MICRO FOCUS

Case Study

Security

Rostelecom-Solar

Rostelecom-Solar, acting as an MSSP/MDR, successfully leverages ArcSight ESM as a platform to provide SOC services to customers.

Rostelecom-Solar

Rostelecom-Solar (Solar Security LLC) is a national provider of services and technologies for the protection of information assets, targeted monitoring and information security management. The company was founded in 2015 and was based on the information security systems implementation division of the Russian system integrator Jet Infosystems. Solar Security also included the first commercial JSOC (Jet Security Operations Center) in Russia, which was commissioned in 2013. By that time Solar JSOC had offices in Moscow in Nizhny Novgorod. In 2018 Solar Security was acquired by Rostelecom, Russia's largest integrated provider of digital solutions and services. That year additional offices in Samara and Khabarovsk were founded and then in 2019 were founded office in Rostov-on-Don.

"ArcSight ESM is a framework. Up to 99% of the work we have done was performed by built-in SIEM system tools. We view this as a great advantage because we don't need to develop additional code, scripts, or integration modules. With ArcSight ESM, you can implement almost any SIEM use case."

MAXIM ZHEVNEREV
Lead Solar JSOC Services Analyst
Rostelecom-Solar

SIEM System for MSSP/MDR

SJSOC was originally built as an information security (IS) incident monitoring and detection service provider operating under an MSSP/MDR (Managed Security Service Provider/Managed Detection and Response) model, so they were looking for a Security Information and Event Management (SIEM) system capable of running on private and hybrid clouds as a service enablement platform.

The specialists were looking for a product that would allow the use of a separate virtual machine instance with a single SIEM license to serve multiple customers simultaneously, while providing a sufficient level of access control to monitored events, running scripts from different customers in the same SIEM system instance and other capabilities required by the MSSP/MDR.

Another important factor was the functionality of the event correlation mechanism. This had to be flexible enough to enable implementation of almost any use case of the SIEM system that the customer might need.

Ростелеком Солар

At a Glance

- **Industry**
  Software & Technology
- **Location**
  Russia
- **Challenge**
  To provide security monitoring services Rostelecom-Solar needed a framework that could detect advanced attacks. They also wanted to minimize maintenance costs.
- **Products and Services**
  ArcSight Enterprise Security Manager (ESM)
- **Critical Success Factors**
  + The first commercial MSSP/MDR SOC in Russia
  + ROI on SOC delivered by the end of the second year
  + Delivery of ArcSight ESM-based services to more than 40 customers
  + Reduced time to connect new customers—from three days

"When we inquired about the choice of SIEM system for the commercial SOC we created in 2012, only ArcSight met these criteria. There were no other similar solutions on the Russian market," recalls Maxim Zhevnerev, Lead Solar JSOC Services Analyst at Rostelecom-Solar.

The vendor of the solution was very well represented in Russia and had a strong position there. ArcSight also benefited from the fact that the JSOC specialists knew this product well and already had experience with it.

JSOC Know-How—Single SIEM Content and Other Practical Ideas

JSOC planned to build a managed content hierarchy that was able to use the same set of rules for different customers, and also be able to make different exceptions for each customer. By using a single event categorization, the costs of creating and running new discovery scenarios were minimized.

Vladimir Dryukov, Director of the Solar JSOC Cyber Attack Monitoring and Response Center at Rostelecom-Solar, says that he and his colleagues have carefully studied the experience of a number of known global SOCs and, after analyzing their methods, have found that they will not work in Russia for various reasons.

"All the ideas that are being used now were developed in projects and then repeatedly tested in practice," says Maxim Zhevnerev.

Content development for ArcSight ESM is also easy: following the general principles of content creation, it is easy to define specific rules for specific tasks that can then be used with almost any customer.

The only international standard that had to be met was the PCI DSS payment card standard, for which certification was obtained in 2015. There were no Russian standards and regulations regarding SOCs when JSOC first came into being. These appeared later, at the end of 2015, after the creation of the State System for the Detection, Prevention and Elimination of the Consequences of Computer Attacks.

The SIEM Solution and Its Ecosystem

As the number of customers has grown, the SIEM ecosystem has evolved: were created backup tools, additional ArcSight tools for creating and testing reference content, scripts and modules for integrating, processing and visualizing individual SIEM systems.

Connecting customers to ArcSight ESM at JSOC today involves one of two main options. In the first, customers forward all the required audit events to the SIEM JSOC cloud infrastructure. The other option is a hybrid one, designed for organizations that want to have their own SIEM system. To do this, the customer purchases an ArcSight ESM license, the provider helps to deploy the product at the customer's site, synchronizes the SecOps processes and the content of the two systems and then begins to provide the customer with MSSP/MDR services.

More than a dozen ArcSight ESM instances at JSOC are integrated into a single infrastructure. This allows to build the processes and deliver services to new customers quickly and easily. The JSOC private cloud uses three ArcSight instances to provide service to customers. In addition, there are several hybrid installations.

A New Stage in Development—JSOC at Rostelecom

"Joining Rostelecom provided us with additional opportunities for service development: access to new data, infrastructure resources, means of integration with external services and, of course, new customers. The team grew and the JSOC infrastructure expanded. But to cope with the growth and successfully deliver services to more customers, we had to make changes to the processes and architecture of the services, including to the way we integrate and automate operations," continues Maxim Zhevnerev.

According to Vladimir Dryukov, Rostelecom-Solar now provides services to more than a hundred of Rostelecom's external customers. ArcSight ESM is used to provide services to more than 40 customers.

Vyacheslav Tupikov, a technical expert at Micro Focus on ArcSight solutions in Russia and CIS, adds: "It is very revealing that JSOC itself leverages ArcSight ESM for its own security."

The Secret to ArcSight ESM's Success is Its Architecture

Talking about the advantages of ArcSight ESM, the specialists at Rostelecom-Solar highlight its very clever architecture, which implements at product-level a functionally rich and fast mechanism to correlate and process events, while event parsing and categorization are transferred to the connector level. This architecture provides the flexibility to customize the solution to a specific customer, allowing normalization and categorization to be adapted to customer requirements by modifying connectors and enriching events with external data.

"Thanks to these ArcSight ESM features we can create unified content and distribute it to our customers," says Maxim Zhevnerev. "The mechanism of active lists, which is poorly developed in many other SIEM systems, has proved to be very useful—they are easy to manage and very stable in operation. Almost all customer scenario configurations are described in the ArcSight ESM active lists. The existing API integration capabilities allow us to develop this functionality and migrate service management from the SIEM console to various external systems, which makes the service even more manageable."

> "The ArcSight ESM licensing model for MSSP/MDR is straightforward, transparent, and predictable. In my opinion, this is one of the most mature models on the market today. Using it, providers can easily create their own pricing scheme."
>
> **VLADIMIR DRYUKOV**
> Director of the Solar JSOC Cyber Attack Monitoring and Response Center
> Rostelecom-Solar

"ArcSight ESM is a framework," says Maxim. "Up to 99% of the work we have done was performed by built-in SIEM system tools. We view this as a great advantage because we don't need to develop additional code, scripts, or integration modules. With ArcSight ESM, you can implement almost any SIEM use case."

The Commercial SOC Platform is Convenient, Fast, and Reliable

JSOC also greatly appreciates the stability of the Micro Focus SIEM system. "In eight years of operation, we've updated the version five or six times. I don't recall any incident that made it impossible to restore ArcSight ESM to normal operation," says Maxim Zhevnerev. "Moreover, we had to restore the SIEM system from a backup just once."

ArcSight ESM proved to be highly efficient in terms of resource consumption, Maxim says. For example, deployed on a 32-core server with 128 GB of RAM, ArcSight processes 50–55,000events per second.

Because of the simplicity and reliability of the system, JSOC staff spend a minimal amount of time supporting the existing ArcSight ESM installations, instead focusing on customer services and content expansion.

Most importantly for the MSSP/MDR, ArcSight ESM proved to be a convenient tool in terms of providing service to customers. Using ArcSight ESM, JSOC specialists can connect new customers very quickly—often within just three days. Provided a new customer already has a mature SecOps process, completing their service connection (including integration to all required sources, customization, and running the right scripts) takes 1-2 weeks.

"Business MSSP/MDR achieved full ROI by the end of the second year after commencing work with JSOC," recalls Vladimir Dryukov. "The ArcSight ESM licensing model for MSSPs is straightforward, transparent, and predictable. In my opinion, this is one of the most mature models on the market today. Using it, providers can easily create their own pricing scheme. Many other SIEM vendors do not seem to have such a convenient licensing model for MSSP/MDR."

ArcSight Will Be Used More in the Future

JSOC specialists are using many of the solutions' features and are expecting to expand the number of features used in the ArcSight product line in the future.

The company is considering implementing the ArcSight SOAR solution. JSOC experts expect to integrate it into the existing operating procedure.

Since JSOC has reached the point where a single data bus is required to distribute data flows across systems, another possible direction for technological development could be implementing the ArcSight Transformation Hub solution. The company's specialists are testing it at the moment.

The ArcSight ecosystem at JSOC will also continue to be developed. In particular, single centralized storage and content updates for all existing instances of the SIEM system will be organized.