



**LogSentinel helps a  
large government  
agency with  
detecting security  
incidents**

# Business challenge

Security incidents, including cyberattacks, are often hard to detect and require a combination of expensive, well-configured and integrated tools.

Having undetected and unaddressed security incidents may invite additional attackers and become a growing organizational vulnerability over time.





# Solution

**LogSentinel SIEM** is integrated with the internal applications, databases and web services of the agency to monitor all **audit logs**. Many security incidents involve anomalous activity within these systems.

With our intuitive dashboard as well as **rule-based an AI-based anomaly detection**, the agency was able to detect and resolve numerous security incidents.

# Key **Benefits**

## 01

### DETECTION

Intuitive UI, rule-based and AI-based anomaly detection allows easily identifying security incidents in real time

## 02

### VISIBILITY

The IT department now has full visibility on the user and system behavior inside the organization as well as any deviations from the norm

## 03

### RESILIENCE

Being able to address security incidents in a timely manner makes the organization more resilient

# 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)