



# REM™ Security Management Console

## Centralized Management and Reporting

Organizations of all sizes rely on the accuracy and integrity of their security information to make efficient, informed decisions when securing their networks. Data returned by vulnerability assessment scanners, network traffic analyzers, and other proactive security components needs to be centrally managed with the confidence that the data is complete and up to date.

REM™ is an enterprise-ready solution for the collection, reporting, and remediation management of security events affecting your network. Regardless of the size or configuration of your network, REM provides a centralized console to manage task delegation and enable efficient review of remediation efforts. Automatic filtering of security events based on location, reporting engine and severity allows for quick and easy delegation of assignments based on your organization's resources.

REM extends your resources by enabling security professionals to create and enforce security policies, schedule and perform vulnerability audits, remediate issues, verify corrective actions, and report on the entire network threat management process. This enterprise security solution provides a complete and efficient way to bring security and IT administrators together under the same workflow umbrella.

### Logical Network Security Management

REM allows security administrators to divide the network into logical, manageable segments. This allows you to focus the appropriate resources and attention on strategic assets within a network. Segments can be created based on department, affected business processes or hardware groupings.

### Centralized Management of Security Applications and Events

Organizations can securely transfer security events (e.g. detected network vulnerability issues) from distributed scanning machines to one centralized location. REM connects with the various product engines via PKI-encrypted channels to collect, store and analyze security data.

### Automated Task Assignment

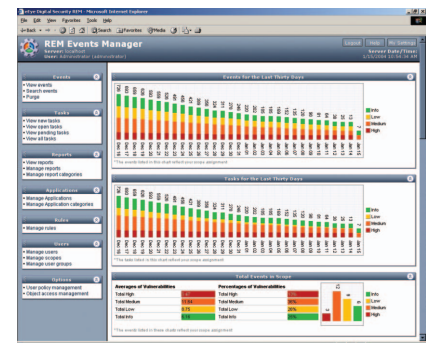
Using REM's rule-based system, security events can be automatically evaluated and assigned to the appropriate resource for remediation. Issues that are uncovered become a security event and are entered into REM's centralized ticketing system. As appropriate, these events can be elevated to tasks and assigned to a user for remediation. REM's open architecture also allows for these events to be integrated with enterprise help desk/trouble-ticketing systems.

### Integration with Events Management Systems

REM's open architecture enables full integration with an organization's existing third-party management system, such as CA Unicenter®, HP OpenView and IBM® Tivoli®.

### Fast Facts

- Browser-based console allows for enterprise-wide management and remediation of network vulnerabilities
- Role-based access configuration for IT personnel and security administrators
- Open architecture allows for integration with third-party platforms and management systems
- PKI-enabled for secure data transfer via encrypted channels
- Scalable for implementation in large, clustered database environments



eEye Digital Security®



# REM™ Security Management Console

## Additional Features and Benefits

- **Advanced Workflow Based on Scopes and Roles**  
REM enables IT organizations to establish roles and responsibilities to accurately reflect the organization's resource structure. This allows enterprise administrators to establish the network authority granted to each team. In order to replicate the logical layout and segmentation of your network, REM also allows for the creation of defined scopes. Scopes permit those tasked with assessment and remediation the ability to review the event data originating from their respective network locations.
- **Intelligent Event Ticketing**  
To remedy an overload of data, REM has an intuitive rules wizard that allows administrators to proactively delegate tasks by filtering issues based on type, origin and severity. This eliminates staff dependency on management for disseminating assignments and facilitates more efficient and accurate remediation.
- **Encryption and Authentication**  
REM incorporates a built-in PKI infrastructure for quick installation of certificates and private key material. Industry standard X.509 certificates in XDA and PKCS#12 formats are also supported for compatibility with existing PKI infrastructure.
- **Open Database Compliance**  
REM is ODBC compliant for high-capacity storage of all network security events. REM enables querying directly into its data store provided the appropriate access controls are available
- **Comprehensive Remediation Management**  
Events can be elevated to tasks via the REM interface and/or rules system. Once a task is assigned, its progress can be tracked and verified. Full instructions on corrective actions are detailed within each ticket to assure accurate remediation of network vulnerabilities.
- **Detailed Reporting**  
Users can track assignments and progress from all parts of the security organization using REM's charts and reports. Executive reports allow for an instant network threat level assessment at a glance and the progress made in correcting various security issues. Management reports enable a view of the network's overall security posture. Administrators can access detailed information pertaining to their assignments and review the progress of their efforts. A sampling of some reports include:
  - *Audit Reports by Name*  
Audit reports show in-depth information about each vulnerability that was found on the network along with information about the steps needed to correct the issue. The reports are grouped either by name or by IP, and it is possible to view lists of all machines affected by individual vulnerabilities.
  - *Delta Reports by IP Delta*  
Delta reports show a side-by-side comparison of vulnerability assessments to show progress made by remediation efforts. It also allows the administrator to view network security issues that have failed to be corrected.
  - *Top 20 Reports*  
Reports are available to help profile the devices that exist on the network. Understanding the most common operating systems, ports, services, and users can be useful in determining strategies for IT security efforts.

## System Requirements

- Microsoft Windows 2000 Server with Service Pack 4 / 2 Windows Updates or above, Microsoft Windows 2003 Server
- Microsoft SQL 2000 Server with Service Pack 3 - Internet Explorer 5.51 or above
- Microsoft IIS Server

## About eEye Digital Security

eEye Digital Security is a leading developer of network security products that deliver unsurpassed levels of vulnerability protection before, during and after malicious attacks. Driven by the world-renowned eEye Research Team, the company has won numerous awards and recognition in the field of network security, including the recent top 10 recognition in the Red Herring Top 100 Innovators awards for 2004. A global company with offices, partners and distribution channels around the world, eEye helps protect the digital assets of major corporations, educational institutions, and government entities in over 80 countries.

eEye Digital Security  
www.eEye.com

U.S. Tel: 1.866.339.3732  
N. America: 1.949.900.4100  
Geneva: +41 22.718.7700  
London: +44 (0) 208.956.2270

N. America: sales@eeye.com  
International: sales.eu@eeye.com



eEye Digital Security®

VULNERABILITY IS OVER