Welcome

Welcome to the September issue of the Bsafe Technical Newsletter.

If there is ever a time to talk about PCI DSS, it would be this month. As many are aware, a key deadline for much of the US market is September 30th and for Asia Pacific it is December 31st.

This month we will explore a few key areas of PCI Security Policy Compliance and how we can use Bsafe Enterprise Security to help customers and prospects comply!

As always, we are open to suggestions that will enhance the Bsafe Enterprise Security Suite. Please send suggestions to don@bsafesolutions.com
NEWS

Reporting – kicking it up a notch!

We have just received the exciting news from our CTO, Mr. Shimon Bouganim, that an update is pending that will enhance Bsafe/ES reporting extensively. The much anticipated reporting tool will include many added functionalities. Customers will be able to choose fields to be included in reports, sort by any fields that were selected and most importantly, there will be Boolean logic built in that will allow you to choose a value for a field to report against.

i.e. Field1 = "XYZ".

PCI Security Policy Compliance

This month, Steve Siklosi, one of our Senior Account Managers, spoke at a local user group (NESTU) on PCI and had some very good response. There were a group of 25 attendees from local companies present and all were really impressed with what Steve had to say regarding the PCI Security Policy Compliance. Way to go Steve!

Also this month, we had a very successful PCI Security Policy Compliance implementation at a customer’s site. Bill Campbell, from Midland Information Systems and I spent three jammed packed days at a client site and implemented Bsafe/ES to help the client comply with PCI. The project is wrapping up nicely.
What is the PCI Data Security Standard?

The PCI Standard grew out of the programs initiated by Visa and MasterCard. It was developed to create a common industry standard for protecting cardholder account information across all card brands, making compliance simpler and more uniform. The standard encompasses virtually all entities with access to cardholder information. This includes merchants, members, and various service providers. The standard is currently endorsed by Visa, MasterCard, Discover Card, American Express, Diners Club, and JCB.

The focus of the PCI Data Security Standard is to ensure that confidential cardholder information is protected from unauthorized access or use wherever it resides. To accomplish this, the Standard defines twelve major requirements for data security, each having one or more sub-requirements. Click here to see the PCI DSS Security Audit Procedures. To see how Bsafe can help, click here.

Covering the requirements of PCI Security Policy Compliance is beyond the scope of this Newsletter; however I do want to use this opportunity to cover a few key modules of Bsafe/ES that will help satisfy PCI Security Policy Compliance requirements.
Module Focus –
System Audit, Central Audit & Alert Center

As we know, the Bsafe Enterprise Security Suite is cleverly designed; all modules, in one way or another work tightly together, but the System Audit, Central Audit & Alert Center are one close-knit family. If properly implemented, these three modules will help satisfy certain areas of the PCI Security Policy Compliance requirements.

In this month’s edition of Module Focus, we’ll explore how to setup auditing with the System Audit module, how to setup alerts against audited information with the Alert Center and then we’ll find out how we can log alerts in the Central Audit module for later use.

Before we actually dive into how to set it up in the Bsafe Client, let’s get a glimpse of how Bsafe has made life easy for the System i community. Let us quickly ascertain what life is like for System i shops without a solution like Bsafe/ES.
As we know, the IBM QAUDJR -- also known as the System Journal -- has to be running in order for system auditing to take place. In fact, Bsafe/ES’s System Audit module displays information from the System Journal.

There are numerous ways of starting the System Journal. One way is to run the CHGSECAUD command from a System i command line and F4 to prompt it. If the system value QAUDCTL, has a value of *NONE, the System Journal is not turned on. If this is the case and you are the System Administrator, you can turn it on by keying the three recommended values like the image below.
Once the System Journal is turned on, the system will start auditing (Journaling). Depending on the size of the shop, receivers can grow very quickly. In fact, it can grow so fast that some shops have to backup receivers and delete them the same day to save disk space (DASD).

To display the captured information, you would have to run the DSPJRN JRN(QAUDJRN) command which will display the window below:
We can enter a 5 to display the detail, but what does all this mean? What an unfriendly way of displaying what we want to see! Where is the Date, Time and Job information? You can hit F10 to see the Date, Time and Job information, but that just makes it that much more cumbersome.

Without a solution like Bsafe/ES, the System i community had no easy way of analyzing their System Audit Journals so they came up with some very creative ways of analyzing this information. Some will dump this massive load of information into a file and would run QRY, SQL statements or write RPG programs to sift through and extract the information they need. Those of you that are curious and want to do it the old fashion way, please let me know, but it’s going to cost you an arm and a leg.
Let’s take a look at how easy it is to setup it all up with Bsafe/ES!

First of all, to start Journaling, we would simply click on the System Policy Icon within the Bsafe/ES System Audit.

To start it all, we would click on “Activate Audit Control”. Then choose what we want to audit; it’s as simple as a few clicks of the mouse. Items with a check mark in the System’s tab will determine what the system will audit.
Now let’s take a look at what the System Journal looks like within Bsafe/ES.

As we can see, it is much more user friendly than the native view. There are numerous built-in functionalities for ease of analysis.
Simply double click on any transactions to see the details. In this example, the system value: QUSRLIBL (User Library) was changed. As we can see, the Old and New values are displayed to show exactly what the changes are.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of entry</td>
<td>A</td>
</tr>
<tr>
<td>System value</td>
<td>QUSRLIBL</td>
</tr>
<tr>
<td>New value</td>
<td>PRODDATA PAYROLL DNGUYEN QGPL QTEMP</td>
</tr>
<tr>
<td>Old value</td>
<td>PAYROLL DNGUYEN QGPL QTEMP</td>
</tr>
</tbody>
</table>

The System Value: QUSRLIBL was changed.
The System Audit module comes with dozens of valuable reports that can be run "as is" or modified.
Now that we have our system auditing set up and have a pretty good understanding of the System Audit module, let’s take brief look at the Bsafe/ES Alert Center!

As they say, why reinvent the wheel. The following is pulled directly from the Bsafe online help. When speaking to prospects, don’t forget to mention the Bsafe/ES extensive online help.

**Introduction**

The Bsafe/Enterprise Security Alert Center is an intrusion detection system (IDS) which provides a mechanism to receive alerts following the occurrence of a significant security event. This may be an access attempt or a system event. Each alert consists of alert criteria and a resulting set of actions. The system consists of three basic components:

- The GUI-based **Alert Center** to define the alerts and view current definitions.
- The **Alert Collector** to identify when events occur and to execute resulting native actions.
- The **Alert Monitor** to execute resulting Windows actions.

**Alert Center**

A part of the Bsafe/Enterprise Security GUI interface. Here you can define event detection conditions and what actions will be taken when such a condition is met. See **IDS Alert Definition**.

**Alert Collector**

Residing on the iSeries, this module monitors two groups of recorded events:
1. Network events recorded in the **Application Audit**.
2. System events recorded in the **System Audit**.

These two logs are scanned continuously for the occurrence of an event defined in the Alert Center. When it identifies the occurrence of an event requiring notification, it executes pre-defined native actions and notifies the **Alert Monitor** on a designated IP address to execute pre-defined Windows actions.

**Alert Monitor**

Resides on one or more PC’s on the network and will receive alert messages via a TCP/IP connection from the **Alert Collector**. Each instance of the alert monitor running will be identified by its IP address or DNS name so that each alert can be directed to the alert monitor of your choice.

For alerts to work on your system, you must first activate the alert collector on your iSeries - see **IDS Activation and Configuration**.
Theories are good, but let’s put theory into practice!

In order to receive alerts, we need to start the Alert collector jobs. These jobs are started from the green screen with user BSAFE. There are two different alert jobs; Application IDS Alerts and System Audit IDS Alerts.

Application IDS Alerts will monitor and alert on FTP (Server & Client), RMTCMD, RMTSQL, DDM...
System Audit Alerts will monitor and alert on anything that is captured by the System Journal (Bsafe/ES System Audit). As we recall, what the System Audit capture depends on what was defined in the System Audit Policy. Refer to table 1 for what is recommended.

Table 1:

<table>
<thead>
<tr>
<th>System Audit Event</th>
<th>Bsafe recommends auditing the Check-marked Audit Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTFAIL</td>
<td>*PGMFAIL - Program failures</td>
</tr>
<tr>
<td>*CREATE</td>
<td>*PGMFAIL - Program failures</td>
</tr>
<tr>
<td>*DELETE</td>
<td>*PRTDATA - Printing functions</td>
</tr>
<tr>
<td>JOBDATA</td>
<td>*SAVRST - Save and restore operations</td>
</tr>
<tr>
<td>NETCMN</td>
<td>*SECURITY - Security tasks</td>
</tr>
<tr>
<td>OBJMGT</td>
<td>*SERVICE - Service tasks</td>
</tr>
<tr>
<td>OFCSRVR</td>
<td>*SPLFDTA - Operations on spooled files</td>
</tr>
<tr>
<td>OPTICAL</td>
<td>*SYSMGT - System management tasks</td>
</tr>
</tbody>
</table>

Bsafe recommends auditing the Check-marked Audit Actions
To be sure that both Application IDS and System Audit IDS jobs are running, run the “WRKSBSJOB QSYSWRK” command on the green screen and look for the following jobs in subsystem QSYSWRK: BSFICOL and BSFSCOL.

A tip for support; if one of your clients called and complained that their alerts are not working, chances are, they have not started the collector jobs!
To setup alerts, we would choose the Alert Center module. In this example, we will setup a System Audit IDS Alert.
Let’s define an alert definition for System Value changes. We define an alert to alert us when the System Value; QUSRLIBL (User part of the library list) changes.

We’ll first setup our Alert Condition. Notice, this is a *SECURITY task.
Then we’ll setup the Action to take place when the Alert Condition is violated. The PCI Security Policy Compliance requires that we alert the appropriate person and keep track of all Alerts, so we’ll choose the options to do so.

![Diagram of Bsafe Change interface]

- **This will log a transaction into the Bsafe Central Audit for later use.**
- **Notifies the appropriate person(s).**
- **Sends a message to a Message Queue.**
The option to send a message to a Message Queue seems very simple, but it is very powerful; both in terms of functionality and selling Bsafe/ES.

From a functionality standpoint, it adds flexibility so a customer can have alerts sent directly to a phone or a pager. We do not have this functionality built into the Bsafe/ES suite, but the flexibility of Bsafe allows customers to interface with their third party applications to carry out certain tasks. Many customers we talk to use envision, CCSS... to monitor Message Queues and send notifications to a phone or a pager. Mentioning this functionality will impress and sell!
Let’s make a change to trigger the alert. We will make a change to the system value -- QUSRLIBL -- by adding library BARNEY to the list.
The Central Audit module is populated with the alert for later use, i.e. when requested by a PCI auditor.
The appropriate message is sent to a message queue; QSYSOPR. i.e. to interface with enVision or CCSS to send phone or pager notifications.

There you have it; we have just used three of the 18 Bsafe/ES modules to satisfy one of the key requirements of the PCI Security Policy Compliance.
The Funnies – The Office

Modern day office jargon:

- **Assmosis** - The process by which some people seem to absorb success and advancement by kissing up to the boss.
- **Blamestorming** - Sitting around in a group discussing why a deadline was missed or a project failed and who was responsible.
- **Salmon day** - The experience of spending an entire day swimming upstream only to get screwed and die in the end.
- **CLM - Career Limiting Move** - Used among microserfs to describe ill-advised activity. Trashing your boss while he or she is within earshot is a serious CLM. (Also known as CLB - Career Limiting Behavior)
- **Dilberted** - To be exploited and oppressed by your boss. Derived from the experiences of Dilbert, the geek-in-hell comic strip character. "I've been dilberted again. The old man revised the specs for the fourth time this week."
- **Flight Risk** - Used to describe employees who are suspected of planning to leave the company or department soon.
- **404 - Someone who's clueless.** From the World WideWeb error message "404 Not Found," meaning that the requested document could not be located. "Don't bother asking him . . . he's 404, man."
- **Percussive Maintenance** - The fine art of whacking the crap out of an electronic device to get it to work again.
- **Prairie Dogging** - When someone yells or drops something loudly in a "cube farm" (an office full of cubicles) and everyone's heads pop up over the walls to see what's going on.