# Table of Contents

PREFACE .......................................................................................................................... 4
OVERVIEW ........................................................................................................................... 5
CUSTOMER ENABLEMENT ASSETS .................................................................................. 6
  MSS BEST PRACTICES .................................................................................................. 6
  MSS eLEARNING COURSES ......................................................................................... 7
  MSS EDUCATION PAGE ............................................................................................... 8
  MSS KNOWLEDGEBase ............................................................................................... 8
  PORTAL MEDIA LIBRARY .............................................................................................. 10
  SECURITY SERVICES RESOURCES .......................................................................... 11
LOGIN PAGE ....................................................................................................................... 12
HOME PAGE ....................................................................................................................... 13
CUSTOMIZING YOUR PORTAL ............................................................................................. 15
  CHECK NOTIFICATIONS .............................................................................................. 18
  CURRENT THREAT ASSESSMENT .............................................................................. 19
  ACTIVE TICKETS & XPS ALERTS .................................................................................. 21
  EVENT TRENDS – QUICK GLIMPSE ......................................................................... 23
SUSPICIOUS HOSTS DASHBOARD ....................................................................................... 26
  IP INTELLIGENCE REPORTING FEATURE .................................................................. 28
DEVICE MANAGER ............................................................................................................. 29
  INTERFACE ENHANCEMENTS ...................................................................................... 30
  DEVICE DETAILS ......................................................................................................... 31
  DEVICE GROUPS ........................................................................................................... 32
  ULA SOFTWARE ............................................................................................................ 34
ASSET CENTER .................................................................................................................... 35
  Essential Features ......................................................................................................... 35
  Getting Started .............................................................................................................. 35
  Adding or Editing an Asset ......................................................................................... 36
  Exporting Assets ............................................................................................................ 36
VULNERABILITY MANAGER ............................................................................................... 37
TICKETS AND INCIDENTS .................................................................................................. 39
  TICKET MANAGER – SECURITY & SERVICE RELATED TICKETS ......................... 39
  TICKET MANAGER – TICKET DETAILS ................................................................... 42
  TICKET MANAGER REPORTS – POLICY CHANGE REQUEST ................................. 43
  SUBMIT A POLICY CHANGE REQUEST .................................................................. 44
  SUBMIT A GENERAL SERVICE REQUEST ............................................................... 47
  CREATE AN INTERNAL TICKET ................................................................................ 48
  CREATE AN INTERNAL SECURITY INCIDENT ......................................................... 49
REPORTS ............................................................................................................................... 50
  IDS/IPS SENSORS REPORTS ..................................................................................... 52
  ATTACK METRICS ...................................................................................................... 53
  EXPLANATION OF ATTACK TYPES ....................................................................... 54
SECURITY LOGS AND EVENTS ..............................................................57
  LOGS DROP DOWN MENU ............................................................57
  LOG QUERY ..................................................................................57
  LOG QUERY – ADVANCED OPTIONS ..............................................58
  LOG QUERY – RESULTS .................................................................59
  LOG SEARCH ...............................................................................60
  ACTIVE ANALYZER .......................................................................61
  ACTIVE ANALYZER – CONTEXT BASED MENUS ..............................61
  ACTIVE ANALYZER – QUERY CRITERIA ..........................................62

CREATING VIRTUAL SOC PORTAL USERS ..........................................64

SOC COMMUNICATIONS ...................................................................66
  SERVICE ESCALATION .................................................................66
  SOC ESCALATION .........................................................................67
  CHAT FEATURE: ...........................................................................67
  MEDIA LIBRARY ............................................................................68

LOG OUT .........................................................................................69

REFERENCE ....................................................................................70
  SOC CONTACTS ............................................................................70
Preface

This document is designed to show you how to make the most out of the IBM Security Services Managed Security Services (“MSS”) customer Portal or sometimes referred to as the Virtual Security Operations Center. The Portal home page is both your snapshot of the most critical security information potentially impacting your network and a jumping point to all of the resources and rich feature sets available to you.

In recognizing the time constraints you face and the security challenges you must overcome, this guide has been organized to provide a strategy of how to efficiently access information when you're only able to use the portal for brief amounts of time each day.
Overview

This guide has been organized to provide a strategy for how to best use the portal and its many features for brief amounts of time each day. The below checklist items facilitate this strategy and will quickly highlight the key feature sets in an easy to follow step-by-step process.

Feature sets vary based on the MSS services you have subscribed to:

Ordered checklist of things to do when making a quick review:

☐ Log In
☐ Check Notifications
☐ Check Alertcon
☐ Check Tickets
☐ Check XPS Alerts*
☐ Event Trend – Quick Glimpse
☐ Check Suspicious Host Dashboard *
☐ Log Out

Selected actions when needed:

☐ Check Security Event Manager*
☐ Check Vulnerability Status*
☐ Device Manager
☐ Check Ticket Manager
☐ Submit Policy Change Request
☐ Submit Service Request
☐ Create an Internal General Ticket
☐ Create an Internal Security Incident
☐ Monitor Live IDPS Events via Active Analyzer *
☐ View and Query Logs
☐ Run a Report
☐ Cursory Log Review
☐ Create VSOC Users
☐ Check Downloads
☐ Service Escalation
☐ SOC Contacts

*Appropriate Service/Service level subscription required
Customer Enablement Assets

IBM Security Services provides numerous education and enablement resources to assist you and support your team’s day-to-day security practices. Most MSS resources are available from the Portal’s Support menu, including Best Practices, eLearning courses, Demonstration and Best Practices videos, core documentation, KnowledgeBase articles, Media Library repository, and Security Services Resources.

MSS Best Practices

IBM Managed Security Services (MSS) Best Practices use an operational framework to articulate recommended activities around MSS processes and procedures that can maximize the value of your subscribed services.

<table>
<thead>
<tr>
<th>Service Initiation</th>
<th>Ongoing Operations</th>
<th>Problem Resolution</th>
<th>Client Security Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>XFTAS Configuration</td>
<td>Device Tuning</td>
<td>SOC Escalation</td>
<td>MSS Interaction Model</td>
</tr>
<tr>
<td>No Log Received</td>
<td>Device Updates</td>
<td>Incident Management</td>
<td>Incident Response</td>
</tr>
<tr>
<td>Baseline Policy</td>
<td>Vulnerability Management</td>
<td>Root Cause Analysis</td>
<td>Management Reporting</td>
</tr>
<tr>
<td>Core Reporting</td>
<td>Unmanaged Assets</td>
<td>Roles &amp; Responsibilities</td>
<td></td>
</tr>
<tr>
<td>Device Outages</td>
<td>Policy Change Request</td>
<td>Security Incidents</td>
<td>Support Roles</td>
</tr>
</tbody>
</table>

MSS Best Practices Implementation Checklist
MSS eLearning Courses

IBM Managed Security Services eLearning allows you to learn at your own pace, using our engaging and interactive online content. The following eLearning job-focused courses, which include hands-on simulations, are available in the virtual SOC Portal:

- MSS Managed SIEM Analysis and Reporting
- MSS Security Intelligence and Analysis
- MSS Security Incident Response
- MSS Security Metrics and Reporting
MSS Education Page

The three tabs on the MSS Education page provide access to eLearning courses, demonstration and best practices videos, and core documentation. You can access the MSS Education page from the Portal Support menu.

MSS KnowledgeBase

The KnowledgeBase (KB) is populated with technical articles authored by senior Security Operation Center resources that will help answer some of the most frequently asked questions. You can search by keyword or select an article by category, as shown below. You can access the KB by clicking “Help” in the top right side of the portal, or by selecting the Knowledgebase option from the Support menu.
The KnowledgeBase opens in a separate window.

Located throughout the Virtual SOC Portal's user interface, you also can access Knowledgebase articles with links to many self-service educational videos and documents designed to provide information on many of the Portal's features and services.
See examples below:

- **Introduction to the Virtual Security Operations Center**  A quick overview of the various Portal features and resources available to assist customers in securing their networks on a daily basis

- **Introduction to the Suspicious Host and IP Intelligence Features** (10 minutes)  A video that demonstrates how to navigate the dashboard and reporting feature as well as some best practices associated (There is also an associated Webcast)

- **Introduction to VMS** (15 minutes)  A video that provides a detailed overview of the service and demonstrates how to use the features

- **Introduction Security Event and Log Management** (20 minutes)  A video that provides a detailed overview of the service and demonstrates how to use the features

**Portal Media Library**

The Portal Media Library provides download access to various documents, including user guides and threat research papers, as well as training videos and simulations, and webcast replays.
Security Services Resources

The Portal Resources site provides access to security research, videos, webcasts, and other information related to IBM Security Services.
Login Page

Open up your web browser and go to the following URL:

https://portal.sec.ibm.com

This is the first page you see when you visit the site is the Client Sign In page. It allows you to log in directly to the Portal, or sign in using your IBM id. Signing in with your IBM id enables the Portal’s single sign-on functionality, which allows you to seamlessly access X-Force Exchange and other IBM Security Services tools.

Note: For more information about using your IBM to access the Portal, refer to the user guide, "VSOC Portal Single Sign-On Using IBM id," which is available for download in the Portal Media Library.
Home Page

The home page acts as a launch pad to the various subscribed features and resources. You have the ability to customize your landing page with security analytic or informational based Portlets (or windows) associated with your security role or personal preference.

Use Case:

Most security teams are made up of more than one professional with a division of duties. For example one may specialize in Threat Analysis or Security Incident response and mitigation and another may focus more on device policy or device maintenance; another may focus strictly on the overall security posture and / policy. With this new enhancement in place each member of your security team has the ability to customize a series of informative Portlets associated with their business role which enables a more efficient customer experience.

Highlights:

- Predefined (and customizable) dashboards based on the business roles of Security Analyst, Operations Manager, and Executive
- Ability to create and personalize multiple dashboard views
- Enhanced security analytic Portlets with drill in and hover over capabilities for quick and efficient access important information (Example below)

- 25 Portlets categorized by Alerts, Firewall, IDPS, Information and Tickets
Home Landing Page:

Portlet Dashboards
Customizing your Portal

To add a new dashboard click on the green plus icon to add a new tab.

You can customize an existing type of dashboard or select, “Empty” to start from scratch. Right click in the open space to edit your dashboard.

Selecting your desired Portlets:
<table>
<thead>
<tr>
<th>Portlet Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alerts (3 Portlets)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Recent XPS Alerts</strong></td>
<td>Summary of the most recent XPS Alerts. Provides links to alert detail.</td>
</tr>
<tr>
<td><strong>XPS Alert Breakdown</strong></td>
<td>Bar graphs showing breakdown of alerts for the configured period</td>
</tr>
<tr>
<td><strong>XPS Alerts Trend</strong></td>
<td>Line graph showing trend in alerts over a configured time frame with links to alert breakdowns</td>
</tr>
<tr>
<td><strong>Firewall (2 Portlets)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Firewall Dropped/Rejected Traffic</strong></td>
<td>Grid display of the top sources of dropped or rejected firewall events for configured time frame</td>
</tr>
<tr>
<td><strong>Firewall Event Trend</strong></td>
<td>Column graph showing FW traffic for a configured time frame</td>
</tr>
<tr>
<td><strong>IDS/IPS (6 Portlets)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Changes In Sensor Activity</strong></td>
<td>List of sensors that have shown the greatest increase or decrease in recent activity</td>
</tr>
<tr>
<td><strong>IPS/IDS Top Destinations</strong></td>
<td>Bar chart showing top destinations for IPS/IDS events for configured time frame</td>
</tr>
<tr>
<td><strong>IPS/IDS Top Sources</strong></td>
<td>Bar chart showing top sources for IPS/IDS events for configured time frame</td>
</tr>
<tr>
<td><strong>Most Active Unblocked High Risk Events (Graph)</strong></td>
<td>Bar chart of most active events during a configured time frame with a comparison to the previous time</td>
</tr>
</tbody>
</table>
Editing existing dashboards: Right click on the dashboard's name tab to open the edit menu.

Be sure to save any desired changes.

Portlet controls; you have the option to Refresh, Configure, Hide and Remove any Portlet.

You can return to the home page at any time from any screen by clicking the “Home” menu option.
Check Notifications

Located under the Operations Portlet Dashboard, you can reference the Notifications and Device Manager Portlets for MSS News and recent changes in a device status that may require your attention.

Click on the Hypertext to launch a Device Details view
Current Threat Assessment

After reviewing any potential device status issues you should then review the current AlertCon level and the Current Internet Security Assessment. You can get to the current threat assessment page which may have additional data, by selecting “more” or clicking on “View All” to view Historical Assessments” within the Security Assessment Portlet.
*Features available in the Portal are dependent on the MSS Service subscription and device type.*
Active Tickets & XPS Alerts

Next you will want to focus on Active tickets, X-Force Protection System or XPS Alerts and Vulnerability Management Service or VMS Remediation Tickets (VMS customers only). **Note:** A full list of all active tickets can be accessed via the Ticket Manager dashboard. Clicking, “View All” in any ticket related Portlet will also launch the Ticket Manager Dashboard. There you can modify query criteria to search for tickets.

To view the details click on the desired Ticket ID hypertext. For a summary hover you’re the Ticket ID:

![Ticket Manager Dashboard](image)

The Recent XPS Alert Portlet will list new alerts. Clicking on, “View All” will launch the Alert Monitor.

![Recent XPS Alerts](image)
Notice that under ticket “Type”, some tickets have blue user icons while others have red user icons. The ticket color represents whether the ticket is an IBM Security Services SOC ticket or your internal ticket. Blue user icon tickets indicate that some sort of SOC intervention has or will occur. Tickets with red user icons are those worked by your own internal work force and have No SOC intervention whatsoever. Note: MSS SOC analysts do not have a view into your grey internal tickets.

Click this hyperlink for additional information regarding SOC Communications including tickets.

The screenshot below shows the Incidents and Alerts Portlet Dashboard.

* Features available in the Portal are dependent on the MSS Service subscription and device type.
Event Trends – Quick Glimpse

Next, in the default configuration, the Sensor Activity Portlet Dashboard contains several bar graphs and tables that provide a quick glimpse of your IDPS and Security Event trends. Hover your mouse pointer over to view count information.

Full reports on firewall and IDPS data are available in the Reports section of the portal.

Note: These Portlet reports are designed for quick reference to flag anomalies or suspicious traffic.
Shows most active events and total % amount

<table>
<thead>
<tr>
<th>Event name</th>
<th>% Total</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH_Brutal_Force</td>
<td>57</td>
<td>449</td>
</tr>
<tr>
<td>TCP Control Segment Anomaly</td>
<td>13</td>
<td>125</td>
</tr>
<tr>
<td>nbss_decoder: NBSS.Invalid.Fragment</td>
<td>12</td>
<td>98</td>
</tr>
<tr>
<td>Inbound TCP SYN or FIN Volume Too ...</td>
<td>5</td>
<td>39</td>
</tr>
<tr>
<td>1458: MS-SQL Slammer-Sapphire Win ...</td>
<td>5</td>
<td>37</td>
</tr>
</tbody>
</table>

Displaying last 7 days

IPS/IDS Top Destinations

Displaying last 24 hours
* Features available in the portal are dependent on the MSS Service subscription and device type.
Suspicious Hosts Dashboard

The Suspicious Hosts Dashboard provides real-time analysis of in and outbound firewall events and IDPS signatures that triggered within this same time period, identifying and tracking activities such as infection attempts.

A Suspicious Host is a public IP address that has been identified to be participating in malicious activities or communicating from vantage points that obfuscate behavior, such as open proxies. The intelligence used to identify this traffic comes from IBM X-Force Research & Development, IP reputation data, and other trusted 3rd parties.

Please note; if you rearrange your columns you may need to “Reset” your data and then “Apply your filter / query again.

* Features available in the portal are dependent on the MSS Service subscription and device type. (FW associated service /data is needed to generate the dashboard)
Additional Suspicious Hosts Dashboard features shown below:

Filtering options:

Features Highlights:
IP Intelligence Reporting Feature

The IP Intelligence Report expands on the Suspicious Hosts Dashboard, providing an even deeper analysis of individual IP addresses, including their Geo-IP location and whois information, and correlation of firewall events (Suspicious Hosts), IDPS events, asset intelligence, vulnerability scan results and associated tickets.

Access to the IP Intelligence Report has also been made easy via shortcuts embedded throughout the Portal. The most common access points to the IP Intelligence report are through the Suspicious Hosts Dashboard, Log Query and Security Event Monitor.
Device Manager

Device Manager provides an interface to view and edit device details and can be found under the “Device” menu. A listing of associated active tickets, group membership, and device information can be found for each device by clicking on the “+” icon next to the desired device.
Interface Enhancements

New enhancements provide a faster and more scalable user interface. You have the ability to customize most of your views.

* Features available in the Portal are dependent on the MSS Service subscription and device type.
Device Details

Device Manager contains context based menus that allow you to view and in some cases, edit the device details, such as defining any protected critical servers and monitored networks. You can also view health charts, XPS Alert Policy Editor, IDPS policy, and Firewall policy. IDPS and Firewall Policy options reflect any tuning and/or policy changes performed by the Security Operations Center. The context based menus can be located by right-clicking on the name of the device. You also have access to a troubleshooting guide within the Media Library or within the Details menu under the “Device Status” field.
Device Groups

Custom device groups can be created by clicking on the Edit Device Groups option located on the Device Manager page. Custom groups can be created in order to set up granular user permissions or for running custom reports and queries. Once you have defined your customer group click submit to save.

Add Critical Assets and Monitored Networks by Right Clicking on the Host Name and selecting Device Details:
Features available in the Portal are dependent on the MSS Service subscription and device type.
ULA Software

This page can be used to obtain the binary distributions of the ULA software (SELM customers only). There are installers for AIX, Windows, HP-UX (ia64 & PA-RISC), Linux and Solaris.

* ULA installation instructions can be accessed from the Media Library.
The Asset Center is a repository that facilitates management of information about critical assets that are not managed by IBM Security Services. This tool gives customers a way to upload or manually enter critical server and device information, and upload third-party vulnerability scan data, which can be used in the correlation and reporting capabilities of the X-Force Protection System (XPS).

**Essential Features**

- Manual upload of asset details and vulnerability scan results (CSV file)
  
  **Note:** This feature supports IBM Hosted Vulnerability Management Service (VMS), as well as third-party scan data.

- Critical server administration; integration with correlation and reporting capabilities

- Advanced filtering and single-click access to IP reputation and profiling reports

  **Note:** For more details about Asset Center features, refer to the Asset Center Quick Reference Guide, which is available in the Portal Media Library.

**Getting Started**

Open your web browser and browse to the following URL: [https://portal.mss.iss.net](https://portal.mss.iss.net)

After logging into the portal, you can access the Asset Center from the “Devices” menu.

**Note:** Customers who subscribe to Hosted Vulnerability Management Services will find their asset details have automatically populated the Asset Center.
**Adding or Editing an Asset**

To add an individual asset, click the “Add” icon. To edit an asset, select the asset and click the “Edit” icon. You also can right click the asset and select the “Edit” option.

---

**Exporting Assets**

The Asset Center allows you to export asset information to a CSV file. Click the “Export” icon to download a CSV file that includes the current data set.

---

**Note:** The exported data set is based on your asset filter settings. Be sure to configure filters appropriately before exporting asset data.
Vulnerability Manager

Vulnerability Manager is located under the VMS menu, and is available to those customers subscribing to the Vulnerability Management Service (“VMS”). The Hosted Vulnerability Management Service (VMS) is a vulnerability scanning service that provides the tools required to support a range of needs, including internal audit and risk assessment, regulatory compliance, and industry compliance requirements. VMS includes a comprehensive suite of functionality, including certified Payment Card Industry (PCI) approved scanning vendor reports. The PCI Approved Scanning Vendor (ASV) service is included for IBM Enterprise VMS customers via a separate tool.

**Note:** For the ASV service tool, scan source IP addresses will be different than those used for the Enterprise VMS tool, and scan results might differ slightly from Enterprise VMS scans. Consequently, the ASV service tool must be enabled and configured separately by IBM MSS. Please work with the SOC to enable the ASV service.

IBM provides VMS as a solution to be operated by you and will provide the scanning application and technical support for the application from the services. VMS is provided in two distinct types of scanning, external and internal, which can be employed together or separately.

External - IBM hosts and manages vulnerability scanners on the Internet. These groups of scanners are known as the IBM Global Scan Pool. External scan engines detect security risk exposures open to the Internet, and thus focus on scanning your public-facing IP addresses and web applications.

Internal - IBM also supports scanning within your enterprise network, using an IBM-managed, on-premises scanning device (called a “scan engine”). These are dedicated engines and cannot be used for any other purpose while under IBM management. They are accessible only via the MSS virtual SOC Portal interface.

This unified vulnerability solution scans your networks to identify assets, and probe for vulnerabilities. The vulnerability checks in VMS identify several sources of security weakness, including operating systems, databases, network protocols, and applications. VMS can even detect some malicious programs and worms, identify areas in your infrastructure that may be at risk for an attack, and with additional access, verify patch updates and security compliance measures.

VMS generates scan data for analysis directly in the Portal interface, where you also have access to customizable reports to facilitate risk assessment and asset remediation. VMS reports are available in multiple formats, and they allow you to filter scan data by vulnerability category and severity, as well as by site, asset group, or specific range and type of assets.
The VMS Console:

* For more VMS information, please access the Help option available from the question mark drop-down menu in the VMS Console.
Tickets and Incidents

Ticket Manager – Security & Service Related Tickets

The Ticket Manager provides an interface to view all of your tickets, which includes Security Incidents, Internal Security Incidents, Service Requests, Policy Change Requests, VMS Remediation tickets (VMS customers only) and Commented Security Investigations. Columns are sortable.

All tickets are available in the Portal for up to one year.

Enhanced filtering and querying options allow you to search by device, issue type, status, event name, and source and / or destination IP. You can also query by last updated dates.

*Note: IBM SOC analysts have no visibility of your internal tickets.
Quick access to worklog information (Click "Add" to update)

Ticket rating system to provide feedback and track satisfaction with ticket handling (To add a comment click on the “pencil icon” feedback will be monitored by the SOC to ensure customer satisfaction)

Hover over feature pop ups will provide a summary of the most recent worklog entry
Ticket templates:

* Features available in the Portal are dependent on the MSS Service subscription and device type.

Multiple templates for more efficient and effective ticket handling
Ticket Manager – Ticket Details

If you were to click on a ticket ID from either a Home Dashboard or the Ticket Manager, a window such as the following will pop up which includes all the details provided in the ticket:

![Ticket Details Window](image)

### Ticket Details

**Service Ticket**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket Number</td>
<td>123456</td>
</tr>
<tr>
<td>Created On</td>
<td>09/01/13 12:00</td>
</tr>
<tr>
<td>Last Modified On</td>
<td>09/01/13 12:00</td>
</tr>
<tr>
<td>File Attachments</td>
<td>Files, Attach a File</td>
</tr>
<tr>
<td>Resolution</td>
<td>N/A</td>
</tr>
<tr>
<td>Priority</td>
<td>Medium</td>
</tr>
<tr>
<td>Requested Time</td>
<td>09/01/13 12:00</td>
</tr>
<tr>
<td>Notification Status</td>
<td>No</td>
</tr>
</tbody>
</table>

**Issue Details**

**Reason for Escalation:** A SQL injection attack involving a defined critical sector has occurred. SQL injection attacks are extremely dangerous when they are used to gather confidential information from a back-end database or are used to modify contents within a database.

**Issue Code:** Site Scan and Scan

**Attack Name:** HTTP GET SQL UNION SELECT

**Source IP:** 12.173.210.9

**Destination IP:** 12.173.210.3

**Critical Server IP:** IP Included in Critical Server List

**Source IP Black Owner:**

```
<table>
<thead>
<tr>
<th>Domain</th>
<th>Organization</th>
<th>Address</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERNET SECURITY SYSTEMS</td>
<td>ISS-100</td>
<td>25400 DENTON OR</td>
<td>SOUTHFIELD</td>
</tr>
</tbody>
</table>
```

**SOC Actions Taken:**

```
<table>
<thead>
<tr>
<th>Action</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>asdf</td>
<td>09/01/13</td>
</tr>
</tbody>
</table>
```

**Recent Events:**

```
<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Scan</td>
<td>HTTP GET SQL UNION SELECT</td>
</tr>
</tbody>
</table>
```

**Chat Transcripts**

<table>
<thead>
<tr>
<th>Contact Name</th>
<th>Start Time</th>
<th>End Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABC</td>
<td>09/01/13</td>
<td>09/01/13</td>
</tr>
</tbody>
</table>

---

**Note:** The window shown is a hypothetical example for illustration purposes. Actual content may vary depending on the ticket data.
Ticket Manager Reports – Policy Change Request

Below is an example of a firewall policy change request report. You will see similar data after clicking on the report icon for a policy change request ticket. Reports are also available for Security Incidents.

---

Ticket Details

**Service Ticket**

<table>
<thead>
<tr>
<th>Ticket Number</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0700720447</td>
<td>Resolved, Pending Closure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Created On</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/01/11 11:27</td>
<td>PCR - Completed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Last Modified On</th>
<th>Priority</th>
<th>Notification Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/10/11 00:24</td>
<td>Medium</td>
<td>No</td>
</tr>
</tbody>
</table>

**Issue Details**

<table>
<thead>
<tr>
<th>Issue Code</th>
<th>Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCR - Change Policy</td>
<td>abcdp-preservation-01 (STG PROSUR)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Src. IP</th>
<th>Dest. IP</th>
<th>Worklog</th>
</tr>
</thead>
<tbody>
<tr>
<td>test test</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Worklog:

- 19/10/2011, 12:24:14 GMT submitted by torres
- PCR Email sent to leonardo.jordino@ibm.com
- A report of Policy Change Request SOC:00700720447 is presented below. If you have any questions or concerns, please contact your Security Operations Center (SOC) and reference the ticket number provided.

---

Policy Change Request

Policy Change Request Number: SOC:00700720447
Customer Name: Demo Customer
Contact: Leonardo Jordino
Status: Resolved, Pending Closure
Submit a Policy Change Request

The options to submit a Policy Change Request (PCR) are located under the Tickets menu. Select the appropriate PCR template for your device type. (Firewall or IDPS)

First, select a device, or device group for the change to be applied to by clicking on, “Select Devices.” Next, provide the change details in the fields provided.
Selecting Devices: The device selecting interface contains filters and a search field to efficiently locate and choose your desired device or group of devices.

After you have selected your device you can review the policy prior to submitting your change request. Click on, "View Firewall Policy" to launch a separate policy window.

After you have submitted your change request a confirmation window will appear with an option to review the ticket details or link to the Chat client for further interaction with the SOC.
After creating your ticket, you can chat with the SOC to schedule a maintenance window or raise the priority of the request.
Submit a General Service Request

General (or “Other”) Service Requests are located under the Tickets menu. You can use this request for general inquiries, as well as requesting delivery of logs (additional charges apply for delivery of logs).

Select the appropriate devices

Select a device group

No devices, select a device group.

Classify the ticket

Request Type:

Request Physical Logs Delivery

Your reference ticket ID:

Describe the request

Request:

File Attachment:

Browse... No file selected.

Please note, the maximum size for file upload is 5MB.

Email Notification on Update?

No

Submit
Create an Internal Ticket

You can create an Internal Ticket via the Tickets menu. This ticket will be assigned to your internal staff. *Please note no SOC intervention will occur.*

**NOTICE.** SOC personnel do not have access to Customer Internal tickets. Any information you submit or update in this ticket will not be accessible by SOC personnel. If you need the SOC to work or see this ticket, please submit it as one of the types that is visible to the SOC.

**Select the appropriate devices**

Select a device group

No devices, select a device group.

**Classify the ticket**

Assigned To:

Please select a contact.

Issue Type: General Ticket

Priority: Low

Your reference ticket ID:

**Describe the request**

Request:

File Attachment: Browse... No file selected.

Please note, the maximum size for file upload is 5MB.

Email Notification on Update?

No

Submit
Create an Internal Security Incident

Like the Internal general Ticket you can also create your own Internal Security Incidents, and assign it to your internal staff under the Tickets menu (Create Internal Security Incident). Once you have filled out the incident, and assigned it to your internal staff click “submit” to save.

**Note: No SOC intervention will occur.**
# Reports

The “Reports” menu contains links to many useful service report templates that will assist you and your security team in day-to-day research and audit control/compliancy.

For more information and best practices, please reference the Reports user guide located in the Media Library.

## The Reports Dashboard:

<table>
<thead>
<tr>
<th>General Service Related</th>
<th>Firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Level Agreement</td>
<td>Firewall Summary Report</td>
</tr>
<tr>
<td>Service Overview</td>
<td>Traffic Analysis - Denied</td>
</tr>
<tr>
<td>Security Manager Overview</td>
<td>Traffic Analysis - Email</td>
</tr>
<tr>
<td></td>
<td>Traffic Analysis - Web Activity by IP</td>
</tr>
<tr>
<td></td>
<td>Traffic Analysis - Web Activity by Website</td>
</tr>
<tr>
<td></td>
<td>Protocol Usage - Allowed</td>
</tr>
<tr>
<td></td>
<td>Protocol Usage - Denied</td>
</tr>
<tr>
<td></td>
<td>Connections Summary - Allowed</td>
</tr>
<tr>
<td></td>
<td>Connections Summary - Denied</td>
</tr>
<tr>
<td></td>
<td>Targeted IP Addresses</td>
</tr>
<tr>
<td></td>
<td>Rule Utilization Analysis</td>
</tr>
<tr>
<td></td>
<td>Suspicious Host Correlation Report</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IDS/IPS Sensors</th>
<th>Log Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Alert History</td>
<td>SELM Server Device Login by Site</td>
</tr>
<tr>
<td>Your Alert History</td>
<td>Event Counts By</td>
</tr>
<tr>
<td>Alerts on Vulnerable Assets</td>
<td></td>
</tr>
<tr>
<td>Prevented Attacks Report</td>
<td>Event Name Trends</td>
</tr>
<tr>
<td>Vulnerability Impact</td>
<td>Multiple Events Breakout Trend</td>
</tr>
<tr>
<td>Event Counts By</td>
<td></td>
</tr>
<tr>
<td>Source IP</td>
<td>Event Counts By</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Device</td>
</tr>
<tr>
<td>Event Names</td>
<td>Log Aggregator</td>
</tr>
<tr>
<td>Sensors</td>
<td>System Activity Events</td>
</tr>
<tr>
<td>Server, Event Names, IP</td>
<td>System Activity Events Details</td>
</tr>
<tr>
<td>Event Trend</td>
<td>System Activity Events By User</td>
</tr>
<tr>
<td>Event Name Trend</td>
<td>System Activity Events By PDI Requirement</td>
</tr>
<tr>
<td>Multiple Events Breakout Trend</td>
<td></td>
</tr>
</tbody>
</table>

### Quick access to report templates by pre-set time intervals

Below are some examples of additional reports:
Daily Summary Report:

We recommend that you subscribe to the Daily Summary Report located under Settings/ My Profile (Email Notifications). You will receive an email with important information including the Current Internet Security Assessment and an active ticket summary.

Customer Security Metric Report:

The CSM report is specifically targeted at executive level customer contacts that don't regularly log into the Portal. The report provides a "sense" for the overall status of the services you have subscribed to and highlights any high level security observations that may be related to security posture and risk.

If you are interested in this report and do not currently have this option please contact the SOC.
IDS/IPS Sensors Reports

The "Event Trend" report gives a comparison of the current period events and trends with the previous period events and trends and also lists any security incidents.
Attack Metrics

This report displays several graphs of information, detailing the numbers and types of attacks detected during the past 30 days. Click on the graph for additional drill-in reporting information.
Explanation of Attack Types

The attack types included in the Attack Metrics report, along with brief descriptions and examples, are listed below.

- **ProtocolSignature**
  A large number of these events in a short time period could indicate an attack.

  **Example:** TLS_Weak_CIPHER_Suite

  Servers and clients use X.509 certificates when establishing communication using Secure Sockets Layer (SSL). An SSL server that allows weak ciphers (with key-lengths less than 128-bits) could allow a remote attacker to obtain sensitive information.

  **How to remove this vulnerability:** Consult server documentation to disable weak ciphers.

- **Netbios_Session_Request**
  A request to initiate a NetBIOS session between two computers. A large number of these events in a short time period could indicate a brute force attack.

  **How to remove this vulnerability:** Analyze the nature of the traffic to determine if this is normal usage. You might want to fine-tune the threshold so that normal use does not trigger this event, while brute force attempts would still be detected.

- **Pre-AttackProbe**
  An attempt to gain access to a computer and its files through a known or probable weak point in the computer system.

  **Example:** Ping_Sweep

  As a prelude to an attack, subnets are often swept with ICMP or other packets that elicit known responses from active hosts. This sort of probe is used to enumerate active hosts on the subnet, and identify potential attack targets. Normal hosts on a network should never engage in sweeps unless they are performing network monitoring or management tasks.

  **How to remove this vulnerability:** Always filter inbound ICMP (other than replies to outbound requests) through your firewall or filtering router, if possible. If a stateful inspection filter is not available inbound, then block all ICMP outbound to prevent replies from reaching the attacker.

- **UnauthorizedAccessAttempt**
  This usually denotes suspicious activity on a system, or failed attempts to access a system, by a user or who does not have access.

  **Example:** SSH_Brute_Force

  This event detects an excessive number of very short SSH sessions initiated by a single client to one or more servers within a specified timeframe. It may indicate a username/password guessing attack, or a DoS attack. To qualify as this type of attack, a session must have completed encryption negotiations so that a login may be attempted, and the time elapsed from the first encrypted client
data until the TCP session ends with a TCP FIN or server RST must be less than the pam.login.ssh.short.session.time (default 4 seconds). The signature is tunable via the pam.login.ssh.count p (default 12) and the pam.login.ssh.interval setting (default 60 seconds).

This signature also detects an excessive number of SSH Server Identifications from an SSH server within a specified timeframe. This may indicate a username/password guessing attack. The signature is tunable via the pam.login.ssh.count, pam.login.ssh.interval and pam.ssh.server.bruteforce.chars settings.

- **Backdoors**

Hidden programs that attackers use to access your computer without your knowledge or consent.

*Example:* RDP_Brute_Force

This signature detects worms, such as Win32/Morto, that allow unauthorized access to an affected computer. These worms spread by trying to compromise administrator passwords for Remote Desktop connections on a network.

*Example:* NetController_TCP_Request

This signature detects a request on port 6969/TCP that may indicate a NetController backdoor running on your network.

*How to remove this vulnerability:* Use an up-to-date antivirus program to scan the target computer to determine if it is infected with a backdoor program. If the program detects a backdoor, follow its instructions to disinfect and repair the computer.

- **DenialofService**

An attack that attempts to prevent legitimate users from accessing information or services. By targeting a user's computer and its network connection, or the computers and network of the site a user is trying to access, an attacker may be able to prevent a user from accessing email, websites, or online accounts for banking or other services that rely on the affected computer or network.

*Example:* Smurf_Attack

In a Smurf denial of service (DoS) attack, ICMP echo request (ping) packets addressed to an IP broadcast address cause a large number of responses. When each host on the subnet replies to the same ping request, the large number of responses can consume all available network bandwidth, especially if data is appended to the ping request. This can prevent legitimate traffic from being transmitted during the attack. This attack is frequently used against third parties, where an attacker forges the target's source address in a Smurf attack against a different target. At the extreme, this attack can simultaneously disable both targets.

Windows systems do not respond to broadcast pings. However, this does not mean that all Microsoft networks are invulnerable to Smurf attacks.

*How to remove this vulnerability:* Reconfigure your perimeter router or firewall to block ICMP echo requests on your internal network and block ICMP echo replies from entering your network. This prevents an internal attacker from using your network to mount a SMURF attack against another target. It also prevents an external attacker from targeting your hosts. However, neither of these actions will stop internal SMURF attacks.
• **Network**

An attack that uses various types of network traffic and protocols for malicious activities.

*Example:* HTTP_eDirectory_Multiple_Connection

Novell eDirectory is vulnerable to a denial of service, caused by an error in the dhost.exe service when processing Connection headers. By sending multiple HTTP requests containing specially-crafted "Connection" headers, a remote attacker could exploit this vulnerability to consume all available CPU resources, resulting in a denial of service.

**How to remove this vulnerability:** Refer to Novell Security Alert Document ID: 3829452 for patch, upgrade or suggested workaround information.

*Example:* ICMP_Redirect

ICMP redirects detected on a network or targeted at hosts with weak TCP/IP stack implementations have been shown to cause system failures and other adverse effects. Some versions of NetWare, Windows, and embedded systems like Microware OS-9 have been shown to be susceptible to attacks using ICMP redirects. An attacker could forge ICMP Redirect packets, and possibly alter the host routing tables and subvert security, by causing traffic to flow on a path the network manager did not intend.

**Caution:** Various networked, embedded controllers may hang or shut down, if they receive an ICMP redirect with an invalid Code. If your network contains controllers attached to automation equipment, manufacturing equipment, HVAC (Heating, Ventilation, and Air Conditioning) equipment, and medical equipment, do not perform ICMP redirects.
Security Logs and Events

Logs Drop Down Menu

There are 4 menu options when viewing the 'Logs' drop down menu:

- Log Query
- Log Search (No export option but is more advanced)
- Log Downloads
- Log Parse

The Log Analysis features of the portal include powerful query engines, with granular query criteria, and filters, than enable you to query multiple log types, and events from multiple devices, and correlate the results through the display in a common interface. You also have the option to schedule log downloads. Log downloads can be retrieved from the Log Downloads menu.

Log Query

The log query enables you to query multiple log types, and correlate the results through a common display. The query criteria are displayed below. There are five steps:

1. Select the time/date or select a time interval. Note that you can also select your time zone so that the correct time is displayed in your results.
2. Select the devices to be included in the query. You can select by device, custom group or site. Refer to page (14) for more information on creating custom groups.
3. Select the log types you would like returned in your search.
4. Select your query criteria is to select options such as logs per page, DNS resolution, sort, and scheduling a download.
5. Enter search terms if applicable. Click on the “?” next to the text box for examples.

There is also the option for Advanced Query Criteria (circled below in red) for more granular control of your queries.
Log Query – Advanced Options

The advanced query criteria can be seen at the bottom of the screen image below. The “=” denotes include, and “!=” denotes exclude. Examples of how to use the filters, can be displayed by clicking on the “?”, or the magnifying glass next to the “Type” field.
Log Query – Results

There are context based menu’s available, for your use in the results of your log queries. Clicking on the “+” next to the log type, will display the raw log. Clicking on the device will give you the option, of viewing the device details, as well as any recently opened tickets relating to the device. Clicking on the event name, will provide filter options, as well as the option to view the security event details. Clicking on the Source/Destination IP, Source/Destination Port, or Action will provide filtering options. There is also an option, to add or remove table columns, to assist you in customizing your results, in a manner that caters to your needs.
Log Search

Log search is the next generation log query tool. First select a device or group of devices then your desired log type(s). You can then select the appropriate date/time range. The fields and details options will allow you to control the information output.

There is an Overview document that will assist you in general use including how to build your log search syntax.
Active Analyzer

Active Analyzer provides close to real-time event monitoring of your IDPS events, with auto-refresh, as well as manual refresh options. With each refresh, the baselines increase in events, and deltas are reflected. You can also view the events from event view, sensor view, source view, or destination view via the “Selected view” drop down menu located at the top right above the auto-refresh options.

Active Analyzer – Context Based Menus

Active Analyzer offers context based menus to assist you in your research and investigation. You can access the context based menus, by clicking on the event name, or the arrow located to the right of the event name.
Active Analyzer – Query Criteria

Active Analyzer’s powerful query tool gives you the ability to query your IDPS events by time interval, sensor, priority, event, and source and destination. To execute a successful query, it’s helpful to be familiar with all the options of this screen.

**Custom Query**
- **Time Interval**: Defaults to “Last 2 Hours”
- **Number of Results**: Defaults to 500
- **Refresh Interval**: Defaults to 30 seconds
- **Device Selection**: Defaults to “All Devices”
- **Submit Query button**: Click this button or press enter when you want to generate the report

**Applied Filters**
- **Priority**: Low, Medium, or High. Leave blank to query all priorities.
- **Event Names**: One or more tag names (aka: signatures). Use the “|” in between multiple entries. Spaces are ignored.
- **Source IPs**: One or more source IP address(es). Use “|” for multiples.
- **Destination IPs**: One or more destination IP address(es). Use ”|” for multiples.

![Active Analyzer Query Screen](image-url)
**Log Parsers**

If you have the subscribed service you can monitor and report upon activity from previously unknown systems and applications that have been missing from your Virtual SOC analysis and / or compliancy initiatives.

The log parser extracts data from raw OS or application log files and then formats them in a way that can be recognized and organized by the MSS Log Management System.

Embedded access to Customer Enablement resources on the right side shown below:
Creating Virtual SOC Portal Users

Authorized Security Contacts can create users, by clicking on “Settings” which is located in the top right hand corner underneath your username of any screen. Next select “Users” from the left side of the screen. You can then select “Create a New User.”
After you have created the new users login credentials, personal information, and email notifications you will need to create portal roles and device permissions for the user.

A description of roles can be viewed by clicking on “Show description of roles.” Note that devices and device groups will not be visible until you select a role, as only groups pertinent to that role will be displayed.
SOC Communications

Service Escalation

This form provides feedback directly to the IBM Security Services Customer Problem Management team. It can be found under the “Support” menu, and then within the “Report a Service Problem” option.

* Note this is not a path for technical escalations but for issues regarding service delivery.
SOC Escalation

You have the ability to contact the SOC for technical support via email, phone or a private and secure chat session. For critical issues we recommend that you call the SOC directly. Please see, “References” for SOC contact information under the Support menu option.

(Toll-Free US: 877-563-8739)

**Chat feature:**

![Chat feature](image_url)
Media Library

This page found under the Support menu section of the portal, allows the client to download service-related documentation and education resources. SOC engineers also can post files, such as diagrams, here for clients to download in a secure manner. It will be noted within the MSS bulletins whether a document or file will be available.
Log Out

To log out of the Portal, from the username menu located in the top right corner of the Portal, select "Logout". You will be returned to the login screen.
Reference

SOC Contacts

This page provides contact information for IBM Security Services support. It can be found under the support menu.