Managed Infrastructure Services

Our managed infrastructure subscription is a partnership between SEMplicity and HPE Professional Services. It provides clients with the security of knowing their ArcSight infrastructure is always monitored, up-to-date and running smoothly. Periodic health checks, constant monitoring, timely problem resolution, on-call response, scheduled product updates and event flow anomaly detection all combine into a monthly subscription offering efficiency, cost certainty and proven ArcSight expertise exactly when and where you need it.

ArcSight – how will you care for it?

ArcSight is the most powerful SIEM on the market, with a broad and complex technology stack. To provide value, it needs proper care and feeding. Storage and network log traffic require monitoring to anticipate problems before they manifest. Hardware and software require periodic upgrades. Event volumes fluctuate, requiring adjustments and tuning. Log sources change, requiring fixes to ESM content and parsing. For many clients, dedicated full-time ArcSight engineering resources are not feasible or too expensive. Nor are they necessary! With our Managed Infrastructure Service, you can subscribe to defined ArcSight ESM services to keep your implementation current, optimized, monitored and documented. Now, you can be sure you are getting all the value a well-maintained and dynamic ArcSight implementation provides. Now, your ArcSight security experts can focus on creating new content to detect emerging threats specific to your environment.

Managed Infrastructure Service – another problem solved.

Our Managed Infrastructure subscription service provides maintenance, monitoring, tuning, problem diagnosis and remediation across the entire ArcSight technology stack. This subscription optionally may also fix broken ESM content, fix parsing problems, monitor critical log sources and onboard a specified number of new log sources per month. It includes implementation of proprietary SEMplicity content, developed to optimize your implementation, detect issues that may become outages and sniff out log flow disruption. Deliverables include monthly reports summarizing your current ArcSight infrastructure, scheduled and completed maintenance, problems reported, upcoming resource constraints and a roadmap for next month's objectives. Here are some of the services this subscription provides:

Service	Benefits

Monthly ArcSight meeting & infrastructure report	Present current state of ArcSight ESM implementation, report on activities in previous month, set objectives for next month, enumerate current infrastructure.
Upgrade ESMs, Connectors & Loggers	Keep your infrastructure at the appropriate release level within a version, and apply all necessary patches and hotfixes. Track licenses, request and install new licenses.
Proactively monitor system health	Periodically, check all SmartConnectors, Loggers and ESMs for potential problems, especially upcoming resource constraints. Remediate and report.
Detect ArcSight device outages	Use SEMplicity content to detect ArcSight device outages and anomalies in real time. Diagnose, report, and remediate or escalate.
Respond to reported problems	Respond to reported ArcSight problems throughout the technology stack, especially outages, log flow spikes or lulls. Diagnose the problem and remediate or escalate.
Respond to ESM content problems.	Diagnose reported problems with existing ESM content no longer working as expected. Remediate or escalate as required.
Optional: monitor critical log sources	Based on input from the client, monitor a specified list of critical log sources for log flow disruption and other anomalies.
Optional: onboard and sunset SmartConnectors	Onboard a specified number of new SmartConnectors per month. De-install obsolete SmartConnectors, by request.
Optional: modify SmartConnector parsing	Create parser overrides and/or 2nd-level regex parsers, modify categorization, implement map files.
Optional: implement new ActionConnector tools	Install and test additional tools developed by the client for the ActionConnector (also called CounterACT). Create integration commands as requested.

Our optional services may be incorporated into your monthly subscription package. These services make it easy to enhance and expand your ArcSight infrastructure using known resources and leveraging our existing services agreement. All this adds up to an offering which enables you to focus on the today's dynamic threat landscape, knowing your ArcSight infrastructure is up-to-date, monitored, running smoothly and supported by on call, proactive resources who are ready to assist.

page 3

STANDARD DELIVERABLES

- A monthly report enumerating current ArcSight infrastructure, including all log sources, ArcSight Connectors, ArcSight Loggers and Managers. Also details current active monitoring and reporting.
- A monthly report detailing tasks performed, roadmap, detected and potential health problems and resource constraints.
- Access to our real-time problem tracking system to view progress on reported and detected issues.

REQUIREMENTS

- Remote VPN access, credentials and access to all hosts running ArcSight.
- Two hours initial with current knowledgeable ArcSight resources to gather initial requirements, scope the project and product an infrastructure report.
- One hour monthly meeting with ArcSight resources to review accomplishments and set objectives.

LIMITIATIONS

- We will keep all ArcSight infrastructure at the current release level within a version. Entirely new ESM and Logger versions may require additional hours from HPE ArcSight professional services.
- We will always attempt to diagnose and remediate ArcSight problems ourselves. Some problems (such as log flow disruption due to a firewall rule) require escalation to internal resources. Other problems may require opening an ArcSight support ticket. In these cases, we will escalate, follow-up and track the problem to its resolution.
- Requires balanced HPE support agreement.

How to proceed...

If our Managed Infrastructure Service subscription sounds exactly like what you need, please contact your HPE Enterprise Security Products salesperson professional services representative. Or contact us directly.