What is a Security Operation Center?

A Security Operation Center is the place where the information infrastructure of the establishment is being supervised against security threats in 7/24 basis, the possible breaches are predicted and prevented, the reasons of a breach detected and negative consequences of a breach are minimized and managed.

Why is a Security Operation Center necessary?

- To supervise the systems used in information infrastructure 7/24 and analyze
- To identify the cybersecurity breaches
- To report the security breaches to the related units
- To ensure the business continuity
- Detailed reporting (usability, performance, etc.)

Those requirements became indispensable for many institution and establishments. Implementation of a Security Operation Center is compulsory to meet those fundamental necessities.

Which components must be in a Security Operation Center?

The main component of a Security Operation Center is SIEM systems. But a SIEM system solely would not be enough. A monitoring tool to observe the information infrastructure and a case management system to inform the related staff members must be installed. Besides, authorized and well-informed staff members must be available in order to work with these programs and take the necessary precautions.

What is ScopSOC?

ScopSOC is a cybersecurity operation software developed by May Cyber Technology. It was developed regarding to the needs and requirements of Security Operation Centers. ScopSOC is an integrated platform which provides solutions as SIEM, Client Management, Event Management, observation, inventory analysis, Vulnerability assessment, end user computer (client) management, cyber threat analysis and security automation. Collecting all security components in one software provides very important advantages. The main components of ScopSOC are:

ScopVision (SIEM)

With the ability of agentless log collecting, data are transferred to the “Big data platform”. During this process, data are standardized and labeled. Unnecessary data’s can be filtered out. This way, you can make advanced analytic analysis on collected data. Advanced correlation abilities make it easier to identify the security threats. The control panel that gives you the ability of high-level customization is based on Kibana.

In order to collect logs, protocols like RPC, WMI, SSH, Telnet, ODBC and JDBC are supported. More than 300 log types are supported. A “full-text” search can be applied on the logs. When analyzing the network traffic; Netflow, Sflow and Sniffing are supported. A search on more 500 TB’s of logs can be realized just in seconds. Advanced correlation features provide the ability of real-time diagnosis, warning and action.

ScopMon (Inventory management)

ScopMon component automatically finds and classifies information system inventories. For this process, no software is needed to setup on the assets. ScopMon can observe and discover with a totally agentless structure. After the observation and classification, ScopMon builds its own inventory list and observes the situation of each asset. It performs vulnerability analysis tests in pre-scheduled periods. With the observing module, it enlightens the events like attacks or defects which effects the performance. Assets and events are correlated automatically.
The observation of server and network components can be executed with Apache, Icmp, PerformanceCounter, Snmp, SnmpTrap, SnmpUtilization, Ssh, Web and Wmi options. The level of risk is calculated and followed according to SIEM, inventory and vulnerabilities.

Central Event Management (Event Engine)

The Event engine component centralize and classifies the events which happened on the whole system. It provides the security experts the ability to evaluate events methodologically.

- Central event and action management
- Automatic actions
- Integration with 3rd party products
- Adding the computer which is diagnosed as vulnerable into the firewall's blocking list
- Automatic e-mail and new events regarding to event logs
- Multiple actions for pre-defined rules
- Usage of all known system data (Assets, Monitoring, Vuln, Logs ..)

ScopDESK (Case Managament)

ScopDESK component is useful to automatize all processes necessary for action on the entire system. After the alerts and warnings, it automatically directs the "to do" list to the staff members.

Processes in SOC structures like Event / Incident / Change management and asset tracking can be executed Event management can be processed by opening automatic calls to the analysts in the SOC platform.

Automatic Response

Automatic Response component helps you to take preventing precautions automatically against the identified threats. In this way, it minimizes the need of authorized staff.

ScopClient (Client management)

Solutions like antivirus or attack blocking systems can be inadequate to identify security breaches and data leakages. Smart client manager is developed for Windows operating systems. With this component, operating system logs, USB and printer activities are recorded, and inventory data can be followed. Active applications can be followed, an unauthorized application can be prevented creating network traffic or change user files. An effective protection against ransomwares is obtained

Why ScopSOC?

- It is developed entirely in Turkey. All codes are written by Turkish engineers and not a single code was taken from outsource.
- It is hardware independent, compatible with all server systems and virtualization platforms. Support for Unlimited expansion is available.
- It can be expanded as wide as you need.
- The scope of the solution can be expanded by adding other components and products from the Scop platform.
- It is developed to meet the requirements of Security Operation Center (SOC) (Observation, Event management, remote command execution, etc.) in one single platform.
- It integrates with the other Scop products via the Scop platform.
- In house or remote support service is available upon request.
- Developments requested by the customers are accomplished in months (not in years) after approval.
- File / Network efficiency can be tracked with the ScopClient software which is designed for the weakest link of the network security.
- Collecting all event records in a distant center is possible without implementing an additional agent on the log sources.
- Implementation of an agent on the log sources is also possible if needed.

Earnings after ScopVISION

• Taking actions for the below stated events with the central event engine
- ✓ Events sourced from log policies
- ✓ Log collecting interruptions
- ✓ Correlation events
- ✓ Identification of a new asset
- ✓ Identification of a new vulnerability
- ✓ System observation (for example; usage of a processor in a critical level, stoppage of a service)

• Matching the events with assets with the automatic asset matching method
• Reaching the data of which event happened on which asset over the asset manager interface• Instead of many users only one user can take an action thanks to the central ID identification infrastructure
• Setting up which user can take which action on which component with the comprehensive authorization
• Integration with the security devices
• Limitation of the data reach of the users with the data authorization.