MAY CYBER TECHNOLOGY

SCOP NET

Important security risks are encountered when unauthorized devices access corporate networks. These machines may contain viruses, which can spread to legitimate computers, or unauthorized users may attempt to access confidential information within the organization. scopNET is an agentless, 802.1X independent solution to prevent unauthorized computer access to corporate networks.

PRODUCT BENEFITS

· Total Control of Infrastructure
Any device accessing the network is tracked, authenticated & authorized.

· Detection of Threats to Critical Systems
Monitoring endpoints and tracking network activity can pinpoint threats targeting critical systems.

· Total Visibility of the Network
The system collects inventory of Windows/MAC/Linux OS and network devices. Collected information enables organizations to perform better planning for future requirements.

· Lower Operational Costs
By creating an automated network enrollment system, less incidents are handled manually. Higher workload due to tracking rogue devices and permission management on network devices is prevented.

· Enabler for Creating a Manageable BYOD (Bring Your Own Device) Strategy
BYOD is an increasing but very challenging trend for many organizations. With scopNET, a BYOD strategy can be implemented with ease.

· Easy to Implement, Easy to Manage
Using multiple methods for detection and prevention, scopNET can be implemented on any type of network without requiring any change on network infrastructure.

MODULES

Process Automation Layer

Network Scanning | Inventory Collection | Threat Analysis | Policy Compliance

MDM Integration | SIEM Integration | Incident Management | Intelligence

Integration Layer

The days of perimeter defense are long gone - modern organizations are permeable membranes, by design. Some of your biggest security threats occur when unauthorized devices access corporate networks. These machines may contain viruses, which can spread to legitimate computers, or unauthorized users may attempt to access confidential information within the organization. scopNET is an agentless, 802.1X independent solution to prevent unauthorized computer access to corporate networks. Traditional NAC deployments employing 802.1X require changes in network configurations which cause work overload for network administrators. Due to this challenge, many NAC implementations are limited to central offices of an organization. The scopNET solution does not require any such modifications.

STRUCTURAL FEATURES

scopNET offers different methods for preventing network access of a computer.
The system is able to integrate with routers, switches and firewalls for device detection and access control. Possibility of using techniques like ARP-Poisoning or TCP-Reset enables organizations to deploy a NAC solution without any dependency to network infrastructure.
The solution does not require the installation of any software in user machines. Sniffing or port mirroring are also not needed. Due to the minimal impact required in the corporate networks, scopNET is a very easy solution to implement.
When a new machine accesses the network an enumeration is performed. Windows WMI, Windows RPC, SNMP and SSH protocols are used for device enumeration. Windows, Linux and MAC Operating Systems are supported. The enumeration process enables organizations to manage their IT Inventory. Real time visibility on inventory information is provided.

MAY
CYBER
TECHNOLOGY

scop NET

PRODUCT INSIGHTS

- Independent of Network Devices &802.1X.
- Agentless Solution for Windows/MAC/Linux OS Platforms.
- Ability to Use Different Methods for Preventing Unauthorized Access.
- Automated Registration for Controlled Access.
- Independent of Additional Hardware/Software for Remote Branch Integration.
- Integrated Inventory Tracking & Threat Monitoring.
- No Network Infrastructure Modifications Required.

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

The built-in captive portal offers a unique end-user experience for external devices. Through integration with Short Message Services, these devices can be audited and a restricted network access is provided to the guest user.
scopNET can be integrated with Mobile Device Management Solutions. The integration enables better management of mobile devices throughout the infrastructure.
By integrating with scopVISION, network access of a device can be disabled based on security events detected throughout the infrastructure. Network scans, abnormal login failures, IPS alerts an be used as a source of information for blocking the network access of the relevant device.

MAIN FEATURES

- Agentless architecture.
- Different methods for detecting network access of a computer:
  - ARP Redirection
  - TCP Reset
  - Shut Switch Port
  - Change Switch VLAN
  - ACL Management
- Different methods for preventing network access of a computer:
  - ARP Poisoning
  - TCP Reset
  - Shut Switch Port
  - Change Switch VLAN
  - ACL Management
- Detailed inventory collection.
- Threat detection for events like port scanning, password scanning, SYN attack, virtual host NAT, rogue DHCP and real IP address detection.
- Central management and deployment.
- No software installations or appliance required in remote locations.
- Distributed architecture support.
- Web-based interface.
- Detailed reporting.
- Captive portal for guest management.
- Integrated SIEM infrastructure.
- Detailed network scanning for device enumeration.