MANAGED SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Managed SIEM: making security *SIEMple*

Security is a responsibility that is hard to keep up with. Not only are companies seeing exponential increases in the sheer volume of threats, but the complexity of those threats is dramatically rising as well. Attempts to counteract this evolving threat landscape have led to a proliferation of security devices that can actually obscure visibility, and ultimately, real threats. The data collected from those devices can be cumbersome to manage without common visibility. Yet IT departments are under pressure to demonstrate the value of security investments.

That is where Security Information and Event Management (SIEM), a big data security technology, can provide the answer. However, companies that have gone through the arduous process of implementing their own SIEM understand the challenges all too well. Without adequate up-front planning, appropriate staffing, and security expertise, SIEM implementations often turn into expensive shelfware or glorified logging platforms, while offering little to enhance a company's true security posture.

The Sungard Availability Services Managed SIEM (MSIEM) solution directly addresses these challenges by simplifying the security information management process. We utilize a highly sophisticated SIEM engine that performs patented, real-time analytics to provide enhanced visibility into the threats facing your environment. We assist with platform installation and creation of custom rules to optimize threat detection. Finally, we provide a world-class team of certified security analysts who monitor security events on your behalf 24x7, assist you with incident response, and regularly collaborate with you to further enhance situational awareness. What's more, global threat intelligence is gathered from around the world and updated daily to help you detect new and evolving threats.

You still retain control by having full access to the SIEM tool through a dedicated portal and a broad variety of centralized reporting capabilities to satisfy your compliance needs.

MSIEM At-a-Glance

A SIEM platform centrally collects data from multiple devices on your network, including your existing security appliances. Through an advanced correlation engine, it is able to proactively identify security events not otherwise detected by standalone security technology.

However, SIEM solutions are complex, costly, and notoriously difficult for companies to install and manage.

The Sungard AS MSIEM offering provides you with platform implementation, correlation rules tuning, active monitoring, and incident management in a simple managed service.

MSIEM Benefits

- Manages evolving threats proactively
- Provides confidence in closing gap between perceived and actual security
- Accelerates time-to-value
- Maximizes value of security investments
- Frees IT staff to focus on business initiatives
- Provides single-pane-of-glass visibility across heterogeneous devices
- Reduces audit effort and expense for PCI, HIPAA, and other standards
- Access to security professionals and expertise

SUNGARD®
AVAILABILITY
SERVICES™

DATA SHEET

Sungard AS Managed SIEM Offers:

Meaningful intelligence and rapid data retrieval

- Supported by a powerful SIEM correlation engine, capable of processing massive amounts of data to build situational awareness and real-time understanding of threat risks and countermeasures
- When seconds are crucial, the SIEM engine rapidly retrieves the data required for investigation and remediation rather than days as is for other tools

Global threat intelligence (GTI) allows for pro-active detection of new threats

- Database of 130 million IP addresses provides accurate, up-to-date understanding of the global threat landscape and threat signatures
- Immediately identifies when any node on your network is communicating with a suspicious or known bad actor and quickly determines the threat's path

Certified security experts and Security Operation Centers (SOCs) extend your security team and capability

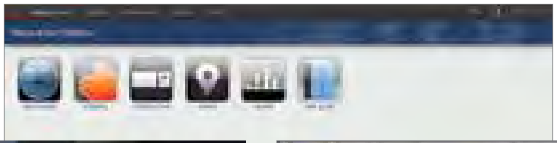
- Included in solution is installation of SIEM platform, building of correlation rules, and tuning to specifically suit your environment
- Certified security analysts with SIEM expertise actively monitor for alerts on your behalf 24/7
- Assistance for incident response and root cause analysis
- Platform is regularly updated with new rules based on evolving best practices and threat landscape
- Periodic ongoing customer collaboration sessions build additional situational awareness of your environment

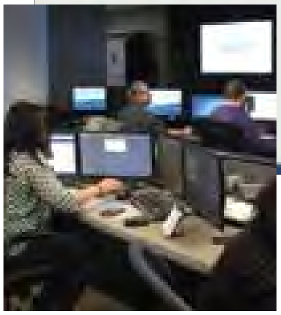
Reduce audit effort and expense for multiple regulations

- Translates machine activities into understandable business events – reducing need to manually parse and decipher data
- Consolidates audit and compliance transactions for over 240 regulations (including PCI, HIPAA, etc.) within a single pane of glass for continuous governance and rapid reporting

Exceptional value

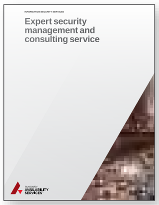
- Professional installation and tuning means accelerated time-to-value
- Intuitive to use and easily extensible to support new data sources and evolving requirements
- Requires no initial capital outlay
- Predictable monthly costs for a level of technology access otherwise only possible through large up-front investments





Additional reading

[4 Steps To Taking Control With Cyber Resilience](#)



Expert security management and consulting service

[Information Security Services](#)

To learn more

To learn more about Sungard AS Managed Security Services, visit **www.sungardas.com/security**.

About Sungard Availability Services

Sungard Availability Services provides managed IT services, information availability consulting services, business continuity management software, and disaster recovery services.

To learn more, visit **www.sungardas.com** or call 1-888-270-3657

Trademark information

Sungard Availability Services is a trademark of SunGard Data Systems Inc. or its affiliate used under license. The Sungard Availability Services logo by itself is a trademark of Sungard Availability Services Capital, Inc. or its affiliate. All other trade names are trademarks or registered trademarks of their respective holders.

Connect with Us

© 2014 Sungard Availability Services, all rights reserved. SEL-239 1014