Flowmon ADS

Anomaly Detection System for Secured Network

Product Brief

INTRODUCTION

Flowmon ADS brings new dimension of benefits and experciences in working with network traffic statistics (NetFlow, IPFIX, NetStream). Thanks to the advanced **Network Behavior Analysis** (NBA) technology, it is possible to **identify threats** that breach corporate network perimeter security, infiltrate the network through various channels like already infected laptops and mobile devices or lack of available signatures. Automatic detection of security incidents, traffic anomalies or configuration issues, **simplifies management and operation of the network**, significantly **improves security** and enables identification of root cause of issues proactively and real-time.

NETWORK MANAGEMENT AND SECURITY

Flowmon ADS combines features important for network administrators, security managers, IT managers or CIOs into single solution that provides accurate and reliable information in form of network events. Automatic notifications and reporting capabilities allow Flowmon ADS to be deployed as a standalone solution while large enterprise environments can integrate with existing monitoring, incident response and Security Information and Event Management (SIEM) systems.

#	Event type	Timestamp	Source	Target	NetFlow source
1	SSHDICT	2014-12-30 20:50:00	.97.92	192.168.47.110	demo.invea.cz
2	SSHDICT	2014-12-30 20:15:25	.97.92	192.168.47.110	demo.invea.cz
3	SSHDICT	2014-12-30 19:15:00	.11.118	192.168.47.110	demo.invea.cz
4	SSHDICT	2014-12-30 18:40:00	.11.118	192.168.47.110	demo.invea.cz
5	SSHDICT	2014-12-30 18:35:00	.11.118	192.168.47.110	demo.invea.cz
6	SSHDICT	2014-12-30 18:30:00	.151.126	192.168.47.110	demo.invea.cz
7	SSHDICT	2014-12-30 17:55:00	.151.126	192.168.47.110	demo.invea.cz

Interactive, easy to read, customizable dashboard provides relevant insight to overall network status with the ability to immediate drill down of individual events and corresponding network traffic statistics. Views also include traffic graphs visualization to support investigation of events and related network traffic. DNS, WHOIS, and geolocation integration enhances the administrators experience and efficiency. Cloud-based **Flowmon Threat Intelligence** delivers IP and host reputation which improves detection of malware and botnet communication. Flowmon Threat Intelligence also updates behavior patterns of detection methods to detect unveiled current threats such as zero-day vulnerabilities, etc.

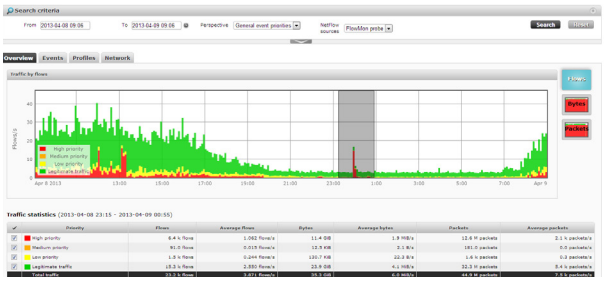
MAIN BENEFITS

- **Automatically identifies threats, attacks, incidents and configuration issues**
- **Complements signature based approaches to improve security**
- **Utilizes network level analysis without the need of client-based software**
- **Lowers Total Cost of Ownership (TCO) by providing:**
  - **Real-time threat, attack, data leakage and incidents detection which minimizes their financial impact**
  - **Simplified network troubleshooting by proactively identifying problem root cause**
  - **Detection of internal threats and resources misuse**
- **Easy to deploy Flowmon ADS provides short time to value (TtV) and quick Return on Investment (ROI)**

SIGNATURE VS BEHAVIOR ANALYSIS

Traditional perimeter and endpoint security systems such as IDS, IPS or Antivirus use signature based detection to identify threats. Signatures are definitions of known malware and malicious activities. Even though NBA is not meant to displace these technologies, Gartner recommends augmenting traditional means of network monitoring.

Network Behavior Analysis detects unknown or specific threats using signature-less approach. Flowmon ADS implements numerous advanced algorithms utilizing Artificial Intelligence (AI) to evaluate individual nodes behavior on the network. It dynamically establishes profiles and base-lines of the expected behavior and points out anomalies. This makes Flowmon ADS an ideal solution for detection of Advanced Persistent Threat attacks (APT).



Flowmon Networks

Flowmon Networks, a. s.
U Vodarny 2965/2
616 00 Brno, Czech Republic

+420 511 205 250
info@flowmon.com
www.flowmon.com

Flowmon ADS

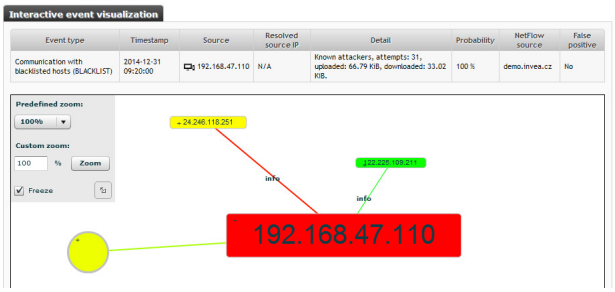
Anomaly Detection System for Secured Network

Product Brief

DETECTION OF INCIDENTS AND ANOMALIES

Flowmon ADS automatically identifies various security and operational issues, network anomalies or undesired user behavior:

- **Attacks on network services** aiming to gain unauthorized access to host and services.
- **Infected devices** and communication with malicious IPs and hosts including botnet command and control centers, known attackers or systems spreading SPAM or malware based on advanced real-time reputation databases.



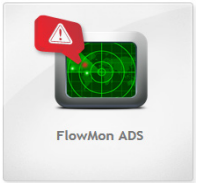
- **Anomalies of DNS** traffic indicating infected devices, malicious software and misconfigured network services.
- **Anomalies of DHCP** traffic indicating network sniffers, spoofed addresses and improper configurations.
- **Port scanning** performed by compromised devices, attackers or malevolent internal users.
- **Unauthorized network applications** such as peer to peer (P2P) networks and messengers.
- **Detection of proxies, TOR** (The Onion Router) used to hide network activities.
- **Outages** and improper configuration of network services.
- **Potential data leakage** and unauthorized data sharing.
- **Detection of Voice over IP (VoIP) attacks**, rogue PBXs and devices.
- **Detection of unusual email traffic** and SPAM.
- **Detection of network services** potentially being used to generate Distributed Denial of Service (DDoS) attacks.

FEATURES

- **Simple installation of Flowmon Probe or Flowmon Collector**
- **Support for NetFlow v5/v9, IPFIX, jFlow, NetStream and sFlow (limited)**
- **Support for NBAR2, analysis of HTTP information, MAC addresses and VoIP attributes**
- **De-duplication and flow pairing (RFC 5103)**
- **Multi-tenancy and limited rights administrators**
- **E-mail notifications and export of events available in various formats (syslog, SNMP, CSV)**
- **Optimized deployment models available to enterprise networks, Internet Service Providers (ISP) and backbone operators**

EASE OF DEPLOYMENT AND EXTENSIBILITY

Anomaly detection services are pre-configured enabling rapid deployment with limited need for time consuming configuration and customization. Flowmon ADS uses over 50 artificial intelligence algorithms (dynamic standard behavior baseline, deviations, dynamic decision trees, machine learning, predictive analytics of time series and clusters) to analyze multiple dimensions of network traffic flow. Integrated configuration templates, false positive handling and deployment wizard ensure Flowmon ADS does not require expert knowledge.



ORDERING INFORMATION

Distributed by

NEOX NETWORKS

sales@neox-networks.com
+49 6103 37 215 910
www.neox-networks.com

Flowmon Networks

Flowmon Networks, a. s.
U Vodarny 2965/2
616 00 Brno, Czech Republic

+420 511 205 250
info@flowmon.com
www.flowmon.com