

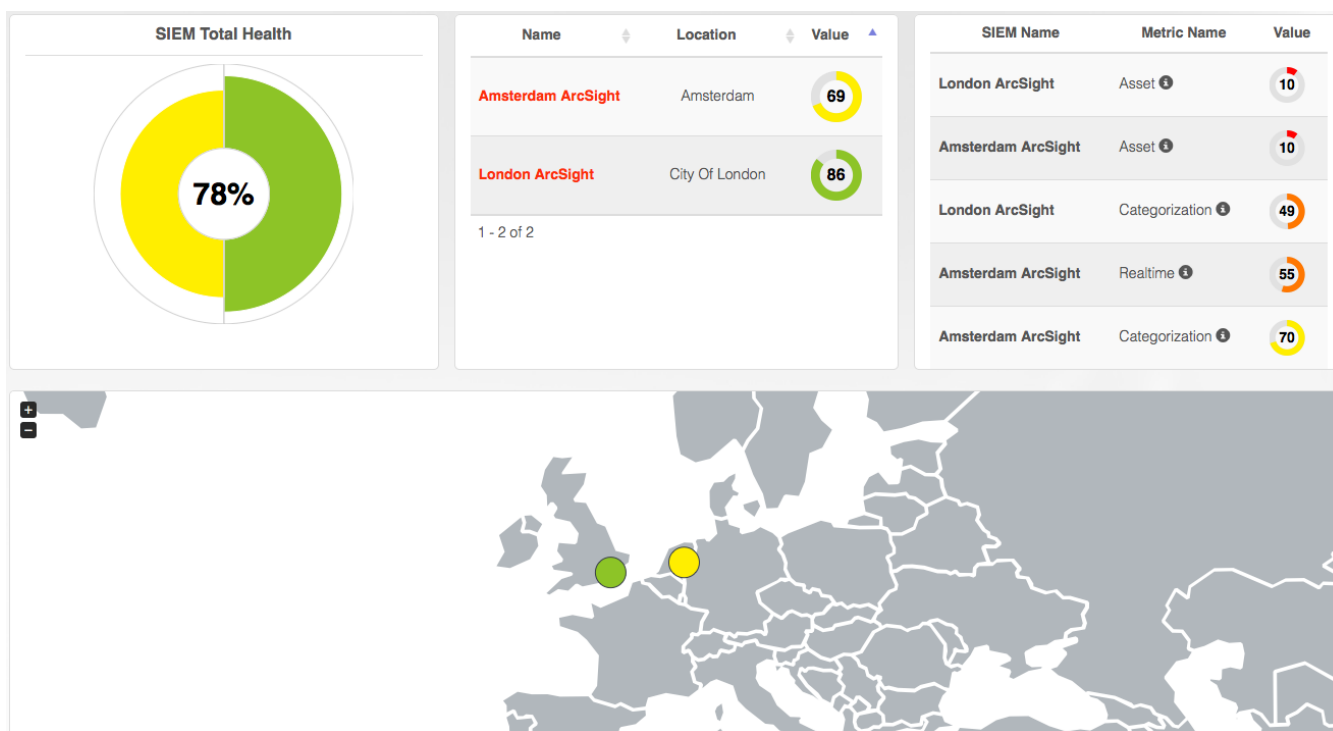
## Enabling Next Generation of Security Operations Center

### Business Value and efficiency of SIEM & SOC are still a challenge

SOC team is too dependent on Support and has to waste valuable time waiting for their answer? Having a hard time measuring ROI and prioritizing SIEM & SOC investments? Don't have evidence of stable SIEM operation? Can't guarantee efficiency of internal controls for your incident management process? Management doesn't have metrics to measure SIEM/SOC team performance?

### Enable transparent Security Operations and return on your SIEM Investment

Empower your organization's security by establishing a common ground between Executive Board, SOC Management and SIEM experts. Reduce Time to Solution from days to minutes, stop reacting to issues – predict & prevent them! Automate the routine processes of SIEM experts to free up their time to actually act on Threats detection, investigation and response instead of wasting it on SIEM tuning. Implement KPIs and operational transparency clear for both SOC team and management.



### Key Benefits

- ✓ Full visibility & easy exploration of SIEM environment
- ✓ Routine SIEM processes automation
- ✓ Early issue detection
- ✓ Multi-tenant, multi-tier, geo-distributed and multi-vendor SIEM deployments
- ✓ Ultra-low hardware requirements
- ✓ Production ready in < 1 hour
- ✓ Take it for a spin, Free of charge

### Business Advantages

- ✓ Man-hour savings
- ✓ License efficiency & savings
- ✓ Smart prioritization of SIEM & SOC investments
- ✓ KPIs and operational transparency for SOC team and management



## Success Criteria for Enterprise SOC Visibility for Executive Board, Increase operations efficiency & decrease TCO

### Man-hour savings as an effect of Predictive Maintenance

- ✓ on issue detection
- ✓ on solution discovery
- ✓ on solution QA and FIX

Category: DNS Priority: 8  
Cannot find information for [HOST]

03.02.2016 17:34:37

Error Name: Cannot find information for [HOST]  
Error Type: WARN  
Error Category: DNS  
Priority: 8  
Count: 847

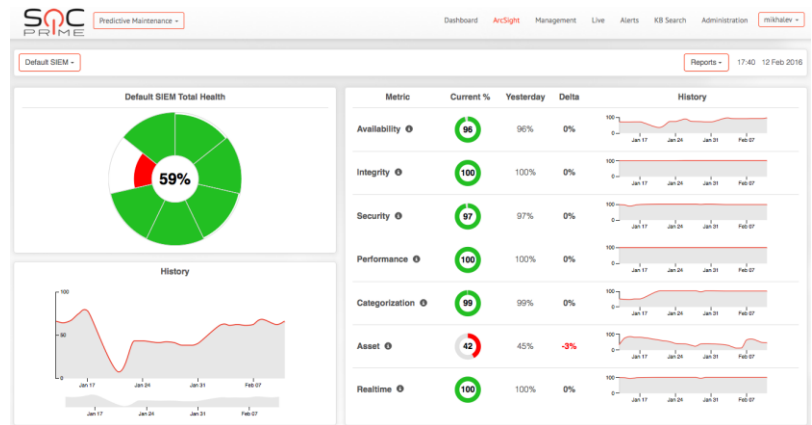
Description: Error occurs if SmartConnector received a message with field that contains Source (Destination) Address / Source (Destination) Host Name that could not be resolved.

Solution: ★★★★★ Perform the following actions on the server where the connector is installed: 1) Check availability of DNS server (ping / telnet). 2) Execute DNS query manually (nslookup). 3) Check if necessary records are available on DNS server and add them if necessary. 4) If not necessary you can disable resolving on the connector. A detailed guide is available from HP Protect link. If you have a lot of these issues - see Advanced Remediation report for DNS.

External Sources: [Protect724](#) [HP KB](#) [Submit Solution](#) [Expert Fix](#)

### Operational efficiency as an effect of Predictive Maintenance

- ✓ KPI on system uptime / availability
- ✓ Internal SLA measurement / adherence



### License efficiency & savings as an effect of Predictive Maintenance

- ✓ Increase of amount of monitored devices per SIEM expert / administrator
- ✓ Increase of SIEM Data quality per EUR spent

Status	Name	Health	Availability	Security	Integrity	Performance	Categorization	Realtime	Memory (MB)	EPS	Full GC
⊖	AmLight Logger (SHOST-IP)	39	0	100	100	100	100	100	5884	0	⊖
⊕	WUC	52.87	100	100	99	100	100	33	159	0.05	⊖
⊕	CheckPoint_FW	71.44	100	100	99	100	44	80	155	0.09	⊖
⊕	SyslogGDP	69.52	100	100	98	100	43	95	147	0.79	⊖
⊕	Syslog-UDP-514-ConnApp	81.6	95	98	100	100	44	100	124	0.04	⊖

Errors on SyslogGDP

Category: Network Priority: 9  
No route to host

Error Name: No route to host  
Error Type: ERROR  
Error Category: Network  
Priority: 9  
Count: 1489

Description: Problems with communication between the connector and the host.

Solution: 1) A manual diagnostic procedure needs to be performed on the server where the connector is installed. 2) Check the network connectivity to the host (ping / telnet). 3) Ensure that the SmartConnector correctly receives remote host name. 4) Check the routing, the default route and the direct route to the host (command route). 5) Check the physical connections of the network infrastructure in the relevant part of the network.

SOC Prime provides Cyber Operations platform that empowers Enterprise, MSSP and Public organizations to proactively defend against ever-changing cyber threats. Backed by the team of cyber security professionals with combined experience of 120y+ in the industry and practical knowledge of implementing more than 50 SIEM & VM projects. SOC Prime is HPE Technical Alliance, IBM Security, Splunk and QualysGuard API Developer partner.

