IBM Security QRadar Network Anomaly Detection

Applying sophisticated analytics to help identify malicious activity and advanced threats

Organizations today are exposed to a greater volume and variety of network attacks than ever before. This makes sense on today’s smarter planet, where instrumented, interconnected and intelligent businesses collect, process, use and store increasing amounts of data. Adversaries are exploiting zero-day vulnerabilities, taking advantage of risks introduced by cloud and mobile computing, and applying social engineering tactics to compromise user accounts. Advanced attackers are both patient and clever, evading detection at the network level. Information security professionals wrestle with efficiently detecting these threats and effectively resolving them.

IBM® Security QRadar® Network Anomaly Detection enhances IBM Security Network Intrusion Prevention System deployments by providing greater insight into network behavior and abnormal activity indicative of security threats. It extends coverage alongside the protocol analysis and other threat protection techniques of the intrusion prevention system (IPS) by providing anomaly detection of network traffic as well as real-time correlation of a broad set of security and network data. In doing so, it complements IBM Security SiteProtector™ System to deliver a more complete and three-dimensional view of an organization’s network activity and security posture. By correlating IPS events, network traffic, vulnerabilities, user activity and threat intelligence in real time, QRadar Network Anomaly Detection can help organizations detect breaches faster, limit their impact and enhance the efficiency of security operations.
QRadar Network Anomaly Detection analyzes the following:

- **IPS and infrastructure logs**—IPS events plus events from selected operating systems
- **Network flows**—Flow data from network and application traffic (NetFlow and others)
- **Vulnerabilities**—Vulnerability scan results from network and application vulnerability scanners
- **User activity context**—Events from Dynamic Host Configuration Protocol (DHCP) and virtual private network (VPN) products, and operating system (OS) authentication
- **Threat intelligence**—Advanced intelligence from IBM X-Force® and third-party feeds

Anomaly detection can be performed through baselining of network flow activity (including seasonality and growth trends) and identification of meaningful deviations.

Anomaly detection and network behavioral analysis

QRadar Network Anomaly Detection analyzes network flows, IPS and infrastructure logs, and user activity events in real time, monitoring for and alerting on any observed activity that falls outside of “normal” behavior. It determines baseline activity levels along virtually any dimension of interest—offering granularity and flexibility—and then triggers alerts as appropriate. Both the learning period and the trigger period can be set through straightforward parameters. Anomaly detection capabilities can account for both seasonality and growth trends.

“Most organizations don’t even know they have been infected by malware. An advantage of the IBM solution is that it can detect the harbingers of new attacks from the outside or reveal covert malicious activity from the inside.”

—Marc van Zadelhoff, vice president of strategy and product management, IBM Security Systems
For example, an alert could be triggered under any of the following conditions:

- Outbound network traffic is detected to a country in which the company does not do business and to which no traffic should be sent.
- A known application (such as Internet Relay Chat [IRC]) is detected on a non-standard port.
- File Transfer Protocol (FTP) traffic is observed in the finance department when finance has never before had FTP traffic.
- A self-propagating worm outbreak occurs.
- A new service is initiated on a known host.

**Behavioral profiling and anomaly detection rules are created through a straightforward rule wizard.**

**Real-time correlation of threat, network, vulnerability and user data**

QRadar Network Anomaly Detection correlates an extensive set of data—including IPS events, network flow data, system and application vulnerabilities, user activity, and threat intelligence—to identify and prioritize threats. It incorporates advanced threat intelligence data from IBM X-Force, providing insight into suspect Internet entities based on knowledge of 15 billion web pages and images. This collective insight extends the value of SiteProtector System and Network Intrusion Prevention System by providing richer context and greater visibility.
“We believe information security is becoming a big data and analytics problem. Some of the most sophisticated attacks can only be found with detailed activity monitoring to determine meaningful deviations from ‘normal’ behavior.”

— Neil MacDonald, vice president, distinguished analyst and Gartner fellow emeritus, Gartner Research

Network flow analysis for deep visibility and insight

QRadar Network Anomaly Detection provides network flow analysis of NetFlow, J-Flow, sFlow and IPFIX data, as well as QFlow data collected by IBM Security QRadar QFlow and VFlow Collector appliances (optional complements to QRadar Network Anomaly Detection). QFlow data includes Layer 7 application content captured for detection and forensic purposes. Its advanced application detection performs stateful analysis of complex applications such as Voice over IP (VoIP), peer to peer (P2P) traffic, database applications and social media traffic. With deep packet inspection capabilities, QRadar QFlow and VFlow Collector appliances also provide visibility into threats such as traffic disguised as other applications. Correlating this flow information with IPS events, user activity, vulnerabilities and threat intelligence provides richer context for a more complete view of potential threats.

Scenarios using QRadar Network Anomaly Detection

- Detection of zero-day threats through traffic profiling—Discover viruses, worms and other malware that leverage zero-day exploits through behavior profiling and anomaly detection at the application host, protocol and network levels
- Improved detection of advanced threats—Enhance the ability to detect stealthy, "low and slow" breaches, where evidence of a compromise is so subtle that it might otherwise escape detection for months or years
- Correlation of vulnerabilities with IPS events to better identify significant threats—Prioritize incidents and reduce distractions by gaining insight into which threats really matter
- Correlation of network traffic with threat intelligence data—Identify suspicious network traffic based on the IBM X-Force Threat Intelligence Feed and third-party intelligence feeds, which help immediately reveal suspicious activity within the network
- Identification of related attacks as a single offense—Simplify incident investigation by grouping attacks from multiple sources against a common host or attacks against multiple hosts from a common source as a single offense, for significant time savings

Automated dashboards and reports

Through flexible reporting on data collected from external sources, IBM Security QRadar offenses (high-priority incidents), and asset profiles, QRadar Network Anomaly Detection enables users to save time and gain insight. Report templates for a variety of security and operational needs are delivered out of the box, and users can create or modify reports to suit their needs. Reports can be run on an ad-hoc basis, or automatically run on a periodic or custom schedule. The solution also provides many predefined dashboards, which can be easily customized. Dashboards can be created and shared with other users, facilitating collaboration and faster resolution. A variety of data within the solution can be charted, using time series trends or aggregated data.
“The future of cyber security is going to require an evolved philosophy that assumes a state of compromise. Real-time network traffic monitoring technology should be configured to empower a more effective alert system.”

—PwC2

Automated asset profiling and identity context
The QRadar Network Anomaly Detection asset database tracks assets by IP address and user identity data. The database automatically builds lists of services running on a host, passively identified via network traffic flows. User attribute context is mapped to asset profiles, which become a centralized repository for mapping identity context to offenses and viewing network activity and IPS events relative to identities (even when identity data is not directly associated with a given data element). This creates deep contextual knowledge about the environment. The solution also collects and normalizes vulnerability data from network vulnerability scanners and IBM Security AppScan®, and stores this data in the asset profile, providing greater context and prioritization for detection and forensics. Asset profiles are used to monitor and correlate network activity, helping to reduce false positives and adjust the severity of offenses based on the criticality of assets involved.

Workflow management to track threats and support resolution
QRadar Network Anomaly Detection creates offenses (high-priority incidents) that contain a complete problem summary and all contextual data. Users can mark offenses for follow-up, close offenses, receive email notification when offenses are updated, and/or dismiss offenses they are no longer investigating. Each offense has a unique identifier and is treated as its own ticket within the solution. The solution also enables external ticketing systems to easily add information to an offense as well as close offenses directly from the external system.

Why IBM?
IBM operates the world’s broadest security research, development and delivery organization. This comprises 10 security operations centers, nine IBM Research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM solutions empower organizations to reduce their security vulnerabilities and focus more on the success of their strategic initiatives. These products build on the threat intelligence expertise of the X-Force research and development team to provide a preemptive approach to security. As a trusted partner in security, IBM delivers the solutions to keep the entire enterprise infrastructure, including the cloud, protected from the latest security risks.
For more information
To learn more about IBM Security QRadar Network Anomaly Detection, contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We’ll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: ibm.com/financing

© Copyright IBM Corporation 2013
IBM Corporation
Software Group
Route 100
Somers, NY 10589
Produced in the United States of America
January 2013
IBM, the IBM logo, ibm.com, QRadar, AppScan, SiteProtector, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.


Please Recycle

WGD03022-USEN-00