IBM QRadar SIEM Support of NIST 800-53 Security Controls

REDUCE COMPLIANCE BURDEN >> PRE-BUILT REPORTS >> MINIMIZE TIME AND ACCURACY OF REPORTING

IBM QRadar SIEM Aids Agencies In Meeting Reporting Timelines

The NIST 800-53 standards and guidelines provide a comprehensive set of security controls laid out in an intuitive, prioritized framework. It is mandated that many state and federal organizations implement this framework to help ensure the security and privacy of the governmental infrastructure and data they manage. Many other types of organizations also choose to implement this framework due to its broad acceptance and completeness of vision.

As organizations implement the controls within the framework, they need to both demonstrate that those controls are in place as well as continuously monitor, analyze, and act upon the information and alerts that they generate.

However, every federal agency CISO (Chief Information Security Officer) and their teams spend enormous amounts of time selecting, implementing, operating, and reporting on what controls are implemented and how they are performing against key metrics that the agencies are held accountable to. As of September 2019, agencies will be assessed under the AWARE algorithm, giving agencies a numerical score of their overall cyber risk.

Each of the control systems under NIST 800-53 produces a constant stream of activity logs, which need to be analyzed for indicators of compromise in as near real-time as possible. Recent guidance under NIST SP 800-137 (ISCM) recommends that the total cycle time for log ingestion, analysis, alerting, response, and reporting should be less than 72 hours. There is no specific archival period mandated for log data, so most agencies retain them on a long-term basis for incident forensics and audit purposes. More recent retention guidance does prescribe a minimum of 36 months.

There are many solutions today that will collect, normalize and retain log data in a common format, but then the question arises of how an organization should best make use of all the log data. Over time, industry and government agencies have learned that there are a growing set of best practices needed but there are many opinions on what is necessary and effective, and what is not. There has been a tremendous amount of debate on how the limited amount of skilled manpower is best utilized to sift through this data to identify indicators of compromise within an organization.

Many organizations have reasoned that simply collecting all of the data into large data lakes satisfies the need for large scale, long term, management, analysis, and compliance. Unfortunately, many of the deployments have little added benefit beyond that of a massive spreadsheet. The challenges with this approach are many, the most critical are highlighted here.

1. There is little if any indexing and data structuring, so search and retrieval is cumbersome and often ineffective.
2. Search terms must be very specific, which will fail to capture the “unknown” activity patterns.
3. There is no real-time correlation of new and existing data, limiting identification of patterns and anomalies.
4. Event chaining in the context of malicious behavior is difficult.
5. Detection of, and response to incidents can take days or even weeks.
6. Mapping activity to control efficacy and compliance is extremely difficult.
7. Correlation happens at CPU speed (millions of times per second), searches happen based on time intervals (i.e. 1 minute, 30 minutes, daily, weekly, etc.
8. Meeting a persistent 72-hour cadence using searches against an unstructured data lake (with or without indexes) is not sustainable at scale and does not meet the spirit of the 800-137 guideline.

SOLUTION

The IBM QRadar SIEM platform is the recognized market leader according to Gartner in their most recent magic quadrant comparison, providing the most comprehensive suite of purpose-built tools available, for large scale log data ingestion into a real-time structured data platform with hundreds of pre-built search terms, advanced analytic algorithms and intelligence that provide near real-time alerting even in the most demanding environments. IBM QRadar SIEM also offers the broadest suite of data extraction connectors (450+ DSM's) and thriving ecosystem of partners, allowing an agency to ingest audit logs from virtually any legacy or contemporary system in their domain.

IBM provides the most comprehensive suite of tools available that are made to ingest large amounts of log data at any scale into a structured data engine with out of the box algorithms and intelligence that provides real-time alerting in the most demanding environments. Originally developed in 2006, this platform has continued to lead the market in capabilities for ingestion of log data, event notification, event correlation and chaining, and many have called IBM QRadar SIEM the most comprehensive security intelligence platform available worldwide.

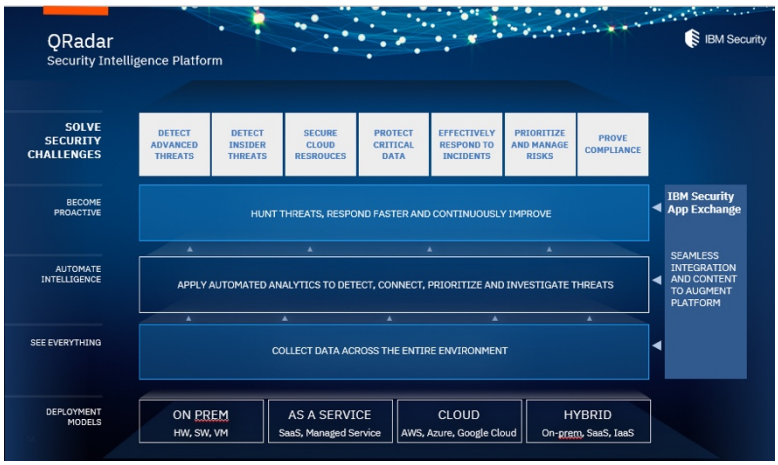

Figure 1. provides a graphical representation of the Qradar system and its capabilities.

NIST 800-53 Compliance Capabilities

The NIST Content Pack for NIST 800-53 compliance provides agencies with a map of observed activity matched to their required security controls. IBM QRadar is not only able to provide the evidence required for each of these controls, but also combines additional analytics and context to alert the security/SOC analysts of the actual intent of the malicious activity, such as privilege escalation, not just the fact that login attempts have failed.

Summary

IBM QRadar SIEM provides the most advanced capabilities of any SEIM platform in supporting government agencies need for compliance under NIST 800-53 standards and guidelines. By integrating the follow-up compliance reporting with the day to day activities of security operations it reduces the timeline, complexity, and burden on the agency's personnel.

For more information visit:IBM

QRadar Homepage: https://www.ibm.com/security/security-intelligence/qradar

NIST CONTENT PACK: http://ibm.biz/QRadar_NIST_800-53

QRADAR SUPPORT FOR 800-53 BY CONTROL GROUP

CONTROL GROUP	FUNCTION	HOW QRADAR SUPPORTS
AC	Access Control	Access Control is supported out of the box with the User Role Management window. You can see alerts to active QRadar users as well as network users.
AT	Awareness and Training	AT is supported upon install as QRadar gives you real time alerting to over 1500 preset rules. Training is done through IBM Security Learning academy.
AU	Audit and Accountability	Out of the Box, changes in QRadar are recorded in the audit logs. You can view the these in plain text.
CA	Security Assessment and Authorization	QRadar comes with two preinstalled apps that help you to manage your apps and content inventory, and the security of app authorization tokens.
CM	Configuration Management	Configuration of QRadar is managed out of the box with the User Groups and allows for Role Based Access to all content
CP	Contingency Planning	QRadar platforms comes standard with High Availability failover and Disaster Recovery set up features.
IA	Identification and Authentication	QRadar can determine who and when someone is accessing your network in real time. With additions such as QRadar Network Insights you will see real time forensics.
IR	Incident Response	QRadar allows you to react in near real time to offenses that occur by email or text message. With the Resilient IRP you can orchestrate any issue.
MA	Maintenance	Service and Support requirements are answered with your purchase of QRadar. With federal client receiving Business Critical Support
MP	Media Protection	With QRadar federal clients receive the ability to maintain their secure information as no media will be shared.
PE	Physical Environment Security	Logging capabilities include the ability to access all physical controls to QRadar
PL	Planning	QRadar supports the ability to report and present who will have access to QRadar and for what reason through the report wizard.
PM	Program Management	QRadar out of the box will allow for roles to be assigned for access to each view.
PS	Personnel Security	With the QRadar User Behavior Analytics application you can assign high risk users different report criteria than low risk users.
RA	Risk Assessment	Upon turn on of QRadar all rule sets are given a risk tolerance score that is associated with Severity, Credibility and Relevance.
SA	System and Services Acquisition	All QRadar physical hardware is serviced on a five-year lifecycle with total cost of ownership available up front.
SC	System and Communications Protection	With Role Based Access control QRadar can report on all network systems and communication links to those systems.
SI	System and Information Integrity	Out of the box QRadar is able to monitor all systems on the network and provide reporting on any and all anomalous activity.