SCOP VISION

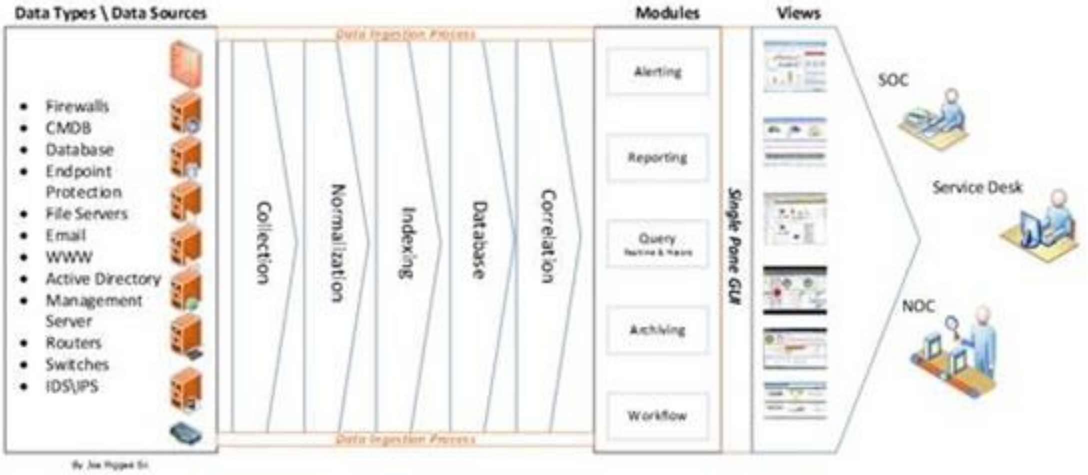
SIEM

Why would I need a SIEM solution?

Headlines of why establishments and institutions need SIEM solutions are:

•Compatibility processes (HIPAA , SOX, PII, NERC , COBIT 5, FISMA , PCI etc.)
•Continuity and observation of processes like ISO 27000, ISO 27001, ISO27002 and ISO 27003
•To collect and to keep logs
•To watch the log records and respond times to events
•To manage the incidents and to create event records
•To apply security policies and to identify the policy breaches

SIEM solutions are expected to meet the requirements for the Act No.5651. Institutions prefer SIEM solutions not only keep their data safe but also to meet the requirements for the compatibility processes. Besides data, trained staff member and financial loss; failed audits cause the order to be broken in the institutions. With a successful SIEM project, all those losses can be prevented.



What are the expectations from a SIEM solutions?

SIEM solutions do not work in “plug and play” concept. After the implementation, SIEM solutions can meet the expectations only after feeding with necessary databases and integrating with the security policies.
SIEM solutions must be job and process oriented. They must spot the important events instantly, inform the experts to take the actions necessary.

Steps that are essential for the SIEM projects to be successful are:
• To identify the necessities, define the concept and project management
• To determine the log sources
• To determine the details and content of the logs
• Log signification, labelling and levelling
• Building advanced correlation rules
• Cyber-security simulation and SOME practice
• Real-time “Security Monitoring Dashboard” design

What is ScopVISION?

ScopVISION is designed for the purpose of centralizing the log records which are produced by various systems in the information networks and using them at incident investigations.
ScopVISION provides a central analysis platform to observe the end user computers, servers, applications and events happening on the databases. By using ScopVISION, security risks on the information systems can be determined instantly.
Thanks to the correlation ability of ScopVISION which works on the collected data, regular examinations are automatized, warnings are generated, and related experts are informed. This way, possible incidents are predefined and can be prevented.

Why is **ScopVISION different**?

- ScopVISION makes it possible to make quick searches and analysis with the Elasticsearch database which is built-on its design.
- ScopVISION, provides real-time and backward correlation possibilities regardless of the volume of the collected data
- ScopVISION, owns strong legal analysis skills which is necessary to investigate data loss.
- ScopVISION provides easy and fast operation ability with the simple design of its interface
- ScopVISION, can work agentless on a remote computer or a server with a local application setup
- ScopVISION can be scaled again after the setup according to the requirements and reach to required performance levels just by adding new servers thank to its horizontal expansion ability.
- The operation cost of ScopVISION is a national and domestic product.
- The operation cost of ScopVISION is very low.
- Usually, to collect logs daily on information systems and observe USB/printer activities and correlation takes more than one product but ScopVISION offers all these features in one system.

Earnings after ScopVISION;

- ScopVISION tracks and reports the network connections of working applications and make it easier to identify the malwares.
- ScopVISION tracks and reports the file movements of the working applications and make it
easier to identify ransomwares.
- ScopVISION tracks all the movements of computers about USB connections, printers, hardware changes and log record.
- ScopVISION tracks the unreliable softwares that can cause data leakage.
- With the geographical location support, ScopVISION reports the countries which are linked
by the applications.
- Collected information provides a better planning of necessities and visibility of the data-flow inside the organization.