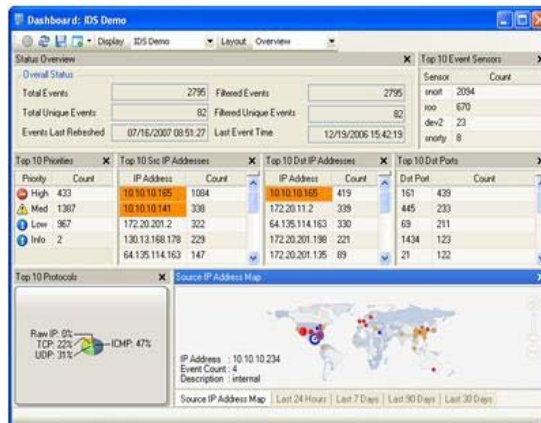


# Activeworx Snort Management (SMC)

a unified security information and log management platform

## ACTIVEXORX ENTERPRISE

- Log Center
- Security Center
- Event Manager
- **SNORT MANAGEMENT**



### Ease of use

SMC's powerful interface is designed for ease of use, so time can be spent on the actual events of interest.

### Save time

SMC contains all the tools necessary for an IDS administrator to quickly identify and respond to events of interest.

### Save money

SMC is a very cost effective solution, starting at less than \$400 per sensor.

Activeworx Snort Management Center (SMC), is a robust, user friendly and cost effective solution for effective management of complex Snort installations. SMC gives users a greater understanding of the reality of their security posture with easy and immediate access to packet headers and payloads, event correlation, and access to on-line intrusion identification information from within the interface.

Visualize intrusion information with easy to understand graphs, charts, geographical maps, and event diagrams, and a comprehensive reporting engine. Quickly view, disable or set suppression for a single rule on a single sensor, or to deploy a rule change to all Snort sensors from a centralized interface, while viewing information about an event that is currently triggering, within the same console view.

Tight integration with the Snort IDS back-end database allows SMC to collect information from existing Snort IDS installations with no modification of the original database schema. Whether it's a new installation or one that has been in place for years, there is no more complete, less intrusive, or more cost effective centralized management console for Snort.

# Features and Benefits

## TECHNICAL SUPPORT

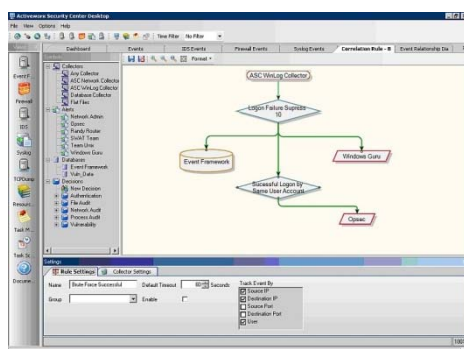
24 Stunden technischer Support durch Knowledgebase des Herstellers.

Telefonischer technischer Support während der Geschäftszeiten oder per E-Mail an:

support@activesphere.net

## ZERO DOWNTIME

Ständige Verfügbarkeit des Supports durch ein weltweites Partnernetzwerk in über 40 verschiedenen Ländern geben telefonisch und per E-Mail Unterstützung in der Landessprache



## Tight Integration with Snort®

Activeworx SMC integrates tightly with the Snort® IDS event database to provide high valued information from your existing Snort® IDS installations, without modifying the original database schema. Whether it's a new Snort® installation or one that has been in place for years with 10's of millions of events, there is no other complete, less intrusive, and less expensive centralized management console for Snort.

## Centralized Management of Snort® Policies

Activeworx SMC™ allows administrators to view, disable or set suppression for a single rule on a single sensor, or to deploy a rule change to all Snort sensors.

## Comprehensive Reporting

Activeworx SMC includes a built-in Report Center to provide intelligence on incidents of interest.

## Flexible Dashboards

Activeworx SMC™ event dashboards are completely customizable. Users have the ability to choose from over 50 different panels to display information and save multiple layouts. The event dashboards provide multiple charts and graphs to visualize information. Each interactive view has the ability to drill down and see the events, perform search correlations, run custom commands on context sensitive values, copy charts into a report and customize charts to better view data.

## Event Visualization

Activeworx SMC™ has a powerful diagram engine that displays events and the relationship between them. Once these events are displayed, you can replay the order in which they occurred, color code the events to highlight different characteristics, perform different types of auto layouts to change the way in which the events are being displayed, or drill down into the events to gather more details.

## Strong Forensic Tool

Activeworx SMC™ enables easy drill down into event information and interactive graphs to provide vital details to help investigate threats and attacks. Activeworx SMC™ also includes a packet payload decoder to enable viewing into the decoded payload from IDS events, and correlation of information among different databases.

## Integrated IP Tools

To get a better understanding about an attacker, Activeworx SMC™ includes a collection of IP tools that are integrated into the product. Tools such as Whois, Ping, Traceroute, NSLookup and geographical lookup are just a click away.