FUJITSU

shaping tomorrow with you

Security Information and Event Management Services

Protecting your organisation 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) Managed Security Services, we provide you with the core components for the collection, detection, response and remediation of security incidents in addition to enabling retrospective analysis to support security investigations and compliance requirements.

Threat Lifecycle Management

The traditional approach to cyber security has been to use a prevention centric strategy focused on blocking attacks. This approach has had limited success in recent years especially as threat actors techniques, tactics and processes have evolved to evade these less agile strategies.

Detecting and stopping attacks as early as possible in the cyber-attack life cycle is a key deliverable of any threat lifecycle management programme where an integrated detect and response strategy is being deployed.

Business-affecting incidents and data breaches can be largely avoided if businesses detect threats early in the threat management lifecycle and respond quickly, reducing costly damage clean-up exercises.

Events that matter

Fujitsu's SIEM services collects events from the organisations critical assets.

We employ best of breed SIEM technologies to store and secure this data. We perform analysis using machine intelligence and rank events of interest based on a risk based prioritisation in order to detect the most relevant threats to your business.

Our Cyber Resilience Centre (CRC) triage the prioritised events of interest and investigate them to determine if the event is a false positive or a true threat that could affect your business.

Identifying and prioritising the true events efficiently helps you to identify existing threats or potential new threats and prioritise them as incidents according to your business

Fujitsu SIEM Services offer

- A managed CRC Service for triaging and incident management
- 24/7 monitoring
- Secure log management services
- SIEM as a Service - supply, integration and management
- Optional advanced intelligence services

Fujitsu SIEM Services

Features

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

- Integration and collection of a wide range of customer environment standard log sources; custom log source integration available upon request
- Pro-active automatic detection, alerting and event correlation across platforms
- Automatic event ticket generation for prioritised security events of interest and escalation to a nominated customer representative
- CRC managed service monitoring, analysis and response to security events
- Standard event packs and optional enhanced event packs including reporting tailored for various business sectors including, but not limited to; Government, Finance, Manufacturing, Retail and Utilities
- Optional security incident management and response capabilities
- End-to-end monitoring and response on a 24 x 7 basis, backed by Service Level Agreements
- Fujitsu's SIEM services provide leading security information and event monitoring services
- Fujitsu can further enhance SIEM services 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 SIEM services helps to reduce operational expenditure and provides predictable operating costs
- The SIEM services utilises a standard deployment model that enables faster realisation of the business investment into SIEM services
- Highly tuned standard and optional Event Packs are available. These are selectable by industry or compliance obligations and include comprehensive reporting

Summary of features:

SIEM as a Service	Standard	Optional
Manage: systems management	✓	
Collect: log management, standard number of agents and SLCs, standard number of retrieval requests	✓	
Collect Options: additional local collectors, remote agents and retrieval requests		✓
Detect: Standard SIEM service including base line analytics event packs, reporting and standard service SLA's	✓	
Detect OPTIONS: additional standard attack or compliance event packs, custom event packs		✓
Respond: CRC managed service, triage, investigation, classification and reporting of events and incidents; including standard SLA's	✓	
Respond OPTIONS: enhanced cyber investigations and optional cyber threat response services		✓

Service Levels

In today's business world, security is a 24*7 requirement; Fujitsu provides around the clock service availability with a number of service level options designed to meet specific business needs.

Fujitsu's Cyber Resilience Centre (CRC)

Fujitsu's state of the art CRC provides a focal point for:

- The co-ordination of security monitoring and security incident management
- Providing situational awareness through the broad view of the security threat landscape due to the breadth of the Fujitsu Client base and the links with Cyber Security agencies and strategic technology partners
- The ongoing support and tuning of the technology platforms to enable the service to retain current against the emerging security threat
- Security event and incident related information to better enable risk mitigation
- Expert security advice and reporting
- Compliance assessment and support of associated reports and remedial actions
- Fujitsu's Advanced Remediation includes options such as - Incident response, Incident Management, End-User blocking, Endpoint re-imaging, end-user education etc...
- Fujitsu's Automation & Orchestration Services allow for full policy based control for clients with the ability to monitor, remediate and quarantine suspicious activity 24*7 seamlessly at machine speed

Benefits

Efficiency

- Reduction in time to detect threats
- Accelerate the speed to respond to threats
- Proactive services that can mitigate threats as they arise

Cost Savings

- Reduces the cost of hiring, training and retaining high quality security professionals
- Flexible aaS model can reduce capex expenditure
- Directs spend to appropriate controls and activities

Security

- Details new and historic active threats
- Enables 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

CONTACT FUJITSU
Email: cybersecurity@au.fujitsu.com

Address:
Lvl 3,4 National Cct
Barton, ACT 2600
Australia
Tel: +61-2-6250-9600