EKRAN

CASE STUDY

Featured story

Privileged User Incident

Rapid incident response and insider threat prevention at the Engineering Design Bureau

Problem

The Ukrainian Engineering Design Bureau with limited access had received information about sensitive project documentation loss.

IT department together with Security service team were charged with finding a suitable solution for malicious insider detection and prevention of all possible violations in future.

The high priority task was to detect intruder and apply appropriate penalties. Security service team was also concerned about the probability of further insider threat occurring.

Implementation of security monitoring product had been dictated by necessity to prevent any possible problems with insiders or third parties having common or privileged access to corporate network.

Solution

Ekran System, being security monitoring and incident response solution, was suggested to solve this problem. As Ekran System provides searchable video records of all terminal, remote, and local sessions, none user activity can be hide from it, even privileged one. Using full-functional playback for target session records as well as advanced search by metadata keywords, the Design Bureau team had easily found key episodes to investigate the security incident. As the result, just in a few days after deployment, Security service team had detected the administrator, who was involved to project documentation loss.

Interestingly, despite the fact that this malicious administrator knew about Ekran System deployment, he didn't expect our solution to be so easy-to-use and able to find him so quickly.

After successful incident response, the Ukrainian Engineering Design Bureau continued to use Ekran System to prevent sensitive data loss and other corporate policy violations.