SEMplicity INC.

DATA SHEET

SEMplicity MSP

Enabling fast search and superior security log analytics with Elasticsearch and ArcSight

The problems with collecting, storing and accessing ever greater volumes of security logs for resource-intensive, higher level security analysis have long been sources of frustration for enterprise security professionals. But there is good news. The integration of the simple yet flexible Elastic Stack with Micro Focus ArcSight offers powerful and fast relief to Security Operations Center (SOC) managers and hunt teams who must navigate a rapidly expanding threat landscape.

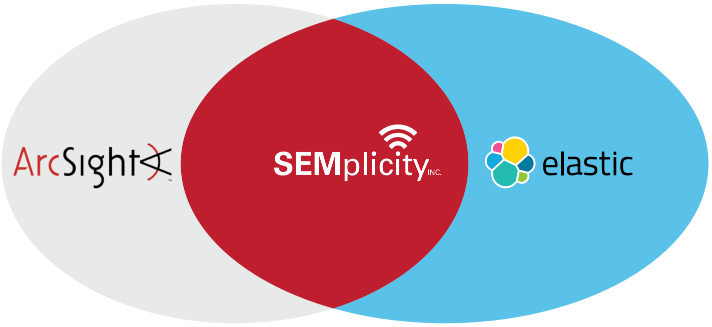
- Elastic is the company behind Elasticsearch, the open-source, extremely fast, broadly distributable, readily scalable, enterprise-grade search engine. Elastic develops the open-source Elastic Stack (Elasticsearch, Kibana, Beats and Logstash), X-Pack (including an array of commercial features) and Elastic Cloud Enterprise (a management suite for large on-prem and cloud-based deployments).
- ArcSight, through the use of Smart Connectors, ArcSight Data Platform (ADP) and Event Broker, provides foundational enterprise security software that collects, normalizes and enriches data and logs to provide analytics in the SOC.
- In September 2017, Elastic and Micro Focus announced a strategic partnership that enables ArcSight users to integrate SmartConnector log collection with the Elastic Stack via LogStash plug-ins and sample Kibana visualizations.

SEMplicity partners with Micro Focus and Elastic, combining skills to stand up ArcSight-Elastic Stack installations using the following technologies and expertise:

- ArcSight Data Platform (ADP): SmartConnectors, Logger and Enterprise Security Manager (ESM), Event Broker
- Elastic Stack: Logstash ArcSight module, Elasticsearch, Kibana
- Apache Kafka®
- Elastic X-Pack and a host of related open-source plugins for managing security and getting the greatest insights from your data
- Hardware and software tools and techniques to get you up and running efficiently, on-prem or in the cloud

SEMplicity connects the best of both worlds

The team at SEMplicity are ArcSight-Elastic experts. We understand how to leverage the strengths of your ArcSight infrastructure to integrate with Elastic Stack and achieve high volume log storage, fast search, cutting-edge visualizations in Kibana, machine-learning enablement and many other benefits.



Whatever your needs, SEMplicity delivers

We can help with the full range of ArcSight-Elastic Stack deployments, from on-prem managed services to cloud-based hosting, and from on-site and remote professional services to managed services that modernize and optimize your entire security log management implementation. With SEMplicity providing the know-how, and a full array of tools and support tailored to your use cases and architecture, you can:

- Ready Elasticsearch for partial or full-on production, so you can dig deeper with fast search and security log analytics
- Streamline operations and assure long-term cost certainty for your SIEM deployment

SEMplicity MSP ArcSight-Elastic Stack Integration Capabilities

Planning

- Needs analysis, sizing, proposed system architecture and functionality
- The full range of Elastic products licensed by SEMplicity are provided for your use, including Logstash, Elasticsearch, Kibana, full X-Pack and Elastic Cloud Enterprise.

Implementation

- Standing up appropriate storage and search capabilities, on-prem or in the cloud
- Onboarding all designated log sources, legacy rules and use cases
- Standard and customized dashboards based on identified use cases and fast, cutting-edge visualizations in Kibana
- Integrated authentication, authorization and auditing with role-based access control

Maintenance

- Skilled production technical support according to your requirements: 5x8, 5x10, 7x10 or 7x24
- Dashboards and alerting for monitoring infrastructure, showing all log storage metrics and detecting log-source disruption
- SLA-level monitoring, storage, reporting and ongoing capacity planning

Extensions

- Roadmap for and implementation of advanced features such as alerting, longitudinal correlation and machine learning
- Elastic fast search and analysis training for SOC analysts
- Knowledge transfer to your team on large volume Elastic log storage

The Benefits of SEMplicity MSP

Cost control	Faster access to security data	Open source advantages	Fully modern, scalable stack
By outsourcing the management of your ArcSight-Elastic Stack integration to SEMplicity, you can significantly lower the total cost of ownership and redeploy resources to higher-value activities.	With SEMplicity standing up your log storage and search infrastructure — on-prem or in the cloud — you can focus on more interesting uses of your security log data, including analytics and correlation.	Leveraging SEMplicity and the open Elastic Stack means your log data is now stored in a commonly used, open format and will be perfectly positioned whatever new cutting-edge log detection technology appears down the road.	Using our approach to storing, accessing and fast-searching huge log volumes in Elasticsearch, as well as extending your log analysis via Kibana, alerting, and machine learning, you achieve an adaptive, modern, resilient and cost-effective log management deployment.

About SEMplicity

SEMplicity is a managed security service provider (MSSP) and consulting firm that specializes in large enterprise log management, searching, correlation and analytics. We are one of the largest Micro Focus Enterprise Security Services Partners, and an Elastic-licensed Managed Service Provider (MSP). Since 2010, we have architected and implemented ArcSight at dozens of the world's largest corporations, including many Fortune 500 companies. Our security engineers are recognized experts in massive deployments of secure log storage and fast log searching using best-in-class proprietary and open-source tools.

For an initial consultation or to schedule a proof of concept, please contact
Doug Calenda, Director of Sales, at 978.427.2989, or email info@semplicityinc.com.

semplicityinc.com