MICRO FOCUS

Case Study
Security

NPC Ukrenergo

Micro Focus ArcSight drastically improves advance threat detection and response through cross-team collaboration and data-driven security analytics

Who is NPC Ukrenergo?

NPC Ukrenergo is a power company responsible for operational and technological control of the Ukrainian energy system and electricity transmission from generating plants to the distribution networks of the regional electricity suppliers. The company network includes eight regional power systems, covering the entire territory of Ukraine and employing over 8,000 people.

National Power Outage Following Cyberattack

A so-called BlackEnergy cyberattack on Ukraine's power grid took place in December 2015 and is considered to be the first known successful cyberattack on a power grid. Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to 230,000 end consumers for a period of one to six hours.

As a critical infrastructure company, this caused NPC Ukrenergo to closely examine its security processes, as Dmitriy Ryzhkov, Senior Information Security Analyst for NPC Ukrenergo explains: "When you need to protect industrial control systems, as we do, different rules apply. Availability and business continuity are paramount, as operations cannot be interrupted without major consequences to the general population. The systems are managed through operations and infrastructure teams, rather than IT teams, and comprehensive security management requires cross-team collaboration. Without this, and security solution support, these systems remain vulnerable to attacks."

"With Micro Focus ArcSight, we don't just detect real attacks quickly, but we also automate orchestrated responses in near-real time. The flexibility of ArcSight helps us intelligently adapt for the future."

DMITRIY RYZHKOV
Senior Information Security Analyst
NPC Ukrenergo

ArcSight Data Basis for Cross-Team Collaboration

Ultimately, the company realized it needed a Security Operations Centre (SOC); a centralized unit that manages security issues on an organizational and technical level. However, a comprehensive Security and Information Events Management (SIEM) solution would provide a great interim step for the organization to learn, protect itself against future attacks, and

UKRENERGO
National power company

At a Glance

- **Industry**
  Energy & Utilities
- **Location**
  Ukraine
- **Challenge**
  Protecting critical infrastructure from cyberattacks by creating visibility into threat data, and encouraging cross-team collaboration
- **Products and Services**
  Micro Focus ArcSight Enterprise Security Manager (ESM)
  Micro Focus ArcSight Logger
- **Critical Success Factors**
  + Improved cross-team collaboration
  + Increased visibility leading to improved alerting and incident response
  + Saved time through advanced capabilities such as scripting and automation
  + Achieved sophisticated vulnerability and risk assessment

> **"The ArcSight ESM data gave us a great platform to start cross-team collaboration, which was encouraged through executive support in the organization. We created dashboards that really pinpointed our vulnerabilities so that IT security, maintenance, and operations teams could work together to address this."**
>
> **DMITRIY RYZHKOV**
> Senior Information Security Analyst
> NPC Ukrenergo

increase its understanding of the elements that make up a SOC. Micro Focus ArcSight Enterprise Security Management (ESM) is widely known in the marketplace as providing powerful, efficient threat detection and response through security analytics, which is just what the team needed to get started.

NPC Ukrenergo started with an infrastructure assessment. "To implement an effective SIEM you need to have a full understanding of the infrastructure and IT systems operations," says Dmitriy. "What data logs are stored? What type of users have what level of access rights? We performed vulnerability scans on our environment to assess the risk level we need to address. The resulting data was then leveraged in a single Arcsight ESM console. It took time to grasp the ArcSight ESM capabilities for us, but once we did, we saw the flexibility and opportunity quite clearly. The ArcSight ESM data gave us a great platform to start cross-team collaboration, which was encouraged through executive support in the organization. We created dashboards that really pinpointed our vulnerabilities so that IT security, maintenance, and operations teams could work together to address this."

Security operators shared cybersecurity trends and information with each other and developed a best practice framework through which custom use cases were built. Adding more event sources to the SIEM was an important success factor. Leveraging ArcSight Flex Connectors, the team connected many data source types to collect, aggregate, clean, and enrich data before feeding it into security analytics. By structuring the data, ESM makes it both more useful and cost-effective. ArcSight Logger helps ease NPC Ukrenergo's compliance burden by preparing compliance documentation faster with built-in content, dashboards, and reports.

Multi-tier SOC for Real-Time Threat Management

As the framework organically grew into a SOC it started to include thread intelligence and incident response. A dashboard maps security events to the MITRE ATT&CK framework, adopted by NPC Ukrenergo. This knowledge base is a foundation for the development of specific threat models and methodologies. With more connected event sources, specific user behavior analytics, and the MITRE ATT&CK framework, the team added more advanced use cases, and the result was a clear risk assessment, more visibility, and improved alerting and incident response.

Following the MITRE principles, NPC Ukrenergo divided SOC responsibility into tiers, as explained by Dmitriy. "Using ArcSight ESM, we created a model with a Tier 1 lead taking responsibility for real-time monitoring and triaging of security events, vulnerability scanning, and emergency alerts. Tier 2 then takes up incident analysis, coordination, and response, as well as forensic artifact handling, and insider threat case support. A system administration lead focuses on the infrastructure operation and maintenance, and tool engineering and deployment. The final tier includes advanced capabilities such as scripting and automation which is a real time-saver for us. The teams work as one and intelligence is shared to help everyone."

He concludes: "Even the most secure organizations will experience a breach at some point. But what separates us now is how quickly we can detect a genuine threat and respond, because the longer a threat remains hidden, the more damage it does. With Micro Focus ArcSight, we don't just detect real attacks quickly, but we also automate orchestrated responses in near-real time. The flexibility of ArcSight helps us intelligently adapt for the future."