data sheet

Managed SIEM Service

Security Information and Event Management (SIEM) technologies play a vital role in assisting you to:
- detect and respond to IT security threats and breaches
- mitigate risk
- ensure compliance

The core feature of SIEM technologies is the ability to gather security data from all of the critical assets residing on your network and to present that data as actionable information via a single interface.

This provides a vast array of benefits by allowing your security team to gain a holistic understanding of your assets' security status, prioritise security incidents, and demonstrate compliance with regulations much more efficiently.

Dimension Data offers a breakthrough alternative to in-house software or appliance based implementations of SIEM products. We deliver value through rapid deployment, ease-of-use, and instant access to expertise.

Dimension Data's Managed SIEM Service provides superior security and compliance for your organisation without the need to install and configure a SIEM product, or the added expense of hardware and people to maintain and manage your solution. In fact, the Managed SIEM Service can be up and running, and protecting your organisation, in just days.

The service provides:

- **a managed SIEM service**, built on commercially supported, industry-leading products from ArcSight, McAfee Nitro, Splunk, and RSA Security Analytics
- **SIEM solution management, monitoring, and maintenance** by experienced security analysts in Dimension Data's Security Operations Centre (SOC)
- **24/7 performance and availability event monitoring**, providing constant vigilance for your perimeter security
- **industry best practices** to ensure a high level of network access and information availability, integrity, and privacy
- **access to highly trained security experts** who act as an extension of your in-house IT team, providing analysis, configuration, content development and maintenance, and use case development
- **a client security portal** that provides full visibility of your security and compliance posture, giving you the intelligence and analytics you need to easily understand your risks, demonstrate compliance, and make better security decisions
- **advanced reporting functionality** integrated across all of Dimension Data's Managed Security Services
- flexible threat analysis options, including Daily Log Analysis or the option to have all or a subset of the logs forwarded to the Dimension Data SOC for 24/7 real-time threat management

Dimension Data offers a **breakthrough alternative** to in-house software or appliance-based implementations of SIEM products.

Benefits to you

- **Custom SIEM system configurations:** focused, cost-effective security solutions for your organisation – regardless of business size or market
- **Guaranteed responsiveness** to availability events or issues with system performance
- **Daily management:** with complete SIEM solution support, including policy backup and restoration, software patches, and system configuration
- **Reduced costs** associated with hiring, training, managing, and retaining high quality security engineering employees
- **Improved agility** by freeing up your internal resources to focus on your core business outcomes and requirements
- **Flexible financial terms:** an opportunity to consume the service as an operational expense, eliminating the need to purchase hardware and software
- **Streamline SIEM system operations** and improve performance
- **Tighter security policy** for improved protection against cyber-attacks
- **Access to our SOC** for 24/7 support and escalated engineering
- **Business intelligence and compliance reporting** through the client security portal
- **Certifications:** ASIO T4, ISO/IEC 27001:2013, ISO 9001, Australian Signals Directorate (ASD) certified gateway up to protected classification level and PCI DSS

Features of the client security portal

- The portal provides integrated business intelligence and analytics tools to help you gain the meaningful insights and new perspectives you need to make better security decisions.
- Highly customisable data visualisations and reports give you point-in-time snapshots, as well as trends over time, across multiple security metrics.
- You'll receive an extensive set of reports for security and compliance.
- Reporting has been specifically designed to help you demonstrate adherence to regulatory requirements and provide enterprise-wide visibility into the performance of security controls.

Service elements	Essential	Advanced
Client Take-on		
Client take-on administration	✓	✓
Infrastructure Readiness Assessment	✓	✓
Client connectivity	✓	✓
SDA deployment	x	✓
Baseline reviews	✓	✓
Asset modelling	x	✓
Use case development	x	Optional
Client security portal establishment	✓	✓
Service activation and acceptance	✓	✓
Real-time Threat Management		
Vulnerability scanning service	x	✓
Log processing		
• log collection	x	✓
• log filtering	x	✓
• log aggregation	x	✓
• log categorisation	x	✓
• log normalisation	x	✓
• log forwarding	x	✓
• log mining	x	✓
Log correlation		
• multi-stage attack correlation	x	✓
• contextual correlation	x	✓
• real-time location correlation*	x	✓
• real-time dynamic network correlation*	x	✓
Identity and role correlation	x	Optional

Service elements	Essential	Advanced
Global intelligence correlation	x	✓
Vulnerability scan data correlation	x	✓
Content aware monitoring	x	✓
Context aware monitoring	x	✓
Predictive intelligence	x	✓
Network behavioural anomaly detection	x	Optional
Insider threat monitoring	x	Optional
Compliance aware monitoring	x	Optional
Event Management		
Performance and availability monitoring and notification	✓	✓
Daily Log Analysis	Optional	x
Incident Management		
Security incident management		
• phase 1: security incident identification	x	✓
• phase 2: security incident investigation	x	✓
• phase 3: security incident response & containment	x	✓
• phase 4: security incident rectification	x	✓
• phase 5: restart	x	✓
• phase 6: monitoring	x	✓
Remote incident diagnosis and troubleshooting	✓	✓
Workaround or permanent resolution identification	✓	✓
Workaround or permanent resolution implementation	✓	✓
Service Asset and Configuration Management		
Configuration backup	✓	✓
Patch release notification	✓	✓
Asset inventory management	✓	✓
Role-based access control	✓	✓
Change Management		
Change request process	✓	✓
Configuration and administration content maintenance	✓	✓
Release and Deployment Management		
Patch installations	✓	✓
Configuration restore	✓	✓
Content maintenance	✓	✓
Reporting		
Threat intelligence service	✓	✓
Online searching and reporting	x	✓
Monthly reporting (system generated)	x	✓
Report validation and review	x	Optional
Core service elements		
Service desk	✓	✓
Escalation management	✓	✓
Request fulfilment	✓	✓
Client security portal	✓	✓
MACD service units	✓	✓
Service management		
• Client services manager	Optional	Optional
• Service management reporting	Optional	Optional
• Service review meetings	Optional	Optional

*** Use case development prerequisite**

Why Dimension Data?

- **Broad expertise** across a variety of technology focus areas, including:
  - the network as the platform
  - communications
  - the next-generation data centre
  - end user computing
  - security
- **Strategic partnerships** with leading security technology vendors, including Cisco, Check Point, Blue Coat, RSA, McAfee, Zscaler, Juniper, Sourcefire, Imperva, Palo Alto, Fortinet, ArcSight, and FireEye.
- **Proven track record:** over 6,000 security clients across all industry sectors, including financial services, telecommunications, health care, manufacturing, government, and education.
- **Global footprint, local delivery:** with over 23,000 employees and operations in 58 countries across five continents, Dimension Data manages more than USD 12.5 billion of network infrastructure through five Global Service Centres on a 24/7 basis, in more than 15 languages.
- **Real-time threat management platform:** an enterprise-wide risk management solution enabling our SOC analysts to centrally manage attacks, threats and exposures by correlating security information from firewalls, intrusion detectors, virus scanners, VPNs, operating systems, authentication solutions, vulnerability scanning tools, and other security controls. The solution enables our analysts to eliminate clutter such as false-positives, while quickly identifying the real security threats to help them respond with adaptive security measures.
- **SOCs:** our SOCs serve as command, control and communications centres for all Dimension Data's security operations and client support centres. Staffed 24/7 with three teams, namely the Watch Team, Security Operations Team and Forensic Team, which are dedicated to maintaining the highest quality of service. The SOCs utilise advanced equipment and technology to monitor and manage the network and identify and resolve problems.
- **Security experts:** our certified security experts collectively bring a wealth of cyber security experience to augment the knowledge base of your IT organisation and provide peace of mind that skilled technicians are there to help you respond to and mitigate threats.
- **Certifications:** ASIO T4, ISO/IEC 27001:2013, ISO 9001, ASD certified gateway up to protected classification level and PCI DSS.

Dimension Data creates, integrates, and manages your security infrastructure in a way that supports your business goals. We offer a broad portfolio of security services coupled with proven technologies from a select group of innovative partners. Our security professionals are recognised for their depth of expertise and passionate client delivery. They're globally connected to bring you the best solutions for your security needs, delivered anywhere in the world.

Contact us

For more information, please contact your nearest Dimension Data office or visit **http://www.dimensiondata.com**

Guaranteed responsiveness
to availability events or issues with system performance.