

**IBM Tivoli Security Information
and Event Manager to
IBM QRadar
Planning Guide for Transition V1**

Table of Contents

Table of Contents	2
1. Objective and Introduction	4
1.1 Contributors	4
2. Overview of Transition Process	6
3. Inventory of the Functional Usage of TSIEM	10
4. Infrastructure Considerations.....	11
4.1 Networking.....	11
4.2 Backup.....	13
5. Deployment Planning and Considerations	14
6. Mapping of TSIEM components to QRadar components.....	15
6.1 Event collection chain	15
6.2 Audited Machines and Asset Profiles.....	17
6.3 User Roles and User Management	18
6.4 Normalization Component.....	19
6.4.1 TSIEM Event Sources	19
6.4.2 QRadar Device Support Modules.....	20
6.4.3 Enhanced User Information.....	22
6.4.4 TSIEM Variables to QRadar Variables Mapping.....	23
6.4.5 TSIEM W7 Model to QRadar Model Mapping	24
6.5 Log Management Component.....	32
6.5.1 TSIEM Data Storage.....	32
6.5.2 QRadar Data Storage.....	33
6.5.3 Collect Methods and Protocols.....	34
6.5.4 Indexing and Forensic Search	35
6.6 Policies, Reports, Alerts, and Distribution.....	36
6.6.1 TSIEM Policies, Reports, and Alerts	36
6.6.2 Log Management and TCR.....	38
6.6.3 QRadar Offences and Reports	39
6.6.4 Compliance Management Modules.....	42
6.7 Reports Transition.....	43

6.7.1	Basic Migration Principles for Compliance Reports	43
6.7.2	Hands-On Compliance Report Migration	45
6.8	Terminology Comparison	50
7.	Plan a QRadar deployment.....	52
7.1	Design the QRadar Architecture	52
7.2	Install Appliances	55
7.3	Reuse the TSIEM IPs and/or reconfigure endpoints	56
7.4	Do Initial Configuration	57
7.5	Convert business logic from TSIEM to QRadar	57
7.6	Migrate data or keep TSIEM online for a period of time for historical queries	61
8.	Appendix.....	62
8.1	Basic Algorithms for TSIEM Data Extraction	62
8.2	Basic Algorithm for QRadar Data Import	63
8.2.1	Processing QRadar Data via Log Source eXtension (LSX)	63
8.3	Determining Average TSIEM Event Flow Volume (EPS)	65
8.4	Data Sources Comparison	67

Index of Tables

Table 5-1	TSIEM W7 Generic Event Model	20
Table 5-2	QRadar Event Model	21
Table 5-3	TSIEM to QRadar variables mapping	24
Table 5-4	TSIEM W7 Reports.....	37
Table 5-5	TSIEM reports transition rules	45
Table 5-6	Terminology Comparison.....	51
Table 7-1	QRadar Appliance Models	53
Table 6-9	TSIEM to QRadar Sources Comparison.....	68

1. Objective and Introduction

IBM Tivoli Security Information and Event Manager (TSIEM) was developed as a compliance management monitoring and reporting product for various operating systems, applications and devices. IBM acquired Q1 Labs in 2011 with its industry-leading security intelligence platform QRadar, providing a security solution that can be used across the entire network.

Anyone who is planning a transition of TSIEM to QRadar should read this document first to determine what steps should be considered to create a transition plan. This document provides a high level description of the steps rather than the detailed technical description of how to perform the actual transition. Tooling is not part of this document although the description may help in designing such tooling. IBM Services or any other IBM Business Partner can help produce the appropriate toolbox to automate the transition. The customer should be prepared to keep their TSIEM installation to support historical reporting or log archive management to meet their compliance or audit requirements. This transition document therefore should only address the replacement of TSIEM by QRadar within the context of regulatory compliancy.

This document will provide a basic overview of TSIEM to QRadar data migration capabilities and options, as well as data storage principles.

Considered software platforms:

- IBM TSIEM 2.0
- IBM QRadar 7.0 MR4

1.1 Contributors

This document is the result of a joined effort by IBM professional services and ScienceSoft. Established in 1989, ScienceSoft is a mature international IT services company with locations in Eastern and Western Europe. The company's expertise lies in custom software solutions, IT consulting and IT outsourcing services. Highlights of the company include a staff of 300 experienced professionals, partnerships with IBM amongst others, ISO-certified processes and a number of industry awards. For years ScienceSoft has been serving a diverse customer base ranging from SMEs to multinationals.

ScienceSoft has substantial background in information security and SIEM. In 2004-2006 ScienceSoft

was a development partner of Consul bv, a leader of SEM/SIM space at that time. After the acquisition of Consul bv by IBM in 2006, ScienceSoft was a vendor of IBM, taking part in the development of TSIEM/TCIM and TSOM. In 2011, ScienceSoft launched a SIEM consulting department and since then has worked on IBM TSIEM implementation and customization projects around the world. In 2011 ScienceSoft also became a QRadar reseller. ScienceSoft has build software tools based on the information shared in this document, to help customers smoothly transition their TSIEM deployment to a QRadar deployment.

2. Overview of Transition Process

Transitioning from TSIEM to QRadar is a multi-step process. It is suggested that this entire guide be read through before starting the process in order to properly plan out the appropriate path. There is not an automated or scripted migration or upgrade, instead there is a series of steps to follow. The transition requires analysis and understanding of the business requirements, use cases, TSIEM configuration, any customizations made to TSIEM, and a basic understanding of QRadar features. Then a QRadar deployment can be planned to map business requirements to the new features in QRadar.

The transition from TSIEM to QRadar involves the following steps:

1. Understand the Current Business Requirements
2. Review the Use Cases using TSIEM
3. Evaluate the TSIEM Deployment
4. Understand the differences in TSIEM and QRadar
5. Plan a QRadar Deployment

At this point the execution of the transition plan can begin. Through each step of this process, IBM and business partners is here to help. Please make use of the Security Intelligence Professional Services group, Qmmunity forums, and the QRadar support help desk.

Note: There is no supported data migration path from TSIEM's depot to QRadar. Part of the planning includes a time period to keep TSIEM available for historic data requests or searches. There are some alternatives listed in the Appendix if data migration is necessary.

1. Understand the Current Business Requirements

Review the current business requirements for Log Management, Security Intelligence, and SEIM. Compare those to requirements used when TSIEM was acquired and implemented. Have

the business owners changed? Have the business drivers changed or business unit changed? Are there new requirements (compliance, regulatory, business) that need to be addressed? What requirements could not be solved in the past with TSIEM? Do other organizations need to be involved? How can QRadar be leveraged?

Before migrating, the organization should have been exposed to QRadar, Risk Manager and other components of the Q1 solution. It is useful to have a representative attend a QRadar training session to understand the solution as part of the planning process.

The customer should determine staffing and maintenance duties while they are planning the transition. The majority of QRadar customers have found they can achieve a greater level of visibility into their security posture with current staffing levels or less, thereby allowing those staff to perform other valuable activities.

Many organizations find adding flow data (Netflow, Qflow, etc) is a next step in their evolution towards Security Intelligence.

2. Review Use Cases with TSIEM

Review the usage of the current TSIEM deployment and take note of how it is used. Determine which log sources are actually utilized, which reports are providing value, etc. It is time to evaluate how TSIEM is being used to fulfill the business requirements. Before looking at the individual TSIEM components, review the following common use cases and see what roles TSIEM plays for the organization. Customers should evaluate their current use cases and requirements. Don't worry if use cases were used, but over time, have moved away from it.

a. Privileged User Monitoring Use Case

A very common use case for TSIEM is to monitor the actions of privileged users such as system administrators and database administrators. In this use case, the actions of these privileged users would be scrutinized to ensure that they were not stepping outside of common user actions. An example of this could be privileged users accessing data

that is not required to perform their regular daily activities, making unauthorized changes, or completing tasks using risky and/or unauthorized tools.

b. Policy Compliance Use Case

Another common use case is to track the activities in logs and comparing them against an acceptable use policy, flagging expectations and calling out particular events for special attention. In this use case, the goal is to be able to do effective log review across a large amount of data across an entire enterprise by white listing acceptable actions. The resulting policy exceptions would be a small percentage of the overall logs produced.

c. Centralized Log Management Use Case

Some customers decide to mainly use TSIEM as a centralized log storage application. The sole action of collecting logs off of endpoints and storing them centrally is often enough to pass certain types of audits. Once the Centralized Log Storage use case is fulfilled and log data is collected, then administrators can use that data for forensics to determine the source of a particular problem. An on-demand reporting database was loaded with the data the administrator needed.

d. Compliance Reporting Use Case

Often, the main business driver for installing TSIEM is to comply with government or industry regulations that require log management and compliance reports. In this use case, TSIEM is configured with a compliance management module which contains the specific reports required by that compliance mandate. These reports are generated on a schedule and reviewed for policy violations. If any problems need to be resolved, a trouble or change ticket is opened in an external ticketing system and routed to the appropriate group.

3. Evaluate the TSIEM deployment

Evaluating the TSIEM deployment is discussed in the next section.

4. Understand the differences in TSIEM and QRadar

Review the document to understand the differences in the two products and understand how that might apply to the current TSIEM deployment. TSIEM is a reporting tool that collects most events based on a batch schedule. That data is then parsed, mapped, analysed, and loaded into a relational database (DB2) also on batch schedule. QRadar collects most events in real-time. Event data is also parsed and mapped, but then QRadar correlates, and stores that data into a flat file based data store (Ariel). These architectural differences can change how you implement your workflows to meet business requirements. For example, TSIEM customers typically load data on a daily basis, allowing for deep analysis on yesterday's data. QRadar's real-time capabilities could enable a business to get alerts via email when something happens, so that quicker remediation can occur.

5. Plan a QRadar deployment

Once the TSIEM deployment has been reviewed and concepts have been considered, then the QRadar deployment can be planned. Here are the steps to a successful QRadar Deployment:

1. Design the QRadar Architecture
2. Install appliances
3. Reuse the TSEIM IPs and/or reconfigure endpoints
4. Do Initial Configuration
5. Convert business logic from TSIEM to QRadar
6. Migrate data or keep TSIEM online for a period of time for historical queries

For details on these steps, see the final chapter.

3. Inventory of the Functional Usage of TSIEM

Before an actual transition is planned, the customer should have a clear understanding of how the TSIEM product is being currently used. Areas to consider include:

- Current event sources that are sending logs to TSIEM
- Current security processes that rely on TSIEM reporting or alerting.
- Current audit and monitoring requirements for regulatory and compliancy purposes. This also includes determining audit configuration requirements needed
- Customization of TSIEM which can include custom event sources and custom reports.

One major difference between TSIEM and QRadar reporting is the actual fields being used for reports in both products. The way QRadar reports are organized gives rather limited possibilities for easy migration of TSIEM Reports as this step requires the suitable mapping of TSIEM variables to QRadar Event Categories. There are about 5000 unique TSIEM 'What-On-What' activities that require manual mapping into 1086 QRadar low level categories ('lowlevelcategories') and 1087 QRadar generic CRE QIDs. There is a high possibility that not all TSIEM Activities can be successfully mapped into QRadar. In this case, new custom QIDs have to be created and assigned to already existing low-level categories. Refer to Chapter 6 for more details on mapping TSIEM to QRadar components.

Additionally, TSIEM Report migration depends greatly on what report criteria is being used, that is a specific data item available within each W7 dimension. Refer to Chapter 6.6.2 on TSIEM Log Management and Tivoli Common Reporting comparison to QRadar features and Chapter 6.7.1 for more details on basic migration principles on compliance reports.

Analyzing all these aspects makes the actual reports migration process very customer dependent because it requires a thorough analysis of the TSIEM Event Sources and reports being used by the customer.

4. Infrastructure Considerations

This chapter contains descriptive information about differences in network, high availability and backup configurations between TSIEM and QRadar deployments.

4.1 Networking

TSIEM is distributed as a software installation package (ISO image) which needs to be installed on one of the supported operating systems, hence there are number of requirements on the environment.

TSIEM Standard Servers use the following default ports to communicate (remotely) with different devices and systems (local communication ports are not considered):

- TCP 5992 - two-way communication between agent(s) and Server
- TCP 16315 - non-secure communications between the TIP and the client browser
- TCP 16316 - same for secure communications
- TCP 31000 - TDS (or LDAP) and the back-end database for TDS
- TCP 31001 - TSIEM Servers and their back-end DB2 databases

With the QRadar appliance there are no any additional configuration steps required except the initial configuration (assigning IP addresses, passwords, etc).

When QRadar is replacing TSIEM on the same network segment, then the QRadar appliance can reuse the TSIEM IP address to minimize network infrastructure reconfiguration. Access to the active ports utilized by TSIEM can be closed on the firewall.

The following ports are used for communications between QRadar components and external infrastructure, and need to be opened on the firewall, if required. QRadar manages a host based firewall on each appliance only opening the required ports. Example: If SNMP collection is not configured, the event processor will not listen on port 162.

- TCP 22 – Bidirectional from the console to the workstation(s) of the QRadar admin(s) for remote management access, retrieving log files, etc. Bidirectional from the console to other appliances if encryption is enabled.
- TCP 25 – Outbound from the console for e-mail alerting
- UDP/TCP 37 – From other appliances to the console for time synchronization. Also required: from the console to the NTP device.
- TCP 80 – From workstations to the console for the admin interface, deployment editor downloads
- TCP 443 – From workstations to the console for access to user interface
- UDP 514 – From log sources to the console and/or event processors for event data feeds (syslog)
- TCP 10000 - web-based server management
- TCP 32000-33999 - Data flows between QRadar managed hosts and Console
- UDP 2055, 9995 - Netflow datagram from components
- TCP 135 - collect data from Microsoft Windows hosts
- TCP/UDP 6543 - heartbeat ping from a secondary host to a primary host in an HA cluster
- TCP/UDP 7789 - testing the network connection between the secondary host and primary host in an HA cluster
- ICMP - testing the network connection between the secondary host and primary host in an HA cluster
- TCP/UDP 7800, 7802 - Real-time (streaming) for events and flows from the Event Collector to the Console

4.2 Backup

The TSIEM backup and restore process requires a manual procedure which implies that the following items require backing up:

- file system objects (installed product core, depot, indexes)
- DB2 database
- stored SSH keys
- Deployment Engine database
- LDAP tree on TDS

QRadar has extensive backup and restore facilities and therefore should be used immediately. By default, QRadar creates a backup archive of the configuration information daily at midnight. The backup archive includes configuration information, data, or both from the previous day (configured via Admin tab of the Console). The restore process might take up to several hours depending on the size of the backup archive being restored.

5. Deployment Planning and Considerations

The customer should have compiled a list of the number of systems from which events are being collected, as well as the typical volume of events (refer to chapter 8.3 for details).

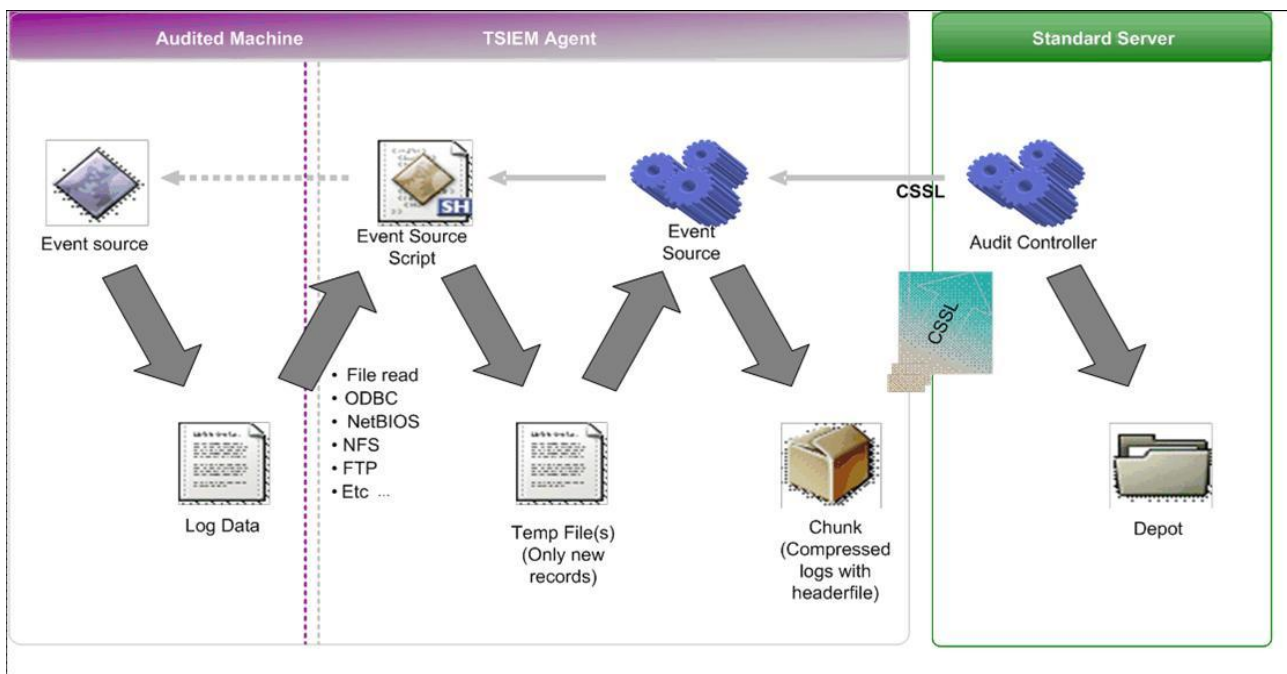
To determine the data volume requirements for the new QRadar deployment, samples can be examined from the TSIEM log depot and by using the Log Manager Dashboard. The transition will involve discontinuing log collection from TSIEM, and starting up log collection on a QRadar deployment. QRadar has high scalability and is expected to replace existing TSIEM servers with QRadar appliances, thus allowing some of the former TSIEM servers to be released for reuse in other applications. Some TSIEM servers will need to remain online, not to collect data, but to be able to provide previously collected TSIEM Data for historical reporting. Existing TSIEM Agents can be removed, and the number of TSIEM Servers needed for processing historical data can be planned once historical reporting frequency is known. The number and configuration of the new QRadar components will be planned based on the expected log volumes and event per second rates determined from current TSIEM collection characteristics, plus any new data (such as QFlow, Netflow, etc.) that was not available under TSIEM.

6. Mapping of TSIEM components to QRadar components

This section describes different SIEM capabilities that should be considered when transitioning between TSIEM to QRadar. Differences between the two products are discussed as well as customer considerations on how to address those differences during the transition.

6.1 Event collection chain

The TSIEM uses agents to collect log information.



A **TSIEM** Agent is the network node where log data extracted from end points is packaged and then transmitted to a TSIEM Log Management Server or SIM Standard Server. The transmission mechanism exploits the TSIEM secure communication protocol (CSSL) in the TSIEM agent process.

On request of the audit controller, running on the TSIEM server, the actuator process, part of the TSIEM Agent, invokes an actuator script to extract log data. The actuator compresses the extracted log data and adds a descriptive header file. A separate actuator process is launched for each event source.

Strictly speaking, separate TSIEM Agents are optional, because the TSIEM Server also acts as an Agent, and can take over its tasks. In TSIEM Agents are available for all supported platforms: AIX, Windows, HP-UX, Sun Solaris, z/OS.

The QRadar event processing pipeline consists of four logical components: Qflow Collector, Event Collector, Event Processor and Magistrate.

QFlow Collector passively collects traffic flows from the network through span ports or network taps. It also supports the collection of external flow-based data sources, such as Netflow, sFlow, J-Flow and etc. A flow starts when the first packet is detected. Each additional packet is evaluated and counts of bytes and packets are added to the statistical counters in the flow record. At the end of a preconfigured interval, a status record of the flow is sent to the Event Collector and statistical counters for the flow are reset.

The Event Collector gathers events from local and remote device sources. It normalizes events, bundles identical events to conserve system usage and then sends the information to the Event Processor.

The Event Processor processes events collected from one or more Event Collectors. When received, the Event Processor correlates the information and distributes it to the appropriate area, depending on the type of event. The Event Processor also includes information gathered by QRadar to indicate any behavioral changes or policy violations for that event.

It is important not to be confused about the term 'Event Processor' as it can refer to two different entities. The first one is a software component of QRadar system described above. And the second one is a physical appliance, QRadar 16xx Event Processor, which has both Event Collector and Event Processor software installed as well as other software components.

The Magistrate provides the core processing components. It processes the event against the defined custom rules to create an offense. If there is no match to a custom rule, the Magistrate uses default rules to process the event. For more information about offenses, please refer to the Chapter 5.6.2.

Event Collector and Event Processor configuration is the subject of the Chapter 8 (Using Deployment Editor) of the QRadar Administration guide.

In some cases it might be useful to use QRadar Adaptive Log exporter (ALE), a stand-alone Windows application that allows integration between local Windows-based sources and QRadar Event Collector using syslog protocol. The application can collect logs from Cisco ACS, CSA, file and XML-file forwarders, Juniper SBR, NetApp Data ONTAP, Windows Event log, Microsoft DHCP and more. For the detailed description of ALE, please refer to the QRadar Adaptive Log Exporter Users Guide.

There is an alternative option to collect information from Windows Event logs using Snare Agent for Windows. Log data is converted to text format, and delivered to QRadar via syslog protocol. Event logs from the Security, Application and System logs, as well as the new DNS, File Replication Service, Active Directory logs and custom Windows event logs are supported. Keep in mind that when using SNARE technical support in case of malfunctioning of the Windows log processing is limited to the problems related to the QRadar Event Collector. See section 7.3 for additional information on replacing TSIEM agents by QRadar logsources.

6.2 Audited Machines and Asset Profiles

In **TSIEM** terms the 'Audited Machine' or 'Audited System' is the system/device being monitored. This is where the events that are being collected originate (as far as the collect process can tell). Audited machine may or may not correspond to the machine that hosts the TSIEM Agent.

The TSIEM Agent or TSIEM Server (if acting as an Agent) makes network connections to the audited machines to get at the log data. When the Agent is installed on the audited machine itself, the log data is read locally.

Audited machines are described by name, type (Server, Agent, Agentless or Inactive), hostname or IP address, agent group and attached Event Source(s). Audited machines are added manually during TSIEM Server configuration.

The nearest analogue in **QRadar** is Assets, or Asset Profiles.

QRadar automatically discovers assets (servers and hosts) operating on the network, based on passive flow data and vulnerability data, allowing QRadar to build an asset profile. Asset profiles provide information about each known asset in the network, including identity information (if available) and what services are running on each asset. This profile data is used for correlation purposes

to help reduce false positives. For example, if an attack tries to exploit a specific service running on a specific asset, QRadar can determine if the asset is vulnerable to this attack by correlating the attack to the asset profile.

Asset profiles are only populated if QRadar have flow data or vulnerability assessment (VA) scans configured. For flow data to populate asset profiles, bidirectional flows are required. It is also possible to configure asset profiles manually.

6.3 User Roles and User Management

TSIEM user management is based on the Roles model. In order for a person to become a user, a userid for that user must be added to the TSIEM system and user roles must be assigned to give that user permission to view data and perform certain tasks in TSIEM. A user can have one or more roles. The User roles mechanism controls various aspects of system access and management, including permissions to access SIM databases and Compliance Dashboard, managing Event Sources and Log Management, Policy Management, User Management and Reporting.

Centralized user management can be enabled by the use of a TSIEM Security Group stored on one Security Server (clustered environment).

There is a flexible way to control access to information in the Portal reports by using the Scoping feature. The purpose of the Scoping feature is to control the amount of visibility users have into the Compliance Dashboard reports. Users within the Scoping application own Who, onWhat and Where groups. Scoping restricts which W7 dimensions of events are visible to the user and Portal shows only the user information about events that are associated with groups that user owns. There is currently no capability in QRadar to support the TSIEM Scoping feature. But through professional services a solution providing scoping secured by an authorization mechanism can be implemented.

TSIEM User management is based on an internal TDS server and it is not possible to use other authentication mechanisms.

QRadar user management is also based on the Roles model. Each user is associated with a role(s), which determines the privileges that user has to access functionality and information within QRadar.

QRadar roles control user access to the tabs in the Console which include: Offenses, Log Activity, Network Activity, Assets, Reports, Risk Management, Admin and IP Right Click Menu Extensions. Most roles have a subset of options which allow control over access to the tasks related to a particular Console tab.

In addition to the basic set of access permissions each user role can be associated with Log Sources, which allows restricting or granting permissions to view logs, events, and offense data received from assigned security and network log sources or log source groups.

QRadar allows configuring an authentication mechanism (local or remote) from one of the following modules: System Authentication (in-build), RADIUS, TACACS, Active Directory and LDAP. There is no need to migrate TSIEM users to QRadar from a functional perspective. Just accounts need to be created for the same endusers.

6.4 Normalization Component

6.4.1 TSIEM Event Sources

A TSIEM Event Source (ES) is a component that provides TSIEM support for a particular log source through the mechanism of collecting log source data, parsing various bits and pieces of each log data record and further mapping this record into TSIEM patented W7 normalization model describing 7 dimensions of the event. These dimensions are described in the following table:

<i>Dimension</i>	<i>Meaning</i>
When	Time at which event has occurred
Who	The user who is responsible for the event
What	The action that was performed

OnWhat	The subject of the action
Where	Host where the event has occurred
WhereFrom	Source of the action
WhereTo	Destination of the action

Table 5-1 TSIEM W7 Generic Event Model

In simple terms, TSIEM Event Sources provide a way of normalizing the events from different log sources by representing the information from these events in a form of Generic Event Model, which is used by TSIEM internally.

6.4.2 QRadar Device Support Modules

QRadar Device Support Module (DSM) is a component that provides QRadar support for a particular log source through the mechanism of collecting log source data, parsing various bits and pieces of each log data record to align them accordingly within the QRadar event database. Each record is represented in QRadar as described in the following table:

<i>Variable</i>	<i>Meaning</i>
EventName	Specific name of the event
EventCategory	Specific category the event belongs to
SourceIp	IP address of the source
SourcePort	Port of the source
SourceIpPreNAT	Real IP address of the source
SourceIpPostNAT	Mapped IP address of the source
SourceMAC	MAC identifier of the source
SourcePortPreNAT	Real port of the source

SourcePortPostNAT	Mapped port of the source
DestinationIp	IP address of the destination
DestinationPort	Port of the destination
DestinationIpPreNAT	Real IP address of the destination
DestinationIpPostNAT	Mapped IP address of the destination
DestinationPortPreNAT	Real port of the destination
DestinationPortPostNAT	Mapped port of the destination
DestinationMAC	MAC identifier of the destination
DeviceTime	Time at which the event has occurred
Protocol	Protocol used
UserName	The user who is responsible for the event
HostName	Host name (or IP address) where the event has occurred
GroupName	Name of the group that the host belongs to
NetBIOSName	NetBIOS name of the host
ExtraIdentityData	User-specific data associated with the event.
SourceIpv6	IPv6 source IP address for the message
DestinationIpv6	IPv6 destination IP address for the message

Table 5-2 QRadar Event Model

Note: Variables in the table are taken from the QRadar Universal Log Source eXtension (LSX) official Technical Note.

Similarly to TSIEM, QRadar DSMs provide a way of representing events from different log source types into an internal QRadar model.

6.4.3 Enhanced User Information

The majority of collected events would contain special user identification (i.e. SID, UID, logon name etc) information of the user who is responsible for the event, unless such identification is not required. This is not a problem if there is only one system involved in the reporting process. however, when there are hundreds or thousands of systems it is difficult to determine the real user to associate with the actions represented in the events.

In TSIEM, this is done with the help of a User Information Source (UIS). The UIS is a module that collects additional user information, like real names, roles, groups etc., from a user repository being used within a network. Later on, during the TSIEM mapping process, logon names are resolved to real names with all the users being assigned to their respective groups and roles. This greatly enhances the reporting functionality as it gives the flexibility when creating reports for particular privileged user groups and roles (i.e. Administrators, Power Users, Backup Operators, Financial Staff, etc.). The most important feature of the UIS is that it can be applied dynamically, i.e. each time collecting and using dynamically changed information about the users within the source.

In QRadar, a similar approach is being used with the help of Reference Sets. A Reference Set is a collection of additional information used in building QRadar rules. In other words, it is a collection of data that can be used for creating special lists, similarly to TSIEM UIS, containing the information about user groups and specific roles within the system. This information can be used in creating reports for particular privileged user groups and roles. The major disadvantage of the Reference Set is that it can only be automatically updated with new entries, meaning that the list does not contain dynamic information reflecting current state of the user repository. However, there are ways of addressing the issue but it is not the subject of this document.

It means that all TSIEM reports that are currently defined for 'Who' dimension and based on user roles and groups Make a point that it is possible but the who groups are not dynamically updated. Future QRadar version introduces an API to manage the contents of reference sets. A more static approach to represent W7 groups for TSIEM policy representation, is by using Building Blocks instead of Reference Sets.

6.4.4 TSIEM Variables to QRadar Variables Mapping

The basic principle behind TSIEM data export to QRadar is to provide the way for QRadar to ‘understand’ TSIEM data represented as Generic Event Model data inside of TSIEM. This can be achieved through assigning suitable QRadar Universal LSE variables for each of TSIEM W7 objects formed by the TSIEM Generic Mapping Language (GML) variables. For better understanding, after parsing and mapping collected data, special BCP files are produced, which contain normalized objects for all TSIEM W7 dimensions. Refer to **Chapter Error! Reference source not found.** for the full list of .bcp files with the explanation. These objects are then loaded into TSIEM GEM database.

Generally speaking, all the data needed to be exported to QRadar is available during the TSIEM mapper process and suitable QRadar variable mappings, that data can be exported to QRadar using the Universal LSE. The following table contains a mapping of QRadar variables to TSIEM variables:

TSIEM Dimension	TSIEM GML variables	QRadar Universal LSX xml variables
When	eventtimestamp	DeviceTime
Who	logonname	UserName
What	eventmainclass eventclass successclass	EventName, EventCategory
OnWhat	objecttype objectpath objectname	EventName, EventCategory
Where	platformtype	HostName

	platformname	
WhereFrom	platformtype platformname	SourceIp
WhereTo	platformtype platformname	DestinationIp

Table 5-3 TSIEM to QRadar variables mapping

6.4.4.1 TSIEM W7 event structure

For successful export of TSIEM W7 data into QRadar, it is necessary to store the complete W7 model for each processed event during the TSIEM mapper work. The output needs to be stored in a separate file (assuming CSV) for each TSIEM Event Source containing all the data that needs to be exported. For simplicity and unification, the following format is used:

When, Who, What, OnWhat, Where, WhereFrom, WhereTo

In terms of GML variables, W7 dimensions are represented by the following variables:

even-
timestamp,logonname,eventmainclass,eventclass,successclass,objecttype,objectpath,objec
tname,platformname_where,platformname_wherefrom,platformname_whereeto

Example:

```
2012-03-15T12:55:10,admin,Delete,Object,Success,OBJECT,-  
,objExample,192.168.1.1,192.168.1.1,10.16.1.10
```

6.4.5 TSIEM W7 Model to QRadar Model Mapping

TSIEM typically maps event types to a combination of eventmainclass, eventclass, and objecttype, also known as an eventtype. QRadar uses a very similar technique and maps event types to an eventname or QID. In case of QRadar mapping the combination of event type and QID is typically unique, but it does not have to be. There is no reason why you could not map event types from non supported log sources to existing QIDs. But you might want to create new QIDs for custom made Log Sources or Universal DSMs.

6.4.5.1 TSIEM events mapping to QID for non-existent QRadar log sources

For non-existent QRadar log sources, successful mapping of TSIEM W7 normalized event model to the QRadar event model is dependent on the TSIEM ‘What-OnWhat’ individual pairs. These pairs are described by the TSIEM GEM Virtual System and represented by three TSIEM GML variables ‘eventmainclass’, ‘eventclass’ and ‘objecttype’. In turn, the QRadar event model is described by two variables EventName and EventCategory, which internally can be represented by ‘QID’ and ‘high/low levelcategory’ values. The challenge here is to manually define the map for all TSIEM ‘What-OnWhat’ pairs into suitable generic event CRE QIDs and their respective categories. Out of total 5034 unique ‘What-OnWhat’ pairs in TSIEM, there are 2717 such pairs that have no QID counter part. A missing pair should be mapped either on one of the existing 1087 QIDs or create a new one.

6.4.5.2 New QRadar QID insertion and mapping

It is clear that during the mapping process, not all TSIEM ‘What-OnWhat’ pairs can be mapped into existing QRadar QIDs. In this case, a new QID needs to be created to provide suitable event associations in QRadar. The mapping process involves some common sense logic along with the best possible match available in QRadar. Additionally, all newly defined QIDs must be assigned appropriate, already existing low-level categories, before any new custom QID can be created in QRadar.

For a better understanding, let’s use an example. Suppose, there is a TSIEM ‘What-OnWhat’ pair called “Delete Object OBJECT”, which in TSIEM terms means that an object of unidentified type is being deleted. Looking at `qradar.public.qidmap` Generic Event CRE entries reveals only two following actions involving ‘delete’ operation:

- `Host-Policy Deleted - Event CRE`
- `File Deleted - Event CRE`

Neither of these suits the input, therefore, a new QID is proposed:

- `Object Deleted - Event CRE`

Before this new QID can be created, an appropriate low-level category must be located for this particular QID. Unlike new custom QIDs, QRadar does not provide a way of creating custom low-

level categories. The list of all available low-level categories in QRadar can be obtained using the following command:

```
/opt/qradar/bin/qidmap_cli.sh -l
```

For this particular example 'Unknown CRE Event' low-level category with the ID 12001 was chosen because none of the existing low-level categories are suitable. Also, depending on the severity of the action (0-10, where 10 is being the highest), an appropriate severity level needs to be specified. For this particular example, severity of 1 was chosen.

In order to create a new QID, the following command needs to be executed:

```
/opt/qradar/bin/qidmap_cli.sh -c --qname "Object Deleted -  
Event CRE" --qdescription "Deletion of an unidentified type  
object is detected" --severity 3 --lowlevelcategoryid 12001
```

Successful QID creation will be indicated by the following script output:

```
Created entry:  
qid: 2000001  
name: _ Object Deleted - Event CRE _  
description: _ Deletion of an unidentified type object is detected  
severity: 1  
low level category id: 12001  
ratethreshold: 0  
catpipename: Delta  
rateshortwindow: 0  
ratelongwindow: 0  
reverseip: false  
rateinterval: 0
```

6.4.5.3 Migrating TSIEM normalization rules (GxL) to QRadar

The next step is to create XML file with suitable parsing rules for the corresponding events coming from the original log source and reconstructed log source from TSIEM BCP files as well. This involves porting the TSIEM GSL parsing rules that identify the original events. These rules have to be encapsulated in XML, which will give QRadar ability to identify log source events that are mapped by TSIEM into 'What-OnWhat' pairs, creating the suitable equivalency. In our particular example,

we need to port TSIEM GSL parsing rule for the “Delete Object OBJECT” in order for QRadar to detect the original log source. Suppose, it is identified by a regular expression like this:

```
^An\sobject\s([\s]+)\swas\sdeleted\.s$
```

According to the previously defined rules for TSIEM-QRadar variables mapping, see Chapter 6.4.3 for the details, we have the following XML entries created:

```
<pattern id="OriginalDeleteObjectOBJECT"
xmlns=""><![CDATA[(^An\sobject\s([\s]+)\swas\sdeleted\.s)]]><
/pattern>

<matcher field="EventName" order="1" pattern-id="Delete Object
OBJECT" capture-group="1" enable-substitutions="false"/>
```

After creating the rules for the event from the original log source, it is time to create a corresponding rule for the TSIEM W7 reconstructed event that comes from BCP files. Suppose the reconstructed W7 record for our example looks like this:

```
2012-03-15T12:55:10,admin,Delete,Object,Success,OBJECT,-
,objExample,192.168.1.1,192.168.1.1,10.16.1.10
```

According to the reconstructed model described in the Chapter TSIEM W7 event structure, the following XML entries have to be created:

```
<pattern id="ReconstructedDeleteObjectOBJECT"
xmlns=""><![CDATA[(^([\s,]+),([\s,]+),(Delete),(Object),([\s,]+),
(OB-
JECT),([\s,]+),([\s,]+),([\s,]+),([\s,]+),([\s,]+))$]]></pattern>

<matcher field="EventName" order="1" pattern-id="Delete Object
OBJECT" capture-group="1" enable-substitutions="false"/>

<matcher field="DeviceTime" order="1" pattern-id="DeviceTime"
capture-group="2" enable-substitutions="false"/>

<matcher field="UserName" order="1" pattern-id="UserName" cap-
ture-group="3" enable-substitutions="false"/>
```

```
<matcher field="HostName" order="1" pattern-id="HostName" capture-group="9" enable-substitutions="false"/>

<matcher field="SourceIp" order="1" pattern-id="SourceIp" capture-group="10" enable-substitutions="false"/>

<matcher field="DestinationIp" order="1" pattern-id="DestinationIp" capture-group="11" enable-substitutions="false"/>
```

Now it is time to put it all together, so the resulting XML file looks like this:

```
<?xml version="1.0" encoding="UTF-8"?>

<device-extension xmlns="event_parsing/device_extension">

  <!-- Do not remove the "allEventNames" value -->

    <pattern id="allEventNames"
  xmlns=""><![CDATA[(.*)]]></pattern>

  <!-- Everything below this line can be modified -->

  <pattern id="OriginalDeleteObjectOBJECT"
  xmlns=""><![CDATA[^An\sobject\s([\s]+)\swas\sdeleted\.$]]></pattern>

  <pattern id="ReconstructedDeleteObjectOBJECT"
  xmlns=""><![CDATA[(^([\s,]+),([\s,]+), (Delete), (Object), ([\s,]+), (OBJECT), ([\s,]+), ([\s,]+), ([\s,]+), ([\s,]+), ([\s,]+))$)]></pattern>

  <match-group order="1" description="Log Source Extension"
  xmlns="">

    <matcher field="EventName" order="1" pattern-id="Delete
  Object OBJECT" capture-group="1" enable-substitutions="false"/>

    <matcher field="EventName" order="2" pattern-id="Delete
  Object OBJECT" capture-group="1" enable-substitutions="false"/>

    <matcher field="DeviceTime" order="1" pattern-
  id="DeviceTime" capture-group="2" enable-substitutions="false"/>
```

```
<matcher field="UserName" order="1" pattern-id="UserName"
capture-group="3" enable-substitutions="false"/>

<matcher field="HostName" order="1" pattern-id="HostName"
capture-group="9" enable-substitutions="false"/>

<matcher field="SourceIp" order="1" pattern-id="SourceIp"
capture-group="10" enable-substitutions="false"/>

<matcher field="DestinationIp" order="1" pattern-
id="DestinationIp" capture-group="11" enable-
substitutions="false"/>

<event-match-multiple pattern-id="allEventNames" capture-
group-index="1" device-event-category="unknown" send-
identity="OverrideAndAlwaysSend" />

</match-group>

</device-extension>
```

All previously described procedures can be automated by writing a suitable script. However, the mapping rules for TSIEM 'What-On-What' pairs to QRadar QIDs and low-level categories have to be written manually.

6.4.5.4 Mapping to QRadar QIDs

The final step in TSIEM to QRadar data and sources mapping would be to manually create a Universal DSM instance in QRadar for each exported TSIEM Event Source and manual configuration of such DSM to 'recognize' newly added original and reconstructed log sources from TSIEM. Unfortunately, QRadar does not provide a way of automatic creation and configuration of such customized Universal DSMs and therefore, it requires user interaction to actually map incoming events to pre-defined patterns in XML.

To create a Log Source eXtension, perform the following operation in QRadar GUI:

1. Login to QRadar with administrator privileges.
2. Navigate to **Admin** tab

3. Click on **Log Source Extensions**
4. In the newly opened windows, click on **Add**
5. In the newly opened windows, click on **Choose File** and select previously created XML file with created LSX parsing rules.
6. After that, click on **Upload**
7. Specify the **Name** and the **Description** accordingly and click on **Save**

This custom LSE (take the note of its **Name**) will be used in the next step during addition and configuration of Universal DSM to be associated with the newly added LSE.

To create a Universal DSM, perform the following operation in QRadar GUI:

1. Login to QRadar with administrator privileges if not already logged in.
2. Navigate to **Admin** tab
3. Click on **Log Sources**
4. In the newly opened windows, click on **Add**
5. In the newly opened windows, specify the **Log Source Name** and the **Log Source Description** accordingly on new Universal DSM
6. In the **Log Source Type** drop down list, choose **Universal DSM**
7. In the **Protocol Configuration** drop down list, choose the protocol required
8. In the **Log Source Extension** drop down list, choose the name of previously saved LSX.
9. Depending on the condition, configure suitable **Extension Use Condition**
10. Click on **Save** to finish the configuration.

Last but not least is the actual process of mapping necessary log source events into the QRadar QIDs. Initially, all the captured events of Universal DSM are of unknown type. This is because no suitable mapping is being created so far in QRadar. In other words, QRadar does not 'know' how to interpret the event even if meaningful words like 'DELETE' or 'ADD' are present within a message.

Unfortunately, there is no automatic way of providing internal QRadar mapping to QIDs and the process is manual.

1. Login to QRadar with administrator privileges if not already logged in.
2. From the **Events** tab, select **Search**, then **Edit Search**
3. Specify the **Time Range** required
4. Under **Search Parameters**, select **Log Source Equals** and specify the log source that was created in the previous step
5. Click **Search** to view the results
6. Double-click on an unknown entry to view the event details.
7. Click **Map Event** in the event toolbar
8. In the newly opened windows, the value **Log Source Event ID** should display an EventName value from the LSX
9. The value displayed as the **Log Source Event ID** must now be mapped to an appropriate QID.

The detailed instructions on how to map to suitable QIDs are available from official QRadar manuals.

6.4.5.5 TSIEM events mapping to QID for already existing QRadar log sources

The most common similarity between TSIEM and QRadar in terms of the log source support is a Syslog protocol for various log sources. Therefore, TSIEM collected Syslog data exported to QRadar requires simple TSIEM chunk extract and resend to QRadar for supported log sources. This will ensure that the data is being parsed by native QRadar DSM rules and mapped to the dedicated QIDs automatically without additional work needed. The complete list of the log sources using Syslog protocol and supported by both TSIEM and QRadar is available in

QRadar 7.0 MR4		TSIEM 2.0 FP5	
Data Source	Protocol	Data Source	Protocol
3Com 8800 Series Switch	Syslog		
Ambiron TrustWave ipAngel IPS	Syslog		
Apache HTTP Server	Syslog	Apache Web Server 2.x (forensic)	Syslog
Array Networks SSL VPN Access Gateways	Syslog		

IBM TSIEM to IBM QRadar Transition Guide

Aruba Mobility Controller	Syslog		
Bit9 Parity	Syslog		
Bluecoat SG Appliance	Syslog, File	Blue Coat ProxySG	File
Bridgewater Systems AAA Service Controller	Syslog		
CA ACF2	File		
CA Top Secret	File	TopSecretVSE	File
CRYPTOCARD CRYPTOSHIELD	Syslog		
Check Point FireWall-1	Syslog, OPSEC/LEA	CheckPoint FireWall-1	File, OPSEC, SNMP
Cisco 12000 Series Routers	Syslog		
Cisco 6500 Series Switches	Syslog		
Cisco 7600 Series Routers	Syslog		
Cisco ACE Firewall	Syslog		
Cisco ACS	Syslog	Cisco Secure ACS	File
Cisco Adaptive Security Appliance (ASA)	Syslog, Cisco NSEL	Cisco ASA (forensic)	Syslog
Cisco Aironet	Syslog		
Cisco CSA	Syslog, SNMP		
Cisco Carrier Routing System	Syslog		
Cisco CatOS for Catalyst Switches	Syslog		
Cisco Firewall Services Module (FWSM)	Syslog	Cisco Firewall Services Module 7.1	Syslog
Cisco IOS	Syslog	Cisco IOS / Switches (forensic)	Syslog
Cisco Integrated Services Router	Syslog	Cisco Integrated Services Router (forensic)	Syslog
Cisco Intrusion Prevention System (IPS)	SDEE	Cisco Intrusion Prevention System (forensic)	Syslog
Cisco IronPort	Syslog, File		
Cisco NAC Appliance	Syslog		
Cisco PIX Firewall	Syslog	Cisco PIX	Syslog, SNMP, File
Cisco VPN 3000 Series Concentrator	Syslog	Cisco VPN (forensic)	Syslog
Cisco Wireless Services Module (WiSM)	Syslog		
Configurable Authentication message filter	Syslog		
Configurable Firewall Filter	Syslog		
Cyber-Ark Vault	Syslog		
CyberGuard TSP Firewall/VPN	Syslog		
EMC VMWare	EMC VMWare		
Enterasys A-Series	Syslog		
Enterasys B2-Series	Syslog		
Enterasys B3-Series	Syslog		
Enterasys C2-Series	Syslog		
Enterasys C3-Series	Syslog		
Enterasys D-Series	Syslog		
Enterasys Dragon Network IPS	Syslog, SNMP	Enterasys Dragon 6 (forensic)	Syslog
Enterasys G-Series	Syslog		
Enterasys HiGuard	Syslog		
Enterasys HiPath	Syslog		
Enterasys I-Series	Syslog		
Enterasys Matrix E1 Switch	Syslog, SNMP		
Enterasys Matrix N Series Switch	Syslog		
Enterasys NAC	Syslog		
Enterasys NetsightASM	Syslog		
Enterasys Stackable and Standalone Switches	Syslog		
Enterasys XSR Security Routers	Syslog		
Extreme Networks ExtremeWare OS	Syslog		
F5 Networks BigIP	Syslog	BIG-IP	Syslog
Fair Warning	Syslog, File		
FireEye	Syslog		
Forescout CounterACT	Syslog		
Fortinet FortiGate Security Gateway	Syslog		
Foundry Fastiron	Syslog		
HP ProCurve	Syslog		
HP Tandem	File	Tandem	File
Hewlett Packard UniX	Syslog	HP-UX	Syslog, File
IBM AIX Server	Syslog, File	IBM AIX 5.1-6.1	Syslog, File
IBM AS/400 iSeries	Syslog, File	OS/400 / iSeries Remote Collect	File, FTP, API
IBM DB2	File	IBM DB2 8.1-9.x	File
IBM IMS	Syslog, File		

IBM TSIEM to IBM QRadar Transition Guide

IBM Informix Audit	File	IBM Informix Dynamic Server	File
IBM Lotus Domino	SNMP	Lotus Notes	File
IBM Proventia Management SiteProtector	JDBC	IBM Proventia Management SiteProtector 2.0 SP6.x	JDBC
IBM Proventia Network IPS	SNMP		
IBM RACF	File		
IBM WebSphere Application Server	Syslog, File	IBM WebSphere Application Server 6.0-7.0	File/JMX
ISC BIND	Syslog		
Imperva Securesphere	Syslog		
ltron Smart Meter	Syslog		
Juniper DX Application Acceleration Platform	Syslog		
Juniper EX-Series Ethernet Switch	Syslog		
Juniper JunOS Platform	Syslog, PCAP		
Juniper M-Series Multiservice Edge Routing	Syslog		
Juniper MX-Series Ethernet Services Router	Syslog, File		
Juniper Networks AVT	JDBC		
Juniper Networks Firewall and VPN	Syslog	Juniper NetScreen FW (forensic)	Syslog
Juniper Networks Infranet Controller	Syslog		
Juniper Networks Intrusion Detection and Prevention (IDP)	Syslog		
Juniper Networks Network and Security Manager	Syslog, Juniper NSM		
Juniper Networks Secure Access (SA) SSL VPN	Syslog	Juniper SSL VPN (forensic)	Syslog
Juniper SRX-series Services Gateway	Syslog, PCAP		
Juniper Steel Belted Radius	Syslog, File		
Juniper T-Series Core Platform	Syslog		
Lieberman Random Password Manager	Syslog		
Linux DHCP Server	Syslog	Linux Auditing Framework	Syslog, File
Linux iptables Firewall	Syslog	Linux Auditing Framework	Syslog, File
Linux login messages	Syslog	Linux Auditing Framework	Syslog, File
Mac OS X	Syslog		
McAfee Application/Change Control	JDBC		
McAfee IntruShield Network IPS Appliance	Syslog	McAfee IntruShield	Syslog
McAfee ePolicy Orchestrator	JDBC, SNMP	McAfee ePO	ODBC
Metainfo MetalP	Syslog		
Microsoft DHCP Server	Syslog, File	Microsoft Windows Server Active Directory 2000-2008	File
Microsoft Exchange Server	Syslog, File	Microsoft Exchange 2000-2003	File
Microsoft IAS Server	Syslog		
Microsoft IIS	Syslog, File	Internet Information Server (IIS)	File
Microsoft ISA	Syslog		
Microsoft Operations Manager	JDBC		
Microsoft SCOM	JDBC		
Microsoft SQL Server	Syslog	Microsoft SQL Server 2000-2008	File, ODBC
Microsoft Windows Security Event Log	Syslog, File	Microsoft Windows NT-2008	File, SNMP
Motorola SymbolAP	Syslog		
Name Value Pair	Syslog	Ubiquitous / W7Log (CSV, XML)	Syslog, File
Niksun 2005 v3.5	Syslog		
Nortel Application Switch	Syslog		
Nortel Contivity VPN Switch	Syslog		
Nortel Ethernet Routing Switch 2500/4500/5500	Syslog		
Nortel Ethernet Routing Switch 8300/8600	Syslog		
Nortel Multiprotocol Router	Syslog		
Nortel Secure Network Access Switch (SNAS)	Syslog		
Nortel Secure Router	Syslog		
Nortel Switched Firewall 5100	Syslog, OPSEC/LEA		
Nortel Switched Firewall 6000	Syslog, OPSEC/LEA		
Nortel Threat Protection System (TPS) Intrusion Sensor	Syslog		
Nortel VPN Gateway	Syslog		
OpenBSD OS	Syslog		
Oracle Audit Vault	JDBC	Oracle Database Audit Trail 8i 9i 10g 11g	File, ODBC
Oracle Database Listener	Syslog		
Oracle RDBMS Audit Record	Syslog, JDBC	Oracle Database Audit Trail 8i 9i 10g 11g	File, ODBC
Oracle RDBMS OS Audit Record	Syslog, File	Oracle 9i 10g 11g	File
Palo Alto PA Series	Syslog		
ProFTPD Server	Syslog		

IBM TSIEM to IBM QRadar Transition Guide

RSA Authentication Manager	File	RSA Authentication Manager	File
Radware DefensePro	Syslog		
Redback ASE	Syslog		
Samhain HIDS	Syslog, JDBC		
Sentriigo Hedgehog	Syslog		
Sidewinder G2 Security Appliance	Syslog		
Snort Open Source IDS	Syslog		
Solaris BSM	Syslog, File	Solaris audit trail	Syslog, File
Solaris Operating System Authentication Messages	Syslog	Solaris audit trail	Syslog, File
Solaris Operating System DHCP Logs	Syslog		
Solaris Operating System Sendmail Logs	Syslog		
SonicWALL UTM/Firewall/VPN Appliance	Syslog		
Sophos PureMessage	JDBC		
Sourcefire Defense Center	SDC Estreamer	Sourcefire Network Sensor	Syslog
Squid Web Proxy	Syslog		
Starent Networks Home Agent (HA)	Syslog		
Sybase ASE	JDBC	Sybase Adaptive Server Enterprise	File
Symantec Endpoint Protection	Syslog	Symantec AntiVirus	File
Symantec Gateway Security (SGS) Appliance	Syslog		
Symantec System Center	JDBC		
Symark Power Broker	Syslog		
TippingPoint Intrusion Prevention System (IPS)	Syslog		
TippingPoint X Series Appliances	Syslog		
Top Layer Intrusion Prevention System (IPS)	Syslog, OPSEC/LEA		
Trend InterScan VirusWall	Syslog		
Trend Micro Control Manager	SNMP		
Trend Micro Office Scan	SNMP		
Tripwire Enterprise	Syslog		
Universal DSM	ANY	Generic ExtendIT	ANY
Vericept Content 360	Syslog		
Websense V Series	Syslog		
		Alcatel Switch 6600 & 7800 (forensic)	Syslog
		BIM Alert Report Writer	File
		BMC Control SA	ODBC
		BlackDiamond Router (forensic)	Syslog
		Cisco Router	Syslog, SNMP
		Guardium 7.0 - 8.0	Syslog, File
		HP Integrated Communication Facility Notification	SNMP
		HP OpenVMS	File
		HP Switch	SNMP
		HP Tru64 UNIX	FTP
		IBM DB2 Audit Management Expert 1.1	File
		IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0-8.1	JDBC
		IBM Tivoli Access Manager for Operating Systems	File
		IBM Tivoli Access Manager for e-Business	File
		IBM Tivoli Directory Server	File
		IBM Tivoli Federated Identity Manager	File
		IBM Tivoli Identity Manager 4.6 - 5.0	JDBC
		IBM Tivoli Key Lifecycle Manager 1.0	File
		IBM Tivoli Security Compliance Manager 5.1.0 - 5.1.1.1	JDBC
		IBM Tivoli Security Information and Event Manager Server	File
		IBM Tivoli Security Information and Event Manager Web Apps	File
		IBM Tivoli Security Operations Manager	File
		IBM Tivoli Security Policy Manager 7.0	File
		ISS RealSecure	SNMP, File
		ISS System Scanner	File
		ISS System Scanner reports	File
		Novell (Nsure) Audit	ODBC
		Novell 4 or 5	API
		Novell Advanced Audit Service	ODBC
		OPICS	File
		Oracle Applications 11.5.9 - 12.0	File

		Oracle Fine-Grained Auditing 9i 10g 11g	ODBC
		Oracle Portal Activity	File
		Oracle Portal Logins	File
		RSA SecurID ACE Server 7 (forensic)	Syslog
		Raptor	Syslog, File, SNMP
		SAP NetWeaver Application Server ABAP 6.10-7.0	File
		SAP NetWeaver Application Server on Java 7.0 - 7.2	File
		SAP R/3	File
		ScanMail for Lotus Notes	API
		ScanMail for MS Exchange	File
		ServerProtect	File
		SiteMinder	ODBC
		Snort	Syslog
		StealthWatch (forensic)	Syslog
		Stratus VOS	File
		Sun Identity Manager	ODBC
		eTrust Access Control (SeOS)	File
		iPlanet Web Server	File
		z/OS	File
		zAlert	SNMP

Table 6-8 TSIEM to QRadar Sources Comparison.

As for the other log sources, which are using more complicated message formats (i.e. XML, binary and other complex structures) a complete reconstruction of the message is required. This step is not being addressed in this guide nor is it being advised because of its complexity, time and resource consuming efforts.

6.5 Log Management Component

6.5.1 TSIEM Data Storage

The main storage for unprocessed information is the TSIEM Log Depot. Each Event Source which collects data stores it in a depot subfolder. A sample depot structure looks like this:

```
C:\IBM\TSIEM\sim\depot\
    10.11.6.229.118\
    172.23.10.33.112\
    172.23.10.34.111\
    sample.domain.com.117\
    srv-ts-10206-2.100\
    srv-ts-10206-2.101\
```

Each depot subfolder name is constructed by combining the Audited Machine name (e.g. sample.domain.com) with the Event Source ID (117).

Information in the Log Depot is stored as portions of log file data called “chunks”. Each chunk consists of:

- A chunk header (plain-text file with platform definition and other internal information)
- One or several gzipped data files, which may contains original data (e.g. binary data not suitable for direct processing) and non-original data (e.g. binary log text dump suitable for processing)

A sample chunk structure looks like this:

0AQ7VL0 (chunk header)

0AQ7VL1 (non-original data)

0AQ7VL2 (original data)

Each sub-chunk name is constructed by combining a hash value constructed from the collection time (0AQ7VL) and sub-chunk ID (0 for chunk header; 1,2,3.. for gzipped data).

Normalized data is stored in GEM (DB2) databases which can be reached via a JDBC connection to the TSIEM host (port 31001, database name “cifdb”, user name “cifdbadm”). For migration purposes (refer to chapter 8.1) data extraction from the database is not the best approach due to the following reasons:

- The database consists of a complicated data structure, separated into many tables
- Each database can contain data from several event sources with different platform (event source) types
- The amount of data extracted will be limited by the amount of data loaded into a particular GEM database (one month of the log data maximum in common scenarios)
- There may be possible data duplication (the same data from a single event source could be loaded into several GEM databases)

6.5.2 QRadar Data Storage

All event and flow data is stored as binary files on the QRadar file system, utilizing Ariel database for management purposes.

Sample data structure:

```
/store/ariel/  
    cv/  
    events/  
    flows/  
    gv/  
    hprof/  
    persistent_data/  
    simarc/
```

If the hashing mechanism is enabled data integrity can be validated using the script, `"/opt/qradar/bin/check_ariel_integrety.sh"`.

The only way to access flows and events stored in the Ariel database directly is to use the AQL Event and Flow Query Command Line Interface (CLI)¹. The AQL allows accessing raw flows and events stored in the Ariel database via the AQL syntax² that is a subset of the SQL92 standard and provides support for two tables: events and flows. The AQL CLI supports interactive and non-interactive modes.

To access the AQL query CLI:

- Log in to QRadar, as root.
- Enter the following command: `/opt/qradar/bin/arielClient`

The Query prompt appears.

¹ Refer to “AQL Flow and Event Query CLI Guide” for details

² The AQL CLI does not provide support for joining tables

AQL queries to event or flow fields may return numeric codes making query responses or searches difficult. The shell script “/opt/qradar/bin/idlist.sh” provides additional information from numeric AQL fields in the events and flows table.

For details on importing data into QRadar log storage refer to chapter 8.2.

6.5.3 Collect Methods and Protocols

TSIEM supports several basic collect methods:

- Syslog/SNMP/OPSEC (real-time)
- OSEvents (Windows 2000-2003)
- Generic (data is returned by platform-specific collect script)

The “Generic” chunk tool is the most common and allows the creation of collection mechanisms using a variety of collect methods, like FTP, File, SSH, WMI, JDBC, JMX, etc, utilizing generic programming interfaces or custom/3rdparty API.

QRadar supports the following set of data collection protocols:

- EMC VMWare
- JDBC / JDBC – SiteProtector / Sophos Enterprise Console JDBC
- Juniper NSM
- OPSEC/LEA
- Log File
- SDEE
- SMB Tail
- SNMP v1/v2/v3
- Sourcefire Defense Center eStreamer
- Microsoft DHCP; Security Event Log; Exchange; IIS

These protocols can be configured with Universal DSM to implement required LSX. The most visible problem for migration purpose is the absence of a “Generic” chunk tool alternative in QRadar.

In many cases original log source data is modified by TSIEM into “non-original” structure used for parsing and normalizing. When possible native QRadar collect protocols should be used; in other cases the analogue of TSIEM collect scripts will need to be created to allow QRadar to utilize native protocols (e.g. Log File via SSH) to collect and analyze pre-processed data.

6.5.4 Indexing and Forensic Search

In **TSIEM** there is a function provided to index the raw log files collected by Log Management and stored in LM Depot. Subsequent keyword searches through the collected log data use the indexing for locating and retrieving matching log files in their native format.

The indexing procedure is running periodically, and when new chunks are collected to the Depot or when a GSL file modification was detected. Indexing time intervals can be configured on the TSIEM server system with the gensub.ini configuration file.

The Log Management Reporting feature generates reports on the content of the collected log files using the index/search capability and the Tivoli Common Reporting services.

QRadar offers a "Free Text Searching" component (BETA feature at the moment this document created) to index collected data for faster searching and filtering capabilities (the Quick Filter feature enables one to search event and flow payloads using a text search string). Free Text was designed to be used on fields not normally indexed such as URLs. It will index the payloads (thus extra space will be needed) and speed up the search results for these types of queries. Performance improvements will depend on the criteria being used (increases may be up to 10x or more on query results).

6.6 Policies, Reports, Alerts, and Distribution

In many security products, reporting capability is a very important component that plays a significant role in prompt notification about internal policy violation or suspicious privileged user activity. This section provides a detailed comparison of such features for TSIEM and QRadar.

6.6.1 TSIEM Policies, Reports, and Alerts

6.6.1.1 TSIEM Policies

A security policy in TSIEM is a set of special groups, policy rules, alerts and attention rules that are being defined for any number of platforms from which TSIEM collects the data. TSIEM applies corresponding policy and attention rules while loading the collected data into the reporting databases, where the data is grouped by grouping rules. Simply speaking, the policy is used in TSIEM for representing original log source data into the viewable normalized events in the TSIEM User Interface.

There are three types of policies within TSIEM:

- **Work policy**
This is used when the policy is being defined or edited. Only manual compliance checks can be done against the Work policy.
- **Committed policy**
This is used when the policy is finalized to make sure no further changes are applied. Automatic compliance checks are run against this policy.
- **Automatic policy**
This is automatically generated based on the grouping information and does not contain any policy or attention rules.

Users have flexibility in making changes to all committed policies according to their specific needs.

6.6.1.2 TSIEM Reports

Both standard and custom TSIEM reports can be based on any number of specific fields (and/or their values) being identified by TSIEM Event Events source in all W7 dimensions. The internal TSIEM GEM model provides a unified way of applying report logic to all the data being loaded into a TSIEM GEM database because the data is being normalized. The following table describes the types of reports for each of TSIEM W7 dimensions:

<i>Dimension</i>	<i>Reports</i>
When	Reports for normal working hours

Who	Privileged user related reports, reports involving specific user groups etc.
What	Reports based on the type of the action
OnWhat	Reports based on the subject type of the action
Where	Reports based on the origin where the event has occurred
WhereFrom	Reports based on the source of the action
WhereTo	Reports based on the destination of the action

Table 5-4 TSIEM W7 Reports

Report logic can involve any number of identified variables and/or their values on any W7 dimension to meet a customer’s reporting requirements.

6.6.1.3 TSIEM Alerts

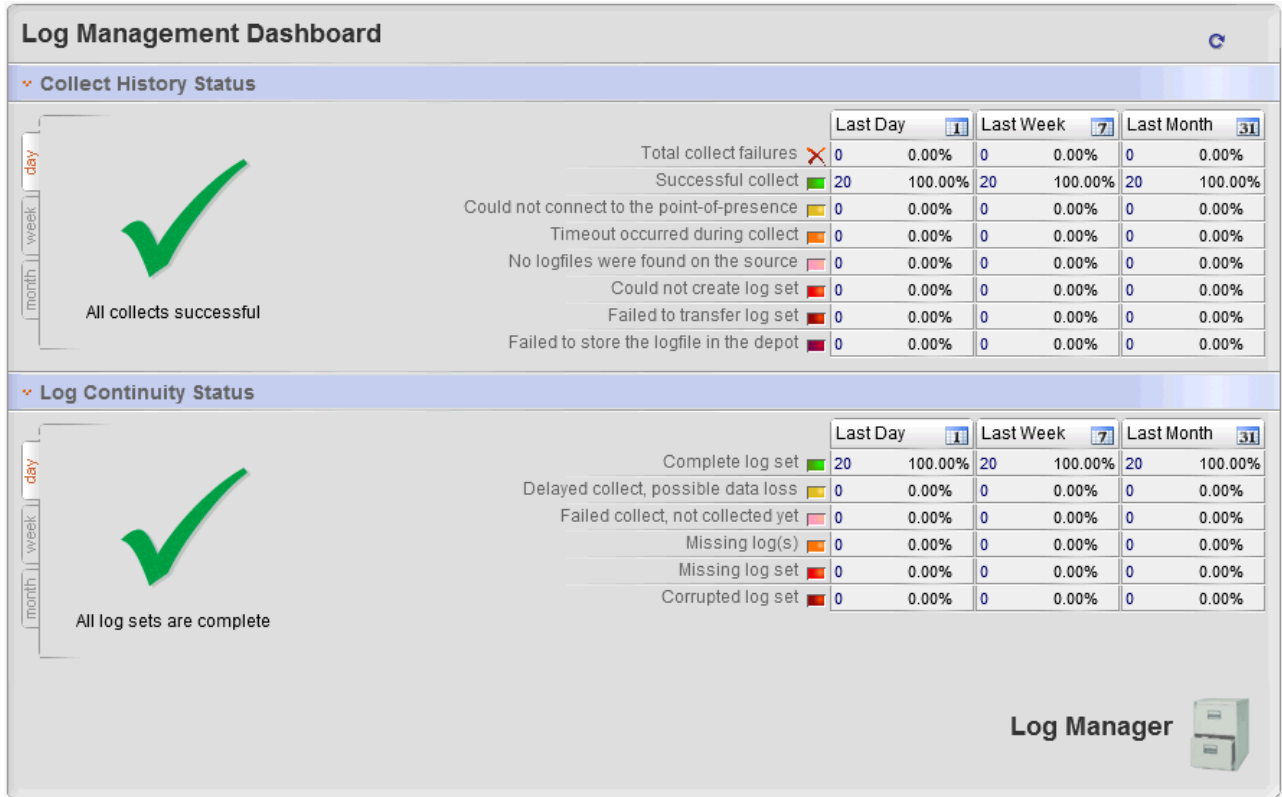
An alert is simply a way of notifying a dedicated person about some suspicious activity being detected. Such activity is defined by the special attention rules that identify the boundaries of patterns of adverse behavior. In TSIEM, an alert is a message being sent when a security threat is detected. The detection is performed by security policy exceptions defined by the severity level of each particular event. Alerts in TSIEM are configured in the following way:

- Protocol being used for the alert (SNMP, e-mail, script)
- Recipient of the alert (e-mail address or addresses)
- Severity of the alert (threshold that triggers the alert)
- Rule Identifiers (list of special rules, triggering the alert if a match is found)

Users have the flexibility to configure the parameters to their specific needs.

6.6.2 Log Management and TCR

TSIEM Log Management provides the means to monitor the log collection process through 'collect history' and 'log continuity' reports. This allows the user to verify that the audit trails are being properly managed.



The audit controller initiates the collection of log data, and ensures that it is stored in the Log Management Depot on the TSIEM server. Normally, log data collection operations are triggered on a user-defined schedule. The audit controller also records the attempted collect operations in the Log Management Database, indicating success or failure. This information is used by the Collect History and Log Continuity reports.

TSIEM introduced the Log Management Reporting feature, which generates reports on the content of the collected log files using the index/search capability (TSIEM Searcher API based on the Apache "Lucene" subsystem) and the Tivoli Common Reporting (TCR) services. TCR Portlets are deployed to support the Log Management Reporting feature using the Business Intelligence and Reporting Tool (BIRT) infrastructure to define and render the reports. This feature provides reports on the content of the files in the Log Management Depot, without doing full W7 normalization. It makes use of the forensic search functionality to accomplish this.

QRadar does not provide reporting functionality similar to TSIEM's 'collect history' and 'log continuity' reports. However, TCR reports are easy to migrate because of simplicity and usage of non-normalized raw log records variables as input data.

6.6.3 QRadar Offences and Reports

6.6.3.1 QRadar Offences

A QRadar offense is a message sent or event generated in response to a monitored condition, which indicates a threat. For example, an offense informs if a policy has been breached or the network is under attack.

The Offense management interface provides a clear and concise vision of the most relevant information.

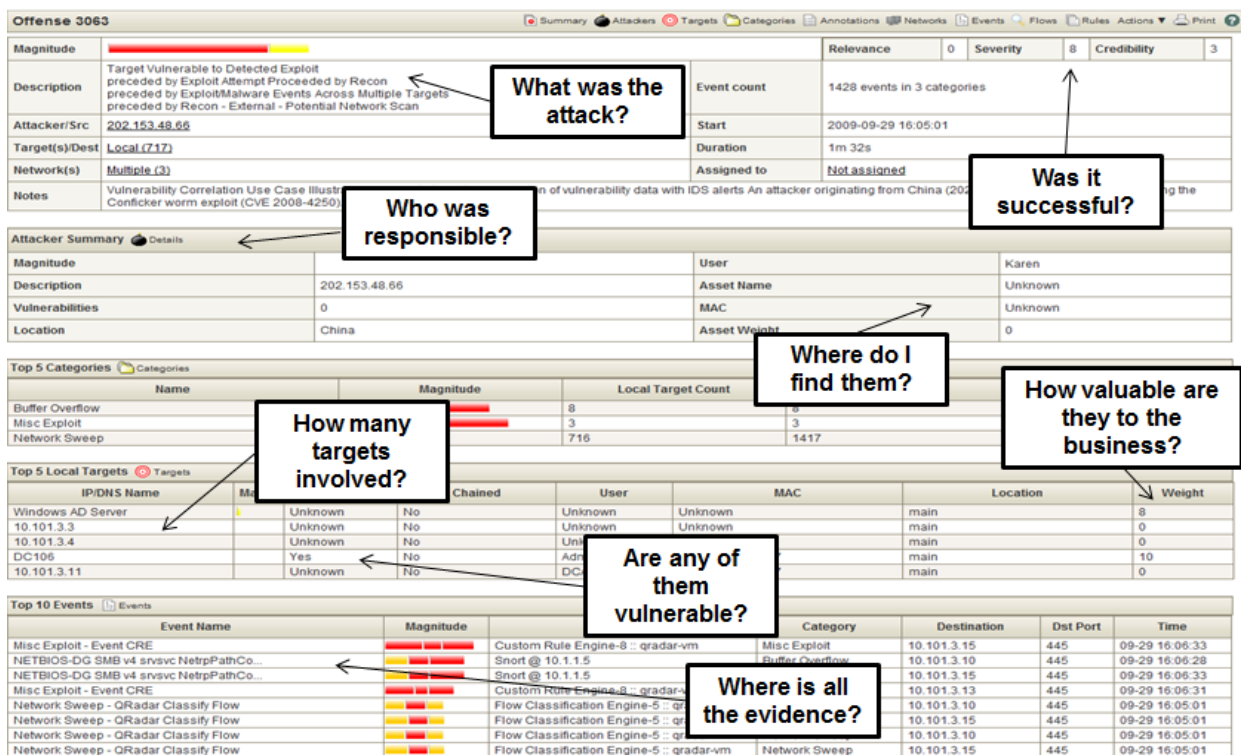


Figure 1. Offense management interface.

The most important characteristic of an offense is the magnitude, which specifies the relative importance of the offense and is a weighted value calculated from the Relevance, Severity, and Credibility, where

- Relevance determines the significance of an event or offense in terms of how the target asset has been valued within the network.

- Severity indicates the amount of threat an attacker poses in relation to how prepared the target is for the attack.
- Credibility indicates the integrity or validity of evidence as determined by the credibility rating from devices reporting the individual security events. The credibility can increase as multiple sources report the same event.

The magnitude bar on the Offenses tab and Dashboard provides a visual representation of all correlated variables of the offense, source, destination, or network. The magnitude of an offense is determined by several tests that are performed on an offense every time it has been scheduled for re-evaluation, usually because events have been added or the minimum time for scheduling has occurred.

The magnitude is calculated by Magistrate which is the core processing component of the solution. The Magistrate provides reports, alerts, and analysis of network traffic and security events. It processes the event against the defined custom rules to create an offense.

When QRadar receives data, the Magistrate is weighing all the different evidence from the various sources. The associated evidence is judged according to its credibility, severity and relevance and all of these weights participate in the creation and observation of an offense. The final magnitude, represented on a scale of 0-10, is the result of combining the three different measurements as they apply to monitored information.

The Fancy formula: $\text{Magnitude} = 50\% \text{ of Relevance} + 20\% \text{ of Credibility} + 30\% \text{ of Severity}$.

Event Relevance calculated as follows:

1. Set to a default value of 5
2. Adjusted up or down by CRE rules (Custom Rule Event)

Event Credibility calculated as follows:

1. Set to a default value of 5
2. Adjusted to the credibility value configured for the log source
3. Adjusted up or down by CRE rules

Event Severity calculated as follows:

1. Set to a default value of 5
2. Adjusted to the severity value assigned to the event
3. Adjusted up or down by CRE rules

Refer to section 7.5.1.3 to learn more about translating exception or attention events into rules and offenses.

6.6.3.2 QRadar Reports

The majority of all standard QRadar reports currently depend on the QRadar Event Category (low-levelcategory) and Building Blocks. There are total of 1085 predefined lowlevelcategories in QRadar and a majority of the reports are more log source dependent, meaning that not all predefined reports can be applied equally for all QRadar DSMs and custom Log Source Extensions (LSE). Custom reports can be based on any number of specific fields being identified by QRadar DSM.

6.6.4 Compliance Management Modules

The Compliance Management Modules (CMM) provides a set of reports and analysis capabilities that enable you to monitor and maintain compliance with a selected standard using TSIEM. Such a modules need to be installed separately as an additional components (Java-based plugins) of TSIEM. The modules typically include the following features:

- Classification Template
- Policy Template
- Reports
- Documentation

The following compliance standards are covered by TSIEM using Compliance Management Modules:

- Basel II

- COBIT
- FISMA
- GLBA
- GPG13
- HIPAA
- ISO27001
- NERC CIP
- PCI-DSS
- SOX (Sarbanes-Oxley)

A just installed CMM could be used to provide compliance reports on existing data; there is no need to collect new data or reload any GEM databases.

QRadar supports following compliance reports out-of-box:

- COBIT
- FISMA
- GLBA
- GSX-Memo22
- HIPAA
- NERC
- PCI
- SOX (Sarbanes-Oxley)

In contrast to TSIEM, QRadar does not require any additional modules to be installed to provide compliance reporting capabilities. Reports are based on the pre-defined or custom search queries over the normalized events and flows. In order to migrate TSIEM compliance reports, each report needs to be analyzed for input data flow, thresholds and boundaries, and then the appropriate

searching queries need to be constructed within QRadar. Refer to Chapter 6.7.1 for a sample use case of a TSIEM report transition into QRadar.

6.7 Reports Transition

6.7.1 Basic Migration Principles for Compliance Reports

This chapter provides a basic overview of the process of migrating TSIEM reports to QRadar reports. All TSIEM reports cannot be migrated to QRadar, and the reports that are migrated will not have the same parameters, flexibility and data fields that were available in the TSIEM reports. Therefore, each report needs to be considered on its own. The following guide contains a high level overview of the transition process along with suitable use cases.

The TSIEM internal data model uses the W7 event model to represent the event data. When moving reports from TSIEM to QRadar, each of the W7 dimensions needs to be considered. The following table contains basic transition rules for migrating TSIEM reports to QRadar:

TSIEM dimension	Description	TSIEM typical use case	QRadar transition rule
When	This dimension identifies the time at which the even has occurred.	All activities out of office hours	A rule condition is specified, defining office hours according to the company's security policy.
Who	This dimension identifies the user responsible for the action.	All activities of privileged users	A rule condition is specified, defining all privileged users. All such users are defined through a reference set containing the information from the user repository.
What	This dimension identifies the kind of action being performed.	All activities that resulted in deleted users	A rule condition is specified, where low-level category is equal to 'User Account Removed'.

OnWhat	This dimension identifies the type of the object being the focus of the action.	All activities related to file objects	<p>A rule condition is specified, where low-level category is equal to the following values:</p> <ul style="list-style-type: none"> 'File Transfer' 'File Print' 'FileTransfer Redirected' 'FileTransfer Queued' 'FileTransfer Delayed' 'FileTransfer In Progress' 'FileTransfer Denied' 'FileTransfer Terminated' 'FileTransfer Closed' 'FileTransfer Opened' 'FileTransfer Reset' 'File Deleted' 'File Created' 'Failed File Modification' 'Successful File Modification' 'Suspicious File Name'
Where	This dimension identifies the location where the event has been logged.	The report criteria for Where, WhereTo and WhereFrom are obvious (host types, names or IP addresses) and do not require any QRadar specific rule conditions or the rule conditions are very simple.	
WhereTo	This dimension identifies the target of the action.		
WhereFrom	This dimension identifies the source of the action.		

Table 5-5 TSIEM reports transition rules

Note: For detailed information on QRadar report creation steps, refer to the 'QRadar User Guide'.

6.7.2 Hands-On Compliance Report Migration

Compliance reports in TSIEM are based on different W7 groups. This chapter will demonstrate migration of the compliance reports shipped with the BASEL II Compliance Management Module of TSIEM into QRadar reports, as BASEL II reports are not available in QRadar out of the box.

1. Navigate to the “Compliance Management Modules” section of the Tivoli Integrated Portal in TSIEM and select “BASEL II” (The BASEL II CMM should be installed)

BASEL II	
Title	
BASEL II External attacks - monthly trend	Number of exceptions in the Expo
BASEL II External attacks - quarterly trend	Number of exceptions in the Expo
BASEL II Internal attacks - monthly trend	Number of exceptions NOT in the
BASEL II Internal attacks - quarterly trend	Number of exceptions NOT in the
BASEL II Policy Exceptions - monthly trend	Number of exceptions month over
BASEL II Policy Exceptions - quarterly trend	Number of exceptions quarter over
BASEL II (5.2,5.2) Classification	Assets defined to the system.
BASEL II (6.3,8.1.3,8.1.3) Security alert	Alerts sent in response to policy

2. Choose the report you want to migrate into QRadar (e.g. “Control of operational software”), check the report conditions in the “Filters” section.

#Events	#Pol. Excp.	#Spec. Att	#Fail.
16	16	0	0
1	1	0	0

Page 1 | < << >> > | Jump to page Go

▼ Help

Control of change and update to system files and resources is essential to control risk. This report shows who accessed and changed which system resources.

▼ Background

Paragraph 10.4.1
Paragraph 10.4.1

▼ Filters

This report is based on the following equality:

What (group)	System Updates
--------------	----------------

3. Log in to QRadar Console, navigate to the “Log Activity” tab and select “New search”

4. Create a new group "BASEL II" using the "Manage Groups" button. Use the "Compliance" group as a parent.
5. Properly fill search properties:
 - "Time Range" as required by compliance policy (e.g. "Recent", "7 days")
 - "Search Parameters" should be selected in accordance with the TSIEM report conditions and help description. For this example, "Category" will be used as the search criteria, which should be equal to the following High Level / Low Level categories (would be different for specific migration task):
 - Audit / Data Update
 - Policy / Failed
 - Policy / Succeeded
 - Risk Manager Audit / Policy Monitor
 - SIM Audit / Risk Manager Configuration
 - SIM Audit / SIM Configuration Change
 - System / Configuration Error
 - System / Failed Application Modification
 - System / Failed Configuration Modification
 - System / Failed File Modification
 - System / Failed Host-Policy Modification
 - System / Failed Registry Modification
 - System / Failed Service Modification
 - System / Failed Stack Modification

- System / File Created
- System / File Deleted
- System / Host-Policy Created
- System / Host-Policy Deleted
- System / Misconfiguration
- System / Registry Addition
- System / Registry Deletion
- System / Service Installed
- System / Service Uninstalled
- System / Successful Application Modification
- System / Successful Configuration Modification
- System / Successful File Modification
- System / Successful Host-Policy Modification
- System / Successful Registry Modification
- System / Successful Service Modification
- System / Successful Stack Modification
- System / System Configuration

Time Range:

Real Time (streaming)
 Last Interval (auto refresh)
 Recent
 Specific Interval

Start Time: 2011-01-17 at [calendar icon] [dropdown]
 End Time: 2011-01-24 at [calendar icon] [dropdown]

Search Parameters

High Level Category:

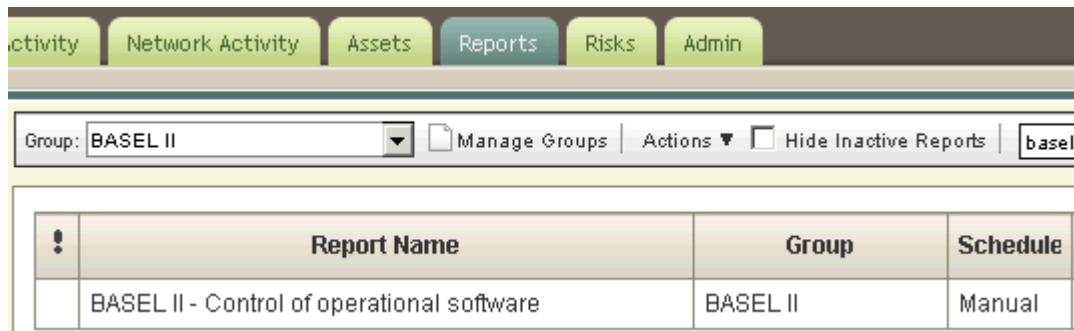
Current Filters

- Low Level Category is Data Update
- Low Level Category is Failed
- Low Level Category is Succeeded
- Low Level Category is Policy Monitor

Note: while using categories as search criteria you may need to double-check specific events supported by QRadar within the selected category (via Event Browser) to make sure that the proper data items will be selected for the compliance report.

1. Update "Column Definition" with fields required for compliance report
2. Press the "Search" button
3. Press the "Save Criteria" button
4. Type "Control of operational software" as a search name and select "BASEL II" as a group, press OK
5. Navigate to "Reports" tabs in QRadar Console and create a group for BASEL II reports by pressing "Manage Groups" button, using "Compliance" group as a parent.
6. Launch Report Wizard by pressing "Actions - Create" button
7. Select required report schedule
8. Select required report layout
9. Type report title ("BASEL II - Control of operational software"), and select Chart Type as "Events/Logs"

10. Fill the container details as required by compliance policy, and “Control of operational software” as Saved Search
11. Proceed to the next Wizard pages and choose report format and distribution
12. Proceed to the next Wizard page and select “BASEL II” as report group, type an optional description
13. Finalize report creation.



6.8 Terminology Comparison

The following table contains the comparison of terms for TSIEM and QRadar with suitable relevance, where applicable.

<i>TSIEM</i>	<i>QRadar</i>
Agent	Adaptive Log Exporter, Event Processor
Agent group	Log Source Group
Alerts	Rule Response
Archiving Data	Backup & Restore
Audited machine	Asset and/or Log Source
Backup & Restore	Backup & Restore
Chunk	No equivalent – data is stored together in Ariel
Compliance Dashboard	Dashboard
Compliance Management Module	No equivalent – all reports are included in QRadar
Consolidation component	Magistrate
Credential Store	Credentials are stored in Postgres
Depot	Ariel

Distribution	Email distribution is configured within the report definition
Enterprise Server	31xx console in a distributed deployment
Event Source	Log Source
Forensics component	Payload search (with optional indexing)
Group Definitions	Building Block
GSL Parser	Universal Device Support Module (uDSM) XML file
GML Mapper	Map Event – available in the GUI
Launchpad (Tivoli Integrated Portal)	Console GUI
Log Continuity Report	No equivalent due to use of syslog for most log sources
Log History Report	QRadar report called “Errors and Failures”
Log Manager Dashboard	Log Sources in the Admin tab
Log Management Activity Report	QRadar report: (Daily, Weekly, or Monthly) Log/Event Distribution by Category
Log Management component	QRadar Log Manager
Log Management Depot Investigation Tool	Payload search (with optional indexing)
Log Management Retrieval Tool	“Raw Log” view in Log Activity
Normalization component	Built-in to QRadar, required part of the event processor
Policy	Building Block
Policy Explorer/Editor	Rules/Building Blocks Editor
Policy Generator	QRadar Tuning Guide
Regulations	Contained within QRadar reports
Reporting Database	No equivalent – QRadar is real-time, with all data going into the same Ariel datastore
Security Information Management (SIM) component	Security Information and Event Management (SIEM) component
Security Group	All QRadar deployments use one User store, the console appliance, unless external authentication is configured
Scoping	User Role (scope by network hierarchy) and User Account (scope by Log Sources)
Significance	Magnitude
Special Attention Rule	Building Block or Rule
Standard Server	All-in-one Console
Trending	Time Series
User Information Source	Reference Set
User Roles	User Roles
W7	No equivalent term, but QRadar has a standard normalization scheme as well

Table 5-6 Terminology Comparison

7. Plan a QRadar deployment

This section details the steps to a successful QRadar deployment. In addition, transitioning from several common concepts in TSIEM are described.

7.1 Design the QRadar Architecture

The first steps will be designing the architecture. There are many ways to architect a QRadar deployment. This guide will only touch on the standard deployments. Please review current QRadar options with an IBM sales team and/or solution architect. To understand the architectural options in QRadar, here is brief rundown of available appliances. EPS stands for Events per Second. FPM stands for Flows per Minute and applies to all supported Netflow versions including CFlow, JFlow, SFlow, VFlow, QFlow, and others. The QRadar Qflow feature listens to a full network packet stream via a SPAN, mirror, or network tap and produces a Netflow-compatible stream with the added bonus of protocol analysis and anomaly detection. QFlow is measured in Mbps (Mega-bits per second) or Gbps (Giga-bits per second).

For comparison purposes, a TSIEM Standard Server could collect about 60 GB per day. If the average event size was 728 bytes, that comes out to about 1000 events per second. This would be equivalent to a 2100 All-in-one

Appliance Model	Use
2000 All-in-One Console	Very Small Business All-in-One Console – Only 200 EPS and 15,000 FPM, 50 Mbps for QFlow, 200 log sources
2100 All-in-One Console	Small to Medium sized business All-in-One Console – 1000 EPS, 50,000 FPM, 50 Mbps for QFlow, 750 log sources. You can add QFlow collectors to a 2100, but not any event or flow processors
31xx All-in-One Console or Enterprise Console	QRadar's standard All-in-One Console - 5000 EPS, 200,000 Flows, and 750 log sources. It does not have any embedded QFlow collectors like the 2000 and 2100. This appliance is also used with enterprise deployments. There are several versions of this appliance that has incrementally more capacity for more storage and/or concurrent users.

Appliance Model	Use
16xx Event Processor	The 16xx series are expansion appliances that are deployed in conjunction with the 31xx. The 16xx series offers real-time collection, prioritization and correlation of event data and can scale to more than 10,000 events per second in the 1601 model, or 20,000 EPS in the higher models (1605, 1624, etc). There are several versions of this appliance that has incrementally more capacity for more storage and/or concurrent users.
17xx Flow Processor	Whether extracting native flow information from the network infrastructure, or working in tandem with QFlow collectors, QRadar flow processors enable the collection, analysis and storage of a variety of flow formats including Netflow, CFlow, JFlow, SFlow, VFlow and QFlow. The 17xx is an expansion appliance that is deployed in conjunction with the 31xx. There are several versions of this appliance that has incrementally more capacity for more storage and/or concurrent users.
18xx Combined Event & Flow Processor	The 18xx series appliances are well suited for organizations looking to provide event and network activity monitoring and processing for remote or branch offices or to larger highly distributed organizations. Tops out at 1000 EPS and 50,000 FPM.
11xx, 12xx, & 13xx Qflow Collector	These QFlow Collectors can be added to a 2100 or 3100. These devices collect full packet capture to produce QFlow for a QRadar Console. There a number of appliance models that have various interfaces and capacities.

Table 7-1 QRadar Appliance Models

Every deployment needs at least one console appliance. If there is one TSIEM Standard Server deployed, the only appliance needed is 3100 All-in-One or smaller. This will give the same capacity as the TSIEM deployment with the added bonus of collected Netflows. It is suggested to have at least one QFlow appliance to capture data going across the internet facing interface. For every interface where there is a network intrusion detection/prevention device(s), that same data should be spanned to a QFlow appliance.

To get an effective sizing from an IBM Security Solutions sales engineer or services, the following information is useful. This will allow IBM to give an accurate sizing.

- Measured or estimated Events per Second
- Measured or estimated Flows per Minute

- Connect bandwidth to remote datacenters or sites
- Will any of these remote sites be over a WAN link?
- Is encryption between QRadar appliances required?
- What version and type of Netflow (Netflow vs. JFlow, etc.)?
- Utilization of the interfaces to be used with QFlow.
- A list of devices that will be log sources
- Data retention requirements.

Considering the power of QRadar, a smaller implementation might be preferable and will allow for some cost savings. A 2000, 2100, and 3100 appliance may be enough to meet requirements. The caution is the upgrade path of the 2000 and 2100. If you undersize a 2000, the upgrade requires replacing the appliance with a larger device. Other appliances allow for adding devices or additional licenses. These All-in-One consoles all have the same application features, just with a smaller scope.

If all the features of a full SIEM are not needed, then consider the QRadar Log Manager. A nice feature of QRadar is that the Log Manager can be upgraded to SEIM with a simple license change. Below is a breakdown of the software features that come with each QRadar product.
















Software Feature	Log Manager	QRadar
Manages network and security events		
Manages host and application logs		
Tamper-proof data archive		
Threshold-based correlation and alerts		
Compliance reporting templates		
Managing flows for full Network Behavior Analysis	<input data-bbox="1214 669 1256 703" type="checkbox"/>	
Asset Profile Creation and Management	<input data-bbox="1214 747 1256 781" type="checkbox"/>	
Work flow and remediation	<input data-bbox="1214 825 1256 858" type="checkbox"/>	
Offense management	<input data-bbox="1214 903 1256 936" type="checkbox"/>	
Integrated network, security, application and identity visibility	<input data-bbox="1214 980 1256 1014" type="checkbox"/>	

Table 7-2 Comparison between QRadar Log Manager and QRadar SIEM

If High Availability (HA) is a requirement, or even a nice to have feature, consider the HA option with the appliances. With real-time UDP protocols like syslog and SNMP, if an event collector is down, events are being lost. Any of the appliances listed above can have an HA pair. HA is very easy to setup because it's built right into the QRadar application.

7.2 Install Appliances

After receiving the new appliances, there are a few things needed to get them configured. In the appliance box, there is a plastic envelope with the activation key and a CD with the installation manuals. The easiest way to get the appliance initially installed is to hook up a monitor and USB keyboard to the appliance. To get through the initial installation process, the following data is required:

- IP Address of the appliance

- Subnet mask
- Gateway IP
- Fully qualified domain name
- DNS server(s)
- NTP server (needed for the console only)
- SMTP Server
- Time Zone
- Activation Key

Follow the installation guide on the CDROM for detailed instructions.

7.3 Reuse the TSEIM IPs and/or reconfigure endpoints

When selecting an IP address for your event processors, consider reusing the Standard Server's IP address(es). This will require some coordination to achieve, but will save time since endpoints using syslog and SNMP will not have to be reconfigured. To do this, have the console configured and online first. Then configure the event processor with the network cable unhooked. Finally unplug the Standard Server and plug in the event processor. On the event console, start the deployment manager and add the event processor. Save and deploy. There should be very minimal downtime.

If this cannot be achieved, the endpoint will need to be configured to point its logs to the new server. This can also be achieved with little to no downtime, but may be a large chunk of work if you have a lot of endpoints. Most devices and servers can have multiple syslog destinations. Just add the new event processor or console IP address in addition to the TSIEM Standard Server.

Any TSIEM agents that were deployed must be uninstalled. In most cases, they will be replaced with QRadar's Adaptive Log Exporter (ALE) agent. As with all event sources, consult the QRadar

“Configuring DSM Guide” documentation to see what are the available choices to support each particular event source

7.4 Do Initial Configuration

To get the solution up and running, some initial configuration steps must be taken. Please review the QRadar Administration Guide and the Tuning Guide for details on these steps.

1. Obtain an account for Qmmunity.Q1Labs.com. This is provided for new customers and Q1 dedicated resources.
2. If there is more than one appliance, use the Deployment Manager to add the managed hosts.
3. Configure HA if needed.
4. Patch your appliances to the newest patch level (downloadable from Qmmunity).
5. Update DSMs, Protocols, and VA Scanners (downloadable from Qmmunity).
6. Create your Network Hierarchy
7. Configure any Vulnerability Scanners
8. Add Log Sources
9. Convert business logic from TSIEM to QRadar (see next section)
10. Do initial tuning (refer to the QRadar Tuning Guide)

7.5 Convert business logic from TSIEM to QRadar

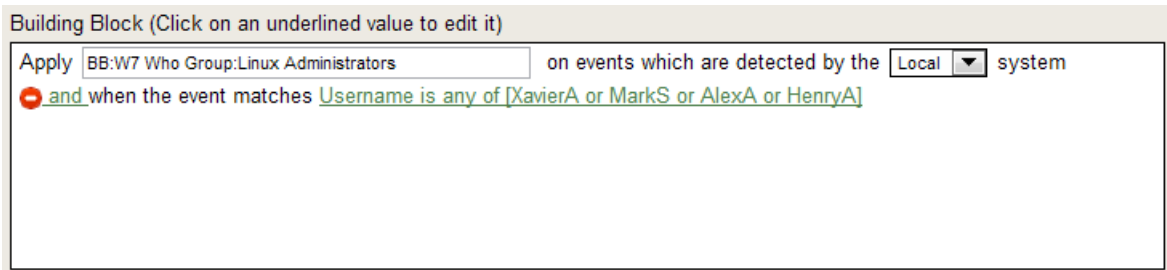
Now it is time to convert the business logic from TSIEM to QRadar. These steps are needed to ensure that business requirements are still met with the new solution. As mentioned in the Overview section, be sure that any business logic and business requirements are still relevant. If it is discovered that a feature of TSIEM like policies, user information sources or special attention rules are no

longer needed, there is no need to spend the time recreating the logic in QRadar. QRadar has many additional features that could fulfill business requirements and some TSIEM features may not be needed.

7.5.1.1 TSIEM W7 Groups

TSIEM uses W7 Groups to help categorize data. These groups are used in several other features of TSIEM including policies, special attention rules, and reports.

To recreate this logic in QRadar, Building Blocks will be created or Reference Sets are used to check specific properties. Because the use of Reference Sets requires skills to create appropriate QRadar rules, we will discuss the usage of Building Blocks to represent W7 Groups. For example, say that there was a W7 Who group that contains all Linux Administrators. In QRadar, a Building Block would be created that listed those user accounts. Then, just like in TSIEM, every event in QRadar will be flagged with that grouping information.



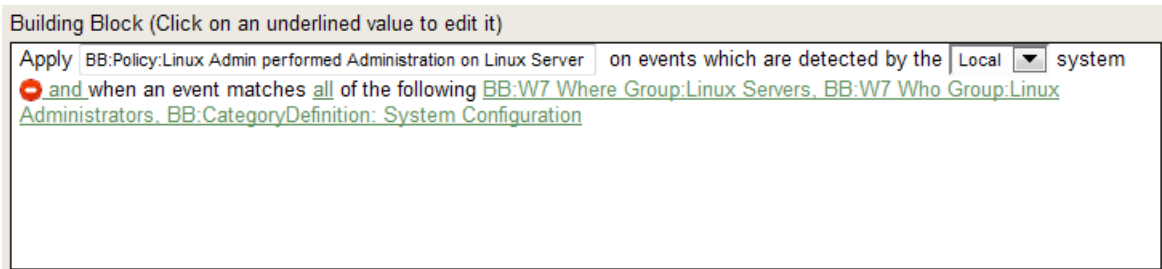
For W7 What groups, many of which are defined out of the box in TSIEM, look at existing Building Blocks (typically in Category Definitions) or utilized QRadar’s event categories. There is a wealth of predefined logic in QRadar that can be used when building your new Building Blocks.

Note: there is no need to “commit policy” in QRadar. As soon as the Building Block is created, it goes into effect. It will only be applicable to the data collected from that point forward. Previously collected data will not have the new Building Block assigned to it.

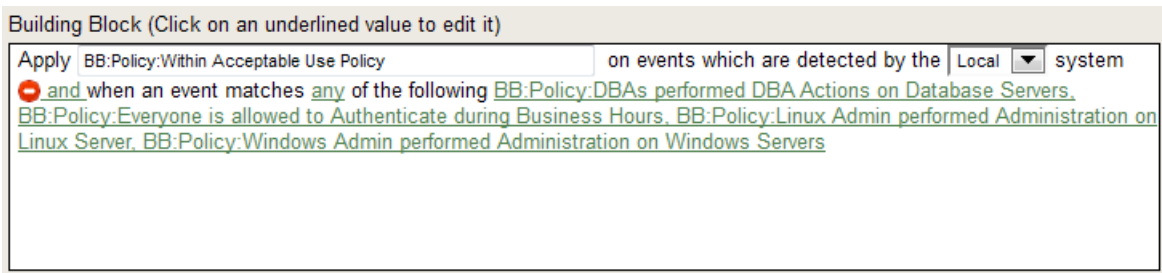
7.5.1.2 TSIEM Policies

TSIEM uses the concept of Policies to define an acceptable use policy. These are rules that help define whether or not a event is white listed or is a policy exception. TSIEM policies are defined using W7 Groups.

In QRadar, the W7 Groups are defined using Building Blocks, so are TSIEM Policies. The best way to implement this is to use multiple, chained Building Blocks. For example, to convert the Policy Rule that said that all Linux Administrators (Who Group) are allowed to do System Administration (What Group) to any Linux Server (Where group), the W7 Groups would all need to be created as a Building Blocks in QRadar. Alternatively, existing Building Blocks can be used. For example instead of creating a new Building Block for the System Administration What group, the built-in building block, “BB:CategoryDefinition: System Configuration” can be used.



Another Building Block named “BB:Policy:Linux Admin performed Administration on Linux Server” is created to define that the event matches all three W7 Group Building Blocks. Finally a master “BB:Policy:Within Acceptable Use Policy” Building block is created to pull all the various policy rules together to flag the event as within policy. Now reports and searches can easily be created that matches the filter “Custom Rule is NOT BB:Policy:Within Acceptable Use Policy” for all events that are policy exceptions.



Note: there is no need to “commit policy” in QRadar. As soon as the Building Block is created, it goes into effect. It will only be applicable to the data collected from that point forward. Previously collected data will not have the new Building Block assigned to it.

7.5.1.3 TSIEM Special Attention Rules and Alerts

Special Attention Rules in TSIEM are structurally the same as Policy Rules, but they are used for a different purpose. While Policy Rules gives a firm delineation on an event being with policy or not, Special Attention Rules are used to call specific events, either explicitly against policy (e.g. a black list) or exceptionally risky behavior (e.g. changes on a production SAP instance). TSIEM can just flag an event as a Special Attention event, or it can send an alert.

QRadar uses Building Blocks as a way to categorize events, but when an action must be taken, like an send out an alert, QRadar Rules are used. If you have basic TSIEM Special Attention Rules with no alerting, create them as Building Blocks. If the Special Attention Rules are configured to send alerts, recreate them as QRadar Rules.

Note: there is no need to “commit policy” in QRadar. As soon as the Building Block is created, it goes into effect. It will only be applicable to the data collected from that point forward. Previously collected data will not have the new Building Block assigned to it.

7.5.1.4 TSIEM User Information Source

In addition to security events, TSIEM can also collect group memberships. Most customers rely on security groups from IBM’s Tivoli Directory Sever or Microsoft’s Active Directory to define user roles. TSIEM uses User Information Sources (UIS) to collect these group memberships, usually once per day, to be available when a reporting database is loaded.

QRadar has a dynamic grouping feature called reference sets. These reference sets can be populated using rules. By feeding QRadar group information via the Universal Device Support Module (uDSM), a rule can be created to populate these reference sets. The nature of these data feeds tends to be on the more advanced side of QRadar configuration, and most customers should seek

guidance from IBM Security Intelligence Professional Services or a Q1 Labs Certified Partner to implement User Information Sources in QRadar.

7.5.1.5 TSIEM Reports and Management Modules

TSIEM comes with a large collection of out-of-the-box reports, plus customers could purchase additional Compliance Management Modules to add specific reports such as PCI, SOX, and HIPAA. Most of these reports utilized W7 Groups for the report definitions. Custom reports in TSIEM were easy to configure with no SQL knowledge needed.

QRadar also comes with a large number of out of the box reports, but with QRadar all the compliance specific reports are included as part of the default installation. These reports are defined using Saved Searches. To recreate any custom reports in QRadar, a user would create a search in the Log Activity tab with any required filters and column, save the search and then create a new report based on the saved search. To create such a report, follow the new report wizard using the saved search that was just created. These steps are called out in detail in the QRadar Users Guide.

7.6 Migrate data or keep TSIEM online for a period of time for historical queries

Once QRadar is up and running, there is a choice on how to handle the data stored in TSIEM's depot. The first and easiest option is to keep the TSIEM server(s) online for a period of time for historical queries. This option will also allow you have TSIEM's configuration available just in case reproducing the business logic in QRadar takes longer than expected. This is the only option supported by IBM support.

If data migration is a requirement, custom development is required. It is strongly suggested that you engage IBM Security Intelligence Professional Services or an authorized IBM business partner to develop a process to migrate the data. The basic methodology for data migration is contained within the appendix to introduce concepts, but the full scope of data migration is beyond the scope of this document.

8. Appendix

8.1 Basic Algorithms for TSIEM Data Extraction

Note: There is no supported method for data migration from TSIEM to QRadar. This appendix introduces basic methodologies that one could follow to develop a migration strategy. It is highly recommended that you engage IBM Security Intelligence Professional Services or an authorized IBM business partner to develop a process to migrate the data.

Before any data extraction can be made, the TSIEM depot should contain all the data necessary for the migration process. This means that all the necessary chunks, previously exported, have to be imported to TSIEM depot.

The TSIEM native data processing flow is initiated by a ~~Python script~~ [homebrew tools](#). The following actions are performed:

- The TSIEM server location is determined by the value of the following environment variable
 - Windows : %TSIEM_HOME%
 - Unix : \$TSIEM_HOME
- The local depot is scanned to get:
 - List of the platforms from chunk headers
 - Total size of platform chunks (compressed) for each platform
 - First and last collect time for each platform
- Chunks statistics are displayed on the screen
- Allow to choose platforms and time frame for exported chunks, e.g.:
 - IBM WAS from 01.11.2009 till 01.11.2011
 - Sun Solaris for last 12 months
- For each platform:
 - Process selected chunks with Gensub to get BCP files with events mapping
 - Process BCP files to get a single file with event data in CSV (comma-separated value) format to be migrated into QRadar

- Display the events and size statistics for each processed platform

Note: data processing may require adjusting GxL scripts to provide all the data significant to QRadar.

8.2 Basic Algorithm for QRadar Data Import

Note: There is no supported method for data migration from TSIEM to QRadar. This appendix introduces basic methodologies that one could follow to do a migration. It is highly recommended that you engage IBM Security Intelligence Professional Services or an authorized IBM business partner to develop a process to migrate the data.

QRadar uses the proprietary Arial Database and its console client does not support an INSERT command. Therefore, the only native way of importing TSIEM collected data is using the QRadar Log Source eXtension.

8.2.1 Processing QRadar Data via Log Source eXtension (LSX)

There is no official support for migrating data from TSIEM to QRadar. However, one approach which would require custom code is to use the QRadar Log Source eXtension Feature. There are some limitations to that approach.

TSIEM data can be uploaded into QRadar using the Universal DSM which allows forwarding events from log sources to QRadar. The data can be contained in structured files such as files in CSV format, There are some limitations to this approach that should be taken into account.

For each event source whose data will be migrated into QRadar, a new log source extension would have to be developed. Even if QRadar has a standard log source for that device or application, in most cases it cannot be used because the data will most likely be in a new format, or a different protocol was used to collect the data in TSIEM. For example, a standard QRadar log source may support collecting via syslog, SNMP or using MS services, the TSIEM data will most likely be in W7 format in CSV format files.

The second limitation is that the QRadar license is based on the EPS and hardware capacity. The appliance has to have enough capacity to handle the current events flow and to process the TSIEM data at the same time. The calculation is quite simple: if the task is to upload a month of history data with 2000 EPS in average ($2000\text{EPS} * 31 \text{ days} * 24 \text{ hours} * 3600 \text{ second per hour} = 5.3 \text{ billion events}$), it may take a month if the system has 2000 EPS unused, or it may take 4 months if free system or license capacity is only 500 EPS.

The final concern, the time difference, is described in the following subchapter 'Log Source Time vs. Start Time and Storage Time'.

8.2.1.1 Log Source Time vs Start Time and Storage Time

The problem to be concerned about is the event time.

During the export of raw logs that are several days old, QRadar maps information about actual time of events to Log Source Time. On the other hand values of Start Time, End Time and Storage Time will be set automatically to current time during data loading process and they will contain time of event received by QRadar, which is significantly different as compared to original event time in exported log files.

```
Jan 01 23:45:02 172.16.0.253 PIX1 %PIX-6-302013: Built outbound TCP
connection 29658131 for outside:87.218.38.186/44433
(87.218.38.186/44433) to inside:Vela/3863 (213.142.196.31/3863)
```

For example, if such log record is uploaded on the 3rd of January, the result will be:

Start Time: 2011-01-03 06:45:55

Storage Time: 2011-01-03 06:45:55

Log Source Time: 2011-01-01 23:45:02

This time difference must be taken into account as most probably all chronological searches and reports have to be adjusted to provide reliable information based on Log Source Time instead of Start Time and End Time which are used by default.

8.3 Determining Average TSIEM Event Flow Volume (EPS)

TSIEM supports up to 5000 event sources with a single Server, and the average Events per Second (EPS) flowing into any real-time syslog or SNMP receiver to around 2000.

Note: in most common scenario TSIEM server (as well as QRadar) does not process (normalize) all the events generated by target platform. Thus actual EPS count generated by the same target platform may vary in both TSIEM and QRadar solutions.

There are several possible ways to determine average EPS count for each platform monitored with single TSIEM server:

1. GEM DB load statistics
2. Forensic search
3. Via tools

EPS count can be calculated from the loaded GEM database statistics. Such information is available from the Compliance Dashboard, when any of the available loaded GEM database is selected:

The screenshot shows the 'Status of the database' section with a database icon and the following details:

- Status of Database: Database loaded successfully
- Loading date: 3/25/12 12:00:59 AM (-0700)
- Number of Days: 1.72
- Automatic policy: 3/22/12 8:45:00 AM (-0700)
- User policy: 12/31/99 4:00:00 PM (-0800)

Below is the 'Data in this database' table with columns: Where (Platform), Start time, End time, #Chunks, and #Events. The row for 'srv-ts-10206-2.scnsoft.com (Microsoft Windows Server 2008/Vista)' is highlighted with a red box and has a red arrow pointing to its 2454 events.

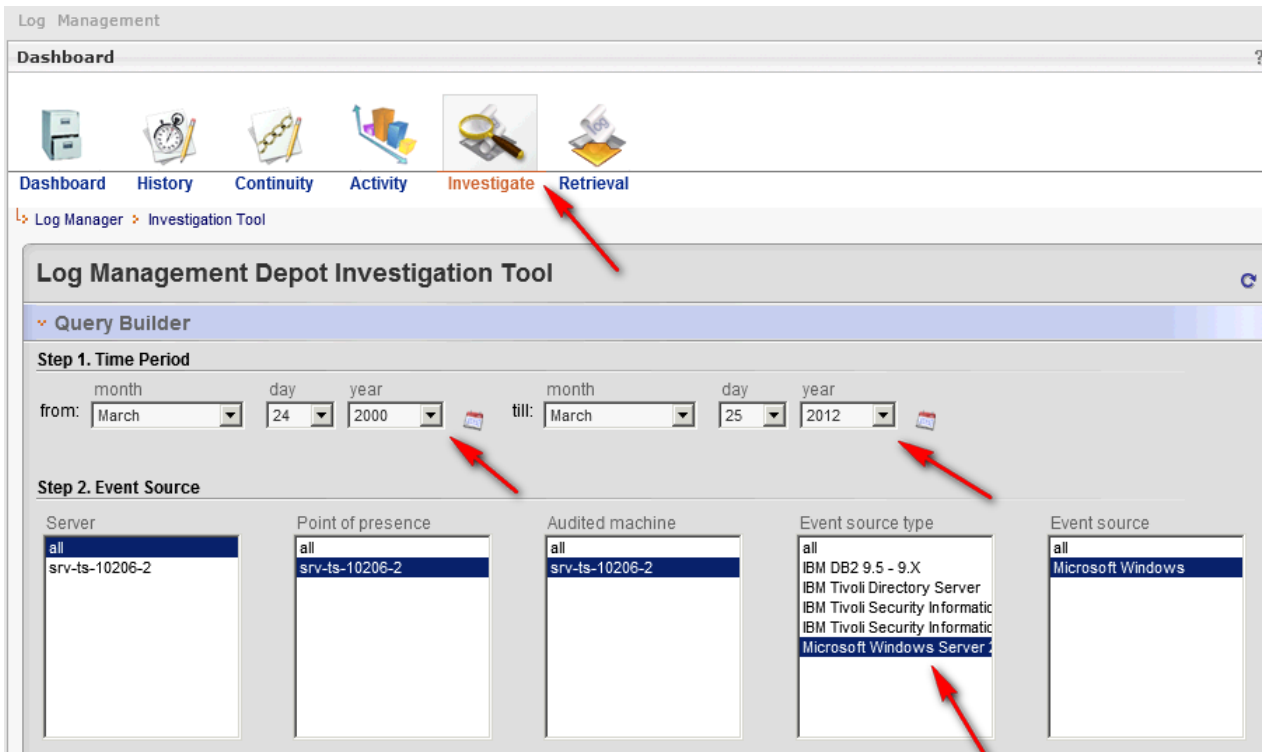
Where (Platform)	Start time	End time	#Chunks	#Events
srv-ts-10206-2 (IBM TDS)	3/21/12 11:51:18 PM (-0700)	3/21/12 11:54:43 PM (-0700)	1	14
26L2233A3-09 (Microsoft Windows Server 2008/Vista)	3/20/12 5:34:28 PM (-0700)	3/20/12 5:35:51 PM (-0700)	1	30
srv-ts-10206-2 (IBM TSIEM)	3/22/12 12:29:07 AM (-0700)	3/22/12 1:45:04 AM (-0700)	4	73
srv-ts-10206-2 (IBM TIP)	3/22/12 12:23:28 AM (-0700)	3/22/12 12:56:33 AM (-0700)	2	77
WIN-3Q3CWQEJDHQ (Microsoft Windows Server 2008/Vista)	3/20/12 8:38:00 AM (-0700)	3/21/12 7:32:19 AM (-0700)	1	82
srv-ts-10206-2 (IBM DB2 9.5 - 9.X on Windows)	3/21/12 11:55:31 PM (-0700)	3/22/12 1:45:04 AM (-0700)	4	498
srv-ts-10206-2.scnsoft.com (Microsoft Windows Server 2008/Vista)	3/21/12 7:31:32 AM (-0700)	3/22/12 1:08:10 AM (-0700)	2	2454

Page 1 | Navigation icons | Jump to page Go

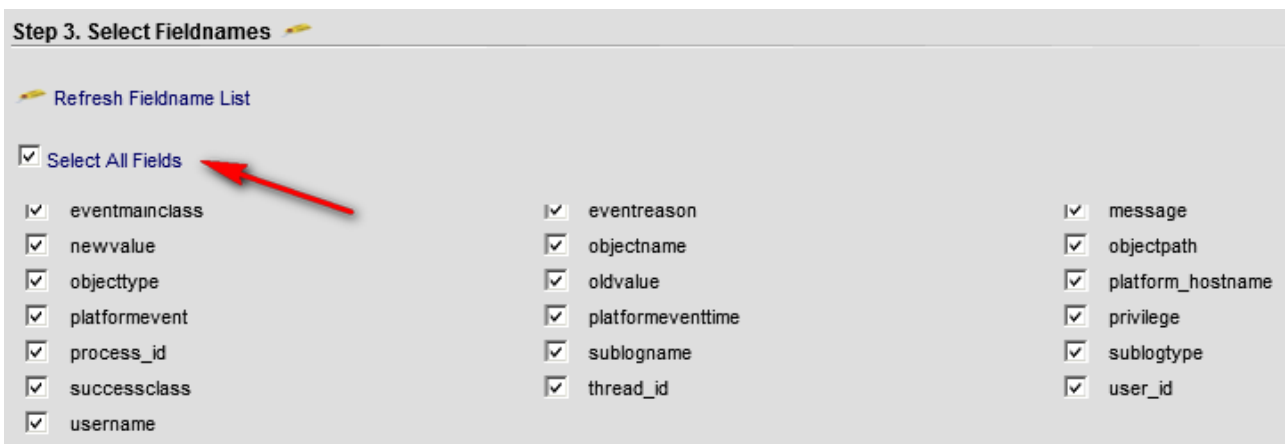
EPS statistics can be calculated for each audited platform. The only limitation of current approach is that precise analysis requires huge amount of data being loaded into the GEM database, which is time and resource consuming procedure.

While determining EPS via forensic search, following steps need to be performed:

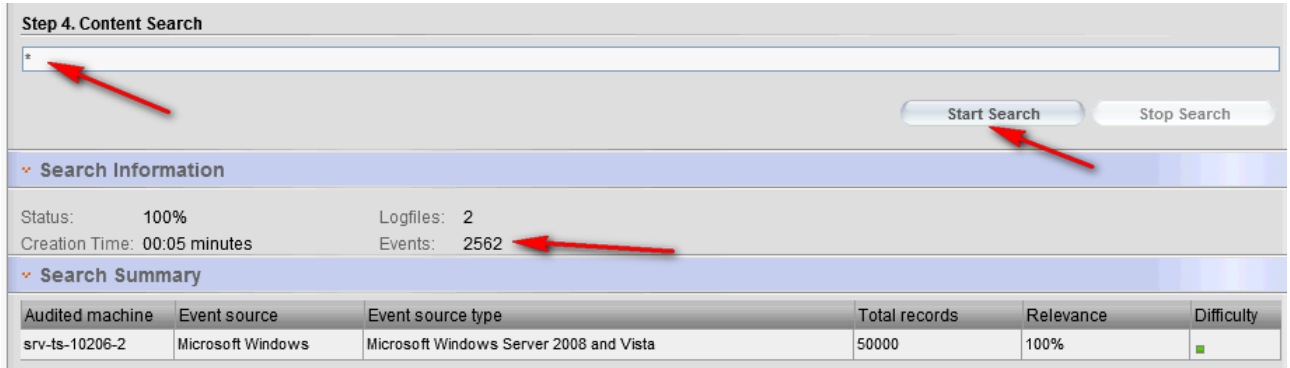
1. Open log manager investigation tool; select appropriate time periods and Event Source type (platform).



2. Select all fieldnames for search



3. Enter the wildcard as search criteria and press the “Start Search” button.



4. When the search is complete, the number of events indexed within selected time boundaries became available, and EPS count could be calculated.

The most flexible way to determine EPS count of the audited platform could be implemented via homebrew tools acting in according to the following algorithm:

- get one (or several) data chunk of the target platform from the Depot
- detect time boundaries (from the chunk headers)
- process chunk(s) with Gensub to generate GEM events (the procedure could be simplified when using indexing mechanism instead of full-processing)
- calculate number of actual events
- calculate EPS

8.4 Data Sources Comparison

The following table compares existing TSIEM Event Sources to QRadar Device Support Modules. The comparison indicates the possibilities for data migration as well as data parsing rules definitions. Color map:

Green	- items suitable for data migration
Violet	- items suitable for both data migration and Event Source migration
Blue	- universal Log Sources

IBM TSIEM to IBM QRadar Transition Guide

QRadar 7.0 MR4		TSIEM 2.0 FP5	
Data Source	Protocol	Data Source	Protocol
3Com 8800 Series Switch	Syslog		
Ambiron TrustWave ipAngel IPS	Syslog		
Apache HTTP Server	Syslog	Apache Web Server 2.x (forensic)	Syslog
Array Networks SSL VPN Access Gateways	Syslog		
Aruba Mobility Controller	Syslog		
Bit9 Parity	Syslog		
Bluecoat SG Appliance	Syslog, File	Blue Coat ProxySG	File
Bridgewater Systems AAA Service Controller	Syslog		
CA ACF2	File		
CA Top Secret	File	TopSecretVSE	File
CRYPTOCARD CRYPTOSHIELD	Syslog		
Check Point FireWall-1	Syslog, OPSEC/LEA	CheckPoint FireWall-1	File, OPSEC, SNMP
Cisco 12000 Series Routers	Syslog		
Cisco 6500 Series Switches	Syslog		
Cisco 7600 Series Routers	Syslog		
Cisco ACE Firewall	Syslog		
Cisco ACS	Syslog	Cisco Secure ACS	File
Cisco Adaptive Security Appliance (ASA)	Syslog, Cisco NSEL	Cisco ASA (forensic)	Syslog
Cisco Aironet	Syslog		
Cisco CSA	Syslog, SNMP		
Cisco Carrier Routing System	Syslog		
Cisco CatOS for Catalyst Switches	Syslog		
Cisco Firewall Services Module (FWSM)	Syslog	Cisco Firewall Services Module 7.1	Syslog
Cisco IOS	Syslog	Cisco IOS / Switches (forensic)	Syslog
Cisco Integrated Services Router	Syslog	Cisco Integrated Services Router (forensic)	Syslog
Cisco Intrusion Prevention System (IPS)	SDEE	Cisco Intrusion Prevention System (forensic)	Syslog
Cisco IronPort	Syslog, File		
Cisco NAC Appliance	Syslog		
Cisco PIX Firewall	Syslog	Cisco PIX	Syslog, SNMP, File
Cisco VPN 3000 Series Concentrator	Syslog	Cisco VPN (forensic)	Syslog
Cisco Wireless Services Module (WiSM)	Syslog		
Configurable Authentication message filter	Syslog		
Configurable Firewall Filter	Syslog		
Cyber-Ark Vault	Syslog		
CyberGuard TSP Firewall/VPN	Syslog		
EMC VMWare	EMC VMWare		
Enterasys A-Series	Syslog		
Enterasys B2-Series	Syslog		
Enterasys B3-Series	Syslog		
Enterasys C2-Series	Syslog		
Enterasys C3-Series	Syslog		
Enterasys D-Series	Syslog		
Enterasys Dragon Network IPS	Syslog, SNMP	Enterasys Dragon 6 (forensic)	Syslog
Enterasys G-Series	Syslog		
Enterasys HiGuard	Syslog		
Enterasys HiPath	Syslog		
Enterasys I-Series	Syslog		
Enterasys Matrix E1 Switch	Syslog, SNMP		
Enterasys Matrix N Series Switch	Syslog		
Enterasys NAC	Syslog		
Enterasys NetsightASM	Syslog		
Enterasys Stackable and Standalone Switches	Syslog		
Enterasys XSR Security Routers	Syslog		
Extreme Networks ExtremeWare OS	Syslog		
F5 Networks BigIP	Syslog	BIG-IP	Syslog
Fair Warning	Syslog, File		
FireEye	Syslog		
Forescout CounterACT	Syslog		
Fortinet FortiGate Security Gateway	Syslog		
Foundry Fastiron	Syslog		
HP ProCurve	Syslog		

IBM TSIEM to IBM QRadar Transition Guide

HP Tandem	File	Tandem	File
Hewlett Packard UniX	Syslog	HP-UX	Syslog, File
IBM AIX Server	Syslog, File	IBM AIX 5.1-6.1	Syslog, File
IBM AS/400 iSeries	Syslog, File	OS/400 / iSeries Remote Collect	File, FTP, API
IBM DB2	File	IBM DB2 8.1-9.x	File
IBM IMS	Syslog, File		
IBM Informix Audit	File	IBM Informix Dynamic Server	File
IBM Lotus Domino	SNMP	Lotus Notes	File
IBM Proventia Management SiteProtector	JDBC	IBM Proventia Management SiteProtector 2.0 SP6.x	JDBC
IBM Proventia Network IPS	SNMP		
IBM RACF	File		
IBM WebSphere Application Server	Syslog, File	IBM WebSphere Application Server 6.0-7.0	File/JMX
ISC BIND	Syslog		
Imperva Securesphere	Syslog		
ltron Smart Meter	Syslog		
Juniper DX Application Acceleration Platform	Syslog		
Juniper EX-Series Ethernet Switch	Syslog		
Juniper JunOS Platform	Syslog, PCAP		
Juniper M-Series Multiservice Edge Routing	Syslog		
Juniper MX-Series Ethernet Services Router	Syslog, File		
Juniper Networks AVT	JDBC		
Juniper Networks Firewall and VPN	Syslog	Juniper NetScreen FW (forensic)	Syslog
Juniper Networks Infranet Controller	Syslog		
Juniper Networks Intrusion Detection and Prevention (IDP)	Syslog		
Juniper Networks Network and Security Manager	Syslog, Juniper NSM		
Juniper Networks Secure Access (SA) SSL VPN	Syslog	Juniper SSL VPN (forensic)	Syslog
Juniper SRX-series Services Gateway	Syslog, PCAP		
Juniper Steel Belted Radius	Syslog, File		
Juniper T-Series Core Platform	Syslog		
Liebman Random Password Manager	Syslog		
Linux DHCP Server	Syslog	Linux Auditing Framework	Syslog, File
Linux iptables Firewall	Syslog	Linux Auditing Framework	Syslog, File
Linux login messages	Syslog	Linux Auditing Framework	Syslog, File
Mac OS X	Syslog		
McAfee Application/Change Control	JDBC		
McAfee IntruShield Network IPS Appliance	Syslog	McAfee IntruShield	Syslog
McAfee ePolicy Orchestrator	JDBC, SNMP	McAfee ePO	ODBC
Metainfo MetalP	Syslog		
Microsoft DHCP Server	Syslog, File	Microsoft Windows Server Active Directory 2000-2008	File
Microsoft Exchange Server	Syslog, File	Microsoft Exchange 2000-2003	File
Microsoft IAS Server	Syslog		
Microsoft IIS	Syslog, File	Internet Information Server (IIS)	File
Microsoft ISA	Syslog		
Microsoft Operations Manager	JDBC		
Microsoft SCOM	JDBC		
Microsoft SQL Server	Syslog	Microsoft SQL Server 2000-2008	File, ODBC
Microsoft Windows Security Event Log	Syslog, File	Microsoft Windows NT-2008	File, SNMP
Motorola SymbolAP	Syslog		
Name Value Pair	Syslog	Ubiquitous / W7Log (CSV, XML)	Syslog, File
Niksun 2005 v3.5	Syslog		
Nortel Application Switch	Syslog		
Nortel Contivity VPN Switch	Syslog		
Nortel Ethernet Routing Switch 2500/4500/5500	Syslog		
Nortel Ethernet Routing Switch 8300/8600	Syslog		
Nortel Multiprotocol Router	Syslog		
Nortel Secure Network Access Switch (SNAS)	Syslog		
Nortel Secure Router	Syslog		
Nortel Switched Firewall 5100	Syslog, OPSEC/LEA		
Nortel Switched Firewall 6000	Syslog, OPSEC/LEA		
Nortel Threat Protection System (TPS) Intrusion Sensor	Syslog		
Nortel VPN Gateway	Syslog		
OpenBSD OS	Syslog		

IBM TSIEM to IBM QRadar Transition Guide

Oracle Audit Vault	JDBC	Oracle Database Audit Trail 8i 9i 10g 11g	File, ODBC
Oracle Database Listener	Syslog		
Oracle RDBMS Audit Record	Syslog, JDBC	Oracle Database Audit Trail 8i 9i 10g 11g	File, ODBC
Oracle RDBMS OS Audit Record	Syslog, File	Oracle 9i 10g 11g	File
Palo Alto PA Series	Syslog		
ProFTPD Server	Syslog		
RSA Authentication Manager	File	RSA Authentication Manager	File
Radware DefensePro	Syslog		
Redback ASE	Syslog		
Samhain HIDS	Syslog, JDBC		
Sentriqo Hedgehog	Syslog		
Sidewinder G2 Security Appliance	Syslog		
Snort Open Source IDS	Syslog		
Solaris BSM	Syslog, File	Solaris audit trail	Syslog, File
Solaris Operating System Authentication Messages	Syslog	Solaris audit trail	Syslog, File
Solaris Operating System DHCP Logs	Syslog		
Solaris Operating System Sendmail Logs	Syslog		
SonicWALL UTM/Firewall/VPN Appliance	Syslog		
Sophos PureMessage	JDBC		
Sourcefire Defense Center	SDC Estreamer	Sourcefire Network Sensor	Syslog
Squid Web Proxy	Syslog		
Starent Networks Home Agent (HA)	Syslog		
Sybase ASE	JDBC	Sybase Adaptive Server Enterprise	File
Symantec Endpoint Protection	Syslog	Symantec AntiVirus	File
Symantec Gateway Security (SGS) Appliance	Syslog		
Symantec System Center	JDBC		
Symark Power Broker	Syslog		
TippingPoint Intrusion Prevention System (IPS)	Syslog		
TippingPoint X Series Appliances	Syslog		
Top Layer Intrusion Prevention System (IPS)	Syslog, OPSEC/LEA		
Trend InterScan VirusWall	Syslog		
Trend Micro Control Manager	SNMP		
Trend Micro Office Scan	SNMP		
Tripwire Enterprise	Syslog		
Universal DSM	ANY	Generic ExtendIT	ANY
Vericept Content 360	Syslog		
Websense V Series	Syslog		
		Alcatel Switch 6600 & 7800 (forensic)	Syslog
		BIM Alert Report Writer	File
		BMC Control SA	ODBC
		BlackDiamond Router (forensic)	Syslog
		Cisco Router	Syslog, SNMP
		Guardium 7.0 - 8.0	Syslog, File
		HP Integrated Communication Facility Notification	SNMP
		HP OpenVMS	File
		HP Switch	SNMP
		HP Tru64 UNIX	FTP
		IBM DB2 Audit Management Expert 1.1	File
		IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0-8.1	JDBC
		IBM Tivoli Access Manager for Operating Systems	File
		IBM Tivoli Access Manager for e-Business	File
		IBM Tivoli Directory Server	File
		IBM Tivoli Federated Identity Manager	File
		IBM Tivoli Identity Manager 4.6 - 5.0	JDBC
		IBM Tivoli Key Lifecycle Manager 1.0	File
		IBM Tivoli Security Compliance Manager 5.1.0 - 5.1.1.1	JDBC
		IBM Tivoli Security Information and Event Manager Server	File
		IBM Tivoli Security Information and Event Manager Web Apps	File
		IBM Tivoli Security Operations Manager	File
		IBM Tivoli Security Policy Manager 7.0	File
		ISS RealSecure	SNMP, File
		ISS System Scanner	File

IBM TSIEM to IBM QRadar Transition Guide

		ISS System Scanner reports	File
		Novell (Nsure) Audit	ODBC
		Novell 4 or 5	API
		Novell Advanced Audit Service	ODBC
		OPICS	File
		Oracle Applications 11.5.9 - 12.0	File
		Oracle Fine-Grained Auditing 9i 10g 11g	ODBC
		Oracle Portal Activity	File
		Oracle Portal Logins	File
		RSA SecurID ACE Server 7 (forensic)	Syslog
		Raptor	Syslog, File, SNMP
		SAP NetWeaver Application Server ABAP 6.10-7.0	File
		SAP NetWeaver Application Server on Java 7.0 - 7.2	File
		SAP R/3	File
		ScanMail for Lotus Notes	API
		ScanMail for MS Exchange	File
		ServerProtect	File
		SiteMinder	ODBC
		Snort	Syslog
		StealthWatch (forensic)	Syslog
		Stratus VOS	File
		Sun Identity Manager	ODBC
		eTrust Access Control (SeOS)	File
		iPlanet Web Server	File
		z/OS	File
		zAlert	SNMP

Table 6-8 TSIEM to QRadar Sources Comparison