POSITIVE TECHNOLOGIES MAXPATROL™ AND IBM® SECURITY QRADAR® SIEM

INCREASE SECURITY AND IMPROVE INCIDENT RESPONSE PERFORMANCE

Highlights

+ Accelerate threat detection of known and 0-day vulnerabilities
+ Manage emerging threats in real-time and speed up incident response
+ Improve network visibility to assure compliance and increase security

THE CHALLENGE

As hackers become smarter and threats become more advanced, the range of security tools employed by enterprises has also expanded to include Intrusion Detection/Prevention Systems, firewalls, antivirus and DLP tools, vulnerability scanners and GRC and compliance solutions. But often these systems work in isolation, each generating huge quantities of raw data which security teams then must correlate and analyze before they can identify, prioritize and tackle risks.

Most large organizations use Security Information and Event Management (SIEM) technology to help with real-time data collection and correlation for millions of security events and alerts generated by network hardware, applications and security tools. SIEM solutions also log data to create audit trails, perform incident discovery and investigation and generate compliance reports.

But a SIEM's ability to alert organizations about potential dangers is directly dependent on the quality of data it receives. If security tools are unable to query certain systems, produce results plagued by false positives or worse yet false negatives, the SIEM alone cannot give a complete, accurate picture of the overall risks. It is therefore essential to select best of breed solutions that work together to provide coverage for your entire infrastructure and deliver results you can trust.

THE SOLUTION:

MaxPatrol and IBM® Security QRadar® SIEM

MaxPatrol™, an all-in-one vulnerability and compliance management solution, is trusted by over 1,000 enterprises to maintain security and compliance. MaxPatrol provides agentless, low-privileged, non-intrusive, black-box and white-box identification of vulnerabilities and misconfigured settings. In addition, MaxPatrol also provides network and system inventories of software, hardware, licenses, removable and wireless devices as well as operational information on users and roles, sensitive data, segregation of duties and much more.

QRadar SIEM allows single pane troubleshooting of issues to create a Security Operations Center. Its powerful rules engine correlates data from a wide range of security systems, detects anomalies and generates a manageable list of an organization's highest priority risks.

Positive Technologies and IBM have partnered to give organizations greater security and confidence with an efficient, integrated solution. MaxPatrol's regular assessments provide QRadar SIEM with extensive audit and vulnerability data on all information and operational assets including network equipment, VOIP, Wireless and RAN telecom equipment, operating systems, databases, desktop and business applications, virtualization and terminal platforms, security systems, and critical infrastructure such as Industrial Control Systems and Enterprise Resource Planning. As new threats emerge, QRadar SIEM can trigger additional MaxPatrol scans to verify your level of risk.

BUSINESS BENEFITS

When used together, MaxPatrol vulnerability and compliance management and QRadar SIEM allow organizations to:

Accelerate threat detection – MaxPatrol's high-quality vulnerability assessment data helps QRadar SIEM to refine the mass of information produced by other security mechanisms such as IPS and firewalls, giving you a faster route to identifying and remediating the REAL weaknesses that threaten your infrastructure and significantly improving your overall security posture

Prioritize threats – QRadar SIEM understands which systems are most critical to you and correlates this information with MaxPatrol's vulnerability data to highlight the most dangerous threats to your business

Reduce false positives – MaxPatrol's scans not only identify vulnerabilities but also the conditions that might prevent attackers from exploiting them. Armed with information on closed network ports, stopped services or firewall rules that block traffic, QRadar SIEM can downgrade the warnings for vulnerabilities that cannot be exploited; letting you focus on the ones that present a real danger

Improve Network Visibility – MaxPatrol's advanced asset discovery techniques identify any unmanaged assets or devices on your network, ensuring QRadar SIEM has a complete picture of your infrastructure, including highlighting gaps such as missing or disabled anti-virus software

Manage emerging threats in real-time – QRadar SIEM is able to trigger additional MaxPatrol scans to verify evidence of emerging risks or unfolding attacks. Daily updates to MaxPatrol, by Positive Research, ensures QRadar SIEM is aware of threats related to the latest 0-day vulnerabilities

Simplify configuration management – MaxPatrol provides key data on systems configurations, allowing QRadar SIEM to analyze system changes over time and how these changes affect the overall security posture of your systems

About IBM Security QRADAR SIEM

IBM® Security QRadar® SIEM is a network security management platform that provides situational awareness and compliance support. QRadar SIEM uses a combination of flow-based network knowledge, security event correlation, and asset-based vulnerability assessment to protect assets and information from advanced threats. It consolidates log source event data from thousands of devices, endpoints and applications distributed throughout a network. It performs immediate normalization and correlation activities on raw data to distinguish real threats from false positives. IBM Security QRadar SIEM can also correlate system vulnerabilities with event and network data, helping to prioritize security incidents.

About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management and threat analysis solutions to more than 1,000 global enterprise clients. Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring compliance with regulatory requirements; and blocking real-time attacks. Our commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on SCADA, Banking, Telecom, Web Application and ERP security, and distinction as the #1 fastest growing Security and Vulnerability Management firm in 2012, as shown in an IDC report*. To learn more about Positive Technologies please visit www.ptsecurity.com.

*Source: IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. Based on year-over-year revenue growth in 2012 for vendors with revenues of $20M+.

© 2014 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.

IBM_PAB_A4.ENG.0033.01.DEC.29.2014

POSITIVE TECHNOLOGIES