Operations Monitoring

Let Logpoint experts keep your SIEM+SOAR solution stable, reliable, and operating optimally, while focusing your resources on your organization's security.

/logpoint

Why you need Operations Monitoring

- **Save up to 50% of your time on maintenance tasks**
  Leave the system operations in our hands and focus your resources on high-priority tasks like incident response and threat hunting

- **Keep your Logpoint platform optimized**
  Our dedicated team will keep your Logpoint platform continuously up to date, stable and reliable

- **Get reviews and advice from our experts**
  Our experts can help you with dashboards, queries, reports, and hardware requirements

- **Get monthly concluding reports**
  Get a monthly overview of operational health, incident overview, and support tickets

- **A dedicated support team**
  We handle the maintenance, reducing the number of support tickets and solving challenges quickly

To protect your organization from threats, your SIEM+SOAR solution needs to be fully operational. Our proactive support, platform monitoring, and maintenance services observe the health and status of the system, helping to detect and prevent failures. Our experts provide system checks, solve issues quickly, and give advice for improved performance. We keep your Logpoint platform fully optimized, help to detect and prevent failures, and ensure maximum availability. Operations Monitoring saves up your time spent on system maintenance and frees up valuable resources, so you can focus on other high-priority tasks.

Keep your system fully monitored and up to date at a predictable price

The cost of our Operations Monitoring is based on the number of nodes – devices sending data, like our SIEM solution. You can avoid unexpected costs with True Predictive Pricing, as the price will stay the same regardless of data volume. Secure your organization to the maximum with Logpoint, without worries of unpredictable costs.

An overview of what you get with Operations Monitoring

Logpoint, OS, and hardware monitoring	•
Recommendations for improved performance	•
Creation and management of support tickets	•
Monthly reports on operational status, performance analysis, and tuning suggestions	•
Logpoint upgrade assistance	•
Automatic system checks and performance alerts identification	Every 5-10 minutes, 24/7
Manual system checks	Once a day
Service hours	While proactive monitoring is delivered 24/7/365, the incident response is dictated by the level of support package (9-5 or 24/7)
Price	Included in Converged SIEM subscription plan Otherwise, pricing based on your SIEM size

/logpoint

What is included in our monitoring services

Regular system checks covered by the Logpoint Operations and Monitoring team

Subject	Monitor/Check
System	Resource shortage/queueing check on CPU, Memory, Disk and Network (swapping, disk queue, queues on networks, dropped packets, etc.)
Hardware status	Check management system logs (only possible when hardware management module is present)
Logpoint service health	Service log check; Service crash/restarts, GC frequency, performance
Logpoint component connectivity	DLP and LPC Connection status Queueing due to connection, configuration, or resource issues
Dashboard widgets & alerts	Status, connectivity, capacity, queueing – verifying functionality of underlying Logpoint components and system
Report	Status on scheduled reports – verifying functionality of underlying Logpoint components and system
Log collection and storage	Status on collection – verifying functionality of underlying Logpoint components and system
Backup	Status of scheduled backups
Storage capacity	Disk usage monitoring
License monitoring	Notify the customer when it is time to renew the license

Additional system checks delivered as part of the service

Subject	Review
Live search query review	Review all queries used in live searches (dashboard widgets and alerts) and suggest optimizations/improvements
Report search query review	Review all queries used in reports and suggest optimizations and improvements
Logpoint service health check	Check memory and thread configuration of JVM and other technology components like number of logs per repo, normalizer performance (policy configs, etc.) and suggest optimizations and improvements
Capacity review/planning	Check current capacity of system and suggest immediate capacity requirements based on current status; Suggest future capacity requirements based on observations of growth in number of logs/storage etc.
Architecture review/planning	Check if the system is configured to meet the demands (e.g. LPC, DLP scaleout, loadbalancer, search head, isolating or distributing log sources, etc.)
Logpoint version assessment and upgrade	Review, recommendation, and planning of Logpoint upgrade to the latest recommended release (patch) with all used integrations. Upgrade is planned and executed by operations team in coordination with the customer.

For more information, contact LogPoint:
https://www.logpoint.com/en/contact/