

# Security Information and Event Management (SIEM)

Protecting your enterprise from cyber-threats requires 24/7 vigilance using advanced security mechanisms and methods. Effective security monitoring is a very demanding task, regardless of the size of your organisation, and requires advanced technology, skilled security specialists and scalable processes. Secode's Security Information and Event Management (SIEM) service reduces the risks of non-compliance, protects your business from intrusion, fraud, downtime and loss of business critical information and revenue, delivering control, expertise and damage prevention.

## SIEM Services

The operating systems, applications, network equipment and security systems supporting today's businesses generate growing amounts of log data. Effective manual analysis of this volume of data is impossible, complex security event and log management tools are now essential to identify security events and take meaningful action.

A SIEM solution collects and correlates log information centrally, giving security specialists a flexible tool for log analysis. However, organisations often lack the people, specialist skills and resources to properly manage and monitor such a solution. A managed SIEM service delivered by security experts provides proactive information and event monitoring, meeting the specific needs of your business.

### Features

- Centralised log management function, guaranteeing a joined-up view of events
- Security event identification, analysis and correlation around the clock
- Statistics for historic analysis and trends for future planning
- Investigation specialists available 24/7
- Support for standard requirements as SOX, PCI, etc.
- Efficient financing and lower TCO
- Well-defined content for the services specified in the Service Level Agreement (SLA)

## Benefits

- Full controlled 24/7 SIEM process
- Traceability for computer forensics.
- Identification of security information in log files from multiple vendors and systems
- Log analysis of large log data files.
- Holistic view of the organisation's overall security status
- Correlation of events from a distributed environment
- Meets and exceeds compliance requirements
- Easy-to-budget modular components
- Frees up internal resources
- Consistent quality
- Traceability of digital forensics
- Eliminates redundant log silos

Centralising the log function is essential for effective log management and ongoing data collection. This includes the detection of missing log data, identification of gaps, truncated files and corrupt data.

Whilst log management has brought log data under control, on its own it is not sufficient to deliver the right intelligence to improve security operations. A real-time joined up view of log data collection, aggregation and reporting, as delivered by a SIEM solution, will meet governance, risk and compliance standards as well as business objectives. The implementation and continuous optimisation of relevant rules, signatures and correlation of filters, requires skilled, experienced personnel to interpret.

## Reporting and Analysis

The Secode SIEM service offers real-time incident reports, interpreted by our specialist consultants and accompanied by recommendations for immediate remediation. We also provide monthly reports detailing all analysed events and incidents with relevant statistics and trend analysis. This report is presented by our Technical Account Manager to enable a comprehensive discussion of an organisation's tactical and strategic approach, defined policies, service levels and risk posture. For those organisations that deploy multiple Secode services, we deliver a consolidated monthly overview to aid prioritisation of resources and reduce risk.

## Results

The SIEM service provides your business with proactive and reactive protection from security events, 24 hours a day, 365 days of the year.

## Business Benefits

Secode's managed SIEM solution reduces the risks of non-compliance of for example, PCI and DSS, by providing you with the detailed information needed to meet compliance. It also gives organisations the ability to respond quickly and effectively to high-risk security events, decreasing the impact of security incidents and preventing loss of business-critical information.

The Secode SIEM service enables you to get more out of your security log and event information, drawing greater value from your investment in security technology.

## Secode Differentiators

An independent subsidiary of NTT Communications, Secode combines global capabilities with local resources, knowledge and presence as the leading IT security provider in the Nordic region, delivering unique value to our customers.

- Industry expertise – professional services are performed by experienced industry experts, providing our customers with well-substantiated knowledge about their security posture
- Innovative prioritisation to drive management decisions, including relative return-on-investment
- Meaningful action plans help prioritise next steps and subsequent priorities for reducing risk
- Well-defined risk management methodology
- Common sense approach, blending people, process and technology
- Independent review of assessment and attestation requirements
- Independent analysis of dashboards and information-sharing capabilities
- A dedicated Technical Account Manager (TAM) with knowledge of your business, acting as your security advisor
- A TAM responsible for the service provided as per the SLA
- Timely, meaningful and personalised analysis and reporting

## Management Benefits

Secode's Managed SIEM solution provides your business with detailed reporting and analysis to support better informed, tactical and strategic security decisions.

With the ability to collect, correlate and analyse security events 24/7, customers can make fast, well-founded decisions, leading to improvements in security and performance and reductions in cost.

The Secode managed SIEM service allows our customers to work with experienced security professionals to both secure a successful deployment and continuously manage and administer the SIEM solution.

The service also provides a consolidated source of information for all stakeholders involved in the SIEM project.

## Operations Benefits

By bringing together security information from the many diverse log sources within your organisation, Secode's SIEM service provides you with a holistic view of your overall security posture. The 24/7 service gives organisations a joined-up view of thousands of disparate events, allowing them to focus on managing the risks to the business.

## Deliverables

Secode provides detailed reports, designed to be relevant to specific stakeholders and also to reflect the individual requirements of senior management, operations and the audit and compliance teams.

A dedicated TAM, acting as your Security Advisor, ensures that the services delivered meet business expectations. Security specialists are available 24/7 to continuously update

and configure the systems to get the most out of your investment.

We enable our customers to have an adaptive information security framework, which meets compliance requirements, reduces costs and saves time and resources.

## About Secode

Scoping and designing compliance, Secode is the leading IT Security Company in Northern Europe. The vision is that the internet and IT is secure for business, transactions and information exchange.

The company offers surveillance and protection services (24/7 Managed Security Services) from the Secode Security Operations Centre. In combination with Secode Security Consulting, companies and organisations gain increased insight, competence and control over their operations from a complete IT security perspective. Secode today has customers across all industries and business sectors.

## Securing Your Business

By asking the right questions, our security specialists resolve complex security, risk and compliance issues. This insight is essential to provide a complete end-to-end service – a service designed to meet specific business objectives, not merely address individual aspects of security. Secode's proven track record gives our customers the confidence to make security decisions based on expert advice at business, management and operational levels.

Secode secures your business.

For more information, visit [www.secode.com](http://www.secode.com)