Product brochure

Your next step into digital

Our cloud and security services

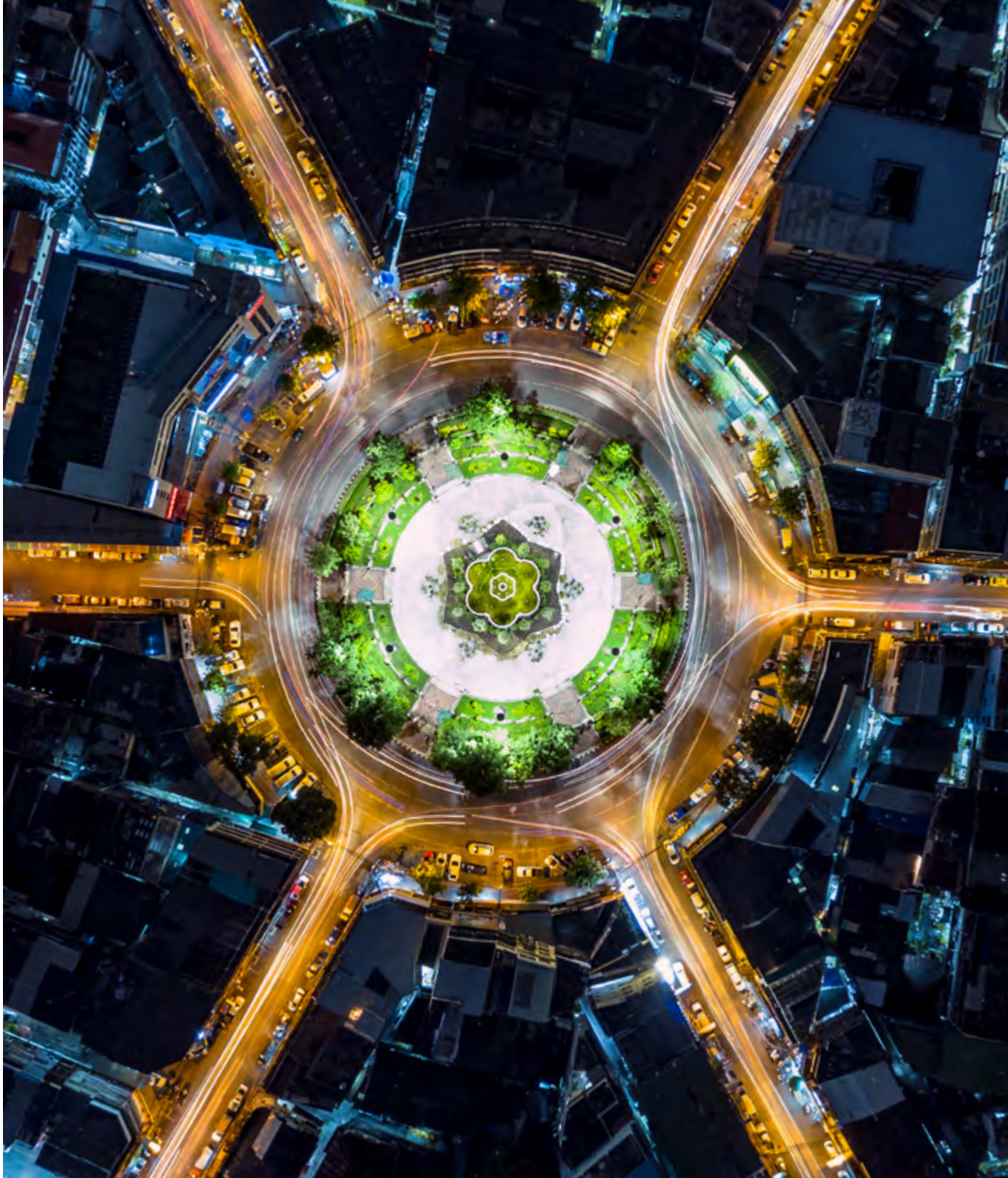
The future is exciting.

Ready?

Managed Security Information and Event Management

vodafone business

Contents



What is Managed Security Information and Event Management?

In today's enterprise, there are many tools and data points through which to monitor the security protection of IT assets. The challenge this brings is the ability to gain a rational view across the enterprise. Our Managed Security Information and Event Management (MSIEM) service accurately detects and prioritises threats across the enterprise and provides intelligent insights that enable teams to respond quickly to reduce the impact of incidents.

What is the service?

The MSIEM solution is designed to help you plan, implement, manage and monitor a SIEM system around your managed cloud environment. It delivers a threat management system that can identify and respond to threats, to create better compliance, optimise infrastructure investment and improve security posture.

The service delivers ongoing actionable data on threats by consolidating log events and network flow data from devices, endpoints and applications distributed throughout the network. Our service includes design, implementation, configuration, optimisation, management and monitoring utilising IBM's QRadar on cloud (QRoC) SIEM system.

Our security consultants initiate the engagement, perform the SIEM assessments, evaluate security governance and processes and design custom solutions to meet unique organisational needs. We then provide around-the-clock expertise in security management, monitoring and reporting to help effectively prevent, and reduce and remediate security events.

What is Managed Security Information and Event Management?

Phase 1

Project initiation and planning

- Kick-off
- Requirements and definition planning session

Deliverable:
Project plan

Phase 2

SIEM system design

- Process and data gathering
- Detailed functional and non-functional requirement definition and documentation
- Architecture design
- System design
- Design review

Deliverable:
SIEM macro and micro design

Phase 3

Implementation

- Install and customise console appliance
- Deploy log flow collector
- Perform initial tuning

Deliverable:
Operational SIEM system

Phase 4

Integration and transition

- Staged transition to operational support
- Reports, definition and validation
- Readiness assessment
- Initiate steady state operations

Deliverable:
Runbook communications plan and first report set

Phase 5

Ongoing operational support

- Real-time event monitoring and notification
- Reports generation, review and analysis (optional)
- SIEM system management
- X-force threat analysis service

Deliverable:
Monthly report set, XFTAS reports, monthly/quarterly/annual reviews

What is Managed Security Information and Event Management?

What do you use it for?

Security monitoring and operations are transforming due to more frequent and persistent cyber-attacks. With the greater awareness of security, the number of monitoring points and volume of alerts can overwhelm an organisation; this situation is unacceptable and a new security protection solution is often required.

The MSIEM service can address a number of challenges faced by an organisation and help ensure they are best prepared for potential security threats.

- Solution analysis, identifying cloud patterns, target the move to the cloud, mobility and increased connectivity of enterprises to the internet has increased the potential attack vectors
- Traditional managed services, monitoring of specific devices, are not adequate to detect sophisticated attacks and as a result, attacks can sometimes go undetected for many weeks or months. Many security events are left unexposed in log files with little or no correlation across the global environment.
- SIEM technology is a security core enabler – but most SIEM environments are typically:
  - not optimised to capture data from across a global organisation
  - not set up to support high priority uses cases
  - not fully capturing data to support use cases set
  - not continuously updated to support current risks (planning)
  - not monitored/managed 24/7
- Once a SIEM system is effectively deployed, it can be a foundation for deeper security intelligence

What's in it for you?

The MSIEM solution leverages proven security operations with specialised security consultants, who design, deploy and optimise an advanced world-class SIEM for your organisation. The key benefits it can bring to your organisation are:

- Providing real-time intelligent monitoring and 24/7 security awareness to ensure that attackers never have an after-hours advantage
- Robust incident escalation and reporting to help manage stringent audit requirements and optimise investigation
- Industry-leading service level agreements for incident response, change management, system monitoring, solution availability and content updates
- Statement on Standards for Attestation Engagements (SSAE) -16 certified security operations infrastructure is maintained to help better address strict industry standards
- Support for leading SIEM vendors including IBM QRadar
- Integrated deployment for more cost effective, end-to-end implementation and operations

What's included in Managed Security Information and Event Management?

The MSIEM solution is a feature-rich solution spread out over five phases to create a comprehensive threat management system to prepare you for potential security threats.

The key features of this service include:

- Development and delivery of a detailed, end-to-end project plan
- A complete architectural and system design for your environment
- Full implementation and configuration of the SIEM system components, with validation that the data is being successfully transmitted and reported
- Development of relevant operational processes and corresponding documentation, with transition management and monitoring to the operational support team
- Comprehensive steady state management and monitoring of the SIEM infrastructure
- Proactive threat mitigation
- 24/7/365 security incident identification, classification, prioritisation, escalation, workflow tracking, data analysis and reporting
- A highly interactive and iterative approach
- Integration into your existing incident management, change management and other IT processes and operational activities
- Access to Security Operation Centres (SOCs) using worldwide delivery personnel 24/7 during Steady State Operations
- Project and service management to ensure successful transitionponent interdependencies and software versioning analysis.

Why Vodafone?

Vodafone Group is one of the world's largest telecommunications companies and provides a range of services including voice, messaging, data and fixed communications. Vodafone Group has mobile operations in 25 countries, partners with mobile networks in 42 more and fixed broadband operations in 19 markets. As of 31 December 2018, Vodafone Group had approximately 700 million mobile customers and 21 million fixed broadband customers, including all of the customers in Vodafone's joint ventures and associates.

By connecting people, places and things, Vodafone Business helps businesses of all sizes to succeed in a digital world. Our expertise in connectivity, together with our leading IoT platform, multi-cloud solutions, digital services and global scale, delivers the results customers need to help them progress and thrive. We are a trusted partner to businesses of all sectors and public services around the world, and work side by side with them to understand the unique challenges they face and the goals they want to achieve.

For more information, please visit:
www.vodafone.com/business

Next step?

If you want to discover more about Managed Security Information and Event Management, please contact your Account Manager.

www.vodafone.com/business

vodafone business