



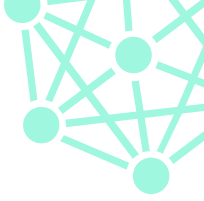
Success Story

Securing Multi-Located Huge Networks

Stronger Together



Securing Multi-Located Huge Networks



Problem:

Securitas was in need of a centralized security operations tool in order to visualize and monitor the network, system and security activities and also prevent possible threats for the all locations it serves.

In addition, the collected data had to be stored to comply with the regulations that Securitas is subject to and reported when necessary. Network security visibility had to be ensured with the help of dashboards that would be created. It was requested that detection, examination and intervention be made quickly against possible threats.

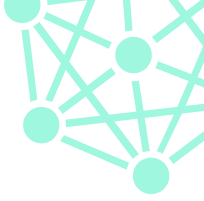


Solution:

Having done the capacity planning, Logsign SIEM has been deployed. Resource integration has been completed for system, network and security devices in all locations.

Alert notification scenarios designed for the usage of banned applications, which have been predetermined by the company, have been developed. In case of triggering alerts, e-mail notifications have been activated for the relevant security teams to intervene quickly. Correlations have been determined for external web application scanning and web-based attacks, and alerts have been activated. Threat intelligence services have been integrated and instant automatic blocking has been initiated on Securitas security devices. In order to control the access of contractors to Securitas systems, asset lists were first defined on Logsign SIEM. Instant supervision and notification with the Logsign correlation library using defined lists have been activated.

In order to meet compliance needs, location-based access reports and dashboards have been generated.



Results:

- 1** All data can now be processed with Logsign SIEM. With the rapid analysis of the data by the IT managers and team, high dominance and awareness in security operations have been achieved.
- 2** Having detected false positives, the alarm rate decreased by over **60%**.
- 3** By defining scheduled reports, the IT team's time to spare for operational work has increased.
- 4** After taking automatic action with threat intelligence data, the number of incidents to be investigated decreased by over **40%**.

Once Logsign was integrated into Securitas with all its capabilities, it added value in terms of more control, monitoring and investigation of events. Especially with regard to regular reports, the content of the reports to be created in line with our request provides the opportunity to get rid of the bulk of information and to examine the main data faster. **We feel safer with Logsign.** Thank you Logsign Team...



Salih Yıldırım
Network Engineer

About Our Customer:



Securitas

Securitas was established as a security company in Sweden in 1934. Over the years Securitas has grown so much that this story has turned into the story of a company that carries the three red dots across the continents, has hundreds of thousands of security guards, and now is the world leader in its sector.

Securitas has over 1000 business partners from 26 different sectors, from industrial facilities to retail chains, from tourism to energy, from shopping centers to aviation. It provides private security, remote monitoring, control support, reception services, risk management and consultancy, as well as firefighting services in 73 provinces via related companies. Securitas Turkey has 11 regional directorates, 74 branch offices, and 20,000 employees.