Comprehensive security monitoring and detection of advanced persistent threats

Purpose of this document

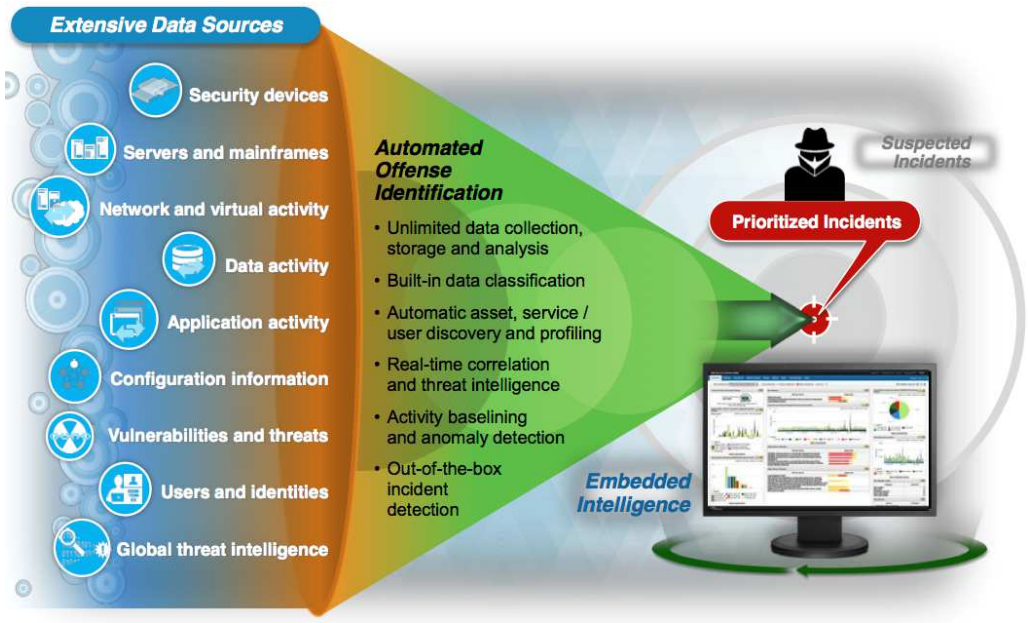
Number of IT solutions and tools in organizations is growing rapidly and requirements on management of these are breaching limits of human abilities. Therefore advanced monitoring system is an absolute must-have to ensure high awareness of network administrators about events in their networks. Such standard may be applied to both, operational monitoring and equally to security monitoring which often used to be neglected in the past. For security reasons, it is necessary to have a detailed 24/7 overview of what is happening within servers, workstations, applications and security tools. Expectations from such solution aren't only its ability to continuously monitor network but also to provide certain level of security intelligence to automatically identify threats and frauds.

This document describes:

- The role of SIEM in security monitoring
- The role of network traffic monitoring in detection of advanced persistent threats and network frauds

Challenge

The first step to secure network infrastructure is to deploy protection at the network perimeter. It is insufficient to block unwanted traffic using fixed set of rules with firewall. It is becoming more important to have ability to detect advanced persistent threats searching through data at application level, revealing hidden malware and more. There are many security systems that cover only specific areas and protect only against particular attack methods or types of threats. However nowadays intruders use not only technical vulnerabilities of specific products, but combination of many existing gaps with a very particular purpose and goal which allows them to break through complex security system using a single attack.



Advanced protection systems designed to protect against such attacks are as known as *Security Intelligence and Event Management* (SIEM). SIEM may be described as a roof top covering monitoring of all applications in the network, detecting undesired behavior using an in-built security intelligence.

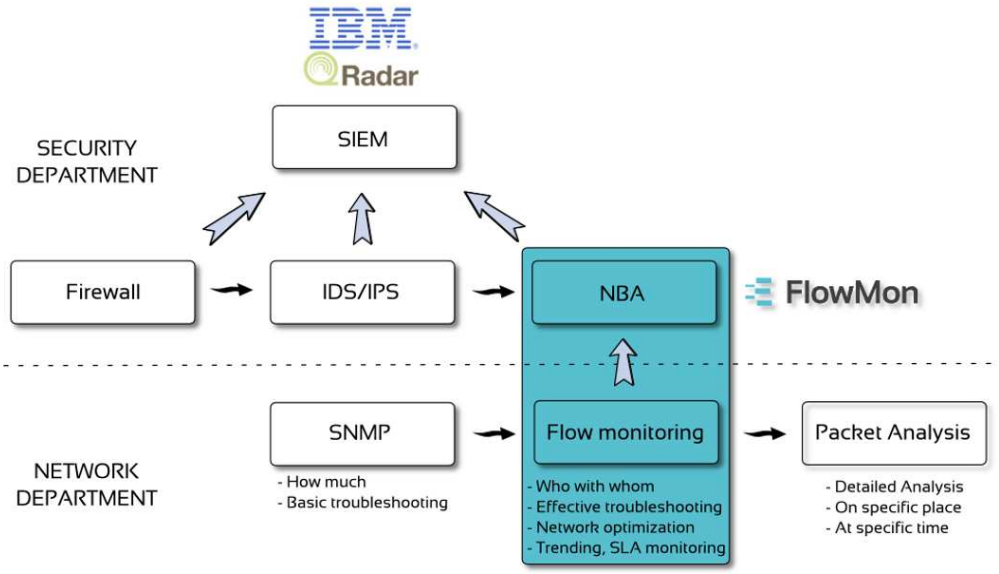
SIEM system - using information about all devices in the network - has ability to detect advanced persistent threats such as user login to a local station without any record in the attendance system about user being at the office at the respective time. Or an attempt of login to database server with an administrator account from a machine, which was attacked last week by computer virus programmed to guess passwords.

Despite the fact that the information from applications seems to be sufficient for an efficient detection of advanced persistent threats, it is not. Intruders use tactics to hide their malicious activities within legitimate network traffic, so it cannot be identified (hiding an application traffic by using non-standard port, etc.). In such cases, it is necessary to supplement the SIEM system with high-end network monitoring solution. A quote that applies here is: *"the network does not lie."* Even if an intruder manages to hide his database server attack, his communication has to pass through the network. Likewise, all command and control communication of malware (BOT net) is running via LAN and WAN.

Solution Architecture

Solution for detection of modern security threats stands on two pillars - SIEM system IBM QRadar SIEM and Flowmon Networks, Flowmon module ADS (Anomaly Detection System).

- IBM QRadar SIEM acts as a central brain for collection and correlation of all data available, both from its own devices (logs) and from the network.
- Deep insight into an internal network using network monitoring solution Flowmon Networks, Flowmon supporting Cisco standards NetFlow v5, v9, NBAR2 and also modern IPFIX standard. With Flowmon native probes and compatibility with a wide range of active network devices, this solution can be deployed to any customers' infrastructure.
- Automatic detection of threats and frauds in an internal network is executed by Flowmon ADS (Anomaly Detection System), which is part of a comprehensive Flowmon solution.



With this synergy of two security solutions customers gain ability to detect unknown threats which are operating within the organization's network. Furthermore the detailed insight into network traffic delivers an overview of operational problems, anomalies in network traffic or occurrence of suspicious activities that are typically followed by successful attacks.

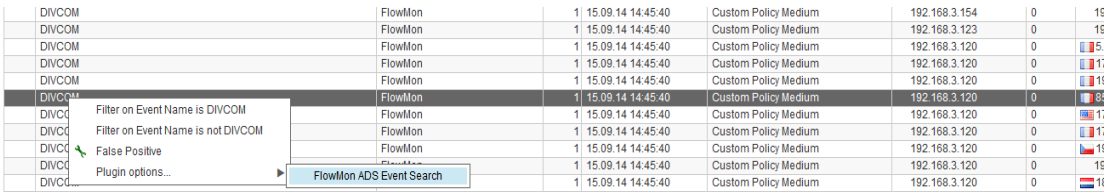
Solution Benefits

This solution for security and efficient management of IT infrastructure aims to provide comprehensive network protection against known, unknown and sophisticated threats to ensure security and stability of network infrastructure. The key benefits of the solution are:

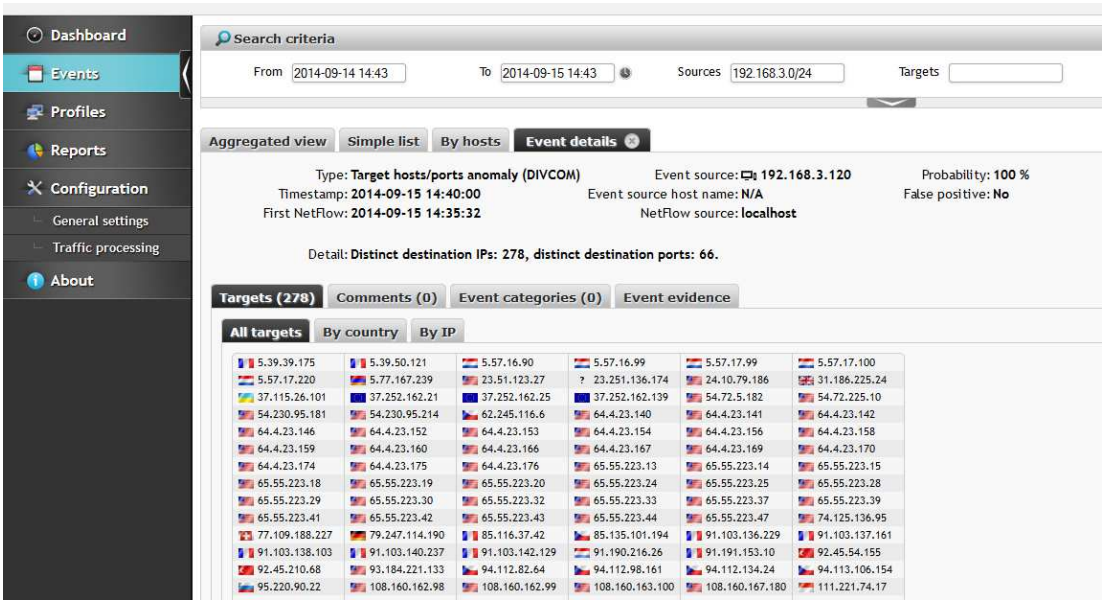
- detection of threats within an internal network – if these threats manage to penetrate perimeter
- ability to identify indicators of threats and carry our preventive actions
- prompt resolution of incidents thanks to an overall visibility of network components and the network itself
- a single focal point to access all data, incidents and events
- intelligent correlation engine processing all data and sophisticated security intelligence module detecting undesired network activities
- scalable, cost efficient and comprehensive network security solution
- simplification and automation of time-consuming and expensive manual process of incident investigation
- availability and simplicity of deployment of extending modules, including attack modeling, threat management, vulnerability scanning, deep packet inspection and more
- integration of many different sources into single central dashboard

Integration of Flowmon Networks Flowmon and IBM QRadar

Uniform and connected system has been achieved by integrating both solutions to each other. Flowmon ADS informs SIEM system about detected incidents and anomalies via event delivered in form of syslog. SIEM thereafter analyzes these syslog files and correlates them with events from other tools for management of IT infrastructure. In case of need for supplementary information about specific event (record of related network traffic) it is possible to enter Flowmon directly from QRadar's context menu.



Integration of the two solutions is performed by deploying an installation package which includes necessary documentation for IBM QRadar configuration. The implementation is very simple, consisting of a few straightforward steps.



Why solution for secure and effective IT infrastructure?

- unified solution for detection of advanced persistent threats as well as unknown attacks
- built on two globally recognized technological solutions
- well integrated with each other
- enhances level of IT security, IT infrastructure and ability to prevent advanced persistent threats and modern attacks
- connection of the two components provides users with convenient way of working with incidents from a single point

For more information

For more information please contact your IBM or Flowmon Networks reseller.

IBM Česká Republika, spol. s r.o.
V Parku 2294/4
148 00 Praha 4
Czech Republic
www.ibm.cz

Flowmon Networks, a.s.
U Vodárny 2965/2
616 00 Brno
Czech Republic
www.flowmon.com