Database Activity Monitoring (DAM): Understanding And Configuring Basic Network Monitoring Using Imperva's SecureSphere

GIAC (GCIA) Gold Certification

Author: Charles Brodsky, charles@charlesbrodsky.com
Advisor: Stephen Northcutt

Accepted: 12/29/15

Abstract

As sensitive data is consolidated into larger, unified databases the protection of that data becomes more and more important. A critical element in securing these systems is monitoring user activity. There are several approaches available for auditing and monitoring these databases. In this paper, we discuss the basics of one of those methods: network based monitoring. We also look at some of the steps involved in implementing it using Imperva's SecureSphere Database Activity Monitoring (DAM) product. We are focusing on network based monitoring because it is a common starting point that many organizations use when beginning to perform Database Activity Monitoring. It also establishes a foundation that can be leveraged for additional types of monitoring as an organization's program matures.

1. Introduction

The growing trend is to consolidate sensitive data into larger databases. One of the side effects of this is that additional groups beyond the traditional DBAs need access to these databases and the information they contain. This includes, customer service, marketing, HR, etc. The result is that monitoring and evaluating user activity to detect abnormal behavior is crucial to protecting the data (Dharani, Sangeetha, 2013). For example, a user accessing 1-5 records that contain PII regularly may be a part of their normal duties, but using that same access to view 5000 records at a time may be a security breach.

There are three basic approaches to auditing database access and activity (Horwath, 2012). The first is native auditing, which uses the built in tools and features databases have to record activity. One of the benefits of using this is that there is no additional cost since it is already part of the database server. A drawback is that this can impact the performance of the database, and you would still need a way to identify abnormal activity. A second method is to use network based auditing. This involves passively monitoring, or 'sniffing', the network traffic to and from the database. Since this is a separate system there is no performance impact and it provides an additional, independent, log source. A limitation to this approach is that it can not monitor encrypted traffic unless it has the encryption keys and it can not see local activity such as a server administrator who accesses the database from a remote shell on the server itself. The third option is to use agent based auditing. With this method an agent is installed on the database server itself that monitors all database activity locally so it will see all types of connections. These agents are usually very closely tied to the server OS Kernel, and can potentially impact system performance. Another concern with agents is that they require multiple teams to be 'on board' with their use, and different groups may have different objectives, and concerns. The Database administrators, Server Administrators, and Security/Auditing team may have conflicting views on their use, benefits, and risks.

When beginning Database Activity Monitoring (DAM) many organizations start with network based monitoring due to it being a good balance between compliance, security, performance, and cost (Horwath, 2012). We begin by discussing some of the basic requirements many organizations have for Database Activity Monitoring, and what drives those requirements. We then look at the necessary architecture to implement network based monitoring. Finally, we discuss how to configure Imperva's SecureSphere product to monitor access to Social Security numbers.

2. Fundamentals Of Network Based Database Activity Monitoring

When using network based monitoring for inspecting your database activity you are examining a copy of the traffic sent to and from the database as it flows across the wire. At its core, this involves the following components: the database, the client system, a monitoring tool, and a device to duplicate the database traffic. The roles of the database, client/application, and monitoring tool are fairly straightforward to understand, but there are some variations on the tools and techniques for duplicating the traffic that need to be discussed.

There are two primary options for duplicating traffic, a 'span port' on a switch, and a network 'tap.' The first option is to use a 'span port' on the database network switch. Most Enterprise class switches support one or more span ports that allow you to duplicate traffic and send it out the span port for monitoring or troubleshooting. You typically have the option of sending all the traffic sent to or from a single port to another port. This will work if you only have a single server you want to monitor, but if you are considering implementing a Database Activity Monitoring solution you probably have multiple databases, or even multiple clusters of databases. For these types of situations you may need to span an entire VLAN/subnet for monitoring. While many switch vendors can support this you may overload the span port capacity depending on network usage.

When you have multiple servers in scope, but not necessarily everything in the VLAN/subnet is in scope, you may need to carve up your traffic to be more efficient with what you have the monitoring tool inspect. Some switches may let you do this at a basic level but there are other options that can provide a significant amount of flexibility. Gigamon has hardware solutions designed to do this. Their products can combine multiple sources of traffic and feed just the traffic you want to your monitoring tools based on IP, ports, etc. (Gigamon, ND). This can help you manage your overall costs because you can size the monitoring devices based on the traffic you want inspected and not just the overall volume of raw network traffic.

Another option if you have a very small number of servers to monitor, or limited database traffic, is to use a network TAP. A network TAP is a piece of hardware that sits inline to the database on the switch port and duplicates the traffic seen by that port. One of the advantages with this approach over the span session approach is that if there is a high network load, span traffic is processed at a lower priority so you may miss some packets (Cisco, ND). Since TAPs aren't involved in processing traffic they don't have this problem. They also let you duplicate frame/packet errors and give you full visibility into everything on the port (Viavisolutions, ND). If you have a limited number of database servers, and stringent monitoring requirements, this could be something to consider for your duplication needs.

As you may have noticed, we have been talking about monitoring close to the database server(s). Since we are trying to inspect the database traffic it makes the most sense to put our monitoring feed as close to the database as possible.

2.1 Benefits And Limitations

We've already discussed one of the primary benefits of network based monitoring during the introduction: no performance or stability risks. Because we are passively monitoring a copy of the traffic we do not increase the load on the database server. This also means that this approach is compatible with any database platform as long as the monitoring tool supports it. By not requiring any additional software on the database server, or clients, we do not introduce any additional stability risk from implementing monitoring.

Some important limitations to this approach that need to be understood include challenges with inspecting encrypted traffic. Because we only see the communication on the wire, any encryption in use will not let the monitoring tool properly inspect the activity. Some tools allow you to import digital certificates, or the encryption key (Imperva, 2015). If you use encryption with your database traffic this is something critical you should investigate before deploying any monitoring system.

Another benefit to starting with network based monitoring is that it can establish a foundation for more robust additions over time. When introducing new technologies there may be concerns within different groups regarding potential operational impacts, or the additional value they may provide. This is a low risk way to introduce this type of monitoring, and allow for the organization to become comfortable with it before expanding to other options like host agents. Since many monitoring tools allow you to use more than one monitoring technique you can typically mix and match your monitoring approach based on your environment and needs.

3. What To Monitor

Determining what you are interested in, where it is stored, and how you will monitor it, is critical. Without a clear scope and plan you won't add value by implementing a system like this.

Oftentimes, when asking someone what they want to monitor and track the initial response is 'everything'. The fear of missing something that is later needed seems to be a common first reaction. Unfortunately, the resources needed to attempt to 'monitor everything' are significant. Even if you did try to capture every read, update, etc. you would still need to be able to store all that information, and have systems capable of processing and analyzing an overwhelmingly large amount of data.

It is important to remember that this probably isn't your only source of auditing and logging. Often, the applications themselves provide logging as well. If that data is stored in a reliable system, and protected location, it may not be necessary to duplicate it in a system like this.

Understanding the risks to your data, the environment you operate in, your compliance and regulatory requirements, and the threats you want to defend against is essential to the success of this program, but beyond the scope of this paper. For our discussions, we will assume you want to monitor Social Security numbers stored in one of your databases. The monitoring configuration we will cover can apply to any type of data stored in a relational database including credit card numbers, bank account numbers, etc.

4. How to configure Imperva's SecureSphere

We will assume you have already worked with the vendor, or reseller, to properly install the system and you are ready to begin configuring it. We will also assume that you know what information you want to protect, and where it is stored (Database, Table, Column.) The configuration steps, and recommendations, come from the vendor's user guide (Imperva, 2015).

4.1 Identifying Database servers to be monitored

Like many other systems, Imperva uses a hierarchical approach when configuring SecureSphere database monitoring. At the top of the hierarchy is the "site". "Sites are the primary container in which all other network objects are located." (Imperva, 2015) Depending on your organization, and how you want to organize your monitoring, sites can be grouped at geographic, physical, environmental, or other divisional levels. For example, a large organization may want to group their sites by country, or city. Another organization may prefer to group them by department such as finance, accounting, or human resources. There is no 'required' approach so you have the flexibility to define them any way that makes sense for your situation.

The next level is "server groups." As you would expect, these are the servers that are being monitored. At this level you can break them down by application, database platform (i.e. Oracle, MS SQL, etc.) database cluster, etc.

The final level in this list is "services." This is where you define the database platform you are monitoring, as well as identify any non-standard ports it may be using. For example, you may have very powerful server hardware running multiple instances of your database on different ports. This will allow you to monitor both instances.

4.1.1 Configuring Sites

The user guide provides details on the setup and options starting on page 73 (Imperva, 2015). The first step in configuring a new site is to go to the "Setup" tab and select "Sites." This window has two panes. The one on the left is a tree view of the sites, server groups, and services we will be setting up. The right pane has the configuration options of whatever is selected in the left pane.

Creating the site is as simple as clicking the green plus at the top of the left pane and entering the name of the site you want to create.

4.1.2 Configuring Server Groups

Once your site has been created you select it, and click the green plus at the top of the left pane again. You will be prompted to enter a server group name then click the 'create' button. When using SecureSphere it is important to keep in mind that buttons and settings apply to what is selected in other parts of the interface. This is why clicking the green plus with nothing else selected the first time created a new site, but when the site was selected the green plus then created our server group. It is also very important to remember that this is a browser-based interface. Like other browser-based interfaces you need to click the 'save' button on the right edge of the screen near the top of the window to save your changes.

The next step is to add the IP addresses of the servers we want to monitor in this group. In the left/main pane of the window there is now a group of tabs and options for the new server group you created. To add server IP addresses you now click the green plus in the "Protected IP Addresses" section of the window. You have the ability to add comments for each server. You may find it useful to have the host name, or other meaningful information here, so you can associate it with the server IP in the future.

You will follow the same steps to create any other necessary server groups. When creating your server groups please keep in mind the following information from Imperva's "server group best practices" on p75 (Imperva, 2015). You should not have more than 30 server groups per monitoring device (also called a 'gateway'), you cannot have the same IP address in more than one server group on your gateway, and you should try to have the servers that support a specific application within a single server group.

4.1.3 Configuring Services

After saving your server groups the next step is to configure the services. First you select the server group you want to add the service to then click the green plus again. You will need to provide a name for the service and select the service type. Service types are the database management systems like Oracle, Microsoft SQL, IBM's DB2, etc. After you click the 'create' button you will see a warning popup that Archive settings are not configured. Archive settings can vary significantly based on your overall implementation, and configuring them is beyond the scope of this paper. In this case we will click the 'ignore button' to continue.

SecureSphere will configure the default ports this database runs on, and show you them in the definitions section of the main window. If you are using any non-standard ports in addition to, or in place of, the standard ones you can add them to the ports field, and click the save button on the right side of the window.

4.2 Identifying Sensitive Tables And Columns

We now want to create a group to identify tables with the sensitive data we are interested in monitoring. We can mark an entire table, or individual columns in a table, as sensitive. To create a 'table group' for monitoring we select 'Setup' from the main tabs and choose "Global Objects" from the drop down menu. We can also click "Global Objects" from the blue menu bar if we are still in the site configuration view from the previous step. The global objects window functions much like the previous windows where the contents in the right pane are settings for what is selected in the left pane, but there is an additional drop down above the window labeled "Scope Selection." This is where you identify the type of global objects you want to work with.

Since we need to create table groups we will select "Database Table Groups" from the scope selection drop down. To create a new table group we click the green plus. In the window that appears we have to provide a name, as usual, but we have additional choices to make. There is a drop down menu labeled "Choose Data Type" that has items like account number, National ID (this is how Imperva labels U.S. Social Security numbers), payment card, etc. Since we are interested in monitoring Social Security numbers for this paper we will select "National ID". We also need to identify the type of database server it will be on, so we will select "Oracle" for this exercise and click the "Create" button. In the main window (right pane) we click the green plus in the "Table Name" column and add in the table that contains the information we want to monitor. We repeat these steps for each of the tables. This will treat all columns in the table as sensitive. If we only want specific columns in a table we can expand the table name after we have saved it in our configuration then add the specific columns with the green plus. Be sure that the check box labeled "Sensitive" is checked at the top of the table group.

4.3 Configuring Monitoring Policies

The next step is to configure an audit policy to watch for activity involving the sensitive tables we identified. On the top row we click the "Policies" tab and select "Audit." To create the new audit policy, we click the green plus again, and choose "DB Audit Service." Give it a name and click the "Create" button.

We are now ready to configure the policy. First we select it in the center window and configuration options will appear in the right pane. The first of those tabs is "Match Criteria." This is where we identify what we want this policy to look for. There is a general list of things it can look for with the plus symbols that can be expanded to show more details in what can be selected. If there is a green arrow pointing up it means this can be added to the list of items that it needs to match for the policy to monitor it. The items at the top with blue arrows pointing down are the things currently being matched.

Since we want to match on the table group we created we will need to scroll down and find the "Table Groups" category in the list and click on the green arrow to move it to the "Match Criteria" section. Once there we will click the plus to expand it. The list of table groups is on the left side of that section with an arrow pointing to the left and another pointing to the right. Scroll until you find your sensitive table group and click the arrow pointing to the right to add it to the "Selected" window. This will configure SecureSphere to match on any of the tables and columns in that table group.

The second tab in that section, "Apply To", is where we associate the policy, sites, and server group(s) it applies to. Clicking the empty box to the left of the name will check the policy and let SecureSphere know it should look for this type of traffic in these server groups.

Although we won't get into the archiving and purging settings, it should be noted that you might want to change the default purging cycle for events and records on this tab. For example, if the "Purge records older than" setting is '1 week' anything older than that will automatically be purged from the database daily. This may not meet your retention needs. Based on the volume of events, and your retention requirements, you may require additional storage, or another mechanism to properly handle this.

After clicking the save button you can view the events by going to the "Audit" tab on the main window and selecting "DB Audit Data." This window has a similar layout to the other windows in that the right pane will display information about what is selected on the left, but there is another section on the left at the top to select the policy and time range that you want to view.

This view will allow you to see summary information, user activity, query activity, etc. You'll probably be most interested in selecting the "Data" section under "Views." This is where you can see the observed activity, and identify what you are interested in.

The first thing to be aware of is that it summarizes the queries in the "Parsed Query" field. This is an aggregation of the tables and operations in the query. It removes the unique specific values in the query (i.e. selecting ID 123 from the account table in one query, and selecting ID 345 from the account table in another query.) By doing this, it allows you to see the communication between clients and servers more easily without filling the window up with the same type of queries over and over. If you do want to see the specifics for a particular query, click the "Parsed Query" link. This will open a window to display the actual queries observed.

4.4 How To Filter Out Service/Application Account Traffic

When you begin looking at the activity in the "Audit" → "DB Audit Data" view from the previous section you may notice traffic you don't want to include. For example, you may already be monitoring some of the application-based activity within the application itself. To exclude the activity you don't want to monitor on, you need to go back to the policy itself (click "Policies" and choose "Audit".)

From here you may want to exclude certain source IP addresses, user names, applications, etc. The process is the same, as when we added the original match criteria except when you select these items you will choose to "exclude" them in the "operation" section of the window. Remember, anything you exclude here will not be captured. Depending on your needs you may want to keep it in the capture filter but exclude it from the reports. The next section will cover how to do this.

4.5 Configuring Activity Reports

There are several ways to create reports. Of course, you have the option of starting from a blank report and adding in what you want, but there is an easier way.

At the end of the "Configuring Monitoring Policies" section we looked at the traffic that our policy collected. This was on the "Audit" tab in the "DB Audit Data" section. You have the ability to add and move columns by clicking the "Select Columns" button in the main window. You also have the ability to filter out unwanted traffic from this view. For example, if you don't want to have a service account's traffic in the report, you can click that account name and choose "Exclude this Value."

After you have made the adjustments you want, there is a button at the top of the main section that looks like a floppy disk that says "Save as Report" when you hover your mouse over it. It will prompt you to name your report and click save. Once it saves there will be a popup window with a link labeled "Go to Report Definition". Clicking this will take you directly to the report you just created or you can manually go there at a later time by choosing "Reports" on the main tab and selecting "Manage Reports."

There are several settings you should be aware of regarding reporting. As with the other parts of the interface, items selected on the left side will have their configuration options appear on the right side. By selecting your report in the center window, the right window will display several tabs to adjust the report settings.

On the first tab labeled "General" you'll have the option to specify the report format as a CSV or a PDF. You'll also be able to specify if you want the report to have a portrait or landscape orientation. The second tab is labeled "Data Scope." This is very similar to the layout and options for the policy configuration we used when defining what activity we want to match against. It also lets us specify how many days of data we want in the report each time it runs. If we set it for 7 days each time the report runs it will display the last 7 days of data. This is probably a good choice for weekly reports. The last of the tabs we will discuss is the "Scheduling" tab (you may need to scroll through the tabs section to see it.) This is where we can configure the report to run at preset intervals. You have the basic options of daily, weekly, and monthly for whatever time you choose. You also have the ability to run them manually on demand, but the scheduled reports will probably be more valuable for most use cases.

To view your reports you can click the "Reports" tab and choose "View Results" or just click "View Results" on the blue menu bar since we are still in the reports section.

Depending on how much monitoring you have running, and how much database traffic matches it, you may have a significant amount of events to report on. If you find that reports are taking too long to run, or the reports themselves are too large, you may need to run them more frequently. An example of this would be taking a weekly report, and running it daily with just the events from a single day. If you still need to process this on a weekly basis, you could have the reports run as CSV files and consolidate the output in Excel, or review it on the main console instead.

5. Conclusion

Monitoring database activity is a critical component of database security, especially as more sensitive information is consolidated into larger databases. Depending on your industry, and the data in your database, you may also have legal, regulatory, and compliance requirements around access and activity monitoring.

The most important first step is to assess your data, and environment, to determine your overall risks, threats, and existing controls. This will help you identify where you need to focus your efforts, and what types of controls you will need to achieve your goals. Don't think of Database Activity Monitoring as a separate initiative, but look at it as another component to your overall security program.

Network based user activity monitoring is a good starting point for this type of monitoring because it allows you to start inspecting database activity without the risk of impacting the performance and stability of your systems. It also provides a foundation to implement additional monitoring as your organization becomes more comfortable with the tools, or your requirements change.

As with any tool it is important to have enough resources to effectively manage, and monitor, the output of this system in order to get value from it.

Additional areas of research may include: implementing agent based monitoring, integrating this tool and its alerts with a SIEM tool, or how do assess database risks to determine when a Database Activity Monitoring solution should be used.

References

Cisco (ND). Cisco Nexus 9300 Platform Buffer and Queuing Architecture. Retrieved from http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/white-paper-c11-732452.html

Dharani, M., & Sangeetha, T. (2013). Improving Policy Based Intrusion Response Component of a Relational Database by Evaluation of User. *IJCTT - International Journal of Computer Trends and Technology*. 4(5), 1115-1117. http://ijcttjournal.org/archives/ijctt-v4i5p32

Gigamon (ND). Adaptive Packet Filtering. Retrieved from https://www.gigamon.com/products/technology/adaptive-packet-filtering

Greer, C (2014). The Network TAP Vs. The SPAN Port: Putting Them To The Test. Retrieved from http://www.garlandtechnology.com/2014/06/16/the-test-span-vs-tap

Gupta, A., & Dubey, S. (2015). Analytical Approach for Security of Sensitive Business Database. *IJDTA - International Journal of Database Theory and Application*, 8(3), 49-56. http://www.sersc.org/journals/IJDTA/vol8_no3/5.pdf

Huth, C., Chadwick, D., Claycomb, W., & You, I. (2013). Guest editorial: A brief overview of data leakage and insider threats. *Information Systems Frontiers*, 15(1), 1-4. Retrieved from http://link.springer.com/article/10.1007/s10796-013-9419-8/fulltext.html

Horwath, J. (2012). Setting Up a Database Security Logging and Monitoring Program. Retrieved from the SANS Institute: InfoSec Reading Room. Web Site: https://www.sans.org/reading-room/whitepapers/application/setting-database-security-logging-monitoring-program-34222

Imperva (2015, December). SecureSphere v11.0 Database Security User Guide. Retrieved from Imperva Customer Portal www.imperva.com

Charles Brodsky, Charles@CharlesBrodsky.com

Matthew, O., & Dudley, C. (2015). Critical Assessment of Auditing Contributions to Effective and Efficient Security in Database Systems. *Computer Science & Information Technology (CS & IT), 8*(5). http://airccj.org/CSCP/vol5/csit53901.pdf

Mogull, R. (2013). Understanding and selecting a database activity monitoring solution. *Securosis.* Retrieved from https://securosis.com/assets/library/reports/DAM-Whitepaper-final.pdf

Roratto, R., & Dias, E. (2014). Security information in production and operations: A study on audit trails in database systems. *JISTEM Journal of Information Systems and Technology Management, 11*(3), 717-734. doi: https://dx.doi.org/10.4301/S1807-17752014000300010

Suganthy, M., & Prashanth, R. (2013). Inside Threat Analyzing and Responding System for Relational Database. *International Journal of Futuristic Science Engineering and Technology*, 1(3), 209-213. Retrieved from http://www.ijfset.org/vol1issue3/paper38.pdf

Viavisolutions (ND). Choosing between a SPAN, Aggregator, or full-duplex TAP. Retrieved from https://observer.viavisolutions.com/support/html_doc/current/index.html#page/ntaps_shared/span_agg_duplex.html