Product Brief I SIEM Predictive Maintenance

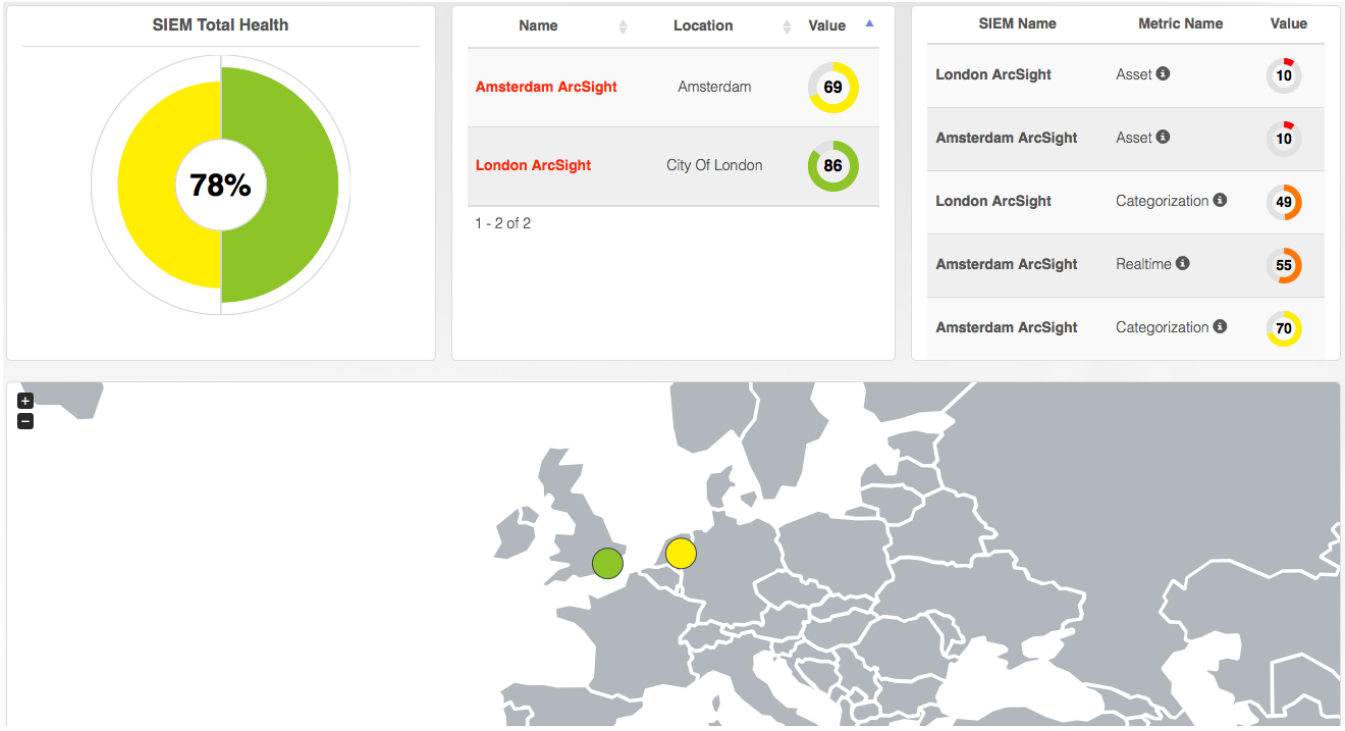
Enabling Next Generation of Security Operations Center

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

© SOC Prime, SOC Prime Logo are registered trademarks of SOC Prime.
All other trademarks are the property of their respective owners

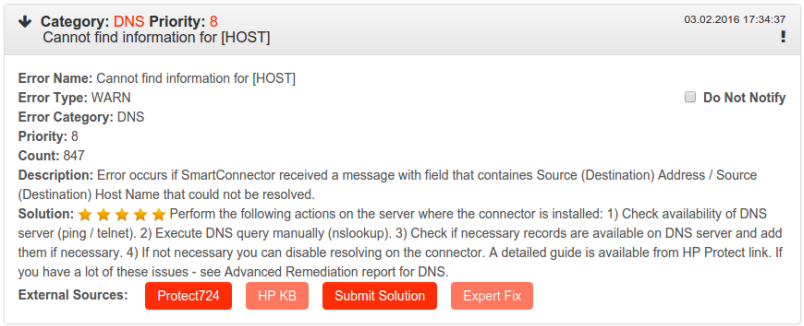
+44 203 769 33 84 sales@socprime.com socprime.com

Product Brief I SIEM Predictive Maintenance

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

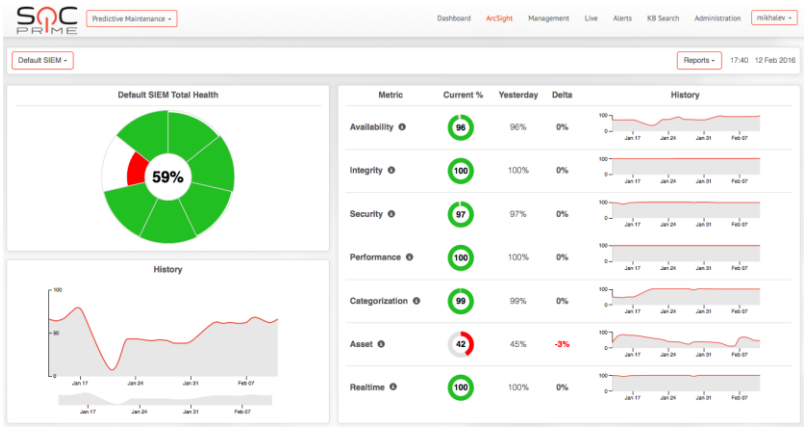
Man-hour savings as an effect of Predictive Maintenance

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



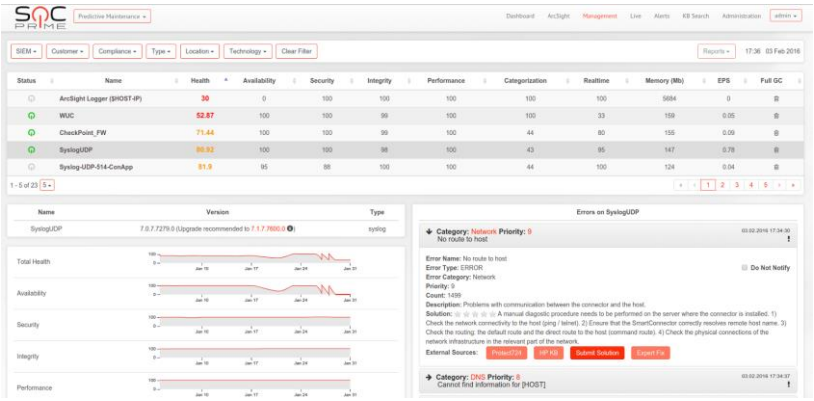
Operational efficiency as an effect of Predictive Maintenance

- ✓ 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



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.

© SOC Prime, SOC Prime Logo are registered trademarks of SOC Prime.
All other trademarks are the property of their respective owners

+44 203 769 33 84 sales@socprime.com socprime.com