Customer challenge

Today we live in an era where data is critical to every organisation. As security risks are becoming more prevalent and increasing day by day, IT environments are growing ever more distributed, complex and difficult to manage. This makes the role of security information and event management (SIEM) technology extremely important to organisations.

Organisations must become smarter at controlling the right information to protect themselves from the data and event security threats and challenges they face every day including:

- Compliance
- Operations Support
- Zero-day Threat Detection
- Advanced Persistent Threats
- Forensics

For example, do you know the answers to:

What were the main attacks on your end user devices, firewalls, networks and datacenters last year?

Did you have the right security measures in place to be able to stop and neutralise attacks?

Do you know the threats and the types of security threats your organisation is likely to be targeted with over the next 12 months?

Corporate information stored in datacenters, servers, PCs and mobile devices are increasingly at risk of attack. This coupled with many security threats not getting any shorter and becoming more sophisticated means analysing your current and future security SIEM requirements is becoming increasingly more important.

The solution and its benefits

SIEM technology is emerging as an organisation’s central nervous system for gathering and generating IT intelligence.

SIEM technology can provide an organisation with real-time analysis of security alerts generated by network hardware and applications. SIEM can also be used to log security data and generate reports for compliance purposes.

Technology Benefits of SIEM include:

- Easier ways to make sure you are compliant with industry rules and regulations
- Better Operational Support
- Zero-day Threat Detection
- More control over monitoring and correlation of events across an organisation
- Provision of forensic and analytical tools to gain a better understanding of attacks

Other Benefits of SIEM include:

- Increased employee productivity and process efficiencies
- Less manual resources needed for reporting
- Better security situational awareness
- Ability to embrace new trends such as BYOD and mobile working
- Prioritise and protect security investments
- Gain an improved understanding of security threats
- Allow the integration of SIEM with firewall and IPS for rapid incident response
- Centralise and have better control over the enforcement of IT security policies

www.computacenter.com
What services do we offer?

Audit & Optimisation
SIEM Assessments allow organisations to automatically assess their compliance status - within minutes, reducing maintenance and compliance costs.

Why should your organisation undertake a Computacenter and McAfee SIEM Assessment?

• Rule compliance – run checks on rules and policies
• Vendor best practice configuration compliance
• Access path analysis
• Customisable access policy: violation discovery, root cause analysis and management
• What-if analysis to virtually check planned changes
• Audit reports and compliance metrics
• Change tracking to access rules and objects
• Side-by-side comparison of past, present, and future SIEM requirements

Network Access & Compliance
Computacenter’s Network Security Assessments provides organisations with the ability to continuously evaluate enterprise networks for access compliance availability, and security risks - in minutes.

Why should your organisation undertake a Computacenter Network Security Assessment?

• Full modelling and simulation of network access
• Device configuration checks
• Network access policy management
• Customisable access policy (security and availability)
• Root cause analysis for access violations
• Compliance metrics and reporting
• Comprehensive device support

Computacenter and McAfee: The Security Specialists
Computacenter has over a decade of experience working with McAfee. Our experts hold sales and technical certifications for over 35 McAfee security solutions including:

• Application Security
• DDoS Protection
• Firewall Compliance & Solutions
• Secure Mail & Web Gateways
• Advanced Persistent Threats
• End Point Solutions
• Mobile Device Security
• Authentication

The security solutions we offer include providing first line and second line support.

We have helped a range of customers, across Retail Banking, Finance, Industry, High Street Retail and the Public Sector shape and execute their security strategies providing them with right-fit, not only-fit solutions.

Computacenter and McAfee moves security from a business cost to a business enabler.

Exploring the possibilities
Mergers and Acquisitions present specific challenges to organisations – how do you open and merge two disparate infrastructures in a secure and controlled way?

Let Computacenter discover and map your environments, analyse your rule bases and define the strategy for taking down your firewalls in a controlled and de-risked fashion.

Computacenter can consolidate and integrate your networks and security stacks saving you money and delivering your business outcomes in a timely manner. Competitive Advatange in an uncertain world.

More Information
Even with the best defence your organisation remains under threat and you need your employees to remain as productive as possible. For a free Computacenter security and business impact assessment contact James or Kate today:

James Naylor
Security Sales Specialist
james.naylor@computacenter.com
07834 350654

Kate Hammett
Security Alliances Manager
kate.hammett@computacenter.com
07775 706377

Alternatively, you can get in touch at enquiries@computacenter.com or visit www.computacenter.com