

Security Information and Event Management: Getting Started with Sentinel Enterprise

Protecting critical information is an ongoing challenge. Micro Focus offers the first identity-enabled, automated security monitoring platform, backed by a team of expert consultants. We help you build a powerful security and information event management (SIEM) and log management foundation that monitors and manages security devices, logs and activities.

Sentinel at a Glance:

■ Sentinel Enterprise Is Ready to Help You:

- Manage security events across a complete range of devices and activities.
- Monitor and audit your Identity Manager solution.
- Meet your most demanding compliance requirements.

Faster, More Efficient Risk Management

For the most efficient next-generation SIEM solution, look to IT Consulting or one of its global partners. We offer on-site consulting engagements to help you plan, deploy and customize a log management solution that matches your business requirements, working with your existing technology infrastructure. A more in-depth NetIQ® Sentinel™ Enterprise Standard Deployment engagement will enable you to complete your SIEM architecture.

Log Management Made Easy

Monitoring and managing logs from multiple sources can be complex and overwhelming. NetIQ Sentinel Log Manager addresses these challenges, providing storage, data management, reporting and search capabilities for organizations' system logs. IT Consulting offers a variety of targeted consulting engagements. These include:

Sentinel Log Manager planning and assessment: A three-day engagement that provides a quick, high-level overview of Sentinel Log Manager's capabilities for addressing business, security and technical issues. We follow an analysis of your existing security architecture with suggestions to integrate network resources and access policies into a comprehensive event monitoring and response solution.

Sentinel Log Manager implementation: A week-long engagement that's ideal for organizations with pressing compliance needs—or those that just want to get started immediately. Select up to five collectors from our predefined collector list and work with experienced consultants to perform the best deployment for your environment.

Custom development: Customize the Sentinel Log Manager open architecture to connect to virtually any data source and provides nearly limitless options for custom reports. This engagement helps you fine-tune the product for full integration within your local policies and procedures.

Sentinel Enterprise Standard Deployment Engagement

Sentinel Enterprise provides one of the most robust and functional SIEM solutions. The Sentinel Enterprise Standard Deployment engagement helps you plan, build and deploy a SIEM solution that meets your objectives and maximizes your investment in our technology. This engagement includes:

- **Assessment and recommendations:** An analysis of your requirements identifies key business drivers and defines critical compliance and regulatory standards.
- **Production deployment road mapping:** Your consulting team will develop a detailed production roadmap that identifies event

Our IT Consulting team and partners will quickly guide you toward a simple, integrated SIEM solution. Start taking advantage of our proven expertise, tools and methodologies—contact your local representative or partner today.

Contact us at:
www.microfocus.com

Like what you read? Share it.



sources, connection methodologies and component capacity specifications; defines system component implementation and rollback plans; and finalizes testing plans.

■ **Pilot implementation of Sentinel**

Enterprise: After lab implementation and testing, your team will deploy a pilot of the solution into your production

environment. This step connects a representative group of devices to the Sentinel Enterprise SIEM solution and tests the range of functionality.

- **Knowledge transfer:** The final step features a walkthrough of the architectural components, roadmap and implementation plan with select members of your IT staff.