



**LogSentinel helps a large government agency with Network and Information Security directive compliance**

# Business challenge

The **NIS Directive** sets a high bar for operators of essential services. The IT department of a government agency that falls in scope of the directive chose LogSentinel to ensure the requirements are met.

Collecting, archiving and protecting logs is one of the requirements in many EU countries that transpose the NIS Directive.





# Solution

**LogSentinel SIEM** is integrated with the internal systems of the agency, including its ActiveDirectory, Exchange, file server and various websites, to ensure that all logs.

LogSentinel SIEM fully **covers the logging requirements** stemming from the NIS Directive and is compliant with other relevant EU legislation as well (e.g. eIDAS).

# Key **Benefits**

# 01

## COMPLIANCE

Covering logging requirements that many EU countries impose based on the NIS Directive

# 02

## VISIBILITY

The IT department now has full visibility on the user and system behavior inside the organization

# 03

## DETECTION

Automatic detection of anomalous behavior, including potential cyberattacks.

# About LogSentinel

LogSentinel is an innovative company that takes compliance and information security to the next level with cutting edge technologies



## Audit trail

Store and analyze every business-relevant event



## Anomaly detection

Detect fraudulent and other anomalous behavior by people and systems



## Integrity protection

Immutable, secure and provable to 3<sup>rd</sup> parties



## Full visibility

Gain full visibility over your IT stack, including legacy systems



[www.logsentinel.com](http://www.logsentinel.com)