MAY
CYBER
TECHNOLOGY

# scop SOC

The importance of cyber security is constantly increasing as organisations are becoming more dependent to information technologies. Implementation of Security Operation Centers is increasing as centralized management and advanced analytics offer new possibilities in identifying security threats. scopSOC is an integrated platform for organizations wishing to implement a comprehensive Security Operation Center. scopSOC is an easy to implement, easy to operate solution with a low cost of ownership.

**PRODUCT INSIGHTS**

- Creation of a Centralized System for SOCs.
- Unified Asset Discovery, Vulnerability Scanning, Monitoring & SIEM.
- Built-in Threat Intelligence for Tracking Access to Malware & Phishing Sites.
- Real Time Search on 250 TB+ Audit Data.
- 15,000 EPS Performance per Single Appliance.
- Discovery of Unknown Applications Creating Network Traffic, or Performing Unauthorized Access to Files.
- Incident Management for Tracking Security Events.
- Advanced Correlation for Real-Time Visibility of Security Risks.

## MODULES

Central Event Management

Asset Discovery | Vulnerability Scanning | SmartAgent | Monitoring

Cyber Intelligence | SIEM | Incident Management | Intelligence

SOC Dashboard / Integration Layer

## STRUCTURAL FEATURES

scopSOC is an integrated platform offering SIEM, endpoint security, incident management, monitoring, asset discovery, vulnerability scanning and threat analysis. By offering a single centralized platform for managing cyber security, implementation of an infrastructure for SOC is significantly lower. Each module provides unique features for managing cyber security infrastructure.

## SIEM

scopVISION is an agentless log collection and correlation system utilizing big data technology. Elasticsearch is employed as the information store, thereby enabling a highly expandable structure. Operational intelligence is the main focus of scopVISION. Through its uniquely designed data analytic engine, the information collected is normalized and tagged to a common logical standard. By using an agentless log collection infrastructure, collected data is filtered and centralized. Any free text format is supported -RPC, WMI, SSH, telnet, ODBC, JDBC are only few examples of supported communication methods. More than 250 different log types are supported. Generic interfaces for reading log files, databases and syslog offer seamless integration with unsupported log types. No parsing is required for searching collected data. Netflow, sflow and sniffing is supported for the analysis of network traffic. Searches on audit data in the scale of more than 250 TB is achieved in seconds. By indexing more than 1 TB/day, scopVISION offers a highly scalable infrastructure. 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.

MAY
CYBER
TECHNOLOGY

# scop SOC

**WHY scopSOC IS DIFFERENT?**

- SIEM solutions employing “big data” architectures offer better scalability compared to legacy SIEM solutions. By utilizing elasticsearch, scopVISION customers can implement a solution which is highly customizable.
- Log search of 250 TB+ log data is realtime. This is unique to big data based SIEM solutions. The cost is significantly lower when storing huge sets of data.
- The integrated SOC platform with Smart Agent is unique to May Cyber Technology. With Smart Agent, unknown processes creating network traffic or accessing user files are discovered and terminated, thereby preventing major security risks.
- Unifying asset discovery, SIEM and status monitoring offer unprecedented centralized management ability.

## SOC DASHBOARD

SOC Dashboard offers a centralized interface to monitor infrastructure, assets, audit data and alerts. All information from monitoring, asset discovery, vulnerability scanning and SIEM modules are consolidated on a single dashboard offering an unprecedented holistic view of the security infrastructure. Geographical maps, link & chord diagrams, topological views are some of the few visualization tools.

## SMART AGENT

Due to the high number of endpoints, it is a major challenge for organizations to track audit data and protect them from breaches. Signature-based security solutions like antivirus or IPS solutions are failing to detect breaches and information leakages. Smart Agent unifies major security features through a single solution. Any audit information from event logs is collected, USB and printer activity is tracked and inventory changes are monitored. Network and File System Activity of Processes are tracked. When an unknown process transmits network traffic or performs an operation like delete on user documents, it can be immediately stopped. Ransomware applications are prevented from accessing user files. The behavior-based analysis provided by Smart Agent provides strong protection against malicious applications.

## MONITORING

All critical components are monitored without requiring any agent installation on endpoints. Servers, network devices and security appliances are monitored using WMI, RPC, SSH, ICMP and SNMP protocols. Monitoring is highly customizable. New metrics using performance counters, WMI and SNMP OIDs can be added with ease.

## ASSET DISCOVERY & VULNERABILITY SCANNER

Automatic asset discovery classifies any device found during the network scans.
All discovered endpoint systems are scanned for vulnerabilities. The collected information is mapped to security risks identified by SIEM. Based on the information retrieved from SIEM, asset discovery, vulnerability information and feed data, a risk level is calculated and tracked historically.

## CYBER INTELLIGENCE NETWORK

Through an integration with a cyber threat intelligence platform, malware and phishing sites are continuously tracked. The collected information is mapped to organization’s network traffic, thereby enabling the discovery of access to malicious sites from corporate network.

## INCIDENT MANAGEMENT

Critical events discovered by SIEM, vulnerabilities, new asset discoveries, or access to malicious sites are managed through created incidents. Escalation, SLA tracking, category-based assignment and LDAP integration are supported.

**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