CONTINUOUS MONITORING
For Government Agencies

Using QRadar to Ensure Compliance and Reduce Risk
Executive Summary Government agencies confront an increasingly hazardous IT security environment. According to the Government Accountability Office, the number of reported security incidents increased by over 650 percent during fiscal years 2006–2010. At the same time, government agencies have widespread deficiencies in security controls, leading to vulnerabilities undetected breaches, and insider fraud.

To help meet these challenges, the federal government is implementing FISMA 2.0, which will replace the annual paper-based exercises of FISMA 1.0 with risk-based IT security strategies based on deploying enterprise continuous monitoring solutions. These solutions will continually assess the actual security state of agencies’ IT networks and systems and provide scoring information that managers can use to prioritize actions needed to reduce risk and improve their security grades. Continuous monitoring will enable agencies to determine their own security health and compare it to other agencies so they can most cost-effectively apply their resources towards identifying and repairing their security gaps and vulnerabilities. FISMA 2.0's scoring will also allow the different lines of business, operations, and finance within an agency to better understand each other and work together, while enabling agencies to gain the same operating efficiencies from IT investments that Fortune 500 companies have realized.

The QRadar® Security Intelligence Platform from Q1 Labs provides comprehensive and in-depth continuous monitoring of an organization's security status and monitors and provides advanced security analytics for any changes that occur to determine vulnerabilities, threats, and breaches. It integrates previously disparate functions — including SIEM, risk management, log management, and network behavior analytics — into a total security intelligence solution that fits the constrained budgets and resources of government agencies. By providing agencies with the most intelligence, reduced complexity, high scalability, more automation and out of the box rules and reports, QRadar delivers a quick return on investment while meeting and exceeding the requirements of FISMA.

A Federally Funded Research and Development Center (FFRDC) recently implemented a continuous monitoring solution by leveraging its existing QRadar assets. The FFRDC follows best practices and chooses best-of-breed security solutions, and it determined that the QRadar Security Intelligence Platform would enable them to comply with the FISMA 2.0 requirements of some of its government contracts. The solution has integrated well with the FFRDC’s systems, and it effectively protects its data and allows secure access by its staff — all within a constrained budget. The FFRDC’s information security manager has no doubt that using QRadar for continuous monitoring has significantly improved his organization’s IT security and situational awareness at an affordable cost.
The Security Landscape

According to the Government Accountability Office (GAO), the number of security incidents reported by federal agencies is constantly rising — increasing by over 650 percent from fiscal year 2006 to fiscal year 2010. (The number of incidents was almost certainly greater because a large number go undetected.) Moreover, the variety and sophistication of the threats and attacks have also been steadily growing. The bar keeps being raised as the attackers get smarter, more experienced, and devote ever-increasing resources to their efforts.

Compounding the growing number and kinds of threats, the GAO and federal agencies have identified significant deficiencies in the security controls on federal information systems, which have resulted in pervasive vulnerabilities, undetected breaches, and unknown damage and theft. These include weaknesses in the security of both financial and non-financial systems and information, including vulnerabilities in critical federal systems. These deficiencies continue to place federal assets at risk of inadvertent or deliberate misuse; financial information at risk of unauthorized exposure, modification or destruction; sensitive intellectual property at risk of theft or vulnerable to espionage; and critical operations at risk of disruption.

Government IT security professionals, who can justifiably feel overworked and underappreciated, not only have to play catch-up with the threats and attacks, but also deal with limited resources and increasing pressures to do more with less. They also have to ensure that they are enabling — rather than preventing — their employees to do their jobs effectively and not inhibiting them from being productive.

The good news is that agencies have an abundance of products and systems to collect and analyze network activity and incident and vulnerability data. Unfortunately, that is also the bad news, because those devices produce a deluge of data that must be analyzed and acted upon to prevent breaches. In most cases, the data is not refined enough for users to quickly resolve. Instead, they must weed through large numbers of potentially risky events and activities, increasing the likelihood that the more significant threats will be missed.

FISMA 2.0 and Continuous Monitoring

The federal government is implementing FISMA 2.0 to help agencies develop risk-based IT security strategies to better handle the threat of attacks. Instead of FISMA 1.0’s annual paper-based exercises that yield instantly obsolete deliverables, FISMA 2.0—in the form of the Continuous Asset Evaluation, Situational Awareness and Risk Scoring (CAESARS) Reference Architecture, released by the Department of Homeland Security (DHS) in September 2010, NIST 800-37, and NIST 800-53 — will require agencies to move beyond a “checkbox” approach to compliance by deploying enterprise continuous monitoring solutions.

The integrated and end-to-end CAESARS approach will enable agencies to:

- Assess the actual state of each information technology (IT) asset under management;
- Determine the gaps between the current state and accepted security baselines;
- Express in clear, quantitative measures the relative risk of each gap or deviation;
- Provide simple letter grades that reflect the aggregate risk of every site and system;
- Ensure that the responsibility for every system and site is correctly assigned;
- Provide targeted information for security and operations managers to prioritize the actions needed to reduce risk and improve their grades.

According to NIST 800-37, an effective organization-wide continuous monitoring program includes:

- Configuration management and control processes for organizational information systems;
- Security impact analyses on proposed or actual changes to organizational information systems and environments of operation;
- Assessment of selected security controls (including system-specific, hybrid, and common controls) based on the organization-defined continuous monitoring strategy;
- Security status reporting to appropriate organizational officials;
Active involvement by authorizing officials in the ongoing management of information system-related security risks.

Making these assessments on a continuous or nearly continuous basis is a prerequisite for moving IT security management from isolated assessments, supporting infrequent authorization decisions, to continuous risk management as described in current federal guidance of the NIST and OMB mandates. According to an April 5, 2010 memorandum from former OMB CIO Vivek Kundra, “Continuous monitoring is the backbone of true security… the threats to our nation’s information security continue to evolve and therefore our approach to cybersecurity must confront these new realities on a real time basis.”

Continuous monitoring of computing and network assets requires up-to-date knowledge of the security posture of every workstation, server, and network device, including operating system and application versions and patches, vulnerabilities, and threat signatures and patterns. Information security managers will use the summary and detailed information to manage and report the security posture of their respective agencies. While each agency is required to implement continuous monitoring, they are not required to implement a “one size fits all” solution. Each agency can implement the continuous monitoring solution that best fits its own requirements and environment as long as its solution provides the required monthly data to the DHS repository known as CyberScope. Defense and intelligence agencies will have to provide their required security data to the Defense Department and intelligence community versions of CyberScope.

Continuous monitoring aims to help agencies determine their security health by translating this data into metrics that will lead to a letter grade for each organization within an agency, and to each agency overall, so that they can regularly determine their security posture and identify their greatest risks and vulnerabilities. Above all, it allows each agency to prioritize these risks and vulnerabilities.

Using regular letter grades will foster a sense of competition among operations and security professionals, bureaus, departments, and agencies, leading to improved scores. Low scores will encourage organizations to take the necessary measures to improve their scores. However, unlike the annual letter grades that came out of FISMA 1.0 drills, the FISMA 2.0 letter grades will not only give agencies (and DHS) a regular, timely security evaluation — they will also provide meaningful and actionable data about where the agencies need to improve and what their priorities should be.

Finally, the FISMA 2.0 scoring mechanism, unlike the annual grades that came out of FISMA 1.0 drills, will translate technical jargon into language understood by lines of business, operations, and finance.

The Business Case for Continuous Monitoring

Since January 2011, federal agencies have been required to report continuous monitoring data to CyberScope on a monthly basis. However, continuous monitoring is not just another onerous mandate with which agencies must comply. Allan Paller, research director at the SANS Institute, put it best in his testimony to the U.S. Senate Committee on Homeland Security and Governmental Affairs in June 2010: Continuous monitoring, as he observed at the State Department, “causes rapid risk reduction with low overhead.” This observation should get the attention of both security and business managers.

Moreover, continuous monitoring makes IT security solutions more relevant to agency business executives. The notion of scoring makes security understandable by anyone. This scoring approach also makes it easy to compare the security status of one business unit or agency with another. It helps system managers and information assurance managers have an understandable, security-focused conversation with their executive management instead of mutually-incomprehensible discussions that have so often occurred. It certainly will resonate with business executives more than the pleas of a network security manager clamoring for more security investments.

Continuous monitoring will also enable agencies to gain the same operating efficiencies from IT investments that Fortune 500 companies have realized — something that is even more relevant when agency budgets are trending downwards.

One of the biggest criticisms of FISMA 1.0 has been that an agency could get an “A” security rating but actually have significant security vulnerabilities and breaches. It could even have foreign adversaries actively penetrating its network and exploiting its assets. At the same time, an agency could get an “F” or “D” but possess a superior security posture to the agency that received an “A,” because of all the actions the “failing” agency had done to identify and reduce its security vulnerabilities.
The scoring employed by FISMA 2.0 will much more accurately reflect the actual security environment of an agency than did the scoring of FISMA 1.0. However, security is a process, not a destination, especially when the attackers from without and within are increasing, evolving, and improving. Likewise, the metrics tracked under continuous monitoring will need to improve to better reflect the true state of the enterprise. This was not possible under FISMA 1.0.

QRadar Security Intelligence Platform from Q1 Labs, an IBM company

The QRadar® Security Intelligence Platform from Q1 Labs integrates previously disparate functions — including SIEM, risk management, log management, network behavior analytics, and security event management — into a total security intelligence solution, making it the most intelligent, integrated, and automated security intelligence solution available. It employs a unified architecture for collecting, storing, alerting on and analyzing log, threat, vulnerability, and risk related data, delivering 360 degree intelligence across your network with full visibility into an organization’s security and risk posture.

QRadar performs industry-leading event correlation, network behavior analysis, and intelligent context gathering — using asset data, vulnerability data, configuration data, network topologies, identity data, third-party security information sources and more. By combining event information, network flow activity, and network and asset context, QRadar delivers warnings of future risks before they are exploited, advanced threat intelligence about possible ongoing attacks, and comprehensive forensics after a breach. This combination enables an enterprise to prepare for and respond to incidents and assess impacts. As an integrated solution, it can also reduce the time spent researching and responding to security incidents by as much as 80 percent compared to siloed systems.

QRadar Continuous Monitoring

QRadar provides comprehensive and in-depth continuous monitoring of the effectiveness of an organization’s security controls over time. Additionally it monitors any changes in the organization’s network which, if not properly planned and implemented — and especially if not authorized — can create vulnerabilities in the network. Its advanced threat detection and policy engines constantly monitor the network for changes that may be potential threats or that impact policy compliance or which may result in security gaps. It also leverages existing vulnerability management data and applies real-time analytics, topology, and policy context to prioritize vulnerability data and make vulnerability assessment (VA) tools more effective. QRadar presents these data and analyses to users in priority order through a simple-to-use workflow interface. (See Figure 2.)

Figure 2: QRadar Security Intelligence Platform allows you to continuously monitor all of your network activity and be able to view everything from a single consolidated dashboard.
QRadar’s Layer 7 activity analyses create an objective view of user and asset activity that is used to profile behavior and detect changes in the network, applications, and more. QRadar continuously compares configuration data from network and security infrastructures, such as routers, firewalls, and IPSs, to an organization’s policies and raises alerts to changes that are made out of policy. This data, combined with network activity analysis, can automatically test the effectiveness of rule policies on security devices. QRadar’s continuous monitoring can also provide forensic evidence that can be used to track down insider fraud and theft.

The QRadar risk management solution can determine exposure from vulnerabilities based on your assets and their location on your network. It automates risk management to gain visibility into the network environment and remediates any potential security, policy, and compliance risks before an incident occurs. The QRadar risk management solution, combined with SIEM, log management, and network behavior analysis, can provide government organizations the “single console” view of their networks that is needed to meet continuous monitoring requirements.

The integrated security intelligence capabilities of QRadar can not only meet but exceed the new requirements of FISMA 2.0. Its unique correlation and integration of all surveillance feeds yield more accurate data for the operator (including fewer false positives), more complete and insightful forensics for an incident response manager, and more complete reporting to provide transparency, accountability, and measurability for auditors.

Figure 3: QRadar Security Intelligence Platform provides the real-time application visibility and flow analysis required to fully understand and respond to the activity taking place in your network.
QRadar Continuous Monitoring in Action: Case Study

To achieve compliance with FISMA 2.0 and respond to increasingly advanced threats, the information security manager of a Federally Funded Research and Development Center (FFRDC) recently made the implementation of continuous monitoring his highest priority. At the same time, he confronted budgetary constraints that compelled the organization to do more with less.

Although it is not required to follow regulations that apply to federal agencies, the FFRDC usually follows NIST guidelines, as well as applicable Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). Moreover, it has some government contracts that do require FISMA and other accreditations. The FFRDC therefore follows best practices—such as NIST 800-53—and chooses best-of-breed security solutions that integrate well with its systems, effectively protect its data, and allow secure access by its staff.

In considering existing solutions already in place within the center, the manager found that their current QRadar SIEM solution was an excellent fit to provide continuous monitoring as well. Extending their use of QRadar to perform continuous monitoring has been easily achieved by deploying QRadar connectors to a handful of additional compliance systems and vulnerability scanning devices and then repositioning existing staff.

According to the manager, continuous monitoring enables his organization to see the actual state of their environment and the threats they are facing, and proactively restrict access as problems or vulnerabilities appear. “My mantra is to have eyes in as many places as possible throughout the network infrastructure and QRadar provided that,” says the manager. “Given the solution’s intelligent correlation of numerous data sources, including network flows, I could not get more value from any other solution.”

The FFRDC has been using the QRadar SIEM solution since 2008. It originally tested a multitude of SIEM products (putting them through their paces to see how they worked in the customer’s actual environment), and ultimately chose QRadar as the most effective and affordable solution.

The FFRDC has been successfully performing continuous monitoring with QRadar since the beginning of 2011, and this is now its highest security priority. “We didn’t implement continuous monitoring because of government mandates but because it was the best practice,” says the information security manager. “Our systems go through certification and accreditation (C&A) but the systems continuously change, just as the security bar gets higher because the attackers are continuously improving their tactics, techniques, and procedures.”

The FFRDC, which needs to stay on top of the latest and greatest technologies, has looked at other products since implementing QRadar, but has not found any other solution that provides as much intelligence, flexibility, or affordability. Q1 Labs also continues aggressively enhancing QRadar, according to the manager, so the solution meets an ever-expanding set of needs. Moreover, “Q1 has provided technical and professional support that has exceeded what we expected or what we receive from other vendors,” says the manager. “They have a sincere desire to help you out and go above and beyond what we’d expect from a normal support organization when we need help.”

The information security manager has no doubt that expanding the use of the QRadar Security Intelligence Platform to perform continuous monitoring has significantly improved the IT security and situational awareness of the FFRDC. “I’m sure that continuous monitoring will deliver a significant ROI for us by protecting against many threats we were previously vulnerable to, and quickly remediating incidents that would have gone unnoticed in the past.”

“I’m sure that continuous monitoring will deliver a significant ROI for us by protecting against many threats we were previously vulnerable to, and quickly remediating incidents that would have gone unnoticed in the past.”

--Information Security Manager from a Federally Funded Research and Development Center
Summary and Conclusion

For years, federal agencies have complained that FISMA was a paper exercise that wasted scarce resources while producing a misleading and instantly outdated picture of an agency’s IT security state of affairs. FISMA 2.0 now requires agencies to carry out risk-based assessments on the basis of continuous monitoring of their IT infrastructures. Unlike many other mandates issued to government agencies, this one goes a long way towards answering the previous complaints and providing a framework for the agencies to measure, compare, assess, and act upon their actual security conditions on an ongoing basis.

With continuous monitoring as a mandate, agencies need to find a solution that best meets federal requirements while meeting increasingly tight budgets, and “doing more with less.” Fortunately, agencies that already use QRadar security products can easily leverage their existing assets to comply with the new mandates and most cost-effectively implement continuous monitoring. Other agencies can adopt QRadar’s industry leading SIEM solution, which easily integrates with almost all systems, applications, and devices to meet the new mandates and stay within budget — all of which are backed up with technical and professional support that consistently earns high praise from customers.

In both cases, agencies using QRadar will be able to fulfill their requirements, significantly improve their security and situational awareness, improve communication and understanding across their enterprises, and attain ROIs enjoyed by Fortune 500 companies.

About Q1 Labs, an IBM Company

Q1 Labs is a global provider of high-value, cost-effective security information and event management (SIEM) products. The growing company’s flagship offering, QRadar, integrates previously disparate functions — including log management, network behavior analytics, and security event management — into a total security intelligence solution. QRadar provides users with crucial visibility into what is occurring within their networks, data centers, and applications to better protect IT assets and meet regulatory requirements. Q1 Labs’ customers include healthcare providers, energy firms, retail organizations, utility companies, financial institutions, government agencies, and universities, among others.

Subject matter expertise for this paper was provided by:

David Wilson, Director of Cybersecurity Strategy for Telos Corporation. Follow him on Twitter @DJWils285 for more insight on IT security.