Managed Security Services Provider

SIEM as a Service

Service Description

Fujitsu's SIEM as a Service provides our customers with Security Information Event Management (SIEM) as a Service that delivers on-demand security event monitoring services with automated alerting and reporting in a cloud-based model.

Fujitsu Service Description

SIEM as a Service

Fujitsu's SIEM as a Service (SIEMaas) has been designed to provide convenient, enhanced security event visibility to organisations in order to provide context across the customer's estate. Fujitsu has partnered with an industry leading provider of SIEM technology to create SIEMaaS that is delivered as a cloud solution. SIEMaaS enables customers to gain insight into their security events which are conveniently automatically prioritised and delivered to the customer. The service is provided on a subscription basis. This document describes Fujitsu's SIEMaaS, which, dependent upon the functionality required, can include:

- Integration of a wide range of customer environment standard log sources
- Deployment of either physical or virtual Site Log Collectors (SLC)
- Pro-active alerting and event correlation across platforms
- Monitoring, analysis and response to security events
- Automatic incident ticket generation for rated security incidents and escalation to a nominated customer representative
- Automatic centralisation and archive of logs with chain of custody
- In depth and expansible reporting and management
- Enhanced Event Packs and reporting tailored for various business sectors including Finance, Manufacturing, Retail and Utility sectors
- Ability to integrate non-standard log sources
- Optional Event Pack enhancements
- Optional security incident management and response capabilities
- End-to-end monitoring and response on a 24 x 7 basis backed up by SLA's for all business sectors
- Choice of services and enhancements

Features & Benefits:

- Fujitsu's SIEMaaS provides leading security information and event monitoring services
- Our 24 hours x 7 days a week service is designed to enhance an organisation's information security defenses through continuous monitoring and proactive response, to help protect customer infrastructure and services.
- Fujitsu can further enhance the SIEMaaS and provide expert analysis of event data and can respond to potential security threats through its in depth managed service and professional services capabilities
- The SIEMaaS helps to reduce operational expenditure and provides predictable operating costs
- Fujitsu has fostered strategic partnerships with leading security vendors to use proactive intelligence to mitigate emergent vulnerabilities and threats
- The SIEMaaS utilises a standard deployment model that fits most business needs
- Detailed and comprehensive reporting
- Additional complimentary Managed Security Services

Key Volumetric Information:

Fujitsu invest time in understanding our customer's business, security policies and infrastructure to understand what is required from their MSSP provider. To ensure that the correct solution is deployed Fujitsu work with our customer to identify the relevant requirements in order to deliver a cost effective service.

For the SIEMaaS, the pricing model is based on a combination of:

- Services purchased and the optional enhancements selected
- Gb of data consumed for Level 1 service
- Messages Per Second (MPS) consumed for Level 2&3 services
- Number of Site Log Collectors deployed

Service

Fujitsu has ISO27001 accreditation and the SIEMaaS MSSP is operated in a dedicated SOC to deliver:

Service Start up

- A workshop is run to identify the key aspects of the service such as topology, number and type of log sources, relevant IP and hostnames, SLC delivery locations and key logical network requirements that shall be detailed in a standard delivery plan

Security Event Incident Notifications

- Identified security events shall be automatically prioritised and where applicable the incident notifications will be emailed to the designed customer contact. For high priority events, Priority 1 & 2, the designated customer contact shall be called and automatic log export to the customer portal shall be undertaken. For Priority 3 events an email notification only shall be sent, should the customer require the relevant supporting logs then a service request will need to be made within 5 days of the event.

Change and Configuration Management

- Fujitsu will maintain its own change and configuration management processes to support the SIEMaaS. Fujitsu will endeavour to notify customers of any emergency changes 24 hours prior to implementation. All other changes will be undertaken during the monthly maintenance window.
- The customer must promptly inform Fujitsu of any planned outages or changes that would impact the operation of the SIEMaaS
- Any additional customer changes to the contracted baseline will be considered a chargeable activity

Service Utilisation

- Fujitsu will monitor customer utilisation of the subscribed services, where services are being over utilised Fujitsu will notify the customer and take remedial actions to protect its shared service.

Service Reporting and Review

Fujitsu will provide monthly reports, which include:

- Executive summary report
- Baseline Security Analytic Event Pack reports on the customer data set
- Service utilisation report
- Incident notifications summary report
- Where optional Event Packs have been subscribed too then these will have their own additional reporting included and delivered

Exceptions

This list shows typical exceptions, however the actual list will depend on which elements are selected by the customer

- Classification or re-classification of security event incident notifications to customer business processing rules
- Transition and transformation services are deliberately excluded from this description as the service is an 'as a service' solution
- Any software licensing and hardware costs that are not part of the SIEMaaS or are not explicitly stated as included
- Hosting, logistics, storage and transport unless specifically included
- Any project costs and activities unless specifically stated as included

*Note: The list of Inclusions is a high level summary of all the service elements that form part of the service. The list of exclusions is a high level summary of some items that do not form part of the service, and has been provided to give additional clarity. The list of exclusions is necessarily not an exhaustive list.

Fujitsu Asia Pte Ltd

Nexus @ one north
1 Fusionopolis Link, #04-01, Singapore 138542
Email: info@sg.fujitsu.com
Web: sg.fujitsu.com