

Comprehensive security monitoring and detection of advanced persistent threats

Purpose of this document

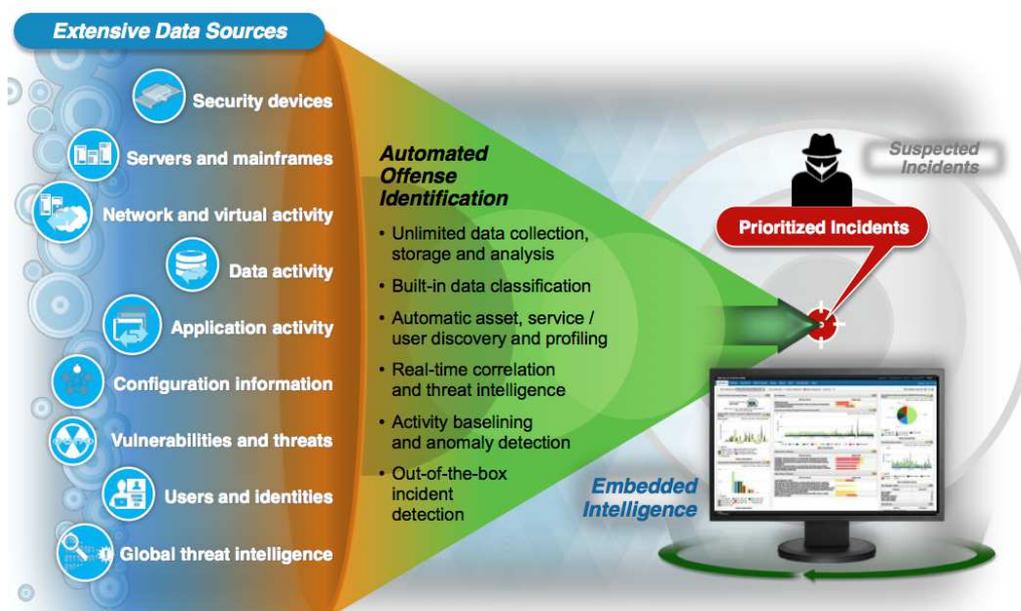
Number of IT solutions and tools in organizations is growing rapidly and requirements on management of these are breaching limits of human abilities. Therefore advanced monitoring system is an absolute must-have to ensure high awareness of network administrators about events in their networks. Such standard 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.

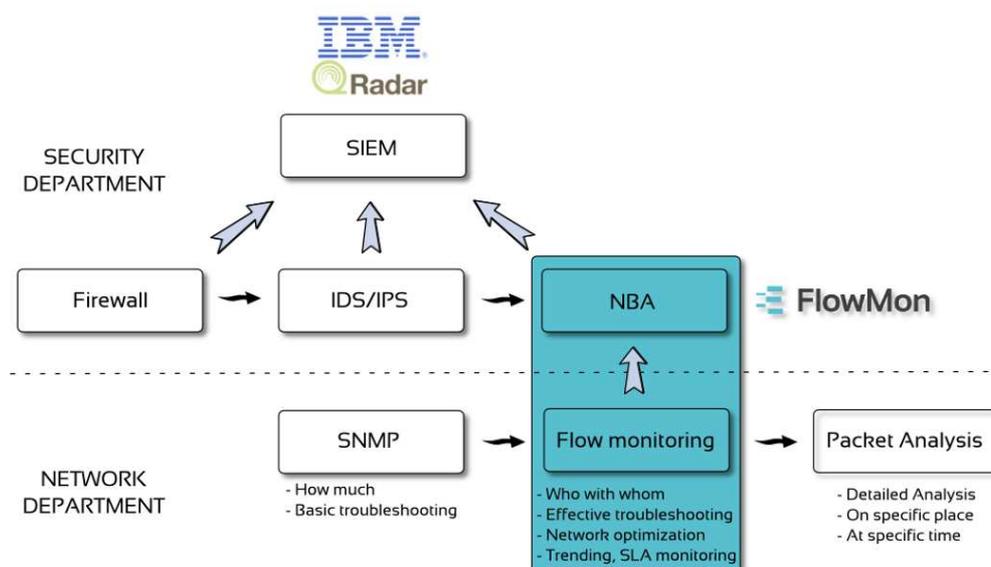
SIEM system - using information about all devices in the network - has ability to detect advanced persistent threats such as user login to a local station without any record in the attendance system about user being at the office at the respective time. Or an attempt of login to database server with 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.



Search criteria
 From: 2014-09-14 14:43 To: 2014-09-15 14:43 Sources: 192.168.3.0/24 Targets:

Event details
 Type: Target hosts/ports anomaly (DIVCOM) Event source: 192.168.3.120 Probability: 100 %
 Timestamp: 2014-09-15 14:40:00 Event source host name: N/A False positive: No
 First NetFlow: 2014-09-15 14:35:32 NetFlow source: localhost

Detail: Distinct destination IPs: 278, distinct destination ports: 66.

Targets (278) Comments (0) Event categories (0) Event evidence

All targets					
By country		By IP			
5.39.39.175	5.39.50.121	5.57.16.90	5.57.16.99	5.57.17.99	5.57.17.100
5.57.17.220	5.77.167.239	23.51.123.27	23.251.136.174	24.10.79.186	31.186.225.24
37.115.26.101	37.252.162.21	37.252.162.25	37.252.162.139	54.72.5.182	54.72.225.10
54.230.95.181	54.230.95.214	62.245.116.6	64.4.23.140	64.4.23.141	64.4.23.142
64.4.23.146	64.4.23.152	64.4.23.153	64.4.23.154	64.4.23.156	64.4.23.158
64.4.23.159	64.4.23.160	64.4.23.166	64.4.23.167	64.4.23.169	64.4.23.170
64.4.23.174	64.4.23.175	64.4.23.176	65.55.223.13	65.55.223.14	65.55.223.15
65.55.223.18	65.55.223.19	65.55.223.20	65.55.223.24	65.55.223.25	65.55.223.28
65.55.223.29	65.55.223.30	65.55.223.32	65.55.223.33	65.55.223.37	65.55.223.39
65.55.223.41	65.55.223.42	65.55.223.43	65.55.223.44	65.55.223.47	74.125.136.95
77.109.188.227	79.247.114.190	85.116.37.42	85.135.101.194	91.103.136.229	91.103.137.161
91.103.138.103	91.103.140.237	91.103.142.129	91.190.216.26	91.191.153.10	92.45.54.155
92.45.210.68	93.184.221.133	94.112.82.64	94.112.98.161	94.112.134.24	94.113.106.154
95.220.90.22	108.160.162.98	108.160.162.99	108.160.163.100	108.160.167.180	111.221.74.17

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