Migration of SIEM from ArcSight to SAF with more then 400 correlation rules for Fintech IT Holding

cybersecurity | finance

Customer

IT-Holding, a provider of comprehensive IT services and custom software development for companies in the financial sector, with a staff of over 10,000 employees and a presence in 160 cities.

Goals

1. increasing the flexibility and scalability of SIEM
2. transferring functional and content developments from the current SIEM
3. expanding capabilities for incident investigation and data handling

Tasks

integration with SOAR, BI, TIP

building a fault-tolerant, scalable system

implementing a flexible role based access control system

aligning with the data model developed for the current SIEM

Results

powerful **search engine**

1. functional improvements
2. flexibility during migration
3. high speed, and extensive analytical capabilities

>75 data lookups

>25K EPS dataflow

400+ correlation rules

Read more

Security Analytics Platform – holistic cybersecurity monitoring and incident management bundle

read >>

Why does your company need the SAF Cybersecurity Bundle?

read >>>

read more use cases