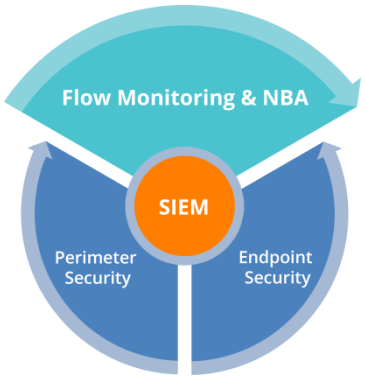
Flowmon & SIEM – Seamless Integration

Flowmon solution delivers the flow-based monitoring and Network Behavior Analysis (NBA) for all organizations and all networks from 10 Mbps to 100 Gbps. It provides the statistics necessary for network monitoring, security, troubleshooting, IP accounting and billing, capacity planning, user and application monitoring, data retention and many more features and customer benefits. Flowmon solution includes autonomous probes, which generate statistical information on network traffic, collectors for the storage, display and analysis of this information and full feature Network Behavior Analysis component **Flowmon ADS** (Anomaly Detection System) for automatic detection of security issues like advanced persistent threats, targeted attacks or malware activities. Flowmon solution provides outstanding network visibility, security intelligence and compatibility with many network components and SIEM solutions.



SIEM (Security Information and Event Management) technology provides real-time analysis of logs and security alerts generated by infrastructure components, appliances or applications. The core features of SIEM are long-term storage, analysis, correlation and reporting of log data or events to provide a comprehensive view of overall IT infrastructure status in terms of security, availability and performance. SIEM and its results depends on the quality input log data, simply said if there are no evidences of incident in primary log data there is no way how SIEM can figure it out.

Deployment scenario

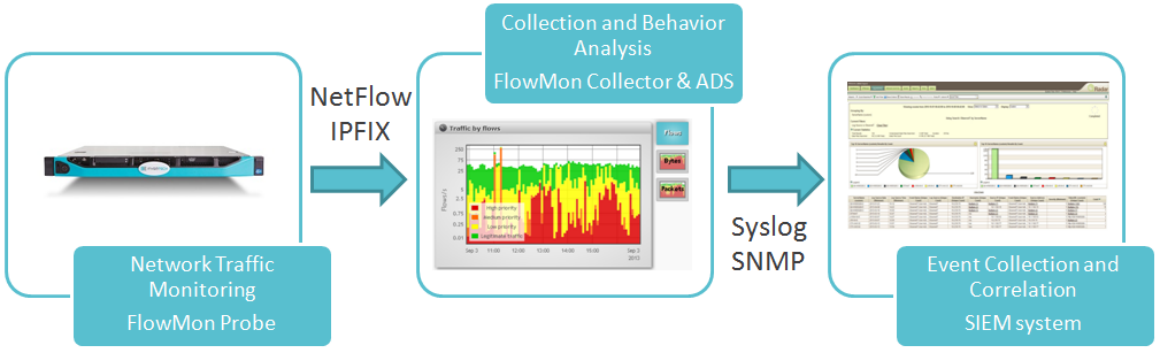
High-performance **Flowmon Probes** provide full network visibility to any IP based network and generate NetFlow/IPFIX traffic statistics collected by Flowmon Collector and processed further.

Flowmon Collector with **Flowmon ADS** system collects NetFlow/IPFIX data from Flowmon Probe and also from other flow sources, stores them for long time and provides detailed network visibility, which besides other includes network traffic reporting & alerting, detailed network analysis with possibility to drill-down up to communication level. **Flowmon ADS** analyzes collected data and detects anomalies, suspicious behavior and attacks including Advanced Persistent Threats, zero-day attacks and polymorphic malware. Detected events are immediately logged to QRadar SIEM using syslog as a transport protocol.

NetFlow, APTs and SIEM

Advanced persistent threats (APTs) demand extension of existing approaches to security information and event management. Network security managers should combine log data with NetFlow (network flow information) for more complete and effective SIEM breach discovery.

SIEM system collects and correlates logs from all systems and devices, including Flowmon ADS as reliable source of network related events detected by advanced NBA system.



Flowmon Networks, a.s., U Vodarny 2965/2, 616 00 Brno, Czech Republic
+ 420 511 205 250 | info@flowmon.com
www.flowmon.com

Summary

From the perspective of SIEM system Flowmon works as valuable and unique sensor that provides visibility into network traffic within whole corporate infrastructure. In contrary to traditional flow-based sensors Flowmon performs advanced traffic analysis known as Network Behavior Analysis to **detect security and operational issues** or network anomalies and report them as events to SIEM system in a similar way like firewall or intrusion detection system. Flowmon provides to SIEM system **additional insight** into network traffic and awareness of advanced persistent threats, targeted attacks and next generation malware events to improve network visibility and detection capabilities of SIEM system. Both solutions can **seamlessly work together** to improve network security and IT governance. As a standalone solution Flowmon provides all the enterprise-level features like unlimited number of flow sources, user roles and privileges, predefined set of reports and dashboards, simple customization, report scheduler, immediate alerts and notifications.

Network Behavior Analysis (NBA)

Network Behavior Analysis provides detailed analysis of network traffic and helps in proactive detection network threats. Core features are visibility into the state of the network and identification of deviations from baselines. After you have deployed firewalls and intrusion prevention systems, you should consider NBA to identify network events and behavior that are undetectable using other techniques.

Compatibility

Flowmon is compatible with wide range of SIEM systems. Integration and event delivery is based on standard syslog protocol or SNMP traps. Flowmon implements industrial standard Common Event Format (CEF) to minimize deployment efforts.

Selected references

Flowmon Networks has more than 500 worldwide references. Flowmon is deployed with various SIEM systems. All the references and success stories are available online at Flowmon Networks web site.

Flowmon Networks, a.s., U Vodarny 2965/2, 616 00 Brno, Czech Republic
+ 420 511 205 250 | info@flowmon.com
www.flowmon.com