastructures, either stand alone or alongside other Log Collation/Analytics platforms.
- Pro-active automatic detection, alerting and event correlation across platforms.
- Automatic event ticket generation for prioritized security events of interest and escalation to a nominated customer representative.
- security monitoring, analysis, analysis, investigation, and reporting capabilities, inclusive of Active Analytics
- SOC managed service monitoring and analysis to security events.
- Standard event packs and optional enhanced event packs including reporting tailored for various business sectors including Public Sector.
- Optional security incident management and response capabilities when taking our MDR service.
- End-to-end monitoring on a 24 x 7 basis, backed by Service Level Agreements
- Tiered service providing you flexibility in terms of:
  - Log collection and management services.
  - detection and response services.
- Event Fully Managed SOC analyst driven triage, classification, escalation and reporting services.

Benefits of this service include:

- It enables potential Cyber Security breaches to be detected or avoided and improves incident handling and containment.
- Monitors the effectiveness of security controls.
- Streamlines the auditing and reporting of compliance obligations.
- Provides information to better inform risk management decisions.
- Provides the central component for a wider MDR service.
- Reduction in the time to detect threats.
- Accelerate the speed to respond to threats.

Security Orchestration Automation and Response (SOAR)

SOAR is the concept of automating incident response by using pre-defined playbooks. New security technologies increase the workload on security analysts. SOAR, as the integration layer makes use of technology API's to alleviate the pressure on analysts freeing them to perform important roles and in some cases removing the need altogether.

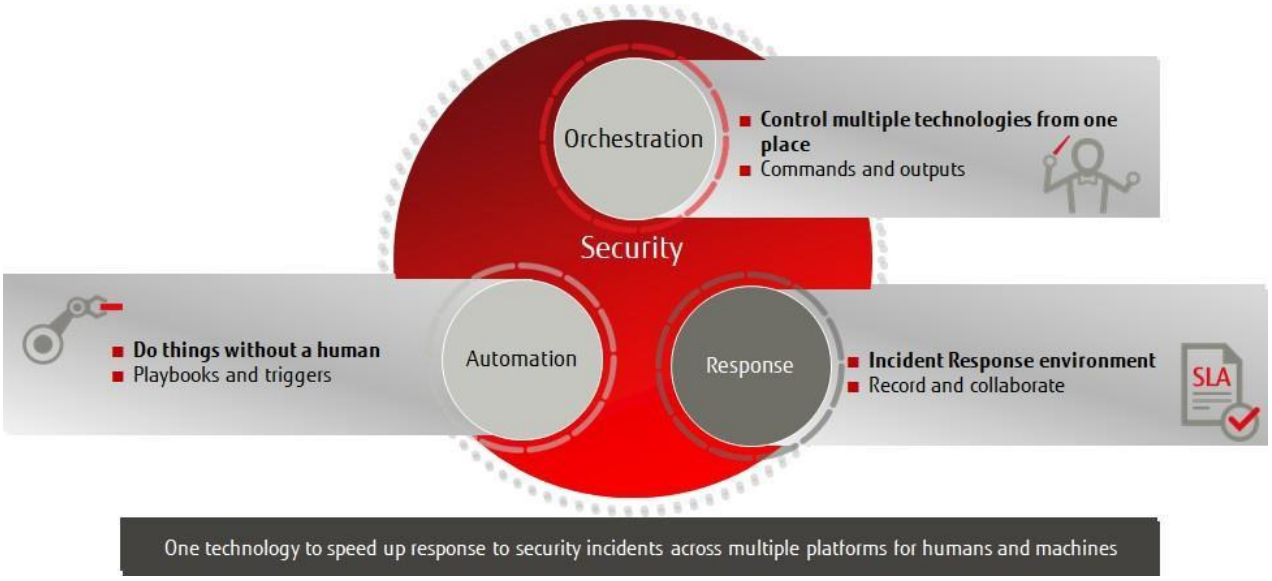


Figure 5: Security Orchestration Automation and Response

Fujitsu's SOAR service follows our "6 Stage Approach" consultancy led service to:

- Define expectations.
- Map tools and processes.
- Prioritise Critical business requirements.
- Identify use cases suited to customers.
- Report the outcomes and benefits of SOAR.

There are 3 key offerings

- SOAR hosed by Fujitsu
  - SaaS MSSP based platform managed by Fujitsu for use by multiple customers.
- SOAR on Premise
  - Dedicated solution designed, implemented, and managed by Fujitsu.
- SOAR Hybrid approach

- SOAR Tenant deployed on premise, but controlled and managed from the master by Fujitsu.

Each service option can be supplemented with additional consultancy including Business Process Analysis to help customers evaluate their current processes along with reviewing their metrics and prioritising these with critical business requirements.

In addition, we offer Playbook as a Service options by utilising standalone playbooks in our MSSP platform. These include

- Phishing Email Response Service (PERS)
- Passive Threat Assessment
- Incident response

Benefits of the SOAR service include:

- Reduced Mean Time to Respond (MTTR)
- Operational efficiencies
- Incident enrichment

Cyber Threat intelligence (CTI)

As cybercrime grows increasingly strategic, traditional security solutions are no longer sufficient. Public Sector organizations require advanced threat protection that uses cyber intelligence to keep attackers out - preventing them from exploiting vulnerabilities using tactics such as social engineering, data theft, spear-phishing, and zero-day.

Fujitsu's Cyber Threat Intelligence provides vigilant and proactive managed security that prevents unwanted parties from accessing your IT infrastructure. Using the latest market-leading insights, gathered from a wide variety of reputable sources, then correlated and analysed by Fujitsu security experts, it identifies, monitors, and mitigates threats throughout their lifecycle and enables you to proactively act against them.

Stop breaches before they happen - Focused threat intelligence incorporates security analytics to flag early warnings of potential cyber-attacks. By gathering, correlating, and scrutinizing relevant information, you get comprehensive visibility of your current security status, along with advice on how to stay protected.

Protect your infrastructure and services - with continuous monitoring and proactive response. Prevent both emerging and potential threats - using real-time expert analysis. Understand your broader security risks - through advanced analytical techniques including honeypots, spam-traps and DNS sinkholes.

We correlate across multiple information sources to provide the predictive context that you need to understand the threat to your business. Dependent upon the level of services taken, the Threat Intelligence Service can include:

- Analysis and reporting of emerging threats.
- Monitoring, analysis, and response to indicators of compromise.
- Real-time pro-active alerting and threat correlation.
- Integration of threat intelligence feed into a MDR solution.
- Detailed malware analysis including safe execution, payload analysis and Fujitsu Threat Intelligence team recommendations for preventative measures / compensating controls.

Benefits of this service include:

- Informs you about cyber threats to your business.
- Can uncover credential and data leakage.
- Supports PCI-DSS 4.0 requirement.

Incident Response (IR)

Historically, organisations have been reactive when it comes to dealing with Cyber Security Incidents. This is not a new phenomenon, nor is it one which is expected to fade away. However, the challenge of being reactive is that your teams are already under pressure to contain the incident. When a cyber incident strikes, the additional pressure can introduce an element of confusion.

Fujitsu's Incident Response Services are designed to offer customers the flexibility they need in ensuring they have sufficient capability in place to deal with a cyber incident. More than that, it affords organisations the opportunity to be proactive and put in place an Incident Response plan supported by access to Fujitsu's Incident Response consultants. Fujitsu's Incident Response services are accredited by the NCSC as Cyber Incident Response Provider

What is Fujitsu's process?

Fujitsu has built out its Incident Response Services capabilities in line with the NIST framework 800-61 . This framework sets out 4 core areas which need to be addressed as part of any incident response scenario:

- **Preparation**: Establishing the Incident Response team, acquiring necessary tools and assessing risks for the prevention, detection, and response to cybersecurity incidents.
- **Detection & Analysis**: Establishing that an Incident is suspected to be in-flight or has occurred and analysing indicators of compromise to inform the next steps required.
- **Containment, Eradication & Recovery**: Here the aim is primarily to contain the incident and prevent further damage. Eradication activities follow on from containment and seek to identify impacted hosts/entities and remediate accordingly. Recovery aims to restore impacted systems to normal operations and may also include remediating vulnerabilities which existed and enabled the incident to occur.
- **Post Incident Activity:** Normally conducted as a postmortem to learn from the Incident and the Response so that feedback and observations can be incorporated into the plan.

An Incident Response team which is:

- Experienced, having dealt with incidents across both the public and private sectors.
- Highly skilled, holding a range of industry recognised certifications, often being sought out to support clients across Europe.
- Trusted, having delivered these services to customers for years.
- Partnered with industry-leading security technology partners and agencies, ensuring that our teams are suitably equipped to deal with whatever a Cyber Security Incident may bring.

An Incident Response Consultancy Service, which you can trust to deliver your business:

- Clarity – Clear Profile of your IR stance against required capabilities
- Actionable Findings – Prioritised list of improvements and potential next steps
- Investment Justification – Findings help create the business case for the next level of design or implementation
- Rationalisation – Better align Incident Response with ITSM toolset, leveraging investments and exploiting synergies.
- Compliance – Demonstrate continuous improvement of business continuity.

Service Delivery

Service Management

Fujitsu's Managed Security Services are operated under an ITIL-aligned, ISO/IEC 20000 compliant service management framework. Fujitsu will implement and maintain the agreed policies for the MSS and any changes to the policies will be managed through the Managed Service Change process. The MSS shall contain the following principal elements:

- Incident Management.
- Problem Management.
- Change Management.
- Release Management.
- Configuration Management.
- Service Level Management.
- Quality Management.
- Availability and Capacity Management.
- Service Continuity Management.
- Continuous Improvement.
- Third Party Management, where required.

Fujitsu's Security Operations Centres (SOC) will respond to security incidents using the following approach:

- Event Analysis - Upon detection, events which impact on security will be analysed to ascertain whether they need to be upgraded to a Security Incident for further action.
- Security Incident Categorisation – If the event is defined as a Security Incident, it will be categorised considering the cause, priority, potential impact, and the urgency of response in line with the agreed ITIL based Service Management framework.
- Security Incident Response – The security analysts, resolver groups and service management team, plus identified Customer stakeholders as defined within the overarching Service Management Framework and Communications Plan, will agree on the most appropriate course of action. When a course of action has been implemented, its effectiveness will be assessed so that if the chosen course of action needs to be extended further appropriate action can be taken.
- Post Incident Analysis - After each Security Incident, post incident analysis shall be undertaken to:
  - Ensure that the conduct of the investigation was appropriate.
  - Consider lessons identified, where conduct of the investigation could be improved.
  - Ensure that all mitigating actions have been taken.

Security and Information Assurance

Fujitsu's MSS are provided from our ISO 27001 certified support organisation and use ISO/IEC 20000 based operational procedures to deliver availability and operational service levels based on a standard service management toolset. Fujitsu provides MSS from its SOCs to several Public Sector Customers.

Business Continuity

Fujitsu has achieved ISO22301 certification and Fujitsu's SOCs and service delivery functions are underpinned by robust and tested Business and Service Continuity. From a MSS perspective Fujitsu will retain configuration back-ups for rebuild/restoration purposes using Fujitsu's standard environment platform backup processes. To support HMG in Business Continuity planning, Fujitsu provide BCP/DR services separately through the G Cloud framework.

Training and Consultancy

Fujitsu has a broad range of consulting capabilities. These range from technical architecture consulting, advising on security best practices, supporting major service transitions, delivery of MSS that support and facilitate highly successful first-time security deployments on a global scale. Fujitsu's experienced Governance, Risk and Compliance (GRC) focused consultants can help customers align their security strategies to those of the business.

Fujitsu can also provide business focused consultants to work with customers to facilitate and enable the required process engineering to rapidly integrate MSS and mature incident response processes that enable you to derive the benefits and return on investment in the MSS. Additionally, Fujitsu's consultants can undertake training of Customer personnel including knowledge transfer and structured maturity development for MSS and the underpinning technologies.

Additional Service Options

Dependent upon the MSS chosen the services comprise service level and enhancement and ancillary services options, dependent upon specific or wider Customer requirements. Where the complete support requirement is not covered by a specific control these can be defined and agreed as part of the requirements definition phase. Examples could be the following:

- Secure DevSecOps and, secure CI/CD for application development.
- Controls to secure data and enable discovery within Cloud based services, lessons identified, and where conduct of the investigation could be improved.
- Security requirements for Applications/Digital Services.
- Asset Management (for integrated delivery with Vulnerability, Patching mechanisms etc.).
- Mail Gateway technologies to support secure connectivity post GCF/GSi requirements.
- Managed Detection and Response (MDR) utilising Extended Detection and Response (EDR) technology

Onboarding and Offboarding

Onboarding

Fujitsu's approach is to work with the G-Cloud customer to define the detailed requirements to produce a quotation that includes the agreed scope of the services and delivery approach. Fujitsu's Onboarding process has five overarching phases:

- Definition of the scope.
- Discovery - conducting a detailed analysis of the current estate.
- Design of the new infrastructure based on definition and discovery.
- Develop the solution.
- Deploy, test and release.

The approach is underpinned by the following key components:

- Project/programme management activities aligned to PRINCE2/Managing Successful Programs.
- Robust change management.
- Externally verified risk management processes.
- Active security management.
- Staged approach with formal entry and exit criteria, controlling stage progression.

Offboarding

Fujitsu will work with you to define the scope and timescales required as part of the Off Boarding. The approach to off boarding will ensure an orderly transition of the transferring services to the replacement supplier.

A key priority for Fujitsu in any service exit event is maintaining the contracted levels of service for the remaining period of the Term. As such, Fujitsu would look to work with the new incoming supplier to:

- Agree a strategy for exit arrangements that is cost effective, and risk managed to maintain the integrity of the service.
- Agree the commercial terms for any exit services required from Fujitsu
- Agree the new supplier's transition timescales, with the aim of ensuring a seamless transfer of services.

Service Levels

Technical response times for the Fujitsu Managed Security Services are outlined below:

Objectives for Availability Incident Resolution Time

Severity	Title	Definition	Resolution Time	% Target
1	Critical	Severe business disruption: business unit or sub-unit unable to operate, critical system component failed or severely impaired	4 hours	95
2	Major	Major business disruption: critical user or user group unable to operate, or business unit experiencing significant reduction in system performance	8 hours	90
3	Medium	Minor business disruption: single user unable to operate with no circumvention available	16 hours	90
4	Low	Minor disruption: single user or user group experiencing problems, but with circumvention available	3 days	90
5	Very low	Enquiry: single user or user group requiring assistance but with no direct impact on business. For example, a request for information. Also used for change requests.	5 days	80

Table 1: Availability Incident Resolution Time

Objectives for Security Incident Response Time

Service Measure	Description	How it is measured	Service Level
Priority 1 Security Event	Support Team will call you within 30 minutes of a Security Event being classified as Priority 1 Security Event	Measured from the time that the work is formally assigned to the appropriate Support Team resolver group until the first attempt by the Support Team to call you. Measured in minutes and seconds within the applicable Hours of Service.	≥90%
Priority 2 Security Event	Support Team will call you within 60 minutes of a Security Event being classified as Priority 2 Security Event	Measured from the time that the work is formally assigned to the appropriate Support Team resolver group until the first attempt by the Support Team to call you. Measured in minutes and seconds within the applicable Hours of Service.	≥90%

Table 2: Security Incident Response Time

Pricing

Fujitsu's Lot 3 Data Protection Service is highly flexible, scalable, and customisable, with the final price being determined very much by individual customer requirements. As there are many customisable options, pricing can only be determined once the Contracting Authority's environment, infrastructure, skills, and desired outcomes are established. As such, an initial scoping and discovery activity (conference call) will be undertaken to determine your resource profiles and requirements so that pricing may be provided

Fujitsu can work with you to develop alternative commercial models, this includes financing options that would allow the spreading of capital expenditure over the term of a contract, effectively removing the capital expenditure requirements and delivering the consulting and technology elements as operational costs.

Commercial

Ordering and Invoicing Process

You will be invoiced for the charges on completion of the set up and provisioning of the Managed Security Service and a monthly in arrears charge for the ongoing management of the service. When remitting payment, you will include the applicable Fujitsu invoice that the payment applies to.

Minimum and Maximum Terms

There is a minimum term of 12 months

Termination Terms

You may terminate a Managed Security Service (MSS) by giving not less than ninety (90) days' notice to the other party. Should you decide to terminate the Service, termination fees will apply as detailed within the contract and will be dependent upon the specific MSS being terminated. Additionally, should you terminate a service, you shall be liable for any Software Licensing or Hardware support costs that arise because of the early termination.

Supplier Termination

Fujitsu may terminate a service by giving not less than ninety (90) days' notice to you.

Consumer Responsibilities

Successful delivery of the Fujitsu Managed Security Service is subject to the following dependencies upon you:

- Maintain the applicable Customer Security Policy regarding the services.
- Advise and agree any security testing with Fujitsu prior to commencement.
- Notify Fujitsu of potential Security Incidents via the Service Desk using the agreed method of incident logging.
- Promptly log all Security Incidents with the required details of the Security Incident.
- Use all reasonable endeavours to ensure that no incidents are reported which relate to equipment and services that are beyond the scope of the Support Services.
- Deploy software components onto servers for log file collection (for example agents) and install all pre-requisite patches and applications within agreed timescales.
- Provide Fujitsu with timely access to customer equipment and designated customer staff
- Utilise the Fujitsu-provided software in accordance with the prevailing license terms.

Service Constraints

Fujitsu shall not be liable for customer take up, non-take up or other discretionary use of the information provided by Fujitsu or of any of the recommendations or options generated from the Service and activities under this Service Definition.

Service Exclusions

The following elements are not included in the Service and are therefore not included within this Service Definition:

- Hardware and software; plus, ongoing licensing and support. These would need to be defined as part of the initial requirements definition with you.

About Fujitsu

As one of the world's leading IT companies, Fujitsu is at the forefront of pioneering technology in the UK since we made our initial investment over 40 years ago. As a key strategic partner we deliver essential services, from our secure hybrid IT which underpins critical national infrastructure to our investment in emerging technologies to boost national capability. Drawing on our Japanese technology expertise we provide bespoke digital transformation solutions. This unrivalled expertise has allowed us to specialise in emerging focus areas; Hybrid IT, AI & RPA, Data analytics, Agile application development/transformation and Security. Together, we offer a full package of solutions to support the UK as a long-term industry supplier.

We believe in realising the significant alignment between the UK and Japan in emerging technologies and in creating a UK-Japan 'Innovation Bridge' to support the UK's science and technology superpower objectives. We are committed to investment in UK skills and research and development, driving customer outcomes and promoting social value. We employ 124,000 people around the globe, including around 8,000 people across the UK, promoting diversity and inclusion as a DWP Disability Confident Leader. We are recognised as a Times Top 50 employer for Women since 2017, a Stonewall Top 100 Employer for 2023 and were awarded an EcoVadis Silver Rating, the world's largest provider for sustainability ratings.

Contact: government.frameworks@fujitsu.com