MAY CYBER TECHNOLOGY

>SCOP VISION

PRODUCT BENEFITS

· Total Control on Infrastructure
scopVISION provides a complete auditing platform for tracking end-points, servers, network devices, applications and databases.

· Detection of Threats to Critical Systems
Security risks are identified in real time. Advanced correlation features enables organizations to detect anomalies, which are not directly realizable from collected information.

· Total Visibility of the Network
The system collects logs, tracks inventory and monitors any activity in USB devices/ printers. Collected information enables organizations to perform better planning for future requirements and provides a total visibility of information flow within the infrastructure.

· Lower Operational Costs
The need for installing and managing multiple products for log collection, log correlation, inventory tracking and USB/ Printer auditing is obsolete.

· Easy to Implement, Easy to Manage
Agentless infrastructure for collecting information and easy to use wizard's bundled with a big data platform security management has never been easier.

scopVISION offers a complete solution to audit information flow activities within the enterprise. Log Collection & Correlation, Inventory Management, Printer Tracking, USB Tracking, USB Authorization, password Management and Process Control are the major modules of the solution. By employing a Lucene Based Big Data Platform scopVISION offers unprecedented analysis abilities on collected information.

CHALLANGES IN SECURITY & INCIDENT MANAGEMENT

Increased Number of Data Breach Sources Increased use of services using Internet and Bring Your Own Device (BYOD) trend is significantly increasing the number sources for databreaches. This increase is creating a huge challenge for organizations in tracking information access to critical data.

High Volumes of Audit Data for Analysis In today's competitive landscape more and more services are provided through IT Infrastructure. Deployed services require more components to be deployed including application servers, web servers, databases, network components and security devices. Parallel to this change the number of users and devices, which they use for accessing these services, is rising. The result is huge amount of audit data waiting to be processed and analyzed.

Information Blindness It is common that security breaches are realized accidentally or during regular audits. By the time it is realized the attacker performing the action is untraceable. The logs on the breach source are erased and the amount of information leaked is unknown. Common reason for this late detection is the inability to analyze audit data.

Tracking End-Points User end-points are the sources accessing the information. They are also a great candidate to track any breach attempt as they are often the first victim due to weaker protection. The high number of end-points and their distributed nature creates a big challenge in creating an auditing infrastructure.

Compliance Requirements Creating an effective auditing infrastructure is a basic requirement in every regulation concerning IT. In complex and distributed IT networks, auditing information activity is a big challenge.

STRUCTURAL FEATURES

In the core of scopVISION is a Lucene Based big data platform for audit data analysis. By using an agentless log collection infrastructure collected data is filtered and centralized. Advanced correlation features enable real-time visibility for security risks. The solution offers correlation analysis based on frequency analysis, long term trend analysis, linking distinct events and linking data for an expected order of occurrence.

For end-point tracking agents are deployed on Windows based devices.

The system polls the computer information from Active Directory or uses IP Range Scans for deployment. The deployments can be performed manually or continuously. In case continuous deployment is used, the system will deploy the agents automatically without any user effort.

MAY CYBER TECHNOLOGY

>SCOP VISION

PRODUCT INSIGHTS

- Easier implementation.
- Utilises ElasticSearch as big data platform.
- Faster search on data, adaptive infrastructure and multi platform support.
- Single solution for all auditing requirements.
- Unmatched customisation through open source technologies.
- Expanding the big data platform does not create spikes in costs.

Turkey Ankara
ODTÜ Teknokent, Mustafa Kemal Mah.
Dumlupınar Bulvarı, 280/G Kat: 2, 06530
Çankaya - Ankara / Turkey
+90 312 227 05 09
+90 312 227 05 75
info@maysiber.com

Turkey Istanbul
Maslak No/1 Plaza
Eski Büyükdere Caddesi No: 1
Kat: 17, 34485
Maslak - İstanbul / Turkey
+90 212 283 00 46
+90 212 283 00 47
info@maysiber.com

After the agents are installed, the statuses of the agents are monitored centrally. In case a problem occurs or an agent is uninstalled in the system, an alert is raised to security administrators. This enables system administrators to identify any problems occurring within the agents. MAY CYBER TECHNOLOGY Agent offers distinctive features for tracking any possible security risks.
Through inventory analysis module software installations/removals, processes running on computers, and many similar events can be tracked. Any inventory information needed can be collected using WMI protocol.
scopVISION also tracks USB and printers. The tracking can be based on the activity record or content. In case content tracking is chosen all data copied to USB or printed is duplicated on a central server for analysis. USB authorization can also be performed permitting only defined USB devices for use within the company network. Other features of scopVISION are process authorization, RDP session tracking and local user account password management.
Withing scopVISION all rules are configured centrally. The rules define what to collect, which data to correlate, and generate alarms for the tracked events.
The alert generation is handled centrally, making it possible to make customizations with ease.

MAIN FEATURES

- Lucene based big data platform for data analysis.
- Ability to handle 15,000 EPS on a single appliance.
- Support of more than 250 different applications and operating systems for log collection.
- Ability to work with or without an agent for log collection for all supported applications.
- Advanced correlation features.
- Detection of unauthorized access (deletion of log data, change of logging settings, failed logon attempts and etc.) to systems in real time.
- Inventory management. Alert generation based on important inventory changes like software installation, memory change etc.
- Management of all local administrator accounts and passwords residing within the computer network.
- Detection of files copied to removable media.
- Content detection for files copied to USB or printed documents.
- RDP session tracking.
- Central deployment.
- Detection of a problem in real-time in case the software stops functioning for any reason like uninstalling or disabling the service.
- Possibility of analyzing all collected data in any required method by using a generic reporting tool through a web interface.
- Completely web-based solution.