Being SIEM Thorough: Would You Trust a Check-up that Didn't Include Your Heart?

How to Mix Mainframe into Your Enterprise Security Strategy

Imagine if during your next annual checkup, your doctor says, "we are beginning a new holistic approach to our patient's health. We're going to monitor your health from head to toe, but we won't be concerning ourselves with your heart". You'd likely question that strategy or look for another doctor, wouldn't you? It's no different when building your security strategy for your entire enterprise.

An all-encompassing security strategy is imperative. When developing your enterprise security strategy, you cannot leave IBM Z mainframes by the wayside. Although security is woven throughout the architecture of the mainframe, it does not secure itself. Finding yourself stuck in this mindset - that the mainframe can be left completely alone - can be dangerous to the confidentiality, integrity and availability of your critical data, and therefore, the applications and transactions that depend on that data.

Securing your mainframe shouldn't be a cumbersome chore. QRadar can help close the security gap between your distributed and mainframe houses by taking advantage of zSecure Alert. Additionally, your security administrators do not need deep mainframe expertise to take advantage of this solution.

Highlights

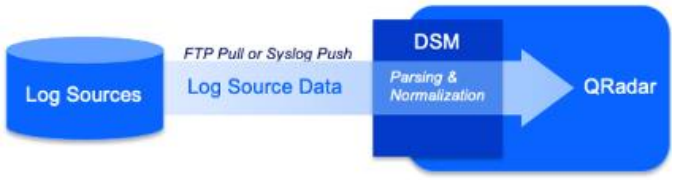
- Gain comprehensive insights to quickly detect, investigate, and respond to potential threat
- Real-time analysis identification to prevent or minimize damage to the organization
- Provide support for several major compliance reporting requirements
- Scale to meet the event log and network flow monitoring and needs of most organization

Background

IBM QRadar (Security Information and Event Management – SIEM) is a highly scalable enterprise solution that consolidates log source event data from thousands of devices distributed across a network, stores every activity in its database, and then performs immediate correlation and application of analytics to distinguish real threats from false positives. QRadar SIEM deploys quickly and easily, providing contextual and actionable surveillance across the entire IT infrastructure, helping organizations detect and remediate threats often missed by other security solutions. These threats can include inappropriate use of applications, insider fraud and theft, and advanced “low and slow” threats easily lost in the noise of millions of events.

To have a better understanding of how QRadar fits into the overall mainframe security architecture, we need to understand how data can be accessed by QRadar.

QRadar ingests events “flows” and vulnerability data from the enterprise. Log sources are from server-type devices while flows are from network-type devices. “Flows” refers to meta-data carved from documents found in packets, in addition to NetFlow. IBM z/OS feeds can be fed into QRadar via FTP pull or syslog stream. When data arrives in QRadar, it is parsed and normalized via a QRadar Device Support Module (DSM). There are five options available today from IBM Security:



High-Level Conceptual Map

Option 1: Free Script for FTP

Free script can read SMF records and generate log files to be pulled into QRadar. The QRadar DSM Editor, a GUI tool, can help create DSMs for incoming data.

Option 2: zSecure Script for FTP

IBM zSecure can read SMF records and generate log files to be pulled into QRadar. There are six public DSMs that support zSecure feeds: z/OS, RACF, TSS, ACF2, DB2, and CICS. Incoming data is parsed and normalized out of box.

Option 3: zSecure Real Time Feeds

IBM zSecure can read SMF records and stream to QRadar real time. The same six QRadar DSMs also apply here. Incoming data is parsed and normalized out of box. Real time rules and analytics process mainframe data out of box.

Option 4: zSecure Alert

Alert is a local security event monitor for z/OS. IBM provides 70+ rules to be processed on z/OS. If a rule discovers something, it can emit an event to QRadar. There is a specific QRadar DSM for zSecure Alert that parses and normalizes for further rule processing and analytics in QRadar.

Option 5: Guardium

Guardium sends alerts to QRadar. Common alerts include failed logins, unauthorized access, SQL error codes, and privilege escalations. QRadar can be configured to automatically add new members to Guardium groups to control access to data. Database vulnerabilities from Guardium is treated as a Vulnerability Assessment (VA) report in QRadar. Vulnerability data is associated with Assets in the QRadar view of all distributed and mainframe assets.

Options	DSM	Auto Detect	QRadar Rule Processing	Event Flow	Set-Up
1 (Free Script for FTP)	No	No	No	Peaky	Hard
2 (zSecure Script for FTP)	Yes	No	No	Peaky	Moderate
3 (zSecure Real Time Feeds)	Yes	Yes	Yes	Stream ~300 per second	Easy
4 (zSecure Alert)	Yes	Yes	Yes	Stream < 100 per day	Easy
5 (Guardium)	Yes	Yes	Yes	Stream ~100 – 1000s per day	Moderate

Summary chart of five QRadar data access options

Now that you have a better understanding of how QRadar can be integrated with your mainframe sources, the next section highlights example QRadar Rules use cases that can easily be adopted into your environment. Let's explore three mainframe security use cases you can leverage with QRadar.

1. Insider Threat
2. Privileged User Monitoring
3. Sensitive Data Monitoring

Insider Threat

Mainframes have built-in layers of security over the years, making them difficult to hack. Corporate employees, already on the inside of mainframe systems, may pose significant threats to data and applications. QRadar processes can be used to guard against insider threats. Mainframe system programmers and database administrators require special security privileges to perform their jobs. However, those jobs do not all require the same privileges. For example, the operating system administrator does not need to have access to database records. According to the Principle of Least

Privilege, each person should have the minimal security privileges required for their role. The Security Operations Center (SOC) must be alerted to inappropriate data access, changes to user privileges, and changes to security auditing processes. Examples of insider threats use case rule include:

- A Mainframe User Account Obtained Privileged Access: Changes to mainframe user account privileges (e.g. SPECIAL level or new authorities)
- Privilege Escalation Pattern Detection: Detects pattern of events associated with privilege escalation scripts found on mainframe hacking resources
- Z System – FTP Violation: Attempts to transfer data to a site outside the mainframe (FTP)

Privileged User Monitor

Privileged user monitoring can be considered an extension of insider threat. However, in this case, we are specifically concerned with actions that are limited to privileged users. Privileged users, such as system or database administrators, have escalated access rights, which makes the account particularly attractive targets for hackers. Examples of privileged user monitoring use case rule include:

- Privileged User Accessing Sensitive Data: Unauthorized data access or access attempt by an internal privileged user
- Unexpected Hour Privileged User Activity: Flagging special user from doing suspicious activity when activity is used outside specified green zone
- Highly Authorized User Revoked for Password Violations: Warning for a privileged user account being revoked on the IBM mainframe for password violations, such as excessive login attempts

Sensitive Data Monitoring

It's critical to protect all the sensitive information within your organization and prevent users from sharing this data outside of your infrastructure. The mainframe often houses your most important data. Whether it is sensitive information that needs to be protected for compliance and safety of employees or clients or key insight you don't want in your competitor's hands, there are major consequences to your critical data being compromised. Data can be compromised from malicious attacks or simply from an employee making a mistake, so how do we begin detecting indicators of compromise? Examples of sensitive data monitoring use case rule include:

- Repeated Failure to Alter Data Set Profile: Alert for excessive failed attempts to alter a dataset profile with insufficient authority
- UACC Set to Read / Update on Data Set Profile: Warning for changing the universal access on a data set profile on the IBM mainframe to Read or Update
- Identify Sensitive Dataset Name: Rule based on dataset high level qualifier that signals sensitive data. Example would be identifying SMHEALTH records

Conclusion

IBM QRadar is an All-In-One solution comprised of vulnerability and risk management, cyber threat hunting, security incident response, and forensics analysis. As mentioned previously, users do not need extensive mainframe knowledge to utilize this solution. You can now refer to the above use cases to jump-start your journey to better secure your mainframe system, the heart of your enterprise.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM Security QRadar SIEM, please contact your IBM representative or IBM Business Partner, or visit the following website: https://www.ibm.com/products/qradar-siem