

SIMCommander

Security Event Management Solution

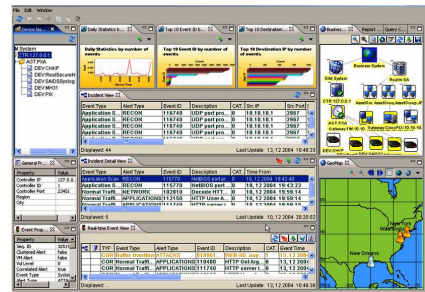
SIMCommander Overview

SIMCommander is a Security Event Management software platform designed for enterprises and government organizations to centrally monitor and manage their security infrastructure. SIMCommander collects, correlates, prioritizes, and visualizes security events/logs data from disparate security and network devices such as firewalls, IDS/IPS, antivirus applications, routers, switches, VPN devices, operating systems, database and applications. SIMCommander automatically transforms these collected data into meaningful and actionable information.

Through a user-friendly graphical user interface, all logs/events can be prioritized and visualized from a single console for security operators or administrators to identify and respond to critical attacks effectively and efficiently. SIMCommander helps enterprises to reduce the total cost of ownership (TCO) and maximize the return of the current security equipment investments. Thus, enterprises can free up more resources from traditional security operations to pursue revenue-generating business initiatives.

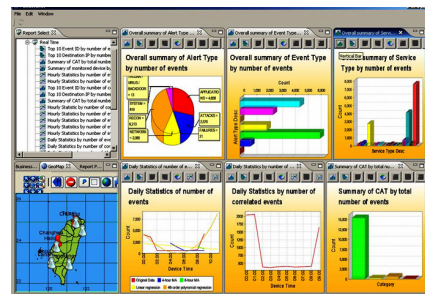
SIMCommander Management Console

SIMCommander Console is a single console which provides a comprehensive and user-friendly graphical interface for security managers, administrators and operators to perform essential security management tasks such as monitoring, analysis, alerting, response and reporting.



Perspective Views

SIMCommander Console also combines views from different perspectives which allows security staff to view reports and perform other SIMCommander features such as monitoring or analysis of security data at the same time.

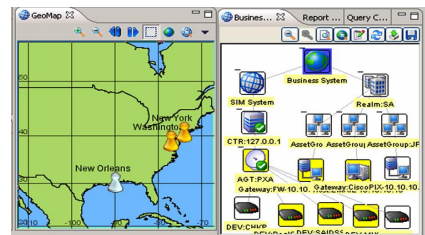


Real-time Reports

SIMCommander Real-time Reports is a security dashboard that allows security management to visualize and summarize major security alerts in graphical views. The reports display real-time security events or real-time security trends according to user-defined configurations.

Visualization

SIMCommander Geo Map and Business View provides a real-time holistic view on overall security infrastructure within the organization. It enables security teams to easily identify where a security threat has occurred and which business assets are being attacked.



Business Impact Analysis

Business View provides the main view of business units and allows users to determine the business value for each asset. For example, a server that contains financial information will be more critical than a demonstration server. When an intrusion has occurred, SIMCommander will increase or decrease the alert severity based on the business value of the server by the Business Impact formula. This helps security managers to focus and take immediate action or allocate resources to handle a security incident from a business's point of view.

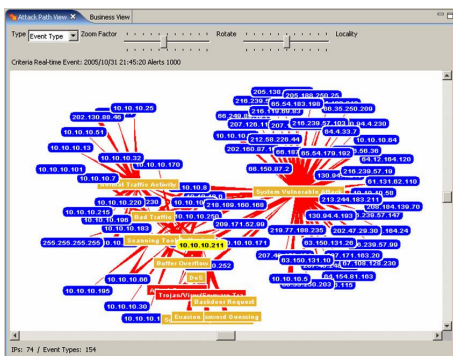
Real-time Correlated Events

With SIMCommander hybrid correlation technology, all security events are correlated and displayed in real-time. This can drastically reduce false positives and allows security teams to only focus on TRUE security threats.

Incident Scenario Tracking and Attack Path Analysis

Most security incidents are comprised of multiple events. Using SIMCommander, security administrators and analysts can drill-down and view the event details that are associated with the incident.

When an attack or incident has occurred, the full attack path from the source to the destination is mapped. SIMCommander Attack Path Analysis visualizes all incidents with attack path details and replays them for security administrators to readily identify and investigate incidents.

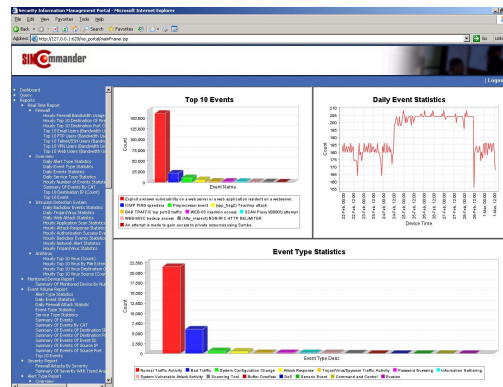


Customer ID

Customer ID allows administrators to configure the permission for user groups to perform security management tasks on pre-defined devices and network segments by individual departments, branch offices and other parties.

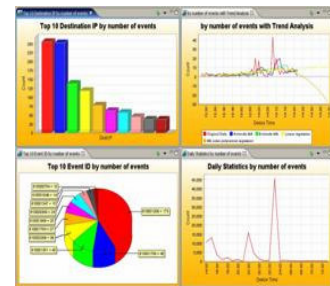
SIMCommander Portal

SIMCommander Portal is a web-based interface that displays the security dashboard. It also allows analysis of security events, generation and scheduling of security reports, querying of Knowledgebase contents. SIMCommander Portal is displayed in a browser and is separate from the SIMCommander Management Console.



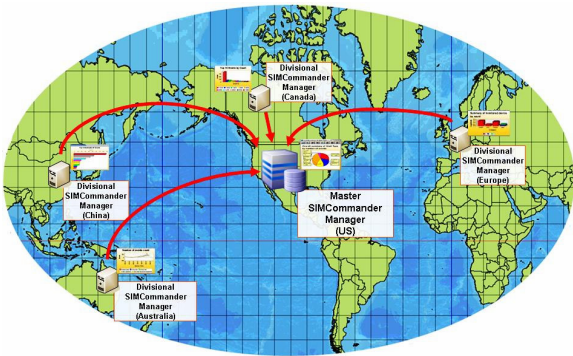
SIMCommander Reports

SIMCommander has over 200 out-of-the-box report templates including Real-time reports, Management reports, Administrator reports, Auditor reports and Alert Statistics reports to target different levels of audiences within the organization. SIMCommander reporting capability also allows administrators to generate customized reports, or create new report templates.



Centralized Escalation and SLA Control

The new SIMCommander hierarchy architecture uses a combination of parent-child and tree analogy that works similar to a family tree. In the hierarchy, a Master SIMCommander Manager acts as the trunk of the family tree and the Divisional SIMCommander Managers as the stems. The Master SIMCommander Manager centralizes events and alerts received from the Divisional SIMCommander managers, and provide security information monitoring, reports generation, alerts query and configuring Divisional SIMCommander Manager's components. The Divisional SIMCommander Manager could escalate events, alerts and incidents to the Master SIMCommander Manager for creating a centralized manage, control and response environment.



MAC Address Supports

Due to internal attacks are more difficult to detect and more costly than external attacks. Thus, SIMCommander supports collecting the MAC address from networking devices such as Routers and Switches. MAC address is a unique identifier attached to most forms of networking equipment, with MAC address, security professionals can increase the root attacker identification to understand the attack from which network segment, especially important in a DHCP environment.

Audit Logs

An audit log is the simplest and one of the most effective forms of tracking temporal information. It is created to record each transition that had been made. When something significant happens, auto log can record what happened and when it happened. In SIMCommander version 3.5.7, an audit log will be created to record each transition that had been made. You can easily query the log for audit trail and generate audit report.

SIMCommander Key Benefits:

- Hierarchy architecture supports distributed deployment and centralized management
- Single console provides holistic view on overall security infrastructure
- Graphical user interfaces for easy monitoring, analysis and reporting
- Geo Map and Business Map for easy identifying where the security threat is being occurred
- Real-Time Reports visualize and summarize major security alerts in graphical view
- Business Impact Analysis to focus on production and critical systems and applications
- Real-time correlated alerts to reduce false positives & identify true security threats
- Drill-down capability to reveal associated events for incident analysis.
- Attack Path Analysis to trace the source of an attack
- Fast and easy deployment
- Streamline Security Operational Process
- Increase productivity and operational efficiency



About SIMCommander

SIMCommander is a leading security event management solution provider which helps corporations effectively manage the risks related to Internet security. SIMCommander combines the “best of breed” security technologies and proven methodologies to centrally manage, monitor, alert and report all security devices throughout their IP network.

Find out more information about SIMCommander please visit www.simc-inc.com.