# TABLE OF CONTENTS

## OVERVIEW

- Purpose .................................................................................................................. 4
- What is the Virtual SOC Portal? ............................................................................. 4

## LOGIN PAGE

- Login Page ............................................................................................................... 5

## HOME PAGE

- Summary .................................................................................................................. 6
- Use Case .................................................................................................................... 6
- Highlights .................................................................................................................. 6

## CUSTOMIZING YOUR DASHBOARD

- Selecting your desired Portlets .............................................................................. 7
- Portlet Controls ....................................................................................................... 7
- Check Notifications ................................................................................................. 8

## USER PROFILE

- Contact ID ............................................................................................................... 9
- Email Notifications ................................................................................................... 9

## ACCOUNT MANAGEMENT

- Login Page ............................................................................................................... 10

## TICKETS AND INCIDENTS

- Ticket Manager – Security & Service Related Tickets .......................................... 11
- Viewing and Adding Worklogs: ............................................................................. 12
- Ticket Rating .......................................................................................................... 13
- Creating a New Ticket - Ticket Templates ............................................................. 14
- Submitting a Policy Change Request ..................................................................... 14
- Submit an Other Service Request ......................................................................... 17
- Create an Internal Ticket ....................................................................................... 18

## SECURITY LOGS AND EVENTS

- Logs Drop-Down Menu ......................................................................................... 19
- Log Query ............................................................................................................... 19
- Log Search .............................................................................................................. 20
- Log Parsers ............................................................................................................. 20

## (VMS) VULNERABILITY MANAGER

- Enterprise (Rapid7) ............................................................................................... 21
- Qualys Essentials ................................................................................................. 22

## DEVICE MANAGER

- Device Details ........................................................................................................ 23
- ULA Software ......................................................................................................... 25

## ASSET CENTER

- Essential Features .................................................................................................. 26
- Getting Started ....................................................................................................... 26
- Adding or Editing an Asset .................................................................................... 27
- Exporting Assets .................................................................................................... 27

## ANALYTICS

- Active Analyzer ..................................................................................................... 28
ACTIVE ANALYZER – CONTEXT BASED MENUS ................................................................. 28
ACTIVE ANALYZER – QUERY CRITERIA ........................................................................ 28
SUSPICIOUS HOSTS ......................................................................................................... 29
FILTERING OPTIONS ....................................................................................................... 30
FEATURE HIGHLIGHTS .................................................................................................... 30

IP INTELLIGENCE REPORTING FEATURE .................................................................... 31

REPORTS .......................................................................................................................... 32
THE REPORT DASHBOARD .............................................................................................. 32

SUPPORT ........................................................................................................................... 33
SOC CONTACTS ................................................................................................................. 33
ESCALATION CONTACTS ................................................................................................. 33
SERVICE ESCALATION ..................................................................................................... 33
SERVICE PURCHASE REQUEST ....................................................................................... 33

CUSTOMER ENABLEMENT ASSETS .............................................................................. 35
MSS BEST PRACTICES .................................................................................................... 35
MSS EDUCATION (ELEARNING/VIDEOS/DOCUMENTATION) ........................................ 35
ELEARNING COURSES .................................................................................................... 35
COURSE SIMULATIONS .................................................................................................. 36
ELEARNING VIDEOS TAB ................................................................................................. 36
VSOC MEDIA LIBRARY ................................................................................................... 38
SECURITY SERVICES RESOURCES ............................................................................. 38
QUESTION MARKS ........................................................................................................... 39
CHAT .................................................................................................................................. 39

LOG OUT .......................................................................................................................... 40
Overview

Purpose
This guide is designed to show you how to make the most out of the IBM Managed Security Services (“MSS”) customer Portal or most commonly referred to as the Virtual Security Operations Center (VSOC).

What is the Virtual SOC Portal?
The IBM Virtual SOC or VSOC is a single, consolidated web interface for managed, monitored and cloud-based security services, providing clients with visibility and transparency into the health, status, and analysis of their data. The VSOC consolidates diverse data and intelligence from multiple services - correlating, alerting, and reporting on it. This unified interface simplifies management, accelerates time to value, and offers clients role-based views that are tailored to the business needs of each VSOC user.

*Please remember the information available is based on your subscribed services.
Login Page

To access the VSOC, open up your web browser and go to the following URL:

https://portal.sec.ibm.com

The Client Sign In page is the first thing you see when you visit the site. It allows you to log in directly to the VSOC, or sign in using your IBM id. Signing in with your IBM id (see Note below) enables the VSOC’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 id to access the VSOC, refer to, User Guide: MSS VSOC Portal Single Sign-on Using IBM id,” which is available for download in the Documents section of the VSOC Media Library.
Home Page

Summary
The VSOC home page is both a snapshot of the most critical security information potentially impacting your network and a jumping point to all of the resources and feature sets available to you. 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, IDS/IPS, Information, and Tickets.
Customizing Your Dashboard

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

You can select an existing template or choose “Empty” to start from scratch.

Selecting your desired Portlets

Right click in the open space to edit your dashboard – or select the drop-down arrow next to each Dashboard. Be sure to save any desired changes.
Portlet Controls
You have the option to Refresh, Configure, Hide, and Remove any Portlet.

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

By accessing the Edit Profile section you can view or edit your contact details and subscribe to notifications. You can also update your PIN, passphrase, and challenge questions. In order to access Edit Profile from the VSOC: Hover over your name in the upper right-hand corner> Edit Profile.

Contact ID

When calling into the SOC you are required to authenticate. Authentication occurs one of two ways. You can provide your Contact ID and PIN or your Verbal Passphrase. In Edit profile, within the Login Credentials section, this is where you can locate your unique Contact ID. You can also utilize the link to update your PIN, Pass Phrase, etc.

Login Credentials

User name: portaluser15

Contact ID: 0010316

Change Password, PIN, or Pass Phrase

Email Notifications

You have the option to sign up for our various email notifications, including the Daily Summary Report. If you want to know what each notification contains, utilize your mouse to hover over each one and a box will appear with a short explanation. This is also where you can subscribe to our XFTAS Daily Threat Assessment emails. If you don’t want to subscribe to XFTAS, the information can also be located within the VSOC via the Intelligence dropdown>Security Assessment.

Email Notifications

- Customer Security Metrics Report
- Daily Summary Report
- MSS Event Invitations
- Maintenance
- SELM Failed Event
- Service Updates & Announcements
- Vulnerability
- XFTAS Email HTML
Account Management

You can view and manage who has access to the account by going to the Users section. Designated Client Admins can add, edit and remove Regular users. If you ever need to add, edit, or remove a Client Admin you must put in an Other Service Request ticket with the SOC. To access this section in the VSOC hover over your name>Settings>Users. Check the Users section often to make sure those who are listed should have access.

To create a new user, click on the Create a New User link. To edit use the pencil icon and to delete use the trash can.

![Create a New User](image)

After you have created the new user’s login credentials, personal information, and email notifications you will need to create Portal Roles and device permissions for the user.

---

### Portal Roles

- **MDP:** Admin
- **MSEIM:** Admin
- **Malware:** Malware Admin
- **Firewall:** Admin
- **XFTAS:** Yes
- **IDS/IPS:** Admin
- **ISM:** Admin
- **IAM:** Regular
- **ILM:** Restricted
- **QoCTM:** QoCTM Admin
- **EndPoint:** Admin

---

What you see here varies based on your services. For a description of each permission level, hover your mouse over the permission side and a box defining them will appear.
Tickets and Incidents

Ticket Manager – Security & Service Related Tickets

The Ticket Manager provides an interface to view all of your tickets, which includes but is not limited to Security Incidents, Internal Security Incidents, Service Requests, Policy Change Requests. Columns are sortable.

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

Enhanced filtering and querying options allow you to search by Device, Issue Type, Status, Priority, Ticket ID, Keyword, Event Name, and Source and/or destination IP. You can also query by Last Updated dates. Once filter criteria have been selected, you must click on Apply.

Quick access to ticket details by expanding the “+” sign icon on the left side. You can also view event details by selecting the down arrow next to each event.
Viewing and Adding Worklogs:

From Ticket Manager, hover your mouse over the Latest Worklog column to see the most current worklog entry.

Expand a ticket to view the most current worklog. An Add… button is provided to add a new entry.

Click on the Ticket ID. Scroll down to the Worklog section. Here you can see all of the worklog entries.
Ticket Rating

The ticket rating system is used to provide feedback and track satisfaction with ticket handling. To add a comment, click on the “pencil icon”. You can change your rating at any time. Feedback is monitored by the SOC and management to ensure customer satisfaction.
Creating A New Ticket - Ticket Templates

Ticket templates are located in the Tickets drop-down menu. Select the template that is most appropriate to your issue/request. If you have questions, use the Chat Online feature located in the Help dropdown menu and the SOC will assist you.

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

Submitting 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, IDPS, or General).

Please note that one PCR equates to a request for change(s) to a single device. Consequently, if you submit a ticket containing change requests for multiple devices, the number of PCRs is equal to the number of affected devices.

All PCRs must be submitted or approved by an authorized contact for the specific devices associated with the ticket. After a PCR ticket is submitted, a SOC engineer checks the customer contact list to ensure the submitter is authorized. If the submitter is not authorized, the SOC cannot process the ticket without approval. In such cases, an authorized contact either will have to resubmit the ticket, or update the work log of the existing ticket, stating that the requested changes are approved for deployment.

Example below on how to complete a Firewall Policy Change Request.
Step 1: Select PCR implementation time

Step 2: Add the affected devices

Step 3: Select applicable action and interface

Step 4: Complete source and destination information

Step 5: Select applicable Protocol/Service
After a PCR has been submitted, you will see the below confirmation message. If any of the conditions mentioned in the message apply to your request, please contact the SOC by phone or online chat.

*If you would like to learn more about PCR’s, please go to: Support>Best Practices>Ongoing Operations>Policy Change Requests
Submit an Other Service Request

The Other Service Request ticket template is located under the Tickets menu. You can use this request for general inquiries, as well as requesting the delivery of logs (additional charges apply please verify with your contract).

Available Request Type options are based on subscribed services.
Create an Internal Ticket

You can create an Internal Ticket via the Tickets menu. This ticket will be assigned to your internal staff. You can also create your own Internal Security Incidents and assign to your internal staff.

* Please note no SOC intervention will occur.

---

**Select the appropriate devices**

---

**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.

**Email Notification on Update?**

- No

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

---

Submit
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)
- Log Downloads
- Log Parser

The Log Analysis features in the VSOC include powerful query engines, with granular query criteria and filters, which 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.
3. Select the log types you would like returned in your search.
4. Select options such as logs per page, DNS resolution, sort, and scheduling a download. *If you schedule the download, when it is finished it will be available in Logs>Log Downloads.
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 (below in the yellow box) for more granular control of your queries.
Log Search

Log search is the next generation log query tool. First select a device or group of devices and 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. The document can be located in either yellow boxed location below.

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.
(VMS) Vulnerability Manager

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

Enterprise (Rapid7)

Located under the VMS menu and available to those customers subscribing to the Rapid7 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. This includes internal audit and risk assessment, regulatory compliance, and industry compliance requirements. Rapid7 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 link.

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.

To learn more about the Rapid7 solution go to Support>Best Practices>Ongoing Operations>Vulnerability Management. You can also select Help via the question mark from the VMS console.
Qualys Essentials

IBM Security vulnerability scanning service provides cloud-based scanning services for large and small to midsized businesses that need to implement vulnerability scanning to comply with internal policies or external mandates and to be proactive in securing their infrastructure against increasing threats. Unlike in-house solutions that carry the burden of hardware, software and maintenance requirements and competitors that may report excessive false positives, IBM helps provide more accurate, robust vulnerability management through a single web-based portal that helps companies identify vulnerabilities across network devices.

IBM is an Approved Scanning Vendor (ASV), qualified by the Payment Card Industry Security Standards Council (PCI SSC). This solution classifies your IT assets and vulnerability data to help you better understand your security posture and more easily manage compliance, prioritizes remediation to help you more effectively manage risk, and can save staff time by providing steps to help correct vulnerabilities.
Device Manager

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

You can also view IDPS policy and Firewall policy in Device Manager. IDPS and Firewall Policy options reflect any tuning and/or policy changes performed by the Security Operations Center (please allow up to 24 hours for changes to reflect). The context based menus can be located by right-clicking on the name of the device.

Device Details

Device Manager contains context based menus that allow you to view and in some cases, edit the device details, such as Customer Device Name. You also have access to a SELM troubleshooting guide and Device Health Charts located in the Details menu in the “Device Status” section.
View the Log Retention period per device. Once you expand the device, on the Details tab locate the Logs section.

* Features available in the VSOC 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 in the documents section (IBM Security Services SELM Admin and ULA Installation Guide).

<table>
<thead>
<tr>
<th>Package</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>mssa-ula-instaler.exe</td>
<td>windows</td>
</tr>
<tr>
<td>mssa-ula-install.aix.bin</td>
<td>aix</td>
</tr>
<tr>
<td>mssa-ula-install.hpux-ia64.bin</td>
<td>hpux</td>
</tr>
<tr>
<td>mssa-ula-install.hpux-parcsc.bin</td>
<td>hpux</td>
</tr>
<tr>
<td>mssa-ula-install.linux.bin</td>
<td>linux</td>
</tr>
<tr>
<td>mssa-ula-install.solaris.bin</td>
<td>solaris</td>
</tr>
<tr>
<td>mssa-ula-install.solaris.x86.bin</td>
<td>solaris</td>
</tr>
</tbody>
</table>
Asset Center

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 third-party vulnerability scan results (CSV file)
  
  **Note:** This feature supports IBM Hosted Vulnerability Management Service (VMS)

- 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 Support>Media Library>Documents>Asset Center Quick Reference Guide.

Getting Started

Access the Asset Center from the “Devices” menu

![Asset Center Interface](image)

**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.
Analytics

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 left 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**
  - 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.
Suspicious Hosts
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 VSOC are dependent on the MSS Service subscription and device type. (FW associated service /data is needed to generate the dashboard)

Bolded IP addresses represent Suspicious Hosts
Click on the “+” Icon to expand and gain access to more information including IP Intelligence
Additional Suspicious Hosts Dashboard features shown below:

**Filtering Options**

- Filter by Inbound and Outbound traffic
- Filter by Specific IP
- Filter by Specific Date or Time Interval

**Feature Highlights**

- Source and Destination IPs
- Geographic Location
- Last Event
- 30 Day FW Trend
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 VSOC. The most common access points to the IP Intelligence report are through Suspicious Hosts, Device Manager, and Alert Monitor via the Alert ID link.
Reports

The Report Dashboard 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, how to schedule a report, and best practices, please reference the Reports user guide located in Support>Media Library>Documents>User Guide: Virtual SOC Portal Reports.

The Report Dashboard

Reports available in the VSOC are dependent on the MSS Service subscription and device type.
Support

SOC Contacts
Provides helpful contact information and authentication required for each method.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Hours</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Chat</td>
<td>24x7x365</td>
<td><a href="https://portal.mss.iss.net/">https://portal.mss.iss.net/</a> Chat Online button under Portal’s Help menu</td>
</tr>
</tbody>
</table>
| Telephone      | 24x7x365| Toll-Free US, Canada, Caribbean: 866-266-4362  
Toll US: +1-404-236-3290  
ARGENTINA: 0800682074  
AUSTRALIA: 1300038641  
AUSTRIA: 0808 203513 |

Escalation Contacts
In the event of an emergency, this section highlights the steps to follow in order to contact the SOC.

Service Escalation
This form provides feedback directly to the IBM Security Services Customer Problem Management team. It can be found under Support>Report a Service Problem.

* Note this is not a path for technical escalations but for issues regarding service delivery.
Service Purchase Request

You can purchase items such as additional PCR's, PDRU's, and other services through this form. Once you submit the form a member from the IBM sales team will contact you.
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 VSOC’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 uses an operational framework to articulate recommended activities around processes and procedures that can maximize the value of your subscribed services.

**Purpose**
The IBM Managed Security Services (MSS) Best Practices are based on lessons learned from working with thousands of clients. This guidance should serve as a useful baseline to help you maximize your organization’s security investment.

**Important:** If you are a new IBM client or a new Virtual Security Operations Center (VSOC) Portal user, you can access MSS Education resources to learn more about your IBM services, as well as key VSOC Portal features and navigation. Also, be sure to check out the Security Services Resources page, which is accessible from the Portal Support menu, for important information and links regarding other IBM Security resources and services.

**MSS Best Practices Framework**
The MSS Best Practices framework consists of multiple ongoing processes and complementary tasks that are optimized to enhance the overall security of your organization. The menu bar above reflects this framework, with selections for Service Initiation, Ongoing Operations, Problem Resolution, and Client Security Organization. Explore the menus to get more information about each Best Practice category and its corresponding practice areas.

MSS Education (eLearning/Videos/Documentation)

IBM Managed Security Services Education eLearning section allows you to learn at your own pace, using our engaging and interactive online content.

**eLearning Courses**
The following eLearning job-focused courses, which include hands-on simulations, are available in the VSOC:

- MSS Managed SIEM Analysis and Reporting
- MSS Security Intelligence and Analysis
- MSS Security Incident Response
- MSS Security Metrics and Reporting
The following eLearning courses are available at no charge:

**MSS Managed SIEM Analysis and Reporting** – Focuses on helping you get the full value from your SIEM technology and the IBM Managed SIEM service. The course describes key IBM roles and responsibilities associated with the service, and how to use essential client tools, including how to:

- Use the Virtual SOC Portal to create a ticket to request a Managed SIEM policy change.
- Access QRadar console from the Virtual SOC Portal.
- Use the QRadar Dashboard tab to create and configure dashboards.
- Use the QRadar Log Activity tab to view and search log data.
- Use the QRadar Reports tab to view and generate a report, create and edit a report template, and manage reports and report groups.

**MSS Security Intelligence and Analysis** – Focuses on the Security Intelligence Analyst (SIA) job role and how to create a successful security partnership with IBM Managed Security Services. The course addresses how to:

- Perform event monitoring and analysis using MSS Customer Portal tools.
- Provide effective initial response to event escalations, and work with various teams to facilitate an appropriate and timely response.
- Perform strategic activities to maintain awareness of trends regarding your local network environment and the general threat landscape.

*Note:* IBM recommends that you complete the Security Intelligence and

---

**Course Simulations**

Scroll down while on the eLearning tab to see the various help videos that require you to follow along.

---

**eLearning Videos tab**

Switch to the Videos tab and watch various Demonstration and Best Practices Videos.

---

Located in Demonstration Videos is where you will find the VSOC Portal Overview video. It highlights the main features of the VSOC.
Demonstration Videos

Learning to use IBM tools will help you do your job, and collaborate more effectively with IBM staff in the Security Operations Center (SOC). Use the video gallery below to view the available demonstration videos.

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 VSOC, or by selecting the Knowledgebase option from the Support menu.
**VSOC Media Library**

The VSOC 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.

<table>
<thead>
<tr>
<th>Categories:</th>
<th>Media types:</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>All</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date uploaded:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any time from</td>
</tr>
</tbody>
</table>

**Security Services Resources**

The VSOC Resources site provides access to security research, videos, webcasts, and other information related to IBM Security Services.
Question Marks

There are question marks located throughout the VSOC. If you hover over or click on one it will provide you with information and customer enablement resources about that section. Within each question mark you can find videos and documents designed to provide information on many of the VSOC’s features and services.

Chat

The Chat Online feature is located in two areas of the VSOC. Should you need to chat with the SOC, it is located in the upper right-hand corner under the Help drop-down menu. You will also find a chat feature in Ticket Details.

*If you utilize the Chat Online feature within Ticket Details, the SOC is going to assume you want to chat about that specific ticket.
Log Out

To log out of the VSOC; from the username menu located in the top right corner of the VSOC, select “Logout”. You will be returned to the login screen.